

Computer ein erster Blick

Einführung in die Thematik

Für Einsteiger

Helmut Keller
23.08.2012



Inhalt

1. Rechnerarchitekturen	8	2.1.1 Windows98.....	13
1.1 Intel-basierende Rechnersysteme	8	2.1.1 Windows 98 Second Edition.....	13
2.1.1 Prozessoren	8	2.1.2 Windows ME	15
2.1.2 Rechnerbusse	8	2.1.3 Windows NT	15
2.1.3 Festplatte.....	9	2.1.4 Multiuser - Windows NT	16
2.1.4 Monitor und Grafik.....	10	2.1.5 Windows 2000.....	16
2.1.5 Betriebssysteme.....	10	2.1.6 Windows XP	18
2.1.6 Standardanwendungen	10	2.1.7 Windows Vista.....	19
2.1.7 Spezialanwendungen	10	2.1.8 Windows 7	20
2.1.8 Netzwerkanwendungen.....	10	2.1.9 Windows 8.....	22
1.2 RISC-Rechner von SUN	11	2.2 Unix-Betriebssysteme	24
2.1.9 Prozessoren	11	2.2.1 Linux.....	24
2.1.10 Rechnerbusse	11	2.2.2 SunOS / Solaris.....	25
2.1.11 Peripheriebusse	11	2.3 Computerviren	26
2.1.12 Betriebssysteme.....	12	3. Cluster	27
2.1.13 Aktuelle Rechner	12	4. Massenspeicher.....	30
2. Betriebssysteme	13	4.1 Überblick.....	30
2.1 Windows	13	4.1.1 Einteilung Primär-, Secundär- und Backup-Datenspeicher	30
		4.1.2 Peripheriebusse	30
		4.1.3 Serielles SCSI	33





4.1.4	Storage Area Network (SAN)	41	4.4.4	Exabyte-Laufwerke.....	60
4.1.5	DSSI-Schnittstelle	42	4.4.5	DAT-Laufwerke	61
4.1.6	IDE-Schnittstelle	43	4.4.6	114"-Magnetbandkassetten-Laufwerke	62
4.1.7	USB-Schnittstelle	43	4.4.7	112"-Magnetbandlaufwerke.....	62
4.1.8	FireWire 1394.....	43	4.4.8	LTO-Laufwerke.....	62
4.2	Primär-Datenspeicher	44	4.4.9	ADR_Laufwerke	63
4.2.1	Einführung.....	44	4.4.10	Ausblick.....	63
4.2.2	Festplattenlaufwerke	44	4.5	Backup-Software	64
4.2.3	Halbleiterplattenspeicher	46	4.6	Netzwerk-Storage-Server	64
4.2.4	RAID.....	47	5.	Arbeitsspeicher	65
4.3	Secundär-Datenspeicher	53	5.1	Speichertechnologien	65
4.3.1	Disketten-Laufwerke.....	53	5.1.1	Nicht flüchtige Speicher.....	65
4.3.2	Wechselplatten-Laufwerke	54	5.1.2	Dynamische Speicher.....	65
4.3.3	Optische Laufwerke.....	54	5.2	Modulbauformen	67
4.3.4	Ausblick.....	58	5.3	Begriffe rund um den Speicher	67
4.4	Backup-Datenspeicher	59	6.	Netzwerke LAN.....	69
4.4.1	Aktuelle Backup-Speicherlösungen	59	6.1	ISO/OSI-Modell.....	69
4.4.2	DLT-Laufwerke.....	59	6.2	Topologien	70
4.4.3	AIT-Laufwerke	60	6.3	Netzwerkprotokolle	71



6.3.1	TCP/IP.....	71	7.1.11	Switches.....	78
6.3.2	OSI.....	71	7.1.12	Router.....	81
6.3.3	IPX/SPX.....	71	7.1.13	Spezielle Features.....	83
6.3.4	NetBIOS.....	71	7.1.14	Gateways.....	84
6.3.5	NetBEUI.....	71	7.2	100 Mbit/s Fast Ethernet.....	85
6.3.6	DECnet.....	71	7.2.1	100BASE-T Zugriffsverfahren.....	85
6.3.7	LAT.....	72	7.2.2	100BASE-T Network Interface Card (NIC).....	85
6.3.8	AppleTalk.....	72	7.2.3	100BASE-T Repeater.....	85
7.	Ethernet.....	72	7.2.4	100BASE-T Switches.....	87
7.1	10 Mbit/s Ethernet.....	72	7.2.5	Verkabelung.....	87
7.1.1	Zugriffsverfahren.....	72	7.2.6	Migration bestehender Netze.....	88
7.1.2	Kabel.....	72	7.3	1000 Mbit/s Gigabit Ethernet.....	90
7.1.3	10BASE5, ThickWire.....	73	7.3.1	1000BASE Zugriffsverfahren.....	90
7.1.4	10BASE2, ThinWire, Cheapernet.....	73	7.3.2	Migrationswege für bestehende Netze.....	90
7.1.5	10BASE-T, TwistedPair.....	74	7.3.3	Gerätearten.....	90
7.1.6	10BASE-F, Lichtleiter.....	75	7.3.4	Verkabelung.....	90
7.1.7	Interfaces.....	75	8.	Token-Ring.....	92
7.1.8	Repeater.....	76	8.1	Zugriffsverfahren.....	92
7.1.9	Terminal- und Printserver.....	76	8.2	Verkabelung.....	92
7.1.10	Bridges.....	77	8.3	Komponenten.....	92





8.4	Zukunft von Token-Ring.....	92	11.2	Laser	100
9.	FDDI	93	11.3	Bluetooth	100
9.1	FDDI-ANSI-Standard	93	11.4	HomeRF	100
9.2	Zugriffsverfahren.....	93	11.5	Datenfunk nach IEEE 802.11	100
9.3	Topologie	94	11.5.1	Wireless LAN.....	100
9.4	Kabel	94	11.5.2	Wireless Bridging	100
9.5	Stationen.....	94	12.	Weitbereichsnetze WAN	102
9.6	Konzentratoren	95	12.1	Analoge Wählleitungen.....	102
9.7	FDDI/Ethernet Bridges/Switches	95	12.1.1	Telex und Teletex.....	102
9.8	Einsatzmöglichkeiten	95	12.1.2	Modems.....	102
9.9	Zukunft von FDDI.....	96	12.2	ISDN.....	103
10.	ATM	97	12.2.1	ISDN-Anschlüsse	103
10.1	Nutzen	97	12.2.2	Kompatibilität.....	103
10.2	Technologie.....	97	12.2.3	Verbindungstypen	103
10.3	Schnittstellen	98	12.2.4	ISDN-Terminaladapter mit serieller Schnittstelle	104
10.4	Verfügbarkeit und Standardisierung	98	12.2.5	ISDN-Adapter mit alb-Schnittstelle	104
10.5	Migration in bestehende Netze	98	12.2.6	ISDN-Controller	104
11.	Drahtlose Datenübertragung.....	100	12.2.7	Aktive/passive ISDN-Karten	105
11.1	Infrarot.....	100	12.2.8	ISDN Bridge/Router.....	105



12.3	xDSL - Digital Subscriber Lines	107	13.5	Netzwerkstrategien.....	122
12.4	Kabelmodems	107	14.	Eingabegeräte	123
12.5	X.25.....	107	14.1	Tastaturen	123
12.6	Frame Relay.....	107	14.2	Mäuse und Trackballs	123
12.7	Datenübertragung über das Stromnetz	108	14.3	Scanner.....	124
12.8	Remote Access	108	14.4	Strichcodeleser.....	124
12.8.1	Remote Control	108	15.	Terminals.....	126
12.8.2	Remote Node	109	15.1	Alphaterminals.....	126
12.8.3	Datentransfer und Datenkopierprotokolle.....	109	15.2	X-Window-Terminals.....	126
12.8.4	PPTP und Virtual Private Networks (VPN).....	110	15.3	PCs und Workstations.....	127
12.8.5	Communication Server.....	110	15.4	Network Computer (NCs) & Co.	127
12.8.6	Datenübertragung via GSM.....	110	15.4.1	Network Computer (NCs).....	127
12.9	Nutzung des Internets	111	15.4.2	Windows Based Terminals (WBTs).....	128
13.	Netzwerkmanagement.....	113	15.4.3	NetPCs.....	128
13.1	Netzwerkmanagementwerkzeuge	113	16.	Ausgabegeräte	129
13.2	Kabeltester und Analysatoren	113	16.1	Bildschirmausgabe	129
13.3	Remote Monitoring (RMON).....	116	16.1.1	Monitor-Grafikkarten-Kombination.....	129
13.4	Netzwerk-Security	117	16.1.2	Grafikstandards	130
13.4.1	Benutzeridentifikation	117	16.1.3	Bildschirmtypen	130
13.4.2	Internet Security	119	16.2	LC-Displays und LCD-Projektoren.....	131





16.3	Drucker.....	132	18.5	Netzwerkweite Kommunikation	140
16.3.1	Farbdrucker	132	19.	Anhang	141
16.3.2	Tintenstrahldrucker.....	132	20.	Notizen.....	142
16.3.3	Thermotransferdrucker	133			
16.3.4	Thermosublimationsdrucker	133			
16.3.5	Phase-Change-Drucker.....	133			
16.3.6	Laserdrucker	134			
16.3.7	Matrixdrucker.....	134			
16.3.8	Druckerprotokolle	134			
17.	Multimedia	136			
17.1	Digitale Kameras	136			
17.2	Sprachanwendungen	136			
17.3	Videobearbeitung	136			
17.4	Videokonferenzsysteme	138			
18.	Unterbrechungsfreie Stromversorgung.....	139			
18.1	USV-Technologien	139			
18.2	Dimensionierung	139			
18.3	Alarmierung/Schnittstellen.....	140			
18.4	Shutdown	140			



1. Rechnerarchitekturen

In den folgenden Abschnitten soll ein kurzer Überblick über intel-basierende Rechnersysteme sowie die wichtigsten aktuellen RISC-Workstations von SUN gegeben werden. Das zentrale und wichtigste, bei größeren Systemen, oft auch der teuerste Teil eines Computersystems, ist die CPU.

Im Bereich der Prozessoren ist zurzeit der Übergang von 32-bit- auf 64-bit-Architekturen das wichtigste Thema. Bei den meisten RISC-Architekturen, wie z.B. SPARC, ist dieser Schritt bereits vollzogen, bei der Intel IA64-Architektur wurde mit dem Itanium im Sommer 2001 der erste Prozessor dieser Architektur fertiggestellt. Der Nachfolger McKinley soll Anfang 2002 folgen, AMD wird mit dem Sledgehammer ungefähr Mitte 2002 folgen.

Wichtig ist hier nicht nur die Verfügbarkeit der Hardware, sondern auch der passenden Betriebssysteme. Microsofts NET, der Nachfolger von Windows 2000, wird 64-bit-Unterstützung beinhalten, für die ersten Systeme hat Microsoft eine spezielle, um 64-bit Funktionalität erweiterte, Windows 2000 Version zur Verfügung gestellt. Im Linux-Bereich steht bereits ein Kernel mit 64-bit-Unterstützung bereit. Für den Benutzer werden die Performanzvorteile der 64-bit Architekturen jedoch erst dann richtig zum Tragen kommen, wenn auch die Anwendungen mit 64-bit-Unterstützung verfügbar sind.

1.1 Intel-basierende Rechnersysteme

2.1.1 Prozessoren

In PCs werden vor allem Prozessoren des Herstellers Intel eingesetzt, wobei Konkurrenzprodukte von AMD stark auf dem Vormarsch sind und Intel sogar Geschwindigkeitsrekorde öfters an AMD abgeben muss.

Während zu Zeiten von Pentium und Pentium Pro die Wahl des Motherboards noch relativ einfach war, wird es durch die unterschiedlichen Bauformen der Prozessoren und durch die Vielzahl von Chipsets immer schwieriger, das richtige Motherboard zu finden. Alleine bei den Steckplätzen für Prozessoren gibt es zahlreiche Möglichkeiten, außerdem hat sich die Lebenszeit der Technologien erheblich verkürzt. Aus diesem Grund ist es praktisch unmöglich, Systeme die älter als ein Jahr sind, z.B. mit den neuesten Prozessoren auszurüsten. Deshalb sollte bei der Planung davon ausgegangen werden, dass nur Hauptspeicher und Festplatten zu einem späteren Zeitpunkt problemlos aufgerüstet werden können. Bei der Leistungsfähigkeit der heute aktuellen Prozessoren besteht auch in den meisten Fällen kein Bedarf zum Update der Prozessorleistung.

2.1.2 Rechnerbusse

Die Entscheidung, welches interne Bussystem gewählt werden soll, ist relativ einfach, da es momentan nur zwei maßgebliche Bustypen für PC-Systeme gibt: PCI-Bus und der AGP-Bus. Andere Bussysteme, wie zum Beispiel der ISA-, EISA- oder Microchannel-Bus, spielen keine Rolle mehr. Praktisch jedes aktuelle System enthält PCI-Steckplätze und einen AGP Steckplatz. Der AGP-Bus unterstützt jedoch nur Grafikkarten.

Im Folgenden soll ein kurzer Überblick über alle Bussysteme gegeben werden, die momentan in PCs und Servern eingesetzt werden.

PCI-Bus

Der PCI-Bus arbeitet in der ersten Version bereits mit 32-bit- und 33-MHz-Bustakt. Mit dem PCI-Bus kann eine maximale Transferrate von bis zu 133 MB/s erreicht werden. In der 64 bit-Version liegt die maximale Transferrate bei 267 MB/s. Ein entscheidender Vorteil des PCI-Busses ist die Unabhängigkeit vom Prozessortyp. Damit ist der Einsatz des PCI-Busses auch mit Nicht-Intel-Prozessoren", wie z. B. in Rechnern mit SPARC-Architektur, möglich. Der PCI-Bus wird von der PCI Special Interest Group unterstützt. Dieser Vereinigung gehören alle bedeutenden Hersteller aus den Bereichen Prozessoren, Systemplatinen, Festplatten, Controller und Grafikkarten an.

PCI-X

Mit den ständig weiter steigenden Anforderungen an die Leistung von Servern ist in absehbarer Zeit die Leistungsfähigkeit des PCI-Busses nicht mehr ausreichend. Aus diesem Grund hat das PCI Steering Committee die PCI-X-Spezifikation entworfen. PCI-X wurde ursprünglich von IBM, Compaq und Hewlett-Packard entwickelt. PCI-X erlaubt den Betrieb eines Slots mit 133 MHz und weiterer Slots mit 66 MHz oder 100 MHz. Damit sind bis zu 1 GB/s an Durchsatz möglich, was einer Verdoppelung gegenüber PCI entspricht. Ein wesentlicher Punkt bei PCI-X ist die Abwärtskompatibilität, das heißt PCI-X-Karten werden in PCI-Systemen funktionieren und umgekehrt. Mehr Informationen sind auf der Homepage der PCI-SIG zu finden: <http://www.pcisig.com>.

InfiniBand

Ein weiterer Vorschlag für eine Hochleistungs-Schnittstelle für Server ist InfiniBand der InfiniBand Trade Association. Diese ist aus der Verschmelzung der Future und NGIO-Gruppen hervorgegangen. Im Gegensatz zu PCI-X bietet InfiniBand keine Abwärtskompatibilität, hat dadurch aber den großen Vorteil, ganz neue Funktionen bieten zu können. InfiniBand ähnelt in den Grundkonzepten sehr stark Fibre Channel: Systeme





werden mittels eines oder mehreren Host-Channel-Adaptern (HCA) an eine I/O-"Fabric" angeschlossen. An diese Fabric werden wieder mit Target-Channel-Adaptern (TCA) Storage- oder auch Netzwerk Controller angeschlossen. Die Adressierung erfolgt mit InfiniBand mit IPv6-Adressen, so dass praktisch unbegrenzt viele Geräte zusammenarbeiten können. Die Bandbreite ist dabei auf bis zu 6 GB/s beliebig skalierbar. Die Verkabelung kann dabei bis zu 17 m mit Kupferkabel und bis zu 100 m mit Glasfaser lang sein. Durch dieses Design erlaubt InfiniBand den Bau wesentlich kleinerer Systeme, da auf Bussysteme im Server völlig verzichtet werden kann. Mehr Informationen sind auf der InfiniBand TA Homepage zu finden: www.infinibandta.org.

AGP

Der Accelerated Graphics Port stellt einen von Intel entwickelten, einzelnen Steckplatz für eine Grafikkarte dar. Bei den herkömmlichen Grafikkarten wird ein Teil des Grafikspeichers für Texturen verwendet. Um immer höhere Auflösungen immer detailreicher darstellen zu können, wurde mehr und mehr Grafikspeicher auf den Karten integriert. Dieser Speicher liegt bei Standardapplikationen allerdings brach. Das Konzept von AGP beinhaltet, dass die Grafikkarte direkt auf im Hauptspeicher abgelegte Texturdaten zugreifen kann. Die Grafikanwendung kann die Texturdaten hinsichtlich Größe, Farbtiefe und Auflösung optimal auswählen und der AGP-Karte im Hauptspeicher bereitstellen. Der Mainboard-Chipsatz und AGP tauschen die Daten mit 66 MHz und 32 Bit aus, entsprechend einer Übertragungsrate von 266 MB/s. Zusätzlich kann die AGP-Karte den so genannten x2-Modus bzw. x4-Modus verwenden. Im x2-Modus werden die Daten an beiden Flanken des Taktsignals übertragen, die Übertragungsrate erreicht dann mit 533 MB/s das Vierfache des PCI-Busses. Eine weitere Steigerung ist durch 4x möglich. Bei AGP 4x kommen noch die komplementären Strobe-Signale AD STB0# und AD STB1# dazu, die mit den Standard-Strobes differenzielle Leitungspaare bilden. Diese vier Strobes arbeiten dann tatsächlich mit 133,34 MHz. Auch bei AGP 4x erfolgt die Übertragung mit der fallenden und steigenden Flanke der ADStrobes. Durch die 133,34 MHz der Strobe-Signale ergeben sich vier Zyklen pro AGP-Takt, was effektiv 266,67 MHz entspricht und somit eine theoretische Bandbreite von 1017 MB/s bedeutet.

AGP ist abwärtskompatibel zu PCI: PCI-Busmaster wie z. B. Framegrabber-Karten können Daten über den PCI-Bus in die AGP-Grafikkarte schreiben. Die hohe Bandbreite, mit der die AGP-Grafikkarte auf den Hauptspeicher zugreifen kann, bedingt den Wechsel zu SDRAM mit 133 MHz oder Rombus-Modulen als Hauptspeichertechnologie.

I20

Auch I20 (Intelligent I/O) ist eine Intel-Entwicklung. I20 basiert auf dem Intel i960RP I/O-Prozessor, welcher ein komplettes Subsystem auf einem Chip darstellt. Aufgrund der On-Chip PCI-to-PCI Bridge kann der i960RP ohne zusätzliche Chips direkt an den PCI-Bus angeschlossen werden. Der i960RP befreit dann die CPU von der Abarbeitung von Interrupts und erhöht so die Gesamt-Performance des Systems, allerdings wird speziell

für diesen Prozessor entwickelte Software benötigt. Trotz dieser Vorteile konnte sich I20 nie so richtig durchsetzen und wird heute praktisch nicht mehr eingesetzt.

PC-Card-Schnittstelle

Die PC-Card-Schnittstelle ist ein Standard für scheckkartengrosse Steckkarten, der von der Personal Computer Memory Card Interface Association (PCMCIA) im September 1990 definiert wurde. Erste Produkte nach diesem Standard waren reine Speicherkarten. Nach und nach wurde der Standard erweitert, so dass auch andere Hardware nach dem PC-Card-Standard entwickelt und eingesetzt werden konnte, zum Beispiel Schnittstellenkarten, Modems und LAN-Adapter. Die PC-Cords haben eine einheitliche Fläche von 85,6 x 54 mm und besitzen eine zweireihige Buchsenleiste mit 68 Anschlüssen und je nach Typ unterschiedliche Kartendicken: Typ I, 3,3 mm, meist für Speicherkarten; Typ II, 5 mm, für Karten und Typ III, 10,5 mm, z. B. für Festplatten. Eine Typ III-Karte passt meist in zwei übereinander liegende Typ II Slots.

Die neueste Weiterentwicklung des PC-Card-Standards heißt Card Bus und beinhaltet Erweiterungen hinsichtlich geringerem Stromverbrauch, verbesserter Kompatibilität und höherer Performance. Die Spezifikation des Card Busses beschreibt einen PCI-ähnlichen busmasterfähigen 32-bit-Bus zum Rechner mit 33-MHz-Takt und einer maximal Datentransferrate von 132 MB/s. Dadurch bringt der Card Bus die Leistungseigenschaften des PCI-Busses auf scheckkartengrosse Peripherie, und für Notebooks kann durch diesen modernen Bus anspruchsvolle Hardware mit hoher I/O-Leistung angeboten werden (z. B. Fast Ethernet). Der PC-Card-Standard ist abwärtskompatibel zum PCMCIA-Standard, das heißt alte PCMCIA-Karten funktionieren im neuen Card Bus-Slot; neue PC-Card-Karten in alten PCMCIA-Slots werden nicht unterstützt.

Einsatzgebiete der PC-Cards sind vor allem bei Notebooks und Laptops zu finden. Da diese Rechnerarten in der Regel nur eine beschränkte Anzahl an externen Schnittstellen und gewöhnlich keine internen Steckplätze für Erweiterungskarten besitzen, bieten PC-Card-Steckplätze eine einfache und vielseitige Erweiterbarkeit.

2.1.3 Festplatte

Vor dem Kauf einer Festplatte stellt sich zunächst die Frage, ob es sich um eine EIDE- oder eine SCSI-Lösung handeln soll. Diese beiden Systeme sind im Kapitel Massenspeicher erklärt. Die Größe der Festplatte richtet sich nach der Anwendung und dem verwendeten Betriebssystem. Der Standard bei Komplett-PCs liegt inzwischen bei etwa 200 GB, was auch durch den rasch fallenden Preis pro MB Speicherkapazität zu



erklären ist.

2.1.4 Monitor und Grafik

Bei der Wahl der Grafikkarte sollte man beachten, ob Treibersoftware für das verwendete Betriebssystem angeboten wird oder im Betriebssystem (wie z. B. bei Windows Me) bereits enthalten ist. Nur in Kombination mit der geeigneten Treibersoftware lassen sich die maximale Auflösung einer Grafikkarte und die maximale Bildschirmfrequenz nutzen. Die Qualität einer Grafikkarte wird hauptsächlich vom verwendeten Grafikprozessor und dem Videospeicher auf der Karte bestimmt. Wichtig ist auch die Wahl des passenden Monitors, da er sowohl alle Anforderungen an einen ergonomischen Arbeitsplatz erfüllen muss (hohe Auflösung, strahlungsarm, hohe Farbtreue usw.) als auch den Leistungswerten der Grafikkarte entsprechen sollte. Eine Grafikkarte, die mit einer höheren Videosignal-Frequenz betrieben wird als der Monitor maximal gestattet, kann den Monitor beschädigen. Da der Monitor in der Regel zukünftigen Anforderungen an das Rechnersystem länger gerecht wird als die anderen Rechnerkomponenten, sollte man beim Kauf den höheren Preis für einen guten Monitor nicht scheuen.

2.1.5 Betriebssysteme

Empfehlungen für Betriebssysteme sollen hier nicht gegeben werden. Die Wahl für ein bestimmtes Betriebssystem ist meistens abhängig von den einzusetzenden Anwendungsprogrammen. Diese Wahl bleibt jedem Anwender selbst überlassen.

Ein wichtiger Punkt bei den Betriebssystemen ist die Größe des benötigten Hauptspeichers, um vernünftig arbeiten zu können. Dabei kann es sein, dass der tatsächlich benötigte Hauptspeicher deutlich über der Empfehlung des Betriebssystemherstellers liegt.

Der empfohlene Mindest-Hauptspeicherausbau beträgt bei einigen Systemen 16 MB. Dies ist für heutige Anwendungen nicht mehr ausreichend. Sobald Windows 98 oder Windows ME eingesetzt wird, sollten mindestens 32, wenn Pakete wie z. B. Microsoft Office eingesetzt werden, mindestens 64 MB auf der Systemplatine vorhanden sein. Ansonsten wird zu viel Rechenzeit des Prozessors für das Ein- und Auslagern von Daten vom Hauptspeicher zur Festplatte und umgekehrt vergeudet. Unter Windows NT bzw. 2000 werden 128 MB für eine akzeptable Arbeitsgeschwindigkeit benötigt. Bei Windows XP sollten es schon 256 MB sein. Beim Einsatz von Unix-Betriebssystemen hängt die Anforderung von dem verwendeten Unix-Derivat ab. In Verbindung mit einer grafischen

Benutzeroberfläche sollten jedoch mindestens 64 MB vorhanden sein.

2.1.6 Standardanwendungen

Standardanwendungen sind: Textverarbeitung, Datenbanken, Tabellenkalkulation und Grafikpräsentationen. Vor der Zusammenstellung des Rechnersystems sollte überlegt werden, ob der Rechner den ganzen Tag über eingeschaltet bleibt und daher eine Stromsparfunktion auf der Systemplatine sinnvoll ist. Als Ergänzungsoption ist ein Bandlaufwerk oder ein CD-Brenner bei Datenbankanwendungen und Grafikpräsentationen zu empfehlen, da hierbei meistens Datenmengen anfallen, die sich nicht mehr einfach auf Disketten sichern lassen. Zusätzlich sind bei Grafikanwendungen noch CD-ROM-Laufwerke und Soundkarten bei Multimedia-Anwendungen geeignet. Wer Präsentationen über den PC in Vorträgen oder Schulungen zeigen möchte, sollte sich auch noch für einen LCD-Projektor entscheiden.

2.1.7 Spezialanwendungen

Spezialanwendungen wie z. B. Multi-Media, Computer Aided Design (CAD), Grafikbearbeitung oder Desktop Publishing (DTP) stellen deutlich höhere Anforderungen an das Rechnersystem als Standardanwendungen. Entsprechend höherwertig muss die Ausstattung des Systems vor allem im Bereich des Prozessors und des Hauptspeichers sein. DVD Laufwerke sind in diesen Bereichen inzwischen auch schon eine Grundvoraussetzung. Als Ergänzungsoption sollte in jedem Fall ein geeignetes Backup-Medium vorhanden sein.

2.1.8 Netzwerkanwendungen

Bei einem Netzwerkserver spielt die Grafikausgabe eine geringe Rolle. Daher reicht für diese Anwendung ein einfacher VGA-Monitor aus. Umso mehr müssen bei einem Servereinsatz die Prozessorgeschwindigkeit, das Bussystem und der Festplattencontroller mit dem Speichermedium optimal zusammenwirken. Auch die verwendete Netzwerkkarte sollte im oberen Leistungsbereich angesiedelt sein. Einige Serverlösungen, wie zum Beispiel Windows NT-Server und einige Unix-Server, gestatten einen nondedicated Serverbetrieb. Das heißt, dass der Server auch noch als Workstation eingesetzt werden kann. Von diesem Verfahren ist jedoch abzuraten, da dadurch die Leistungsfähigkeit der Serverfunktionen stark eingeschränkt wird.





Systemplatinen mit Power-Management können zwar auch in Servern eingesetzt werden; diese Funktion sollte man jedoch hier nicht nutzen, da die Antwortzeiten für angeschlossene Stationen nach einem Stand-By (Modus mit minimalem Stromverbrauch) einige Sekunden betragen können.

Eine sinnvolle Ergänzung zu einem Netzwerkserver ist ein geeignetes Backup-Medium, das entweder im Server oder in einer Workstation eingerichtet wird. Dies reicht jedoch nur bedingt aus, um den Server vor Datenverlust zu bewahren. Eine optimale Lösung stellt ein RAID-System dar. Auf jeden Fall sollte eine unterbrechungsfreie Stromversorgung (USV) (Seite 214) zum Serversystem dazugehören, da ansonsten selbst ein RAID-System keine Datensicherheit garantieren kann.

Ein noch so gut ausgebauter Server stößt mit wachsender Zahl der angeschlossenen Stationen an die Grenzen seiner Leistungsfähigkeit.

Bei Netzen mit sehr hoher Auslastung sollte daher untersucht werden, ob die Belastung eines Servers durch die Trennung in mehrere Unternetze - verbunden über Bridges oder Router - oder durch den Einsatz von mehreren Servern gesenkt werden kann.

Die Konfiguration eines Arbeitsplatzrechners ist abhängig von den Aufgaben, die damit durchgeführt werden. Ein Arbeitsplatzrechner benötigt nicht unbedingt eine eigene Festplatte mit einem Boot ROM auf der Netzwerkkarte ist es möglich, direkt von der Serverfestplatte zu booten.

1.2 RISC-Rechner von SUN

2.1.9 Prozessoren

Sun Microsystems stellt die dritte Generation der Ultra SPARC Microprozessorfamilie vor. Der III Prozessor wurde entwickelt, um dem rasanten Wachstum des Internets und der damit verbundenen Datenmengen Rechnung zu tragen. Er setzt neue Maßstäbe an Skalierbarkeit, Leistung und Datendurchsatz und ist das Herz der neuen Produktgeneration von Sun und transtec. Sun Microelectronics bietet somit momentan drei Prozessortypen an: Ultra IIe, II und neu den III. Diese Prozessoren gibt es wiederum in verschiedenen Taktraten.

Die-Prozessoren von Sun sind mit 360, 400, 450, 480 MHz getaktet und haben bis zu 8 MB L2-Cache. Diese Prozessoren kommen in allen-Modellen zum Einsatz. In einem Enterprise-Server können bis zu 64 CPU's installiert werden. Die Modelle mit Ultra IIe gibt

es nur als Single-Prozessor-Version mit 500 MHz. Der neue III Prozessor ist momentan mit 600, 750 oder 900 MHz getaktet. Die Roadmap von Sun geht bis ins Jahr 2003. Dann sollen Taktraten von bis zu 2,1 GHz erreicht werden. transtec bietet in vielen Bereichen Alternativen zum original Sun-Modell an, die sich entweder gar nicht oder nur in kleinen Details unterscheiden. Diese Unterschiede können der Tabelle am Ende dieses Abschnittes entnommen werden.

2.1.10 Rechnerbusse

Zwei unterschiedliche Bussysteme für Erweiterungskarten kommen in Sun-Systemen zum Einsatz:

Den S-Bus gibt es in zwei Varianten, zum einen als 32 Bit mit einer Transferrate von 40 MB/s, zum anderen mit 64 Bit und einer Transferrate von 100 MB/s. Das System erkennt automatisch, welcher Kartentyp installiert ist und stellt die Geschwindigkeit darauf ein. Das zweite Bussystem, das in allen aktuellen Modellen wie z. B. Ultra60 und Ultra450 und auch in den ganz neuen Ultra III-Systemen "Blade 1000" und "SunFire" 280R zu finden ist, ist der PCI-Bus. Die PCI-Modelle unterstützen die PCI-Bus-Spezifikation in einer 64-bit, 66 MHz-Konfiguration und erreichen einen Durchsatz von theoretisch 528 MB/s. Das Angebot von Zusatzkarten ist momentan noch stark begrenzt. Die meisten Kartenhersteller liefern nur Treiber für die Windows-Betriebssysteme mit. Für Solaris werden spezielle Treiber benötigt werden. Der PCI-Bus hat in allen Rechnersystemen den S-Bus komplett abgelöst. Als Prozessorbus dient der UPA-Bus, der in allen-Systemen zum Einsatz kommt. Je nach Rechnermodell stehen bis zu 64 UPA-Steckplätze zur Verfügung, weitere Informationen können der unten stehenden Tabelle entnommen werden.

Die Ultra Port-Architektur (UPA) nutzt einen internen Cross Bar Switch, der die CPU, Memory, und I/O-Komponenten des Systems verbindet und koordiniert. Mit einem Durchsatz von bis zu 2,4 GB pro Sekunde erzielt die UPA eine herausragende Leistung. Die UPA nutzt in höchst effizienter Weise die Leistung des 64 bit-Prozessors mit integriertem 64 Bit Processing.

2.1.11 Peripheriebusse

Die neuen Modelle von Sun sind mit FireWire (IEEE 1394) und USB ausgestattet. Der Universal Serial Bus dient in erster Linie zum Anschluss von Tastatur und Maus. Ein FibreChannel-Arbitrated Loop ist in Zukunft sowohl für die internen Festplatten als auch für externe Storage Arrays geeignet. Eine UltraSCSI Schnittstelle ist auch weiterhin für externe Peripherie vorhanden. Das Netzwerk wird über ein 100Base-T Interface angeschlossen. Für alle High-End-Anwendungen im Grafikbereich stellt der CREATOR



Frame Buffer, der in einen UPA-Steckplatz gesteckt wird, hohe Performance zur Verfügung. Die CREATOR-Karte kombiniert den Großen linearen Speicher eines Framebuffers und den direkten Anschluss an die 128-bit breite UPA-Systemarchitektur mit dem mächtigen Visual Instruction Set (VIS) der-CPU.

2.1.12 Betriebssysteme

Das auf den SPARC-Rechnern eingesetzte Betriebssystem ist meistens Solaris3 das als sehr ausgereift und stabil bekannt ist. Die aktuelle Version, Solaris 8, ist voll 64-bit-fähig und bietet höchste Ansprüche an Sicherheit und beste Performance für Java Applikationen. Weitere Informationen zu Solaris sind im Kapitel Betriebssysteme. Linux als Betriebssystem ist ebenfalls verfügbar, aber noch nicht sehr verbreitet.

2.1.13 Aktuelle Rechner

Sun bietet eine große Auswahl an Workstations und Servern. Waren bisher SPARC-Rechner bevorzugt im technisch-wissenschaftlichen Bereich eingesetzt, finden sie immer stärkere Verbreitung bei kommerziellen Anwendern wie z. B. Banken und im Versicherungswesen, wo Enterprise-Server mit bis zu 64 CPUs zum Einsatz kommen. Sun unterscheidet zwischen Workstations und Server:

Desktop: Ultra5, Ultra10, Ultra60, Ultra80, Ultra450 und neu die Sun Blade 1000 mit III Architektur und als Low-Cost-Workstation mit Ultra IIe Prozessor, die Blade 100 .
Workgroup-Server: Enterprise 220R, Enterprise 250, Enterprise 420R, Enterprise 450 und ganz neu die Sun Fire 280R im 19" Rackmount.

Enterprise-Server: Enterprise 3500, Enterprise 4500, Enterprise 5500, Enterprise 6500, Enterprise 10000
SPARC-cluster, Sun Media Center Ultra SPARC.

Ultra III Midframe Server: Fire 3800, Fire 4800, Fire 4810 und Fire 6800.

Einen Überblick über die Workstations und Server von Sun und transtec gibt die Tabelle. Die Systeme können durch Third Party-Peripherie zum Teil auch über die genannten Werte erweitert werden.

Model	Architektur	max. CPU's	Taktrate von bis MHz	Hauptspeicher (MB) (Stand. Max.)	VPA-Creator	S-Bus	PCI	Enhanced IDE	Wide	Ultra-Wide	Fast-Ethernet	USB	IEEE-1394	FC-AL	Rackmount
SUN Ultra 10	Ultra Axi	1	440	64-1 GB	1	4									
SUN Ultra 60	Ultra Sparc II	2	300-450	128-2 GB	2	4									
SUN Ultra 80	Ultra Sparc II	4	300-450	128-4 GB	2	4									
SUN Ultra 450	Ultra Sparc II	4	300-450	128-4 GB	2	10									
SUN Ultra Enterprise 105	Ultra Axi	1	440	64-1 GB	1	4									
SUN Blade 1000	Ultra Sparc III	2	600-900	4-8 GB	2	4									
SUN Ultra Enterprise 80	Ultra Sparc II	4	300-450	128-4 GB		3			2						
SUN Ultra Enterprise 250	Ultra Sparc II	2	300-450	32-2 GB	2	4									
SUN Ultra Enterprise 250	Ultra Sparc II	2	300-450	32-2 GB	2	4									
SUN Ultra Enterprise 280R	Ultra Sparc II	2	600-900	1-8 GB	2	4									
SUN Ultra Enterprise 450	Ultra Sparc II	4	300-450	128-4 GB	2	10									
SUN Ultra Enterprise 3500	Ultra Sparc II	8	250-336	256-8 GB											
SUN Ultra Enterprise 4500	Ultra Sparc II	14	250-336	256-14 GB											
SUN Ultra Enterprise 5500	Ultra Sparc II	14	250-336	30 GB											
SUN Ultra Enterprise 6500	Ultra Sparc II	30	250-336	256-30 GB											
SUN Ultra Enterprise 10000	Ultra Sparc II	64	167-333	64 GB											
SUN Blade 100	Ultra Sparc	1	500	128-2 GB		3									
SUN Fire 3800	Ultra Sparc III	8	750	64 GB		12									
SUN Fire 4800	Ultra Sparc III	12	750	96 GB		16									
SUN Fire 4810	Ultra Sparc	12	750	96 GB		16									
SUN Fire 6800	Ultra Sparc III	24	750	192 GB		32									





2. Betriebssysteme

In den folgenden Abschnitten wird ein kurzer Überblick über die Betriebssysteme von Microsoft und die gängigsten Unix-Betriebssysteme gegeben.

2.1 Windows

2.1.1 Windows98

Windows 98 beinhaltet zahlreiche Detailverbesserungen: Eine neue Benutzeroberfläche erleichtert den Umgang mit einem Windows 98-PC im Vergleich zu Windows 95 erheblich. Assistenten und Dienstprogramme sorgen dafür, dass die Systeme zuverlässiger laufen und einfacher zu verwalten sind. Wesentliche Bestandteile sind:

Das Standard-Dateisystem FAT32 ist eine verbesserte Version des Dateisystems FAT, mit dem Festplatten mit mehr als 2 GB Kapazität als einzelnes Laufwerk formatiert werden können.

FAT32 wurde vorher nur von der Windows 95 OEM Version unterstützt. Verbessertes Power-Management durch die Unterstützung des Advanced Configuration and Power Interface (ACPI). ACPI ist eine von Intel, Microsoft und Toshiba vorgeschlagene offene Industriespezifikation, in der Hardware-Schnittstellen definiert werden, die ein standardisiertes Power-Management durch das Betriebssystem für alle Komponenten eines PC-Systems ermöglichen.

Der Assistent zur Datenträgeroptimierung steigert mit Hilfe der Defragmentierung die Ladegeschwindigkeit der Anwendungen und erleichtert den Zugriff auf die Dateien, die am häufigsten benutzt werden. Dazu legt der Assistent eine Protokolldatei an, in der aufgezeichnet ist, welche Programme am häufigsten verwendet werden. Nachdem diese Datei angelegt wurde, kann der „Assistent zur Datenträgeroptimierung“ die Dateien, die mit diesen häufig ausgeführten Programmen verknüpft sind, nacheinander auf der Festplatte ablegen. Durch diese kontinuierliche Anordnung werden Anwendungen wesentlich schneller ausgeführt.

Die Funktion Windows-System-Update sorgt dafür, dass immer die neuesten Treiber und Systemdateien verwendet werden. Es handelt sich um einen neuen Web-basierten Dienst (in Form eines ActiveX-Bedienelements), der das System durchsucht und feststellt, welche Hardware und Software installiert ist. Anschließend vergleicht er diese Informationen mit einer Back-End-Datenbank und ermittelt, ob neuere Treiber oder Systemdateien zur Verfügung stehen. Ist das der Fall, kann der Dienst die neuen Treiber automatisch installieren. Der Benutzer kann diesen Vorgang vollständig konfigurieren.

Das Dienstprogramm zur Systemdateiprüfung stellt auf einfache Weise sicher, dass die

Systemdateien von Windows 98 nicht verändert oder beschädigt wurden. Dieses Dienstprogramm bietet außerdem eine einfache Methode für die Wiederherstellung der Originalversionen von veränderten oder fehlenden Systemdateien.

Die Systeminfo Utility sammelt für den technischen Support Informationen über die Systemkonfiguration. Dieses Dienstprogramm besteht aus einer Sammlung von ActiveX-Bedienelementen, von denen jedes für das Sammeln und Anzeigen einer bestimmten Kategorie der Systeminformationen im richtigen MS-Info-Fenster zuständig ist. Ein Support Techniker kann einem Benutzer, bei dem Probleme aufgetreten sind, die Bedienung von MS-Info erklären und ihn durch die erforderlichen Schritte führen, um die benötigten Informationen zu sammeln.

Das Win32 Driver Model ist ein völlig neues Modell für Treiber, die sowohl unter Windows 98 als auch unter Windows 2000 funktionieren. Das WDM ermöglicht für einige verbreitete Gerätetypen (z.B. USB und IEEE 1394) den Einsatz eines einzigen Treibers für beide Betriebssysteme. Das WDM wurde implementiert, indem mit Hilfe eines speziellen virtuellen Gerätetreibers (NTKERN.VXD) bestimmte NT-Kerndienste zu Windows 98 hinzugefügt wurden. Auf diese Weise ist Windows 98 in der Lage, alte Treiber ohne Einschränkung zu unterstützen und gleichzeitig den Einsatz neuer WDM-Treiber zu ermöglichen.

Mit der integrierten Internet Benutzeroberfläche wird der Internet-Zugriff zum festen Bestandteil der Benutzeroberfläche. Der Anwender muss nicht mehr die Bedienung mehrerer Umgebungen erlernen. Mit diesem universellen Programm können lokale, Netzwerk-, Intranet- und Internet-Daten auf die gleiche Weise angesehen werden.

2.1.1 Windows 98 Second Edition

Die Windows 98 Second Edition beinhaltet Erweiterungen im Internet-Bereich sowie neue und verbesserte Hardware-Treiber für USB, IEEE1394 und ACPI. Außerdem ist das Windows 98 Service-Pack enthalten. Die Internet-Erweiterungen sind: Internet Explorer 5, NetMeeting 3 und Internet Connection Sharing, welches den gleichzeitigen Zugriff mehrerer Benutzer über einen Internet-Zugang erlaubt. Die Windows 98 Second Edition wird als Update für bestehende Windows 98-Systeme vorinstalliert auf neuen Systemen angeboten. Einzelne Teile, wie z.B. der Internet Explorer 5 und das Service Pack, können auch kostenlos aus dem Internet geladen werden. Die aktuellen transtec Systeme werden mit dieser Version von Windows 98 ausgeliefert.

Mehr Informationen über Windows 98 sind auf der Microsoft Windows-98-Homepage unter <http://www.microsoft.com/Windows98> zu finden.





2.1.2 Windows ME

Windows ME (Millennium Edition) ist der Nachfolger von Windows 98 und gleichzeitig das letzte Produkt der Windows-Familie, das DOS enthält. Die Benutzeroberfläche unterscheidet sich kaum von Windows 98, nur an einigen Stellen wurden Icons und Menüfunktionen von Windows 2000 übernommen. Zudem wurden neue Funktionen implementiert. Noch stärker als Windows 98 ist Windows ME auf den privaten Anwender zugeschnitten. Die wichtigsten neuen Funktionen in Windows ME sind:

System Restore erstellt automatisch in regelmäßigen Abständen eine Kopie der Systemkonfiguration, inklusive aller wichtigen Dateien. Sollten Probleme mit einer Konfiguration auftreten, kann der Anwender anhand einer Liste eine funktionsfähige Konfiguration auswählen und das System wieder in diese Konfiguration bringen. Der Anwender kann jederzeit auch selbst eine solche Kopie anlegen.

System File Protection schützt die wichtigsten Betriebssystemdateien vor Löschen oder Überschreiben. Damit ist gewährleistet, dass diese Dateien dem Betriebssystem immer zur Verfügung stehen.

Zertifizierte Treiber stellen sicher, dass die Stabilität des Betriebssystems auch nach der Installation neuer Hardware gewährleistet ist. Treiber ohne Zertifizierung können nicht installiert werden.

Private Netzwerke können für das Sharing von Druckern und Internetverbindungen mit neuen Assistenten sehr einfach eingerichtet werden.

Vor allem für den privaten Anwender ist die stark erweiterte Unterstützung von digitalen Medien sehr interessant. Viele neue Hilfsmittel und Programme für die Bearbeitung von Audio, Video und Grafik wurden integriert.

2.1.3 Windows NT

Windows NT ist das leistungsstarke 32-bit-Betriebssystem von Microsoft. Es ist speziell für den Netzwerkbetrieb in Verbindung mit dem Client/Server-Konzept optimiert.

Microsoft vertreibt Windows NT in zwei Versionen: Windows NT Server und Windows NT Workstation, die jeweils auf CD-ROMS ausgeliefert werden. Windows NT 4.0 stellt sich in der Oberfläche von Windows 95 dar, hat jedoch im Inneren einen völlig anderen Aufbau. Im Windows NT Server ist auch der Internet Information Server (Web-Server) integriert.

Der Internet Information Server bietet die Errichtung eines eigenen Web-Servers mit den Diensten WWW, Gopher und FTP.

Windows NT 4.0 enthält einen DNS-Server (Domain Name Service), der in der alten Windows NT 3.51-Version oft vermisst wurde. Mit dem Remote Program Load (RPL) ist es möglich, diskless Workstations (ohne Festplatte) unter Windows 95/98 vom Windows NT Server zu booten. Datenbankanbindungen über ODBC können über Internet-Server realisiert werden.

Windows NT ist ein Betriebssystem das - ähnlich der Unix-Struktur - auf einer Kernel-Architektur aufgebaut ist, also nicht, wie Windows 3.11, nur auf eine DOS-Struktur aufsetzt.

Windows NT unterstützt sowohl preemptives Multitasking und Multithreading sowie auch Multiprocessing (Verteilen von Programmteilen auf mehrere CPUs). Es ist auf bis zu 32 CPUs skalierbar (Windows NT Workstation kann max. 2 CPUs ansprechen, für Windows NT Server gibt es je nach Prozessoranzahl unterschiedliche Lizenzen). Pro System werden 4 GB RAM unterstützt. Jeder Anwendung kann bis zu 2 GB virtueller Arbeitsspeicher zugewiesen werden. Datenspeicher werden vom System bis zu 402 Mio. Terabyte unterstützt.

Netzwerkdienste von Windows NT

Im Lieferumfang ist die Unterstützung der Protokolle TCP/IP, NetBEUI, IPX/SPX, DLC und AppleTalk enthalten. Windows NT enthält Telnet und FTP-Clients sowie in der Server-Version einen FTP-Server-Dienst. Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die dynamische Einrichtung und Verwaltung von TCP/IP-Adressen. Windows Internet Naming Service (WINS) ordnet den TCP/IP-Adressen Namen zu. Für den Administrator und Benutzer wird es dadurch leichter, in einem TCP/IP Netzwerk zu arbeiten.

Es ist ebenfalls leicht möglich, Windows NT in ein NOVELL NetWare-Netzwerk zu integrieren. Der Client Service für NetWare (CSNW) ermöglicht den Zugriff auf die Datei- und Druck-Services eines NetWare 3.x Servers. Der Gateway Service für NetWare (GSNW) bietet Arbeitsstationen im Windows NT Server-Netzwerk den Zugriff auf NetWare Server. Weiterhin werden Migrationstools angeboten, welche die Benutzerinformationen und Verzeichnisse übernehmen. Es ist somit möglich, mit einem Windows NT Server die komplette Benutzerverwaltung von NetWare zu übernehmen oder zu steuern.

Windows NT unterstützt Fernzugriffe mit den Protokollen NetBEUI, IPX/SPX und TCP/IP; dies kann über ISDN, X25 oder analoge Telefonleitungen realisiert werden. Als Client erlaubt Windows NT Unix über PPP/SLIP, NetWare, LanRovers, Windows 3.x, Windows



95 sowie LAN Manager. Über diesen Remote Access Service (RAS) sind bis zu 256 gleichzeitige Verbindungen erlaubt.

Mit RaRAS (Routing and Remote Access Service) bietet Microsoft einen Software-basierten Multiprotokoll-Router für Windows NT Server 4.0. Der Service erweitert Windows NT um Multiprotokoll-Routing-Fähigkeiten sowie den Support von Virtual Private Networks (VPN) über PPTP (Point to Point Tunneling Protokoll). Für Windows NT 4.0 ist das Add-On kostenlos über den Microsoft-Webserver verfügbar. In Windows 2000 ist es als fester Bestandteil enthalten.

RaRAS unterstützt Routing von TCP/IP und IPX. Als Routing-Protokolle werden RIP und OSPF unterstützt, sowie statisches Routing. Bei der Authentisierung über PAP/CHAP greift RaRAS auf die Windows NT Domain-User-Authentisierung zurück. Unterstützt werden zudem RADIUS-Clients. Zentraler Bestandteil von RaRAS ist der Routing Table Manager. Hier werden die Routing-Tabellen verwaltet. Für Konfiguration und Management steht eine grafische Oberfläche zur Verfügung. RaRAS ist eine Alternative zu Hardware- Routern, besonders, wenn es um die Kopplung kleinerer Netze oder die Anbindung von Außenstellen an ein zentrales Unternehmensnetz gibt. Die typische Übertragungskapazität dürfte sich in der Praxis zwischen 10.000 bis 50.000 Paketen pro Sekunde bewegen. Ein Kostenvorteil gegenüber einer Hardware-Lösung ist, gerade bei ISDN, derzeit allerdings kaum mehr gegeben, da die nötige aktive ISDN-Karte kaum noch Preisvorteile gegenüber einem kleinen ISDN-Router bietet.

Systemadministration unter Windows NT

Mit dem transaktionsbasierenden Dateisystem NTFS erlaubt Windows NT eine Drag & Drop-Benutzerverwaltung, unter dem auch die Netzwerk-Zugriffsrechte bearbeitet werden können.

Werkzeuge wie der Systemmonitor, der die Server- und Netzwerkleistung analysiert, und die Ereignisanzeige, die die Serveraktivität protokolliert, ergänzen Windows NT. Es erlaubt zudem Festplatten-Duplexing, Plattenspiegelung und Datenträger-Stripping mit Parität (RAID5, nur bei Windows NT Server). Eine USV Shutdown-Software ist ebenfalls im Betriebssystem integriert, mit welcher es möglich ist, über einen seriellen Port des Windows NT Systems die USV zu verwalten.

2.1.4 Multiuser - Windows NT

Windows NT ist zwar ein Multitasking-, aber im Gegensatz zu Unix kein Multiuser Betriebssystem. Dieses Defizites hatte sich der amerikanische Softwarehersteller Citrix Systems angenommen. Bereits 1992 schlossen Citrix und Microsoft ein Abkommen über eine strategische Partnerschaft zur Entwicklung des Multiuser NT WinFrame. WinFrame ist die Grundlage für Application Publishing, einem neuen Weg für moderne Client/Server Architekturen im PC-Umfeld. Die Grundidee von Application Publishing ist nicht neu. Das Prinzip erinnert in weiten Teilen an Unix-basierende Netze mit X-Window Terminals. Bei Application Publishing laufen die Anwendungen nicht auf dem einzelnen Arbeitsplatz-PC, sondern auf dem Server. Der Arbeitsplatzrechner bekommt nur die Fensterdarstellung über das Netz zugespielt, braucht also weder installierte Anwendungen noch hohe Rechenleistung oder Speicherausbau.

Microsoft bietet die entsprechenden Erweiterungen in der Windows NT 4.0 Terminal Server Edition an. Damit können Windows Based Terminals (WBT) und PCs mit Windows 3.11, 95, 98 und Windows NT Workstation als Client eingesetzt werden. Microsoft setzt im Gegensatz zu Citrix auf das Remote-Display-Protokoll für die Kommunikation zwischen Server und Client. Für Systeme mit anderen Betriebssystemen, wie z.B. Unix, bietet Citrix Metaframe an. Mit dem darin enthaltenen Serviceprotokoll ICA (Independent Computing Architecture) können diese Systeme ebenfalls auf den Windows NT 4.0 Terminal Server zugreifen.

Mehr Informationen sind auf der Windows NT 4.0 Terminal-Server-Homepage unter www.microsoft.com/ntserver/basics/terminalserver und auf der Citrix-Metaframe-Homepage unter www.citrix.com/products/metaframe/ zu finden.

2.1.5 Windows 2000

Microsoft Windows 2000, früher unter der Bezeichnung Windows NT 5.0 bekannt, wurde um etliche neue Eigenschaften und Funktionen erweitert. Dazu gehören die Bereiche Administrierbarkeit, Skalierbarkeit und Erweiterbarkeit sowie Storage- und Hardware Management. Microsoft bietet Windows 2000 in vier Versionen an: Windows 2000 Professional entspricht der Windows NT Workstation und unterstützt bis zu vier GB

Hauptspeicher und zwei Prozessoren.

Windows 2000 Server ist der Nachfolger des Windows NT Server und bietet Hardware Unterstützung für max. vier GB Hauptspeicher und vier Prozessoren. Bereits in dieser Server-Version sind die Windows Terminal Services enthalten, welche die Windows NT





4.0 Terminal Server Edition ersetzen.

Die Windows NT Enterprise Edition wird als Windows 2000 Advanced Server weitergeführt. Hier werden bis zu acht GB Hauptspeicher und acht Prozessoren unterstützt. Zusätzlich zu den Funktionen des Windows 2000 Servers sind noch IP-Loadbalancing (mit bis zu 32 Servern) und Failover-Clustering für zwei Server enthalten.

Der Windows 2000 Datacenter Server bildet das obere Ende; er unterstützt bis zu 32 Prozessoren und 64 GB Hauptspeicher und bietet gegenüber dem Windows 2000 Advanced Server folgende zusätzliche Funktionen: Failover-Clustering für vier Server und Prozess Kontrolle für Workload-Management. Ein wichtiges Feature ist auch die Unterstützung von virtuellen Servern. Dabei können auf Multiprozessor-Servern mehrere Instanzen des Betriebssystems laufen, z. B. können auf einem 8-Prozessor-Server zwei virtuelle Server mit jeweils vier Prozessoren eingerichtet werden.

Installation von Windows 2000

Die Installation von Windows 2000 auf einem Rechner ohne Betriebssystem erfolgt mit einer bootfähigen CD. Plug-and-Play hält nun auch bei Microsoft Windows 2000 Einzug, was die Installation vereinfacht. Eine weitere Vereinfachung gegenüber Windows NT ist, dass ein Reboot seltener notwendig ist. Ebenso ist die USB-Unterstützung in Windows 2000 implementiert. Im Gegensatz zum Windows NT Server muss nicht bereits bei der Installation festgelegt werden, ob der Windows 2000 Server als Domänencontroller genutzt werden soll. Mittels des Assistenten zur Serverkonfiguration kann der Dienst für das Active Directory (Verzeichnisdienst insbesondere zur Benutzerverwaltung) auch nachträglich installiert werden.

Reparaturmechanismen: Windows 2000 ist mit einem verbesserten, abgesicherten Boot-Modus ausgestattet. Ein weiterer, verbesserter Reparaturmechanismus ist in der Kommandozeile implementiert.

Administrierbarkeit: Microsoft Windows 2000 implementiert Active Directory als zentrale Plattform, die den Zugriff auf und das Management von Netzwerk- und Systemressourcen vereinfacht. Benutzer können - anders als im Benutzermanager für Windows NT - im Active Directory, hierarchisch in Container gegliedert, angelegt und verwaltet werden. Bei Windows 2000 ist die Benutzerverwaltung nicht nur strukturierter, die Grenze von ca. 20-40.000 Benutzern pro Domäne unter NT wurde bei Windows 2000 faktisch aufgehoben. Weitere Features sind ein zentralisiertes Konfigurationsmanagement sowie die konfigurierbare und erweiterbare Microsoft Management Console (MMC).

Die IntelliMirror-Technologie erlaubt die zentrale Konfiguration von Windows 2000 Arbeitsplätzen. Mit Hilfe des Active Directory werden dabei die Konfigurationsvorgaben

für Benutzer oder Gruppen zentral angelegt. Der Benutzer findet dann immer an allen Windows 2000-Arbeitsplätzen genau die gleiche Konfiguration vor, vom Benutzer benötigte Software wird dabei automatisch auf dem jeweiligen Arbeitsplatz installiert. Dabei kann auch festgelegt werden, dass die Konfiguration vom Benutzer nicht verändert werden kann.

Skalierbarkeit und Erweiterbarkeit: Die neue Version von Microsoft Windows NT unterstützt bis zu 64 GB physischen Speicher. Mit dem Microsoft Cluster Server können zwei oder mehr Server im Verbund arbeiten. Dabei überwachen sich die Geräte gegenseitig, um bei einem Ausfall eines Servers ohne Unterbrechung den Betrieb aufrecht zu halten. Während des normalen Betriebes können die Server die Arbeitslast untereinander aufteilen, um eine höhere Produktivität zu erreichen.

Storage Management: NTFS implementiert nun auch eine Quotierung, wodurch der den Benutzern maximal zur Verfügung stehende Plattenplatz festgelegt werden kann. Die NTFS-Erweiterung EFS (Encryption File System) ermöglicht die Verschlüsselung sensibler Daten auf Datei- oder Verzeichnisebene.

Mit dem verteilten DFS-Dateisystem lassen sich die auf Windows 2000/NT-, NetWare und Unix-Servern verteilten Strukturen von Ordnern und Dateien zusammenfassen und übersichtlich präsentieren. Auf diese Weise können Benutzer Dateien im Netzwerk wesentlich einfacher finden.

Hardware-Management: Plug-and-Play ermöglicht den problemlosen Betrieb von PC-Cards in mobilen Rechnern. Zusätzlich soll durch Erweiterung des Windows Driver Models (WDM) erreicht werden, dass in Windows 98 und Windows 2000 identische Treibersoftware zum Einsatz kommen kann.

Sicherheitsfunktionen: Zur Erhöhung der Betriebssicherheit verhindert Windows 2000 das Löschen von für das Betriebssystem wichtigen Dateien. Außerdem erlaubt es nur die Installation von zertifizierten Treibern.

Netzwerksicherheit: Bereits in Microsoft Windows NT 4.0 ist das Security Service Provider Interface (SSPI) implementiert, zum Beispiel im NT LAN Manager und im Secure Sockets Layer (SSL). In Windows 2000 wird SSL erweitert und zusätzlich die Kerberos-Authentifizierung nach Kerberos5 eingeführt. Des Weiteren ist in Windows 2000 die Unterstützung von Smart Cards integriert, womit sich die Sicherheit bei der Anmeldung von Benutzern oder bei der digitalen Signierung von E-Mails steigern lässt.

Mehr Informationen zu Microsoft Windows 2000 sind auf der Microsoft-WWW-Homepage unter <http://www.eu.microsoft.com/germany/windows2000> zu finden.



2.1.6 Windows XP

Windows XP (NT 5.1) kam am 25. Oktober 2001 auf den Markt und ist der technische Nachfolger von Windows 2000 (NT 5.0) mit Windows NT-Kern. Zusätzlich löste es Windows ME der MS-DOS-Linie in der Version „Home Edition“ als Nachfolger in der Produktlinie für Heimanwender bzw. Privatanutzer ab. Die MS-DOS-Linie wurde von Microsoft eingestellt.

Die auffälligste Neuheit in Windows XP ist die neue Benutzeroberfläche „Luna“, die im Auslieferungszustand eine farbenfrohere Desktop-Oberfläche bietet, als dies bisher bei Windows 2000 der Fall war. Es steht aber wahlweise auch eine modifizierte Version der alten Oberfläche von Windows 2000 zur Verfügung („klassisch“).

Windows XP gibt es in mehreren Variationen

Die „**Professional Edition**“ wurde für den Einsatz in Unternehmen entwickelt und enthält Funktionen wie z. B. Fernverwaltung (Remote Control), Dateiverschlüsselung (EFS), zentrale Wartung mittels Richtlinien oder die Nutzung von mehreren Prozessoren (SMP).

Die „**Home Edition**“ ist als preiswerte Variante um einige Eigenschaften der Professional Edition gekürzt, basiert jedoch auf demselben NT-Kern.

Die „**Tablet PC Edition**“ basiert auf der Professional Edition und enthält spezifische Erweiterungen für auf Stifteingabe optimierte Laptops/Notebooks, die über einen im Display integriertes Grafiktablett verfügen (Tablet PCs). Augenscheinlichste Merkmale sind die Unterstützung handgeschriebener Notizen und Bildschirmrotation. Diese Version wird zusammen mit entsprechenden PCs verkauft und ist nicht separat erhältlich. Zu erwähnen ist die Handschriftenerkennung, die die Handschrift des Benutzers erlernt und das handgeschriebene Wort direkt in elektronische Schrift übersetzt.

Die „**Media Center Edition**“ basiert ebenfalls auf der „Professional Edition“ und enthält spezifische Erweiterungen für auf multimediale Inhalte sowie deren Wiedergabe spezialisierte Computer, die in der Regel mit einer TV-Karte ausgestattet sind. Augenscheinlichstes Merkmal ist die Möglichkeit der vereinfachten Bedienung durch Darstellung auf einem normalen Fernsehapparat und Steuerung mittels Fernbedienung. Microsoft versucht damit, die Lücke zwischen reinem Computer und Media-Center-Computer für das Wohnzimmer zu schließen. Windows XP Media Center Edition erfuhr 2003 die erste Aktualisierung, die aktuelle Version ist Windows XP Media Center Edition 2005. Während die erste Version der Windows XP Media Center Edition nur im Paket mit entsprechenden Computern vertrieben und nicht als Einzelprodukt verfügbar war, sind die aktualisierten Fassungen auch einzeln über den Vertriebskanal „System Builder“ zu erwerben. Seit der letzten Version können Consumer-Endgeräte wie z. B. DVD-Recorder,

Xbox 360 etc. über eine Netzwerkverbindung mit dem Betriebssystem kommunizieren. Hierfür ist in diesen Endgeräten ein Windows XP Media Center Edition als „embedded Version“ oder ein zur Media Center Edition kompatibles Frontend implementiert.

Windows XP „Embedded“ für spezielle Haushalts- und Unterhaltungselektronik, Digitalempfänger, Geldautomaten, medizinische Geräte, Kassenterminals oder Voice-over-IP-Komponenten. Diese Version basiert auf demselben Programmcode wie Windows XP Professional.

Windows XP „x64 Edition“ ist eine spezielle 64-Bit Version, die ausschließlich für AMD- und Intel-Prozessoren mit AMD64-Erweiterung entwickelt wurde. Sie läuft nicht auf 64-Bit-Prozessoren anderer Hersteller und ist ansonsten identisch zu Windows XP Professional, bis auf die Tatsache, dass es auf dem Systemkern von Windows Server 2003 basiert und somit eine modernere Basis (NT 5.2) besitzt. Die x64 Edition ist als OEM- und als System-Builder-Lizenz erhältlich. Im Zusammenspiel zwischen Prozessor und Betriebssystem kann auch eine konventionelle 32-Bit-Software ausgeführt werden. Somit ist es nicht erforderlich, dass die auszuführenden Programme als 64-Bit-Version vorliegen müssen. Dieses Verfahren des x64-Prozessors wird auch *Mixed-Mode* genannt - also das Ausführen von 64- und 32-Bit-Software gleichzeitig auf einem Prozessor. Jedoch ist es erforderlich, dass die Gerätetreiber als 64-Bit-Version vorliegen. Die Treiber werden vom Hardware-Hersteller für das Betriebssystem hergestellt und zur Verfügung gestellt.

Windows XP „Home Edition N“ und **„Professional Edition N“** sind angepasste Windows-Versionen die – aufgrund einer Auflage der Europäischen Kommission – ohne Windows Media Player und andere multimediale Bestandteile ausgeliefert werden. Möchte der Benutzer die gleiche Funktionalität wie in der regulären Version von Windows XP nutzen, kann er die erforderlichen Elemente dennoch kostenfrei von der Microsoft-Homepage herunterladen.

Windows XP „Home Edition KN“ und **„Professional Edition KN“** sind angepasste Windows-Versionen die – aufgrund eines Gerichtsbeschlusses in Korea ohne Windows Media Player und Windows Messenger ausgeliefert werden. Möchte der Benutzer die gleiche Funktionalität wie in der regulären Version von Windows XP nutzen, kann er die erforderlichen Elemente dennoch kostenfrei von der Microsoft-Homepage herunterladen.

Für den Vertrieb in finanziell weniger starken Regionen und Entwicklungsländern gibt es eine funktional stark eingeschränkte **Windows XP Starter Edition** (maximal drei Anwendungen zur gleichen Zeit mit max. je drei Fenstern, keine lokalen Netze oder Benutzerkonten, niedrige Bildschirmauflösung, maximal 256 MB RAM und 40 GB Festplattenspeicher usw.).

Anders als in den vorherigen Windows-Versionen gibt es keine Server-Version von Windows XP. Die Serverprodukte zu Windows XP sind in der „Windows Server 2003“-





Produktfamilie zusammengefasst.

Die einzelnen Windows-Server-2003-Versionen gliedern sich in „Standard Edition“, „Enterprise Edition“, „Datacenter Edition“, „Web Edition“ und „Small Business Server“, wobei die Datacenter Edition ausschließlich als OEM-Lizenz in Verbindung mit entsprechender Hardware erhältlich ist.

2.1.7 Windows Vista

Windows Vista ist der Nachfolger des Betriebssystems Windows XP. Der interne Entwicklungsname lautete „Longhorn“ und die interne Versionsnummer NT 6.0. Nach einer Reihe von Verzögerungen ist Vista für Firmenkunden im November 2006 und für Privatkunden am 30. Januar 2007 erschienen. Die Entwicklungsarbeit an der Version für Firmenkunden wurde am 8. November 2006 abgeschlossen, während die Entwicklung der Version für Privatanwender noch einige Wochen weiter lief.

Erstmals wurde Windows Longhorn von Microsoft im Sommer 2001 angekündigt, noch vor der Veröffentlichung von Windows XP. Damals war es als Zwischenschritt zwischen XP und der übernächsten Version Windows 7 (ehemals Vienna, damals Blackcomb) gedacht und sollte bereits Ende 2003 erscheinen. Außerdem hatte Microsoft kurzfristig auch *Shorthorn* in Planung, eine Zwischenversion zwischen Windows XP und Longhorn. Diese Zwischenversion wurde dann aber verworfen, damit Longhorn schneller fertig wird. Einige Eigenschaften von Shorthorn wurden jedoch in das Service Pack 2 für Windows XP integriert. Da viele Funktionen, die ursprünglich erst für Blackcomb geplant waren, schon in Vista implementiert wurden, verschob sich das Veröffentlichungsdatum mehrfach. Zudem fielen zunächst vorgesehene Funktionalitäten und Neuerungen weg. Die eigentlich für Vista geplante assoziative Dateiverwaltung WinFS wurde erst auf einen Zeitpunkt nach Veröffentlichung von Vista verschoben, um, so Microsoft, die Entwicklung von Vista in einer „vernünftigen Zeitspanne“ abzuschließen. Mittlerweile wurde WinFS als eigenständiges Projekt völlig eingestellt. Auch war ursprünglich geplant, unter dem Namen Next-Generation Secure Computing Base in Windows Vista eine Trusted-Computing-Umgebung einzuführen. Als Folge von Entwicklungsproblemen und massivem Protest wurde dieser Plan jedoch wieder verworfen. Heute gibt es 6 Versionen:

Systeme	Beschreibung
Windows Vista Starter	Ähnlich wie die <i>Windows XP Starter Edition</i> ist diese Version stark eingeschränkt. Vista Starter ist vor allem für Entwicklungsländer konzipiert und soll dortigen illegalen Kopien vorbeugen. Wie schon beim Vorläufer ist es nur erlaubt, drei Programme gleichzeitig zu starten, sie ist auch die einzige Version, die nur eine 32-Bit-Unterstützung enthält.
Windows Vista Home Basic	Vista Home Basic stellt eine abgespeckte Version für den Hausgebrauch dar. Der erweiterte Grafikmodus Aero Glass ist standardmäßig nicht aktiviert und lässt sich nur über eine Änderung in der Registry einschalten). Vista Home Basic bietet Basisfunktionalität und ist weniger für einen erweiterten Multimediaegebrauch geplant.
Windows Vista Home Premium	Diese erweiterte Version von Vista Home Basic ist für den privaten Markt konzipiert. Sie hat einige zusätzliche Funktionen wie zum Beispiel die Unterstützung von HDTV und das Schreiben von DVDs. Außerdem weist Microsoft darauf hin, dass die Premium-Edition eine Xbox 360 als Windows XP Media Center Edition-Extender nutzen kann. Diese Version ist also vergleichbar mit Windows XP Media Center Edition, ihr fehlt aber zum Beispiel die Möglichkeit, einer Domain beizutreten.
Windows Vista Business	Ähnlich wie Windows XP Professional zielt diese Version auf den Firmenbereich. Sie unterstützt Windows Server Domains und ist mit einer neuen Version des Webservers IIS ausgestattet.
Windows Vista Enterprise	Diese Version ist vor allem für Großkunden gedacht. Sie hat, auf Vista Business basierend, zusätzlich unter anderem die Festplattenverschlüsselung BitLocker, den PC-Emulator Virtual PC Express sowie ein Subsystem für Unix-basierte Anwendungen, mit dem Unix-Programme (unverändert) unter Vista laufen. Diese Version wird in einer sogenannten Volumen-Lizenz an Großkunden verkauft. Im Gegensatz zu Windows XP müssen Vistas Volumenlizenzen auch aktiviert werden. Um den Administrationsaufwand in Firmennetzwerken zu verringern, stellt Microsoft einen eigenen Aktivierungsserver für Firmennetzwerke zur Verfügung.
Windows Vista Ultimate	Vista Ultimate ist schließlich die Version von Vista, die die Funktionen aller anderen Versionen vereinigt, und richtet sich laut Microsoft an Kleinunternehmer, die ihren PC privat und geschäftlich nutzen, und an Privatanwender, die ihren Rechner sowohl zu Hause als auch im Unternehmensnetzwerk betreiben.



2.1.8 Windows 7

Während das Unternehmen eine Betriebssystemversion mit dem Codenamen *Longhorn* entwickelte, die später als Windows Vista veröffentlicht wurde, begann Microsoft zunächst unter dem Codenamen *Blackcomb*, ab 2006 als *Vienna*, die Entwicklung der nachfolgenden Version. Im Oktober 2008 gab der Hersteller „Windows 7“ als Namen für das Nachfolgesystem von Windows Vista bekannt.

Die erste Vorabversion wurde am 28. September 2008 an die Teilnehmer der PDC (Professional Developers Conference) verteilt.

Anlässlich der Consumer Electronics Show 2009, die am 7. Januar begann, wurde eine Beta-Version offiziell für MSDN- und TechNet-Mitglieder zugänglich gemacht und anschließend am 9. Januar der Öffentlichkeit zum Download bereitgestellt (Build 7000).

Aufgrund des großen Interesses musste Microsoft den Download wegen Serverüberlastung zwischenzeitlich stilllegen, um die technische Infrastruktur zu erweitern. Das Download-Limit von 2,5 Millionen Downloads wurde danach aufgehoben und die Verfügbarkeit der Software bis zum 24. Januar festgelegt. Einen Tag vor der Beendigung wurde der Zeitraum verlängert, somit konnte der Beta-Download bis 10. Februar begonnen und bis 12. Februar 2009 beendet werden.

In der ersten Beta-Phase wurde nur die *Ultimate*-Edition, die alle Funktionen des Betriebssystems enthält, zum Download angeboten. MSDN-Subscriptions-Inhaber und Microsoft-Connect-Mitglieder hatten auch Zugang zu anderen Editionen, beispielsweise *Home* und *Professional*. Die Laufzeit einer (aktivierten) Beta-Version war bis zum 1. August 2009 begrenzt. Nach der Beta 1 folgte keine weitere öffentliche Beta-Version.

Es folgte der Release Candidate, Build-Nummer 7100, welcher am 30. April für TechNet- und MSDN-Abonnenten und am 5. Mai 2009 für die Öffentlichkeit erschien. Die Laufzeit eines (aktivierten) Release Candidate war begrenzt bis 1. März 2010. Nach diesem Termin fuhr das Betriebssystem alle zwei Stunden automatisch herunter. Seit Anfang Juni 2010 verweigert der Release Candidate den Start endgültig.

Am 15. Juli 2009 wurde Windows 7 Home Premium in einer Vorverkaufsaktion zu einem Sonderpreis von 50 Euro in stark limitierter Zahl angeboten, es war in Deutschland zumeist innerhalb weniger Minuten vergriffen.

Am 22. Juli 2009 wurde die Fertigstellung des Betriebssystems bekannt gegeben, das intern bei Microsoft bereits am 13. Juli 2009 kompiliert und am 22. Juli 2009 nach erfolgreichem Abschluss aller Tests bei Microsoft als finale RTM-Version (*Release To Manufacturing*) mit Build-Nummer 7600.16385 deklariert wurde. Großkunden mit Volumenlizenzen erhielten seit Anfang August Zugriff auf die RTM-Version, seit Mitte August war sie auch in verschiedenen Sprachen verfügbar. Inzwischen sind auch

verschiedene Lizenzschlüssel für alle Editionen von Windows 7 im Internet vorhanden, mit denen man Windows 7 illegal aktivieren kann; diese bedienen sich der integrierten Option, die Microsofts Partner zur Massenaktivierung von Vorinstallationen nutzen (OEM-Preactivation).

Bis zum 22. Oktober 2009, dem internationalen Verkaufsstart, wurden alle Sprachpakete („Language Packs“) für Windows fertiggestellt.

Editionen

Das Betriebssystem ist in sechs verschiedenen Editionen zu gestaffelten Lizenzpreisen erhältlich:

- **Starter Edition** (für Wachstumsmärkte und Netbooks),
- **Home Basic** (für Schwellenländer),
- **Home Premium** (inklusive Media Center – für den breiten Markt),
- **Professional** (für kleinere Unternehmen),
- **Ultimate** (vereint alle Funktionen der anderen Versionen, ausgenommen Starter) und
- **Enterprise** (Umfang wie Ultimate; Vertrieb nur mit Volumenlizenzen an Firmen und Organisationen; Version der 90-Tage-Testversion).

Die Unterschiede liegen im Funktionsumfang, in der Reichweite der Lizenz und bei der Supportdauer. Die genannten Versionen sind auch als Upgrade von Windows XP erhältlich, erfordern aber jeweils eine Neuinstallation.

Windows 7 Starter

Diese Edition ist die einzige Version, die nur als 32-Bit-Version verfügbar ist und bei der der Arbeitsspeicher auf maximal 2 GB beschränkt ist. Außerdem gibt es nur die Aero-Basic-Oberflächen und der vorinstallierte Windows Media Player ist in seiner Funktion eingeschränkt. So können im Windows Media Player beispielsweise keine DVDs abgespielt werden. Die Restriktion, dass außer systemgestarteten Prozessen (wie dem Desktop) maximal drei Benutzerprozesse gleichzeitig ausgeführt werden können, wurde im Vergleich zu den Starter-Editionen von Windows XP und Vista aufgehoben. Zudem lässt sich der Desktophintergrund nicht verändern. Die Oberfläche lässt sich zwar auf einem weiteren Monitor darstellen, der Darstellungsbereich lässt sich aber nicht durch einen zweiten Monitor erweitern bzw. vergrößern. Diese Version ist ausschließlich (meist vorinstalliert auf Netbooks) als OEM-Lizenz erhältlich.





Windows 7 Home Basic

Home Basic stellt eine in der Ausstattung verminderte Version von Home Premium dar. Es bietet Basisfunktionen und enthält kein Windows Media Center. Dafür ist der Windows Media Player enthalten. Home Basic und alle höheren Versionen unterstützen mehrere Monitore und ein schnelles Wechseln zwischen Benutzern ist möglich, jedoch unterstützt diese Edition maximal 4 GB Arbeitsspeicher in der 32 Bit Version. In der 64 Bit Version werden 8 GB unterstützt.

Windows 7 Home Premium

Diese Version ist für den privaten Markt konzipiert, die Limitierung des Arbeitsspeichers beträgt 16 GB. Im Vergleich zu *Home Basic* hat sie einige zusätzliche Funktionen wie z. B. die Unterstützung von HDTV und das Abspielen und Schreiben von DVDs. Der Windows Media Player und das Windows Media Center sowie einige Spiele sind ab Home Premium enthalten.

Windows 7 Professional

Diese Version von Windows 7 zielt vor allem auf den Unternehmensbereich. Sie beinhaltet alle Funktionen der Home Premium Edition und besitzt, wie auch die weiteren Editionen Ultimate und Enterprise, eine Limitierung des Arbeitsspeichers von 192 GB. Sie unterstützt Windows Server Domains. Der XP-Modus erlaubt die Ausführung von Programmen, die unter Windows 7 sonst nicht funktionieren würden. Bei der Professional-Version sind die Spiele wie Minesweeper, Solitär oder FreeCell standardmäßig nicht installiert, können aber nachträglich hinzugefügt werden. Der Spiele-Explorer hingegen ist standardmäßig installiert, da er nur ein spezieller Ordner im Windows-Explorer ist. Microsoft bietet für die Editionen Professional und Enterprise nach Ablauf der Mainstream-Support-Phase eine Extended-Support-Phase an.

Windows 7 Ultimate

Windows 7 Ultimate enthält die Funktionen aller anderen Versionen und richtet sich an Kleinunternehmer, die ihren PC privat und geschäftlich nutzen, sowie an Privatanwender, die ihren Rechner sowohl zu Hause als auch im Unternehmensnetzwerk betreiben. Ultimate bietet zusätzlich unter anderem die Festplattenverschlüsselung BitLocker und das Starten von virtuellen Festplatten im VHD-Format. Auch ermöglicht es dem Anwender, jederzeit die Systemsprache zu ändern.

Windows 7 Enterprise

Diese Version ist im Grunde ein Windows 7 Ultimate, das unter Volumenlizenz vertrieben

wird. Bei der Enterprise-Version sind jedoch, wie bei der Professional-Version, Spiele wie Minesweeper, Solitär oder FreeCell standardmäßig nicht installiert.



2.1.9 Windows 8

Microsoft Windows 8 wird seit 2007 als Nachfolger des Betriebssystems *Windows 7* des Softwareherstellers *Microsoft* entwickelt. Microsoft hat drei Vorabversionen veröffentlicht, zuletzt im Juni 2012 die *Windows 8 Release Preview*. Die Veröffentlichung von Windows 8 ist für den 26. Oktober 2012 angekündigt. Die Oberfläche soll sich an der Gestaltung von Windows Phone 7 orientieren und damit besser für Touchscreens geeignet sein. Zudem ist auch eine Bedienung mit Computermaus und Tastatur möglich.

Oberfläche und Bedienung

Auf der Build-Konferenz im September 2011 betonte Microsoft, Windows 8 solle die Möglichkeiten der Nutzung eines Computer mittels Touchscreen und Maus vereinigen. Die Möglichkeit zur Verwendung einer Tastatur oder einer virtuellen Tastatur auf dem Bildschirm bleibt erhalten. Das Betriebssystem soll in eine neue Oberfläche (früher „Metro“ genannt) und die klassische „Desktop“-Oberfläche unterteilt werden, wobei die aus Kompatibilitätsgründen übernommene Oberfläche aus Windows 7 nur über die neue Oberfläche gestartet werden kann.

Der **Bootmanager**, welcher beim Start zur Auswahl des Betriebssystems dient, wurde ebenfalls für die Touch-Eingabe optimiert, lässt sich jetzt aber auch erstmals mit der Maus bedienen. Er enthält zudem eine grafische Oberfläche, über die sich erweiterte Einstellungen aufrufen lassen.

Secure Boot

Auf Computern, die für Windows 8 zertifiziert sind, wird ein Boot-Verfahren namens *Secure Boot* eingesetzt, das den Start von Schadsoftware während des Boot-Vorgangs unterbinden soll, aber auch bei Computern mit ARM-Architektur das Booten freier Betriebssysteme unmöglich macht.

Benutzeroberfläche

Metro ist Microsofts Codename der neuen Oberfläche, die in *Windows 8* bevorzugt verwendet wird. Aufgrund einer Klageandrohung der Metro AG wegen Verletzung des Markenrechts entschloss sich Microsoft, die Benutzeroberfläche in der endgültigen Version von Windows 8 umzubenennen.

In ihr sollen sämtliche Menüs ins Bild „gestreift“ werden können. Der Grundgedanke hierbei ist, die Menge der Steuerelemente der Benutzerschnittstelle zu reduzieren (zusammengefasst als „Chrome“ bezeichnet), und den Inhalt einer Anwendung in den Vordergrund zu rücken. Ebenso werden Ideen zur Anordnung von Text und Kontrollelementen aus Typografie, Bauhaus-Design, Swiss-Design und Motion-Design

eingesetzt.

Bei der Bedienung mit Maus kann das oben erwähnte „Streifen“ im Falle der Systemleisten links und rechts mithilfe der sogenannten „Hot Corners“ erreicht werden. Dabei bewegt man die Maus in die jeweiligen Ecken und die Leisten werden eingeblendet. Durch einen Rechtsklick innerhalb einer Anwendung werden applikationsspezifische Menüs angezeigt.

Mithilfe der Tastenkombination **Win + Z**, **Win + C** und **Win + Tab** können anwendungsspezifische Menüs, die Charms und die zuletzt verwendeten Apps respektive angezeigt werden.

Windows 8 sollte ursprünglich sogenannte Kacheln (englisch *tiles*) statt Programmicons nutzen und damit einige Neuerungen von Windows Phone 7 übernehmen. Aufgrund der Kritik, das Metro-Design sei nicht benutzerfreundlich genug, wurden einige Parameter wie die Kachelgröße abgeändert. Die Kacheln seien zu groß und ließen sich nicht personalisieren.

Die Desktopoberfläche *Windows Aero* weicht ebenfalls dem Metro-Design und wird künftig durch eine sehr schlichte Gestaltung der Fenster ersetzt.

Viele Firmen haben bekanntgegeben, ihre Programme an Metro anzupassen (z. B. Mozilla seinen Firefox Browser). Für den Browser Google Chrome existiert mittlerweile eine Metro-Entwicklervorschau.

Metro-Anwendungen (auch kurz *Metro-Apps* genannt) werden die Möglichkeit haben, Inhalte direkt an andere Anwendungen weiterzugeben bzw. diese zu empfangen. So ist es unter anderem möglich, eine Textpassage im Browser zu markieren und anschließend über eine beliebige Social-Media-Anwendung mit Freunden oder Bekannten zu teilen. Außerdem ist das Verwenden von Inhalten wie Bildern aus Anwendungen, welche auf Cloud-Dienste wie Flickr zugreifen, möglich, ohne dass die Anwendung, die diese Inhalte anfordert, Zugriff auf die Login-Daten der Online-Bildergalerie hat.

Editionen

Wie Microsoft am 16. April 2012 bekannt gab, wird das Betriebssystem in vier verschiedenen Editionen erhältlich sein:

- **Windows 8 (eingeschränkter Funktionsumfang für den breiten Markt),**
- **Windows 8 Pro (erweiterter Funktionsumfang),**
- **Windows 8 Enterprise (voller Funktionsumfang; Vertrieb nur mit**





Volumenlizenzen an Firmen und Organisationen),

- **Windows RT (Spezialversion für ARM-Prozessoren),**

ohne den Windows Store installieren zu können.

Windows 8

Die Standardversion stellt eine in der Ausstattung verminderte Version von *Windows 8 Pro* dar. Gegenüber der *Pro*-Version werden BitLocker, das Booten von VHDs, Hyper-V, das Beitreten einer Domäne, die Verschlüsselung des Dateisystems, Gruppenrichtlinien und Remote Desktop fehlen. Das Windows Media Center wird enthalten sein.

Die Standardversion wird sowohl für x86-, als auch x64-Prozessoren angeboten werden. Ein Upgrade von einer bestehenden Installation wird nur für die Vorgängerversionen *Windows 7 Starter*, *Windows 7 Home Basic* und *Windows 7 Home Premium* möglich sein. Upgrades von Windows XP, Windows Vista oder *Windows 7 Professional* oder *Windows 7 Ultimate* werden nicht möglich sein.

Windows 8 Pro

Windows 8 Pro wird gegenüber der Standardversion einen erweiterten Funktionsumfang bieten und richtet sich an Kleinunternehmer, die ihren PC privat und geschäftlich nutzen, sowie an Privatanwender. Das Windows Media Center wird nicht enthalten sein, kann aber über ein separat erhältliches „Media Pack“ erworben und nachinstalliert werden. Das ist jedoch nur noch für *Windows 8 Pro* möglich.

Windows 8 Pro wird sowohl für x86-, als auch x64-Prozessoren angeboten werden. Ein Upgrade von einer bestehenden Installation wird für die Vorgängerversionen *Windows 7 Professional* oder *Windows 7 Ultimate*, Windows XP, Windows Vista oder *Windows 7 Starter*, *Windows 7 Home Basic* und *Windows 7 Home Premium* bei Neukauf eines PCs mit vorinstallierter Version verfügbar sein.

Windows 8 Enterprise

Diese Version ist im Grunde ein *Windows 8 Pro* mit erweitertem Funktionsumfang „in den Bereichen PC-Management, Deployment, Sicherheit und Virtualisierung, das unter Volumenlizenz vertrieben wird. Zu den exklusiven Funktionen gehören *Windows To Go*, mit dem eine Windows 8-Installation von einem USB-Stick aus gestartet werden kann, *DirectAccess*, mit dem eine VPN-lose Remote-Verbindung zwischen Client-Rechnern und Firmennetzwerken aufgebaut werden kann, *BranchCache*, mit dem Firmenserver erstellt werden können, *AppLocker*, mit dem der Umgang mit Firmendaten eingeschränkt werden kann, und die Möglichkeit zum Side-Loading, das es ermöglicht, Metro-Apps

Windows RT

Windows RT wird eine Spezialversion von Windows 8 für Geräte mit ARM-Prozessoren sein, die nur vorinstalliert vertrieben wird. Das Installieren und Ausführen von herkömmlichen x86- oder x64-Anwendungen wird nicht möglich sein. Darüber hinaus werden gegenüber der Standardversion *Windows 8* der Windows Media Player und die Storage Spaces fehlen. In *Windows RT* wird Microsoft Office mit Word, Excel, Powerpoint und Onenote vorinstalliert sein; in den anderen Editionen ist Office nicht enthalten.

Microsoft hat am 18. Juni 2012 das Surface-Tablet vorgestellt, auf dessen Version mit ARM-Prozessor Windows RT laufen wird.



2.2 Unix-Betriebssysteme

Derzeit noch vorherrschend in der Workstationwelt sind Unix-Betriebssysteme. Eigentlich muss hier von einer Betriebssystemfamilie gesprochen werden, denn praktisch jeder Workstation-Hersteller liefert sein eigenes Unix aus, das sich zumindest in der Benutzerschnittstelle deutlich unterscheidet. Es gibt hier allerdings eine Tendenz, die Vielfalt an Oberflächen zu überwinden, da einzelne Hersteller angefangen haben, ihr System auf Fremdarchitekturen zu portieren.

Die Unix-Implementationen lassen sich in zwei Standards zusammenfassen: Berkeley Unix (BSD) sowie AT&T's System V Release 4 (SVR4). Letzteres ist momentan dabei, den Vorrang zu gewinnen - neu entstehende Unix-Versionen folgen diesem Standard. Im Allgemeinen gilt: Ist ein Programm für einen der beiden Standards geschrieben, so lässt es sich ohne allzu große Probleme auf ein anderes System des gleichen Standards portieren.

Auch bei den verwendeten Benutzeroberflächen (GUI - Graphical User Interface) gibt es unterschiedliche Standards. Die neueren folgen aber alle der X11 Definition. Seit einigen Jahren ist die - ebenfalls auf X11 basierende - MOTIF Definition klar auf dem Vormarsch. Mehr und mehr Unix-Implementationen bedienen sich dieser Oberfläche, während der Einsatz konkurrierender Oberflächen, wie OPENLOOK, eher rückläufig ist.

2.2.1 Linux

Linux ist ein frei verfügbares Multitasking- und Multiuser-Betriebssystem. Linux wurde von Linus Torvalds und von einer Vielzahl von Entwicklern in aller Welt weiterentwickelt. Linux wurde von Anfang an unter die GPL, die General Public License gestellt. Es kann frei und kostenlos verteilt, eingesetzt und erweitert werden. Entwickler haben so Einblick in sämtliche Quellcodes und können dadurch sehr einfach neue Funktionen integrieren bzw. Programmierfehler schnell finden und eliminieren. Treiber für neue Adapter (SCSI-Controller, Grafikkarten etc.) können dadurch sehr schnell integriert werden.

Linux kann auf zwei verschiedene Arten bezogen werden: Alle benötigten Teile können kostenlos aus dem Internet geladen werden. Damit kann fast zum Nulltarif ein individuelles Betriebssystem zusammengestellt werden. Einfacher ist der Einsatz einer so genannten Distribution; diese wird von verschiedenen Firmen angeboten und enthält neben einer Vielzahl von Anwendungen auch Installationsprogramme, welche die Installation von Linux wesentlich vereinfachen.

Die Distributionen unterscheiden sich vor allem in den beigelegten Komponenten, wie Programmierumgebungen, Netzwerksoftware und grafische Benutzeroberflächen. Wir empfehlen Distributionen von SuSE oder Red Hat. Diese beiden Linux-Distributionen sind sehr ausgereift und enthalten eine umfangreiche Dokumentation sowie eine grafisch geführte Installation. transtec Linux-Systeme werden grundsätzlich mit den aktuellen Versionen von SuSE und Red Hat zertifiziert und angeboten.

Auf 7 CDs bzw. 1 DVD bietet SuSE 7.2 Professional mehr als 1500 Anwendungsprogramme. Professional enthält alle wesentlichen Serverbestandteile und 90 Tage Installationsupport. Die Personal Version bietet auf 3 CDs alle wesentlichen Programme für eine Workstation-Installation und beinhaltet 60 Tage Installationsupport. Installations- und Konfigurationshandbücher sind in beiden Varianten enthalten, die Professional Version enthält zusätzlich noch ein Know-How-Handbuch.

Die Red Hat 7.1 Deluxe Edition enthält 10 CDs und 3 Handbücher sowie 30 Tage Telefoninstallationsupport und 90 Tage Web-basierten Installationsupport. Sie ist in erster Linie für Workstation-Installationen vorgesehen.

Die Red Hat 7.1 Professional Version umfasst 15 CD-ROMS und 4 Handbücher sowie zusätzlich 30 Tage Web-basierten Apache-Konfigurations-Support. Diese Version ist für Server-Installationen zugeschnitten.

Linux wird mittlerweile von mehreren Millionen Anwendern weltweit erfolgreich eingesetzt. Die Benutzergruppen reichen von privaten Anwendern über Schulungsfirmen, Universitäten, Forschungszentren bis hin zu kommerziellen Anwendern und Firmen, die in Linux eine echte Alternative zu anderen Betriebssystemen sehen.

Der umfangreiche Netzwerksupport von Linux, der verschiedene Server, wie z. B. Appletalk-, Netware- oder LAN-Manager-Server, umfasst, sowie die Vielzahl an unterstützten Netzwerkprotokollen macht Linux zu einem sicheren und stabilen Netzwerk-Serversystem.





2.2.2 SunOS / Solaris

Das auf den SPARC-Rechnern ursprünglich beheimatete Betriebssystem der Firma Sun heißt SunOS. Es wird zusammen mit der OPENLOOK-Benutzeroberfläche OpenWindows angeboten. Dieses Bundle wird als Solaris bezeichnet. SunOS 4.1.x (als Teil von Solaris t.x) ist ein BSD Unix-System und unterstützt Multiprocessing, aber noch kein Multithreading. Die Weiterentwicklung von Solaris 1 wurde Ende 1998 eingestellt. Parallel zu Solaris 1.x hat Sun eine Version 2.x auf den Markt gebracht. Dabei handelt es sich um eine System V-Implementierung. Sie unterstützt seit der Version 2.2 auch Multithreading, also das Verteilen von Teilprozessen auf mehrere Prozessoren. Die Zuweisung der Prozessoren geschieht automatisch, so dass sich der Anwender darum nicht kümmern muss.

Ab der Solaris-Version 2.5 werden 64-bit-Prozessoren und die Verwendung der UltraCreator-Grafik für 2D- und 3D-Anwendungen unterstützt. Solaris 2.5 beinhaltet für das Networking NFS Version 3, dynamische IP-Adressierung für das Point-to-Point Protokoll und Send-Mail-Version B. Zusätzlich sind Security-Applikationen implementiert worden, wie Access Control Lists und NIS+ Password Aging. Vor allem aber wird zu dieser Version und alle darauf-folgenden nun auch eine MOTIF-Oberfläche mitgeliefert (CDE - Common Desktop Environment).

Die momentan am weitesten verbreitete Version, Solaris 8 bietet volle 64-bit-Funktionalität und hohe Performance für alle Java-Applikationen, Große Sicherheit und Stabilität. Die Installation, Administration und Konfiguration funktionieren vollständig über Web-basierende Oberflächen. Folgende weiterentwickelte RAS- (Reliability, Availability and Serviceability) Eigenschaften sind enthalten:

- Dynamische Rekonfiguration
- UNIX-File-System (UFS)-Protokollierung
- Fehlerbehebung im Kernel
- Verbesserte Core Dump-Analyse
- Hot Plugging
- Schnittstellen-Standards: X/Open UNIX 98
- SMB, AppleTalk, DECnet und andere Standards
- Internet-Standards: HTTP, ftp, telnet, DNS, NTP, IMAP4, DHCP, SNMP, SMTP

LDAPv31ETF RFCs 1323, 1510, 1652, 1869, 1870, 1891-1894, 1985, 1996, 2018, 2136, 2045, 2078

Systemanforderungen

Zur Installation sind mindestens 1 GB Massenspeicher und 64 MB Hauptspeicher nötig. Solaris ist sowohl für SPARC- wie auch für Intel x86-Architektur verfügbar. Alle transtec Hamstations werden immer mit der aktuellsten Version von Solaris ausgeliefert; bei der Intel-Version ist unbedingt auf die Kompatibilität zu achten. Eine Kompatibilitätsliste ist auf <http://soldc.sun.com/support/drivers/hcl> zu finden.

Solaris 8

Die aktuelle Version Solaris 8 ist bereits in der zweiten Generation der 64-bit-Technologie. Mit der Unterstützung für IP Version 6 macht Solaris 8 Schluss mit den Beschränkungen von Windows und anderen Welten. Unterstützt werden praktisch unbegrenzt viele Internet Adressen (mehr als eine 1 mit 38 Nullen), 18 Exabyte-Hauptspeicher (d.h. 10 hoch 18 Bytes) und bis zu eine Million gleichzeitiger Prozesse. Das Betriebssystem Solaris 8 unterstützt ebenfalls die neuesten Technologien vom Desktop bis zum Internet. Dazu gehören das unternehmenskritische Java 2SE für die Entwicklung Web-zentrischer Software-Applikationen, das Java Media Framework für das Media-Streaming, X-Server Video Erweiterungen, die Synchronisierung von PDAs (z.B. Palm Pilot) und die Networked Real Time-Verarbeitung. Solaris 8 bietet auch zusätzliche Mainframe-typische Fähigkeiten:

Jobs, Projekte und Buchhaltungsfähigkeiten für die Abrechnung der Computerbenutzung (ideal für Service-Provider); automatische dynamische Rekonfiguration zur Verbesserung der Uptime; und Hot Patching zur dynamischen Änderung des Betriebssystems ohne Herunterfahren des Systems. Ein Web-Install-Werkzeug macht die Software-Installation sehr einfach. Bereits vorhandene Solaris-Applikationen sind mit der Solaris 8 Software kompatibel. Für alle Systeme mit Ultra III oder Ultra IIe ist Solaris 8 unumgänglich.



2.3 Computerviren

Die Verbreitung geschieht langsam, da eine Infektion nur beim Booten von Disketten möglich ist.

Ein trauriges Kapitel auf fast allen Computerplattformen und Betriebssystemen sind Computerviren. Heutzutage werden diese praktisch nur noch über E-Mail und das Internet verbreitet.

Virenarten

Ein Computervirus ist eine Befehlsfolge, deren Ausführung einen Speicherbereich verändert, in dem es eine Kopie von sich in diesen hinein kopiert. Der Speicherbereich kann eine ausführbare Datei oder ein Programm auf Diskette, Festplatte etc. oder auch im RAM sein.

Dateiviren

Dateiviren lagern sich an ausgewählte Programme an und bedienen sich dabei unterschiedlicher Techniken. Die Verbreitung erfolgt immer dann, wenn ein bereits infiziertes Programm aufgerufen wird. Residente Dateiviren stellen insofern eine Steigerung dar, dass sie sich nach ihrem Aufruf resident im Speicher festsetzen. Somit wird bei jeder Programmausführung neu infiziert. Diese Gattung von Viren ist schwerer zu eliminieren, sie überlebt in manchen Fällen sogar einen Warmstart des Rechners. Die überwiegende Anzahl der heute bekannten Viren fällt in diese Klasse. So genannte Stealth-Viren wurden entwickelt, um Viren-Scanner, Prüfsummenprogramme oder Wächterprogramme zu unterlaufen. Ähnlich wie amerikanischen Tarnbomber verfügen sie über einen Tarnmechanismus, der es ihnen ermöglicht, ihre eigene Existenz zu verschleiern.

Polymorphe Viren sind die derzeit modernsten und gefährlichsten Varianten der Dateiviren. Unter diese Klasse fallen Viren, die bei jeder neuen Infektion ihr Erscheinungsbild ändern. Gewöhnlich wird dies erreicht, indem sie den Virus-Code mit einem wechselnden Schlüssel bei jeder Infektion neu verschlüsseln.

Systemviren nutzen bestimmte Programmbestandteile wie Masterbootrecord, Partitionsbootrecord, Diskettenbootsektor, FAT und Wurzelverzeichnis (Root) des Betriebssystems als Infektionsmedium. Diese Systembereiche sind an den jeweiligen Datenträger gebunden, und eine Übertragung setzt das Arbeiten mit den jeweiligen Datenträgern voraus.

Bootsektor-Viren greifen ausschließlich den Bootsektor auf Disketten und Festplatten an.



3. Cluster

Ein Cluster ist die Verknüpfung mehrerer Systeme zu einer Gruppe, die über eine Cluster-Software verwaltet und gesteuert wird. Physisch gesehen ist ein Cluster eine Gruppe von zwei oder mehreren unabhängigen Servern, die auf dieselben Daten zugreifen können und dieselbe Gruppe von Clients bedienen. In Anbetracht des heutigen Stands der Technik bedeutet dies meistens, dass die Server mit gebräuchlichen I/O-Bussen und einem normalen Netzwerk für den Client-Zugriff verbunden sind.

Logisch betrachtet stellt ein Cluster eine einzelne Verwaltungseinheit dar, in der ein beliebiger Server jedem autorisierten Client jede verfügbare Leistung anbieten kann. Die Server müssen Zugriff auf dieselben Daten haben und ein gemeinsames Sicherheitssystem besitzen. Dem heutigen technischen Standard entsprechend bedeutet dies, dass in der Regel Server in einem Cluster dieselbe Architektur besitzen und unter der gleichen Version des gleichen Betriebssystems laufen.

Obwohl es verschiedene Möglichkeiten gibt, wie Cluster aufgebaut sein können, bieten alle die folgenden drei Vorteile:

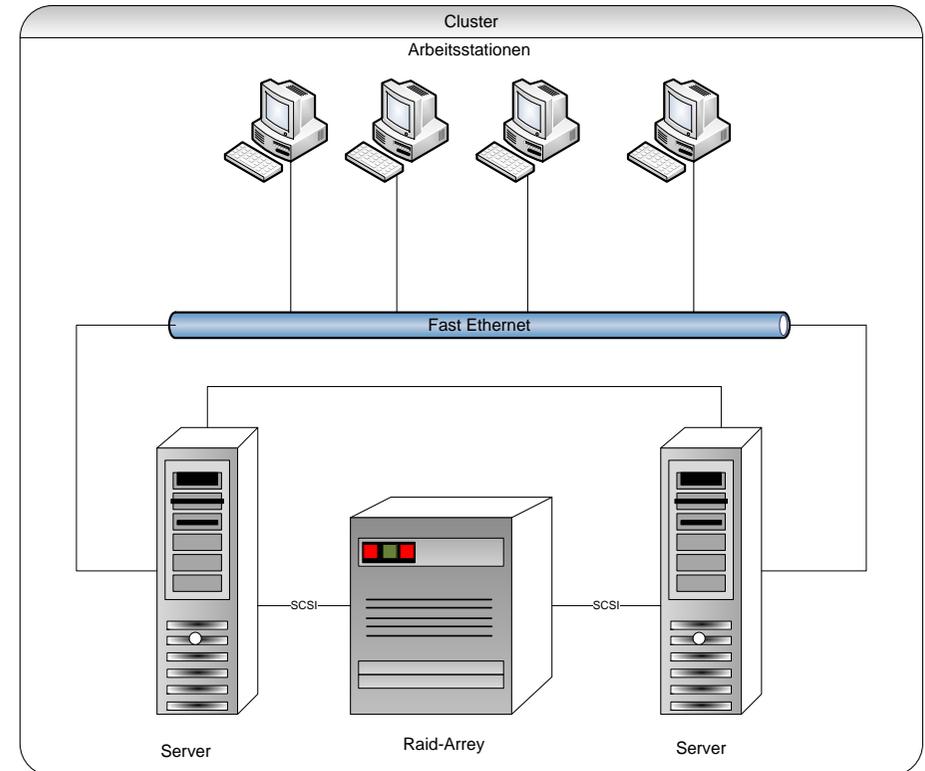
- fehlertolerante Hochverfügbarkeit bei Anwendungen und Daten;
- Skalierbarkeit von Hardware-Ressourcen;
- Einfachere Verwaltung großer oder schnell wachsender Systeme.

Höhere Verfügbarkeit

In unternehmenskritischen Umgebungen bildet die Hochverfügbarkeit von Diensten (z.B. Webserver, Datenbanken oder Netzwerk-File-Systemen) die Voraussetzung für den Erfolg des Unternehmens. Häufige Gründe für Verfügbarkeitsprobleme von Diensten sind unterschiedliche Formen von Systemstörungen. Die Störung kann in der Hardware, Software, Anwendung oder im Ablauf begründet sein. Man kann sich gegen diese Störungen absichern, indem ein Cluster als Anwendungs- oder Datenserver verwendet wird. Cluster bieten neben redundanter Rechenleistung, I/O- und Speicherkomponenten auch die Möglichkeit, dass beim Ausfall eines Servers ein anderer Server dessen Arbeit unterbrechungsfrei übernimmt. Somit ermöglichen Cluster eine hohe Verfügbarkeit der Server-Dienste auch bei einer Störung.

Die Abbildung zeigt ein einfaches Cluster, bestehend aus zwei vernetzten Servern und

einem RAID-System zum Speichern der Daten.



- Wenn an einem Server Hard- oder Softwarestörungen auftreten oder der Server abstürzt, kann der andere Server dessen Funktion übernehmen;
- Wenn die Netzwerkschnittstelle eines Servers ausfällt und dadurch die Verbindung zu den Clients abbricht, können die Clients weiterhin auf die Leistungen des zweiten Servers zurückgreifen;
- Wenn ein I/O-Bus oder Adapter ausfällt, kann über einen alternativen Pfad auf die Daten des RAID-Systems zugegriffen werden;
- Wenn eine Platte ausfällt, sind die Daten durch das RAID-System weiterhin verfügbar.

In allen Fällen müssen Server und Clients die Störung erkennen und beheben. Zwar



kommt es hierbei zu einer Unterbrechung der Leistung des Cluster-Dienstes, diese beträgt jedoch bei der Verwendung von Clustern normalerweise nur wenige Sekunden, im Gegensatz zu Minuten oder Stunden bei sonst üblichen Wiederherstellungsmethoden.

Skalierbarkeit

Ein weiterer wichtiger Vorteil einiger Cluster-Architekturen ist die Skalierbarkeit, die ein Anwendungswachstum über die Kapazität eines einzelnen Servers hinaus ermöglicht. Viele Anwendungen besitzen mehrere Threads relativ abgegrenzter Aktivitäten, die nur gelegentlich interagieren. Anwendungen mit mehreren Threads können als pseudo-parallele Prozesse auf einem Server mit einem Prozessor laufen oder als echte parallele Prozesse in symmetrischen Multiprozessorsystemen (SMP). In einem Cluster können Gruppen der Anwendungs-Threads auf verschiedenen Servern ausgeführt werden, da die Server auf dieselben Daten zugreifen können. Wenn eine Anwendung zu groß für einen Server wird, kann ein zweiter Server installiert werden, um ein Cluster zu erstellen und so die Anwendungskapazität zu erhöhen.

Damit die Server auf dieselben Daten zugreifen können, ist Koordination erforderlich. Diese Koordination kann durch eine Anwendung, einen Datenbank-Manager oder ein verteiltes Dateisystem erfolgen. In einem Cluster, in dem diese Koordination fehlt, ist der gleichzeitige direkte Zugriff mehrerer Server auf eine beliebige Datei nicht möglich. Jedoch lassen sich selbst mit diesem begrenzten Zugriff einige Anwendungen skalieren. Die Anwendungen können so aufgeteilt werden, dass die einzelnen Programme unterschiedliche Daten verwenden.

Einfachere Verwaltung

Der dritte Vorteil von Clustern ist die einfachere Verwaltung. Cluster vereinfachen die Komplexität der Systemverwaltung, indem sie den Umfang der von einem einzelnen System verwalteten Anwendungen, Daten und Benutzerdomänen vergrößern. Die Systemverwaltung umfasst unter anderem folgende Bereiche:

- Betriebssystem,
- Middleware,
- Anwendungspflege,
- Verwaltung von Benutzer-Accounts
- Konfigurationsverwaltung und - Datensicherung.

Komplexität und Kosten für die Systemverwaltung hängen von der Größe und

insbesondere von der Anzahl der verwalteten Systeme ab. Beispielsweise ist die tägliche Datensicherung für alle Server nötig, die wichtige Daten speichern - unabhängig von der Menge der zu sichernden Daten. Auch Änderungen von Benutzer-Accounts müssen auf allen Servern aktualisiert werden, auf die der Benutzer zugreift.

Cluster verringern die Anzahl der einzelnen Systeme - und somit die Kosten für die Systemverwaltung - indem sie eine größere Anzahl von Anwendungen, Daten und Benutzern zu einem einzigen Rechnersystem zusammenfassen. Ein Vorteil davon ist, dass in einem Cluster-System nur jeweils ein einziger Satz von Benutzer-Accounts, Dateizugriffsberechtigungen, Datensicherungsregeln, Anwendungen, Datenbank-Managern etc. enthalten sein muss. Obwohl die durch unterschiedliche Cluster-Architekturen erstellten Einzelsysteme variieren können, ist es normalerweise günstiger, ein einzelnes Cluster anstatt der entsprechenden Anzahl unverbundener Server-Systeme zu verwalten.

Die Lastverteilung zwischen den einzelnen Cluster-Servern erfolgt automatisch. Sowohl Unix- als auch OpenVMS-Cluster bieten automatische Lastverteilung und Skalierbarkeit, Windows 2000 Cluster bieten zurzeit lediglich eine bessere Verfügbarkeit. Mit dem Cluster-Server des Windows 2000 Advanced Servers können zwei Server, beim Windows 2000 Data Center Server vier Server zu einem Cluster verbunden werden. Die vom Cluster-Server unabhängige automatische IP-Lastverteilung erlaubt die Verteilung von Web Applikationen auf bis zu 32 Systeme.

High Performance Computing / Beowulf Cluster

Die Beowulf-Cluster-Architektur besteht im Prinzip aus einer Anzahl von Rechenknoten und einem oder mehreren Zugangsrechnern. Die Zugangsrechner werden als Front End oder als Server Node bezeichnet. Ein Nutzer loggt sich, meist remote, nur auf diesem Server Node ein. Von dort aus kann er sich eine beliebige Menge von Rechenknoten für seine Arbeit (seinen Rechenauftrag) reservieren und benutzen. Dementsprechend benötigen die Rechenknoten keinerlei Ein- oder Ausgabe-Peripherie wie Tastatur, Maus oder Bildschirm. Sowohl Zugangsrechner als auch Rechenknoten erfordern keinerlei spezielle Hardware, in der Regel kommen Standardsysteme mit x86- oder Alpha-Prozessoren zum Einsatz. Die Koppelung der Systeme kann mit jeder beliebigen Netzwerk-Infrastruktur erfolgen. Als Betriebssystem kommt in der Regel ein freies Betriebssystem (Linux, FreeBSD usw.) zum Einsatz.

Ein Beowulf Cluster dient zur preisgünstigen Lösung von Aufgaben, die sehr viel Rechenleistung erfordern. Die Einrichtung eines solchen Clusters ist jedoch keine einfache Aufgabe, da es kein fertiges Paket gibt. Das Cluster muss, den Anforderungen entsprechend, aus mehreren Softwareteilen zusammengestellt, und die Anwendung muss dann noch parallel programmiert werden.

Hochverfügbarkeits-Cluster mit SGI Failsafe





Die SGI-Failsafe- Clustersoftware ist ein universelles, frei konfigurierbares und fehlertolerantes Hochverfügbarkeitssystem, mit dem einzelne Dienste (Services) redundant aufgebaut werden können. Mit Hilfe der Software kann ein Dienst im Fehlerfall automatisch oder manuell auf einen anderen Node (Server) migriert werden. Wobei der Fehlerfall nicht nur in defekter Hardware liegen muss: Applikationsfehler, desolante Prozesse und kritische Systemzustände werden ebenfalls als solche erkannt und entsprechend behandelt. Dazu müssen die einzelnen Nodes des Clusters auf gemeinsame Datenbereiche zugreifen können, um den Datenbestand im Fehlerfall zu übernehmen. Hierzu kann eine SCSI RAID oder SAN-Architektur genutzt werden, die es den Servern ermöglicht, Datenbereiche im Fehlerfall zu übernehmen.

Wurden die Datenbereiche erfolgreich übernommen, kann der aktive Cluster-Server die Dienste neu starten und unter der gleichen IP wieder zur Verfügung stellen. Die Downtime eines Dienstes ist somit kalkulierbar und in gewissem Rahmen sogar steuerbar, da man verschiedene Kriterien für die Dienstmigration konfigurieren kann. Mit entsprechend redundanten Serversystemen ist mit dieser Lösung ein Verfügbarkeit von 99,99 % realisierbar.



4. Massenspeicher

4.1 Überblick

4.1.1 Einteilung Primär-, Sekundär- und Backup-Datenspeicher

Massenspeicher gibt es in einer kaum überschaubaren Anzahl von Technologien, die in einer Reihe wichtiger Eigenschaften grundlegend differieren. Sie lassen sich in Primär-, Sekundär- und Backup-Datenspeicher einteilen.

Bei der Wahl des Massenspeichers und des dazu passenden Hostadapters müssen unter Anderem berücksichtigt werden: die Auswahl der geeigneten Laufwerkstechnologie, Einbau, Hardware-Anschluss, Software-Einbindung, Performance und Kapazität.

Primär-Datenspeicher:

Darunter versteht man Massenspeicher, die auf Daten im Random Access (direkter Zugriff auf Informationsblöcke, z. B. Magnetplatte) zugreifen. Zu dieser Gruppe zählen magnetische Festplattenlaufwerke und RAM-Drives.

Sekundär-Datenspeicher:

Das sind wechselbare Massenspeicher, die Daten ähnlich wie Primär-Datenspeicher speichern. Der direkte Zugriff auf alle gespeicherten Daten ist jedoch erst nach dem Einlegen des Datenträgers möglich. Zu dieser Gruppe zählen magnetische und magneto-optische Wechselplattenlaufwerke, Diskettenlaufwerke und Memory-Card-Drives, CD- und DVD Laufwerke.

Backup-Datenspeicher:

Dazu zählt man in der Regel Massenspeicher, die sequenziell arbeiten. Der wahlfreie Zugriff auf Dateien und Programme ist nicht möglich, da die Suche nach Informationsblöcken in der Reihenfolge stattfindet, in der sie auf dem Datenträger stehen.

4.1.2 Peripheriebusse

SCSI Schnittstelle

SCSI (Small Computer Systems Interface) ist ein in seiner ursprünglichen Form 8 Bit breiter, paralleler, später auch seriell definierter I/O-Bus, der für den Anschluss von Massenspeicherlaufwerken aller Art, aber gelegentlich auch von Scannern und anderen Peripheriegeräten an verschiedenen Rechnersystemen verwendet wird und sehr weite Verbreitung gefunden hat. Die Vorteile von SCSI waren von Anfang an eine relativ hohe maximale Übertragungsrate sowie eine flexible und einfache Konfiguration. Bei SCSI ist viel Intelligenz im Laufwerk selbst vorhanden, denn die SCSI-Schnittstelle ist keine Schnittstelle im klassischen Sinne, sondern ein Peripheriebus, über den Laufwerke und Hostadapter miteinander kommunizieren. Die erste SCSI-Norm wurde bereits 1986 von ANSI als Standard verabschiedet. Hinter SCSI verbirgt sich ein dreischichtiges Regelwerk mit Kommando-, Protokoll- und Interfaceebene. Den Kern von SCSI bilden die so genannten Primary Commands (SPC). Diese Befehle müssen alle Geräte beherrschen. Darauf aufbauend existieren spezielle Kommandos für einzelne Gerätegruppen: Controller Commands (SCC) für Hostadapter, Block Commands (SBC) für Festplatten, Stream Commands (SSC) für Bandlaufwerke, Multimedia Commands (MMC) für CD-ROM und Medium Changer Commands sowie die bisher selten genutzten Graphic Commands (SGC) für graphisch orientierte Geräte wie Drucker, Plotter und Scanner. Aus diesen Befehlen setzt sich die so genannte Kommandoebene zusammen. Unterhalb dieser Kommandoebene auf der Protokollebene liegen die Protokolle der verschiedenen Schnittstellentypen. Diese logischen Protokolle regeln, wie ein SCSI-Befehl auf dem jeweiligen Interface abgebildet wird und wie die einzelnen Geräte miteinander kommunizieren. Das klassische SCSI-Interface (8 bit- und 16 bit-SCSI) nutzt das Interlocked Protocol (IPC). Die neuen Interfaces bauen auf eigenen Protokollen auf: das Serial Storage Protocol (SSP) für SSA sowie das Generic Packetized Protocol (GPP), die Anbietern anderer Interfaces den Zugang zu SCSI erleichtern sollen. Die unterste Ebene schließlich ist die Interfaceebene, in der die verschiedenen physikalischen Übertragungsmedien definiert sind.

Der Vorteil dieses modularen Modells zeigte sich bei der Einführung neuer serieller Technologien: Fibre Channel und SSA konnten problemlos in den am weitesten verbreiteten Standard, nämlich SCSI eingebettet werden. Das spart einerseits Kosten und beschleunigt andererseits die Einführung der neuen Interfaces.

Die Ausdehnung des ursprünglichen, parallelen SCSI (1 und 2) auf serielle Übertragung wird unter SCSI-3 subsumiert. SCSI-3 ist im parallelen Bereich abwärtskompatibel. Bei Verwendung der seriellen Interfaces (Fibre Channel, SSA) werden wesentlich größere Datentransferraten erreicht, und die beim parallelen SCSI gegebene Aufteilung in die schnellere Datenphase (20 MB/s bei Ultra SCSI) und eine langsamere Befehlsphase (5 MB/s) entfällt.

Im Folgenden sollen nun die verschiedenen Protokolle und Interfaces näher beschrieben





werden (siehe auch Tabelle Platteninterfaces im Überblick).

Paralleles SCSI

- SCSI-1

Die erste verabschiedete SCSI-Norm war SCSI-1. Sie unterstützte primär nur Festplatten und Bandlaufwerke. Auch hinsichtlich seiner sonstigen Leistungsdaten ist SCSI-1 nicht mehr konkurrenzfähig. Der Overhead bei der Datenübertragung liegt bei bis zu 90%. Der im asynchronen Modus durchgeführte Datentransfer erreichte Transferraten von maximal 1 MB/s, im synchronen Modus bis 5 MB/s. SCSI-1 wird seit 1990 nicht mehr verwendet.

- SCSI-2

Die SCSI-2 Norm wurde 1986 entwickelt und beinhaltet wesentliche Verbesserungen. Der SCSI-2-Kommandosatz enthält eine Reihe zusätzlicher Kommandos, welche die Unterstützung von Festplatten, Band- und MO-Laufwerken, CD-ROMS, Scannern oder auch Jukeboxen verbessern bzw. erst ermöglichen. Neben dem neuen standardisierten Kommandosatz (Common Command Set) enthält die SCSI-2-Spezifikation auch eine höhere maximale Transferrate von 10 MB/s (Fast-SCSI, mit der üblichen Busbreite von 8 Bit) sowie die Möglichkeit, die Breite des Datenpfades auf 16 Bit (Wide-SCSI) zu erhöhen. Durch eine Kombination von Fast- und Wide-SCSI sind somit Transferraten von bis zu 20 MB/s auf dem Bus möglich. Die Angabe der SCSI-2-Unterstützung bei einem Gerät bedeutet nicht automatisch, dass es dem kompletten SCSI-2-Umfang (inkl. Fast- und WideSCSI) entspricht, jedoch haben aktuelle Laufwerke in der Regel Fast-SCSI implementiert. Fälschlich wird teilweise die Wide-SCSI-Version (16 Bit breiter Datenbus) von SCSI-2 als SCSI-3- sowie Non-Fast-SCSI-2 als SCSI-1-Norm bezeichnet.

- Ultra SCSI

Noch einmal verdoppelt wurde der Transferrate bei Ultra SCSI, einer vollabwärtskompatiblen Erweiterung von SCSI-2. Durch die Verdoppelung der Taktrate auf dem Bus verdoppelt sich auch die Transferrate auf 20 MB/s (8 Bit) bzw. 40 MB/s (16 Bit). Dies betrifft allerdings nur die Datentransferrate. Die Befehlsübertragung geschieht weiterhin mit 5 MB/s. Auch Stecker und Kabel wurden aus Kompatibilitätsgründen beibehalten. Die Performance-Steigerung hat ihren Preis: Die zulässige Kabellänge verkürzt sich bei SingleEnded auf 1,5 Meter und bei Differential entsprechend auf 12,5 Meter. Eine aktive Terminierung ist unbedingt notwendig, um eine störungsfreie Übertragung zu gewährleisten.

Um dem Anwender die Konfiguration des SCSI-Busses zu erleichtern, enthält die Ultra SCSI-Spezifikation das Feature SCAM (SCSI Configuration Auto Matically). Das angeschlossene Gerät konfiguriert sich also selbst. Die Implementierung von SCAM in

die Devices ist jedoch jedem Hersteller selbst überlassen.

- Ultra SCSI (LVD - Low Voltage Differential)

Produkte mit Ultra SCSI sind seit 1998 auf dem Markt. Auch hier wurde wieder die Datentransferrate verdoppelt, auf 80 MB/s bei 16 Bit. Die bisherige 8 bit-Version wird sich nach und nach verabschieden. Da außerdem eine weitere Halbierung der Kabellänge bei SingleEnded-Verkabelung den Bus praktisch unbrauchbar machen würde, wurde dieser Standard nur noch als LVD (Low Voltage Differential) definiert, eine Differenzial-Verkabelung, die darüber hinaus mit einem Drittel der Signalspannung arbeitet. Die maximale Kabellänge beträgt hier immerhin noch 12 m.

Um auch diesen Standard mit den bisherigen kompatibel zu halten, werden Ultra2-Laufwerke mit einer autosensing Schnittstelle ausgerüstet, die den Betrieb an herkömmlichen Single-Ended-Controllern (nicht am Differenzial) ermöglichen, wenn auch nur mit Ultra SCSI-Geschwindigkeit. Allerdings verfügen sie nicht über interne Terminierung, was die Verwendung von separaten Terminatoren auch innerhalb der Rechner notwendig macht.

- Ultra 160 SCSI

Ultra160 benutzt die gleiche Verkabelung wie Ultra2 LVD-SCSI. Die Verdoppelung der Transferrate wurde durch die Datenübertragung an der auf- und absteigenden Flanke des Signals erreicht. Die effektive Leistung (der Nettodatentransfer) dürfte an die des momentanen Fibre Channel heranreichen.

- Ultra 320 SCSI

Obwohl von vielen Seiten gedacht wurde, dass mit Ultra160 das Ende der Steigerung beim parallelen SCSI erreicht wäre, ist bereits Ultra320 absehbar, die ersten Hersteller haben ihre Unterstützung und Produkte schon angekündigt.

- SCSI 3

SCSI-3 beinhaltet sowohl die Normen des parallelen SCSI als auch die der weiter unten beschriebenen seriellen Interfaces.



Schnittstelle	Datenbits	Max. Transferrate MB/s	Max. Anzahl Laufwerke	Max. Kabellänge (m)
Single-Ended	8	5	7	6
Single-Ended-Fast	8	5	7	3
Single-Ended-Ultra	8	20	7	1,5
Single-Ended-Wide	16	20	15	3
Single-Ended-Wide-Ultra	16	40	15	1,5
Differential	8	5	7	25
Differential	8	10	7	25
Differential	8	20	7	12,5
Differential	16	20	15	25
Differential	16	40	15	12,5
Ultra 2 LVD	16	80	15	12
Ultra 160	16	160	15	6
Ultra 320	16	320	15	6

SCSI-Schnittstelle

SCSI-Schnittstellen

Die parallele SCSI-Schnittstelle gibt es in unterschiedlichen Varianten (siehe Tabelle), die sich in der Art der Datenübertragung unterscheiden. SCSI-Signale können entweder auf 8 Bit (Narrow) oder 16 Bit (Wide-SCSI) breiten Bussen übertragen werden. Bis zu 7 Laufwerke können am 8 bit-Bus angeschlossen werden, bis zu 15 Laufwerke am 16 bit-Bus. Beide Busbreiten verfügen wiederum über die Verkabelungsarten Single-Ended (SE) oder Differenzial (D). Bei SE-SCSI wird jedes Signal nur auf einer, bei D-SCSI dagegen auf zwei untereinander verdrehten Leitungen übertragen. Letztere sind daher gegen elektrische Einflüsse unempfindlicher. Die Vorteile von D-SCSI sind bessere Störsicherheit und, daraus resultierend, größere Kabellängen (siehe Tabelle). Nachteilig sind lediglich die - im Vergleich zu SE-SCSI - höheren Kosten für Laufwerke und Hostadapter.

Bei der Auswahl eines Subsystems ist zu beachten, dass die SCSI-Schnittstelle des Hostadapters mit der des Laufwerks übereinstimmt.

Grundsätzlich können 8 bit-Geräte an einen 16 bit-Bus angeschlossen werden, jedoch

sind dabei eine ganze Reihe besonderer Konfigurationsregeln zu beachten.

Single-Ended- und Differential- oder LVD-SCSI können nicht gleichzeitig am Bus betrieben werden. Der Versuch kann zu Schäden an Laufwerk und Controller führen. Lediglich LVD-Laufwerke stellen sich selbstständig auf Single-Ended um.

Synchroner und asynchroner Datentransfer

Bei parallelem SCSI gibt es den asynchronen und den schnelleren synchronen Datentransfer. Beim asynchronen Datentransfer wird jedes Byte separat gesendet und bestätigt, während beim synchronen Transfer mehrere Bytes auf einmal gesendet und dann gemeinsam bestätigt werden. Dadurch ist der Overhead beim synchronen Übertragungsmodus kleiner und die Transferrate höher. Grundsätzlich können alle Peripheriegeräte asynchron arbeiten. Synchronlaufwerke bzw. -Controller stellen vor dem Datenaustausch beim so genannten handshaking fest, ob der andere Kommunikationspartner auch synchronen Transfer beherrscht, und benutzen dann automatisch die entsprechende Datentransferart. Heutige SCSI-Laufwerke und Hostadapter unterstützen in der Regel die Synchronübertragung.

Kabel für paralleles SCSI.

Um einen problemlosen und fehlerfreien Datentransfer zu ermöglichen, sind einige grundsätzliche Dinge bereits bei der Auswahl des richtigen SCSI-Kabels zu beachten: Die SCSI-Kabel müssen nach UL (Underwriter Laboratories) und CSA (Canadian Standard Association) spezifiziert sein. Die einzelnen Drähte des Kabels müssen aus Kupferlitze bestehen (besser kupferverzinkt). Sie müssen paarweise verdreht sein. Zusätzlich sollte das Kabelbündel noch einmal über die Länge von max. 1 m verdreht sein. Das gesamte Kabel braucht weiter eine doppelte Abschirmung. Dies wird in der Regel durch eine Silberfolie und ein zusätzliches Drahtgeflecht über dem Kabelbündel erreicht.

Werden mehrere Peripheriegeräte an einen SCSI-Bus angeschlossen, sollten die einzelnen Verbindungskabel möglichst kurz sein und optimalerweise dieselbe Länge haben. Dadurch wird die Störanfälligkeit des Busses reduziert.

Da es bei den Kabeln keinen Unterschied zwischen Single-Ended und Differential-SCSI gibt, können die Kabel für beide Schnittstellentypen verwendet werden.

Terminierung der Subsysteme

Mit wachsender Übertragungsrage steigen auch die Anforderungen an die Datenkabel und an die SCSI-Bus-Terminierung. Differential-SCSI und aktive Terminierung gewinnen immer mehr an Bedeutung.





Grundsätzlich können 8 bit-Geräte an einen 16 bit-Bus angeschlossen werden, jedoch sind dabei eine ganze Reihe besonderer Konfigurationsregeln zu beachten. Single-Ended- und Differential- oder LVD-SCSI können nicht gleichzeitig am Bus betrieben werden. Der Versuch kann zu Schäden an Laufwerk und Controller führen. Lediglich LVD-Laufwerke stellen sich selbstständig auf Single-Ended um.

Der Forced Perfect Terminator (FPT) ist eine vor allem in der IBM-Welt (RS/6000) verwendete Variante der aktiven Bustermiierung. Hierbei wird die Impedanz des SCSI Busses dynamisch angepasst. Wenn allerdings FPT verwendet wird, so muss dies auf beiden Seiten des Busses - also auch auf der Hostadapter-Seite - geschehen.

Grundsätzlich wird die Verwendung von aktiven Terminatoren empfohlen, da diese im Gegensatz zur passiven Terminierung wesentlich störsicherer sind.

Anschluss von Subsysteme

Beim Anschluss von externen SCSI-Subsystemen gibt es folgende Möglichkeiten:

1. Bisher ist noch kein externes Subsystem am SCSI-Port angeschlossen: In diesem Fall benötigt man ein entsprechendes SCSI-Kabel für die jeweilige Rechnerplattform. Bei allen externen Subsystemen werden im Preislistenteil Kabelauschoptionen für die entsprechende Rechnerplattform angeboten. So sind anstelle der Standardkabel auch Kabel mit dem in der Preisliste angegebenen Steckern erhältlich. Das Subsystem lässt sich auf diese Weise direkt mit dem richtigen Stecker an den jeweiligen Rechnertyp anschließen. Die unterschiedlichen Steckertypen sind im Kapitel SCSI-Kabel und -Terminatoren (Seite 180) abgebildet. Des Weiteren wird noch ein Terminator benötigt. Immer muss auch die maximale Kabellänge berücksichtigt werden, wobei Kabel in den Gehäusen (Rechner, Platten etc.) mitzuzählen sind.

2. Externe Subsysteme sind bereits vorhanden und mit HD68-Steckern ausgerüstet: Mit dem mitgelieferten Kabel kann das neue Subsystem beliebig an die bestehenden Subsysteme angehängt bzw. zwischen diese eingefügt werden.

3. Externe Subsysteme sind bereits vorhanden, haben aber keinen HD68-Stecker: Hierbei gibt es zwei Möglichkeiten:

§ Man schließt das neue Subsystem an die letzte vorhandene Box an. Hierzu muss mittels einer Tauschoption das Standardkabel gegen ein Kabel mit passendem Stecker getauscht werden. Zusätzlich wird dann noch ein entsprechender Terminator mit Stecker benötigt.

§ Das neue Subsystem wird als erstes direkt an den Rechner angeschlossen. In diesem Fall wird, wenn nötig, das Standardkabel gegen ein Kabel mit einem für den Rechner passenden Stecker getauscht. Außerdem wird dann noch ein zusätzliches Kabel zum Anschluss des neuen Subsystems an die bereits vorhandenen benötigt. Passende Kabel hierfür sind in dem Kapitel SCSI-Kabel und -Terminatoren aufgelistet.

4.1.3 Serielles SCSI

Fibre Channel

Der Name Fibre Channel ist etwas irreführend, denn der serielle Bus ist nicht nur für Lichtleiter, sondern auch für Kupferkabel spezifiziert. Auf beiden Medien sind Übertragungsraten von 12,5 MB/s bis hin zu etwa 400 MB/s vorgesehen. Die physikalische Transferrate liegt mit 132 Mbit/s bis 2 Gbits/s noch etwas höher. Die daraus resultierende etwas höhere Bruttodatenrate wird für einen 8-zu-1 0-bit-Code genutzt, der eine einfache Fehlererkennung erlaubt. Innerhalb eines Fibre-Channel-Systems können verschiedene Kabelarten gemischt werden. Die einfachste Variante ist ein abgeschirmtes Twisted-Pair-Kabel. Große Distanzen oder höhere Transferraten erfordern wahlweise Kupfer- oder Glasfaserkabel. Somit lassen sich mit ein und demselben Interface sowohl Low-End- und Low-Cost Systeme als auch High-End-Systeme aufbauen. Die Glasfaserverbindungen werden über einen Duplex-SC-Stecker angeschlossen, die Kupferverkabelung über einen DSub 9pol. Stecker und die Twisted-Pair-Kabel mittels eines 9-poligen HSSDC (High Speed Serial DC Steckers).

Fibre Channel ist die allgemeine Bezeichnung für eine Normenreihe, die von der ANSI (American National Standards Institute) entwickelt wurde und weiterentwickelt wird, um neue Protokolle für eine flexible Informationsübertragung zu schaffen. Diese Entwicklung begann im Jahr 1988 als Erweiterung der Norm Intelligent Peripheral Interface (IPI) Enhanced Physical und verzweigte sich in mehrere Richtungen.

Die vorrangigen Ziele dieser Entwicklung sind:

- § unterschiedliche Typen physikalischer Schnittstellen zu unterstützen
- § ein Mittel für die Vernetzung dieser unterschiedlichen Schnittstellentypen anzubieten
- § eine Hochgeschwindigkeitsübertragung großer Datenmengen zu ermöglichen
- § das logische Protokoll wird von der physikalischen Schnittstelle transportiert; dies erlaubt den Transport verschiedener Protokolle über eine gemeinsame physikalische Schnittstelle (ggf. simultan)
- § eine Entlastung von der zunehmenden Zahl physikalischer



Schnittstellen, die nur begrenzte Verbreitung haben

Fibre Channel ist in Systemen unterschiedlichster Größen zu finden, doch derzeit wird es zunächst in Großrechnersystemen Anwendung finden und später in Workstations. Auf preiswerten PCs dürfte es kaum verwendet werden, doch später wird es in den Desktopsystemen von Profianwendern implementiert werden, die an Netzwerke angeschlossen sind.

Kanäle

Kanäle operieren in der Regel in einer geschlossenen, strukturierten und vorhersehbaren Umgebung, in der alle Geräte, die mit einem Host kommunizieren können, im Voraus bekannt sind, und jede Änderung erfordert auch Modifikationen der Host-Software bzw. der Konfigurationstabellen. Diese komplexeren Wissensstufen werden von den meisten Kanälen bewältigt.

Gegenwärtig sind systemgebundene Lichtwellenleiter-Schnittstellen in einigen Desktop-Systemen und Workstations zu finden. Die Anwendung sehr schneller Fibre-Channel-Schnittstellen wird zunehmen, sobald ihre Geschwindigkeit und ihre Funktionen diesen Anwendern bekannt werden. Dazu zählen auch kleine Arbeitsgruppen, die zwecks Datenaustauschs mit Hochgeschwindigkeitsleitungen vernetzt werden müssen.

Das Host-System enthält das gesamte Wissen der an diesen Host angeschlossenen Kanäle. Gelegentlich wird hierfür auch die Bezeichnung Master-Slave-Umgebung verwendet. Peripheriegeräte wie Band- und Plattenlaufwerke sowie Drucker sind direkt an das Host-System angeschlossen. Der Host ist dabei der Master, und die Peripheriegeräte sind die Slaves.

Zu nennen sind zwei grundlegende Peripherieprotokolle für die Gerätekommunikation: Kanäle und Netzwerke. Üblicherweise bezieht sich der Begriff Kanal auf eine periphere I/O-Schnittstelle (mit einem Hostcomputer), die große Datenmengen zwischen dem Host und dem Peripheriegerät hin- und hertransportiert. Der Systemverarbeitungsaufwand wird so gering wie möglich gehalten, indem die Datenübertragung in der Hardware mit geringer bis gar keiner Software-Beteiligung gehalten wird, sobald eine I/O-Operation beginnt. Dagegen bezieht sich der Begriff Netzwerk auf eine I/O-Schnittstelle, die in der Regel zahlreiche kleine Übertragungen mit größerem Systemverarbeitungsaufwand impliziert, der in der Regel auf eine Softwarebeteiligung am Informationsfluss zurückzuführen ist. Netzwerke unterstützen in der Regel eine Host-to-Host-Kommunikation.

Kanäle werden für die Datenübertragung benutzt. Mit dem Begriff Daten sind Dateien mit Informationen gemeint, die viele Tausend Byte umfassen können. Eine wichtige Anforderung für die Übertragung von Daten ist die fehlerfreie Übergabe, wobei die

Übertragungsverzögerung zweitrangig ist.

Netzwerke

Auf der anderen Seite arbeiten Netzwerke in einer offenen, unstrukturierten und im Grunde genommen unberechenbaren Umgebung. Fast jeder Host bzw. jedes Gerät kann jederzeit mit jedem anderen Gerät kommunizieren. Diese Situation erfordert eine intensivere Software-Unterstützung zur Prüfung der Zugangsberechtigung, zur Einrichtung von Übertragungssitzungen und für Routing-Transaktionen zum richtigen Software-Dienst.

Diese unstrukturierte Umgebung, die davon ausgeht, dass die angeschlossenen Geräte alle gleichberechtigt sind, wird Peer-to-Peer-Umgebung genannt. Mehrere Workstations und Mainframe-Computer können vernetzt werden. Dabei ist jedes System unabhängig vom anderen, und gelegentlich tauschen sie mit Hilfe von Netzwerkprotokollen Informationen aus. Eine Workstation und ein Mainframe sind im Verhältnis zu anderen derartigen Systemen gleichberechtigt. Insofern ist diese Umgebung vergleichbar mit der Art und Weise, wie das Fernsprechsysteem arbeitet, bei dem alle Fernsprengeräte gleichberechtigt sind. Analogien zum Fernsprechsysteem werden daher gerne gebildet.

Netzwerke werden nicht nur zur fehlerfreien Datenübermittlung, sondern auch zur Sprach- und zur Videoübertragung genutzt, bei der die rechtzeitige Übergabe vorrangig und eine fehlerfreie Übergabe zweitrangig ist. Wenn die Übergabe beispielsweise bei einer Videoübertragung verspätet erfolgt, werden die Daten nutzlos; wenn jedoch ein oder zwei Pixel verloren gehen, wird dies gar nicht bemerkt, solange das Bild nicht flimmert.

Unterstützte Protokolle

Fibre Channel versucht, die besten Aspekte dieser beiden konträren Kommunikationsverfahren in einer neuen I/O-Schnittstelle zu kombinieren, die die Bedürfnisse von Kanalbenutzern und zugleich von Netzwerkbenutzern erfüllen.

Fibre Channel unterstützt die Übertragung von ATM (Asynchronous Transfer Mode), IEEE 802 und sonstigem Netzwerkverkehr. Alle, die mit Internet Protocol (IP), E-Mail, File Transfer, Fernanmeldungen und sonstigen Internet-Diensten vertraut sind, werden feststellen, dass diese Protokolle in Fibre Channel mit höheren Geschwindigkeiten unterstützt werden.

Hierbei handelt es sich um wichtige Aspekte für den Anschluss von Systemen, die auf Fibre-Channel-Basis arbeiten, an die wichtigsten globalen Netzwerke sowie an bereits von Unternehmen installierten LANs. Dazu zählen SONET-basierte Systeme und LANs wie Ethernet.



Ein wichtiger von Fibre Channel geleisteter Beitrag besteht darin, dass diese beiden Schnittstellentypen, d. h. Kanäle und Netzwerke, jetzt das gleiche physikalische Medium teilen können. In den letzten Jahren wurden I/O-Kanäle dahingehend ausgebaut, dass sie Netzwerkanwendungen mit einschließen (z. B. mit Hilfe von SCSI, um zwei Workstations zu vernetzen). In gleicher Weise bewegen Netzwerke mit Hilfe von Netzwerk-Dateitransfer-Protokollen Daten zwischen Systemen und Dateiservern hin und her (z. B. Network File System (NFS)).

Mit Fibre Channel ist es jetzt möglich, dasselbe physikalische Medium und dasselbe physikalische Transportprotokoll über einen gemeinsamen Hardware-Port zu benutzen, um sowohl Kanal- als auch Netzwerkaktivitäten zu verwalten. Es ist möglich, Informationen an ein Netzwerk zu senden, das über Fibre Channel an die Rückwand einer Workstation angeschlossen ist, und zugleich Fibre Channel zu benutzen, um intern mit den lokalen Peripheriegeräten zu kommunizieren (z. B. mit Platten- und Bandlaufwerken).

Protokollmerkmale von Fibre Channel: Fibre Channel enthält keinen Befehlssatz wie beispielsweise SCSI und IPI, sondern stellt einen Mechanismus zur Verfügung, um andere Protokolle auf Fibre Channel aufzusetzen. Dies ist möglich, indem Fibre Channel als Träger für diese Befehlssätze dient, und zwar so, dass der Empfänger zwischen beiden unterscheiden kann. Dies impliziert, dass diverse Befehlssätze älterer I/O-Schnittstellen, für die bisher Software-Investitionen erforderlich waren, direkt auf Fibre Channel angewendet werden.

Die Trennung der I/O-Operationen von der physikalischen I/C-Schnittstelle ist ein wichtiges Leistungsmerkmal von Fibre Channel und ermöglicht die simultane Benutzung unterschiedlicher Befehlssätze. Die verschiedenen Befehlssätze, wie z. B. SCSI, IPI-3, IP etc., werden üblicherweise an ihren eigenen, speziellen Schnittstellen verwendet. Fibre Channel definiert hingegen einen einzigen gemeinsamen, physikalischen Übertragungsmechanismus für diese Befehlssätze.

Fibre-Channel

§ ist sich des Inhalts oder der Bedeutung der gerade übertragenen Informationen nicht bewusst

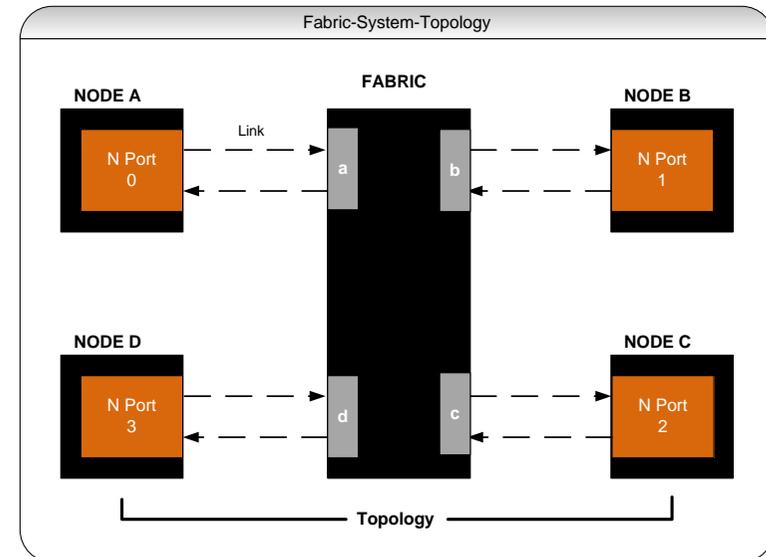
§ erhöht die Konnektivität von Dutzenden auf Hunderte oder sogar Tausende von Geräten - vergrößert den Maximalabstand zwischen den Geräten

§ erhöht die Übertragungsrate um das Vier- bis Fünffache gegenüber den verbreitetsten Kanälen und um das Hundertfache gegenüber gängigen Netzwerken.

In den folgenden Abschnitten wird beschrieben, wie Fibre Channel den Aufbau eines Netzwerks erlaubt.

Vernetzungstopologien

Fibre-Channel-Geräte werden auch Knoten (engl. nodes) genannt, von denen jeder mindestens einen Port hat, um einen Zugang zur Außenwelt (d. h. zu einem anderen Knoten) zu schaffen. Die Komponenten, die zwei oder mehr Ports miteinander verbinden, werden unter der Bezeichnung Topologie zusammengefasst. Alle Fibre-Channel-Systeme besitzen lediglich diese beiden Elemente: Knoten mit Ports und Topologien.



Jeder Fibre-Channel-Port verwendet ein Leiterpaar - einen Leiter, um zum Port gehende Informationen zu übertragen, und einen, um vom Port kommende Informationen zu übertragen. Bei Fibre Channel handelt es sich entweder um elektrische Leiter oder um Lichtwellenleiter. Dieses Faserpaar wird Verbindung (engl. link) genannt und ist Bestandteil jeder Topologie, siehe Abbildungen 2 bis 4.

Daten werden immer in Einheiten (so genannten Frames oder Rahmen) über diese Verbindungen übertragen. Die Fibre-Channel-Norm definiert drei Topologien, doch liegt die Betonung vor allem auf einer Topologie, die auch Fabric-System genannt wird und als Erstes beschrieben werden soll.



Fabric-Topologie

Ein Fabric-System (siehe Abbildung) erlaubt dynamische Kopplungen zwischen Knoten über die an dieses System angeschlossenen Ports. Zu beachten ist, dass der Begriff Fabric in dieser Anwendung als Synonym für die Begriffe Switch bzw. Router gelten kann. Jeder Port in einem Knoten, ein so genannter N -Port oder NL-Port, ist an das Fabric-System über eine Verbindung angeschlossen. Jeder Port in einem Fabric-System wird F -Port genannt. Jeder Knoten kann mit jedem anderen, an andere F Ports desselben Fabric-Systems angeschlossenen Ports mit Hilfe der Dienste des Fabric-Systems kommunizieren. Bei dieser Art von Topologie werden alle Leitwegoperationen für die Rahmen vom Fabric-System anstelle der Ports durchgeführt.

Dieser Jeder-mit-jedem- bzw. Peer-to-Peer-Dienst ist ein wesentlicher Bestandteil der Auslegung des Fibre Channels. Ein System, das für Peer-to-Peer-Dienste ausgelegt wurde, kann so verwendet werden, dass das Master-Slave-Kommunikationsverfahren des Typs Host emuliert wird. Auf diese Weise kann Fibre-Channel-Kanal- und Netzwerkprotokolle simultan unterstützen.

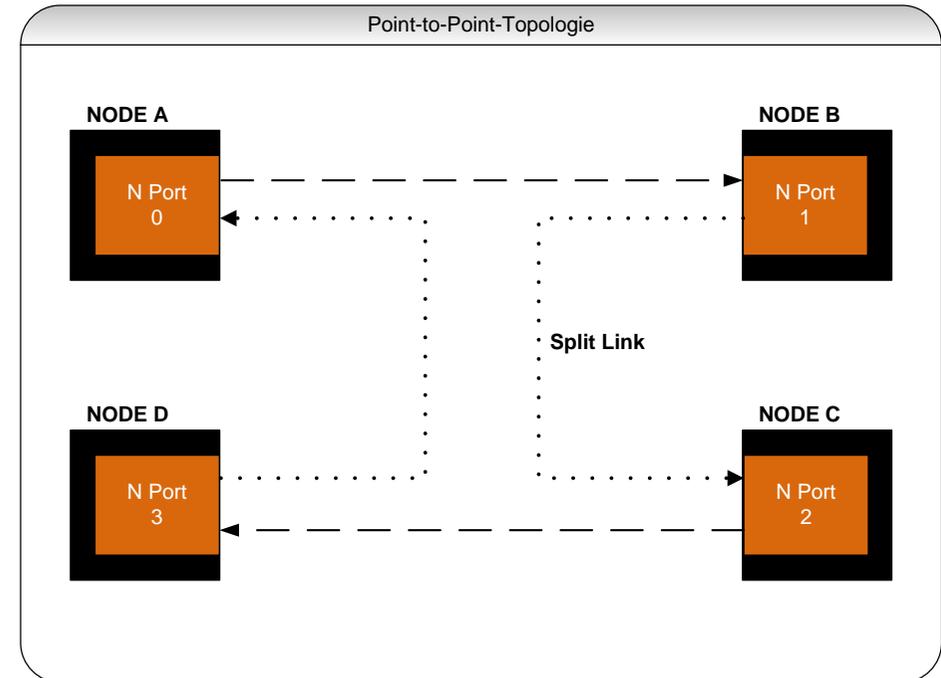
Wie ein Fernsprechsysteem

Die Funktion des Fabric-Systems ist der eines Fernsprechsystems vergleichbar - wir wählen irgendeine Rufnummer, das Fernsprechsysteem findet den Pfad zum gewünschten Zielanschluss, der Rufton ertönt, und der Angerufene antwortet. Wenn eine Vermittlungsstelle oder Verbindung abstürzt, leitet das Fernsprechunternehmen die Anrufe über andere Pfade um, was der Anrufer selten bemerkt. Die meisten von uns wissen nichts von den Zwischenverbindungen, die das Fernsprechunternehmen schaltet, um unseren einfachen Anruf erfolgreich werden zu lassen.

Wir geben dem Fernsprechunternehmen jedoch einige Hinweise zu unserem Anruf. Die Rufnummer beginnt beispielsweise (in den U.S.A.) mit der Ziffer 1 - gefolgt von zehn Ziffern in Form einer Ortsvorwahl- (3), Vermittlungsstellen- (3) sowie Teilnehmernummer (4). Wenn am Anfang der Rufnummer nicht die Ziffer 1 steht, gilt der Anruf innerhalb des Ortsvorwahlbereichs des Anrufers, und es werden lediglich sieben Ziffern verwendet. Diese Hinweise helfen der Fernsprechgesellschaft, die Verbindung herzustellen. Die Rufnummer entspricht dem Fibre-Channel-Adress-ID. Ein Teil der Adress-ID wird verwendet, um die betreffende Domain des Fabric-Systems zu bestimmen, und der Rest dient dazu, den speziellen Port zu ermitteln.

Zu beachten ist, dass das Fernsprechsysteem nicht am Inhalt des Gesprächs zwischen den beiden Fernsprechteilnehmern beteiligt ist (bzw. von ihm betroffen ist); es sorgt lediglich für die Herstellung der Verbindung. In gleicher Weise sorgt Fibre Channel für die Verbindung, und die aufgesetzten Protokolle (z. B. SCSI oder IPI) tragen die Befehle.

Diese Protokolle spielen eine ähnliche Rolle wie die Sprachen in Fernsprechsysteemen. Fibre Channel und die anderen Protokolle sollten als integraler Bestandteil des Informationsaustauschs gesehen werden.



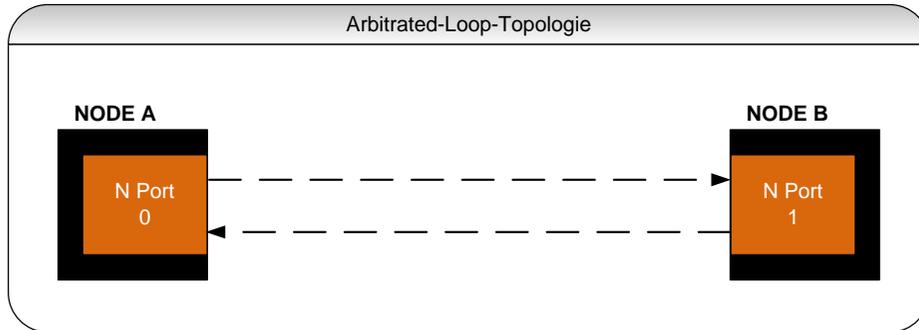
Der Weg von A nach C

Die Komplexität eines Fabric-Systems ist vergleichbar mit der von Vermittlungsstellen des Fernsprechsystems; die entsprechenden Fabric-Geräte werden Fabric-Elemente genannt. In Abbildung 2 wird nur ein Fabric-Element mit vier F Ports dargestellt, die mit a, b, c und d gekennzeichnet sind. Wenn Knoten A mit Knoten C sprechen muss, wird die Information zunächst an das Fabric-System in F -Port a gesandt. Das Fabric-System stellt eine interne Verbindung oder eine Reihe von Verbindungen zu F_Port c her. Die Information wird dann an Knoten c gesandt. Es ist u. U. erforderlich, mehrere Fabric-interne Pfade auszuwählen, ehe man zu F -Port c gelangt.

Das Fabric-System kann aus einem einzigen oder mehreren Fabric-Elementen bestehen. Wie bei Fernsprechsysteemen wissen wir nicht (bzw. kümmern uns nicht darum), durch wie viele Switches (Vermittlungsstellen) wir gehen müssen, solange wir mit der richtigen



Zielstation verbunden werden.



Ein Fabric-System wird auch vermittelte Topologie oder Koppelpunkt-Vermittlungstopologie genannt. Die Leitweglenkung (Routing) über verschiedene Switches erfolgt, indem die Fabric-Elemente die Zieladresse-ID im Rahmen interpretieren, sobald es in jedem FabricElement ankommt.

Das Fabric-System lässt sich physikalisch als einzelnes Fabric-Element mit mehreren F Ports implementieren (wie aus Abbildung 2 ersichtlich), oder es kann als eine Reihe mehrerer derartiger, untereinander verbundener Fabric-Elemente implementiert werden. Die Leitweglenkung bzw. Vermittlung jeder Kopplung ist transparent für die beiden N - Ports, die über F -Ports an die Fabric-Außenkante angeschlossen sind.

Wenn die Topologie von den Knoten getrennt ist, wie dies beim Fernsprechsistem und Fibre Channel der Fall ist, können neue Technologien für die Leiter eingeführt werden. Neue Geschwindigkeiten und neue Funktionen können im Fabric-System implementiert werden, ohne dass dadurch alle vorhergehenden Investitionen in vorhandene Knoten verloren gehen. Fibre Channel erlaubt die Kombination von Zusatzgeräten mit unterschiedlichen Geschwindigkeiten oder Eigenschaften.

Andere Topologien

Neben der Fabric-Systemtopologie definiert die Fibre-Channel-Norm zwei weitere Topologien. Die eine trägt die Bezeichnung Point-to-Point-Topologie (siehe Abbildung 3) mit nur zwei angeschlossenen Ports. In diesem Fall findet keine Leitweglenkung statt. Die dritte Topologie heißt Arbitrated Loop (siehe Abbildung 4). Hierbei handelt es sich um eine einfache und preisgünstige Topologie für den Anschluss mehrerer Dutzend NL-Ports an einen Loop. Die Ports in einer Arbitrated-Loop-Topologie, die NL Ports und FL-Ports heißen, unterscheiden sich geringfügig von den N_Ports und F_Ports. Sie beinhalten alle Funktionen von N Ports und F -Ports und können ordnungsgemäß in einem Fabric-

System arbeiten. Beim FL-Port handelt es sich um einen Port in einem Fabric-System, der das Arbitrated-Loop-Protokoll verarbeitet.

Beim Arbitrated Loop sieht jeder Port alle Meldungen (wie beim Token-Ring-Protokoll) und übergeht und ignoriert diejenigen Meldungen, die kein Token-Acquisition-Protokoll besitzen.

Um die Funktion einer Fabric-Systemtopologie besser verständlich zu machen, soll im Folgenden die Analogie zum Fernsprechsistem weitergeführt werden: Sie wählen die Rufnummer eines Freundes. Dazu brauchen Sie den genauen Leitweg nicht zu kennen, den das Fernsprechsistem bis zum Haus Ihres Freundes verfolgt, wenn Sie ihn anrufen. Die Leitweglenkung besorgt das Fernsprechsistem. Das Fabric-System von Fibre Channel hat die gleiche Funktion: Man gibt eine Zieladresse ein, und das Fabric-System leitet die Daten zum Ziel-N Port.

Wenn Sie eine falsche Rufnummer wählen, teilt Ihnen das Fernsprechunternehmen mit, dass es unter dieser Nummer keinen Anschluss gibt. Das Fabric-System weist Rahmen für ungültige Ziele in vergleichbarer Weise zurück.

So wie das Fernsprechunternehmen zahlreiche Leitwege zwischen unterschiedlichen Punkten konfigurieren kann und dies auch tut, um einen zuverlässigen Dienst bereitzustellen, kann ein Fabric-System zahlreiche Pfade zwischen Fabric-Elementen haben, um den Verkehr abzuwickeln. Dies ermöglicht auch die Bereitstellung von Reservepfaden für den Fall, dass ein Element oder eine Verbindung ausfällt.

Die Fabric-System- und Arbitrated Loop-Topologien von Fibre Channel können miteinander in einem System gemischt werden, um den Knoten eine Vielzahl von Dienst- und Leistungsgraden zu verleihen. Zudem kann das Fabric-System andere Netzwerke wie etwa SONET oder ATM über SONET zwischen Fabric-Elementen benutzen, um Abstände zwischen Knoten zu überbrücken, die zu groß sind, als dass sie von der Verbindung zwischen N -Ports bewältigt werden könnten. Diese speziellen Verbindungen können zwischen Fabric-Elementen bestehen, die über ein größeres geografisches Gebiet verteilt und nicht direkt an Knoten angeschlossen sind.

Die Fähigkeit, andere Typen von Verbindungen zwischen Fabric-Elementen hinzuzufügen, die Erweiterungsports bzw. E -Ports genannt werden, erhöht den Wert jedes an das FabricSystem angeschlossenen Laufwerks. Bestimmte Attribute von Fibre Channel und eines Fabric-Systems ermöglichen es Ports mit unterschiedlichen Geschwindigkeiten und Medientypen, miteinander entweder über kurze oder lange Entfernungen zu kommunizieren, wenn ein Fabric-System vorhanden ist.

Im Fabric-System selbst können auch Technologieverbesserungen implementiert werden, ohne dass die N Ports in irgendeiner Weise verändert werden müssen. Der

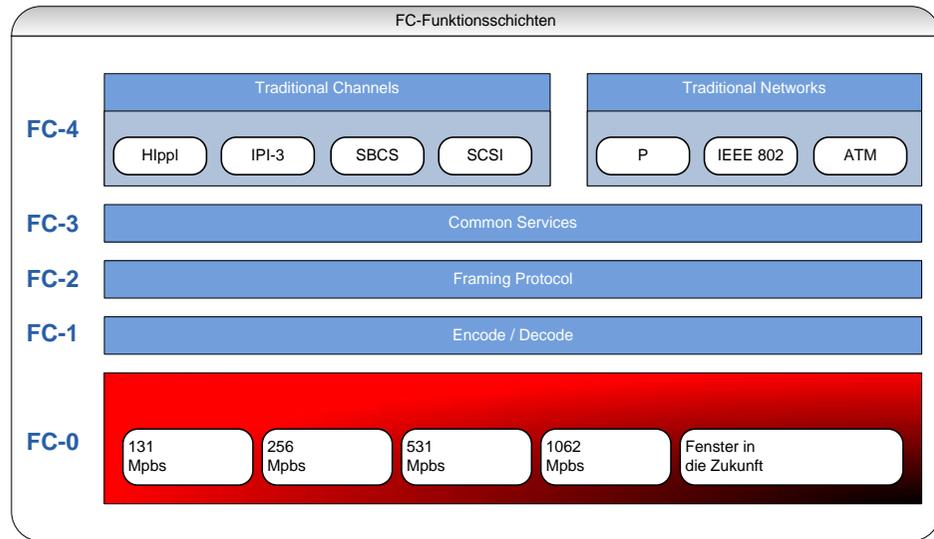


Großteil des Nutzens der neuen Technologie wird aufgrund der höheren Geschwindigkeit indirekt an die Knoten weitergegeben, da die Geschwindigkeit, die Zuverlässigkeit bzw. die Kommunikationsdistanz innerhalb des Fabric-Systems erhöht werden.

Funktionsschichten

Manche Themen gehören einfach naturgemäß zusammen, was auch für Fibre Channel gilt. Aspekte, die mit dem Aufbau zuverlässiger und prüfbarer Lichtwellenleiter-Verbindungen zu tun haben, haben wenig mit der Frage zu tun, wie Probleme aufgrund eines verloren gegangenen Rahmens behoben werden können. Diese unterschiedlichen Interessengebiete werden in der Fibre-Channel-Norm Funktionsschichten genannt. Definiert werden in dieser Norm fünf Schichten, die jeweils mit FC-x gekennzeichnet sind.

Wie viele N_Ports können implementiert werden? Das Fabric-System wird lediglich durch die Zahl der N -Ports begrenzt, die im Zieladressfeld im Header des Rahmens genannt wird. Diese Begrenzung liegt bei etwas mehr als 16 Millionen Ports, die gleichzeitig bei einem Fabric-System mit 24-bit-Adress-ID angemeldet werden können. Bei einzelnen integrierten Systemen dürfte dies alle Erfordernisse für eine ganze Weile abdecken.



In der Fabric-Systemtopologie ist die Adress-ID in drei Teile unterteilt: Domain (8 Bit), Gebiet (8 Bit) und Port (8 Bit), was insgesamt 24 Bit ergibt. Diese Bestandteile sind vergleichbar mit denen einer Rufnummer mit Ortsvorwahl-, Vermittlungsstellen- und Teilnehmernummer. FC-0 definiert die physikalischen Fibre-Channel-Anteile, einschließlich der Medientypen, Anschlüsse sowie der elektrischen und optischen

Leistungsmerkmale, die für die Port Anschlüsse benötigt werden. Diese Schicht ist in der FC-PH-Norm beschrieben.

FC-1

-definiert das Übertragungsprotokoll, einschließlich der 8B/10B-Kodierung, der Reihenfolge der Wortübertragung und der Fehlererfassung. Diese Schicht ist in der FC-PH-Norm beschrieben.

FC-2

definiert das Signalisierungs- und Framingprotokoll, einschließlich Rahmen-Layout, Inhalt des Rahmen-Headers und Anwendungsregeln. Es definiert zudem bestimmte protokollunabhängige Rahmen und Protokolle wie etwa die Benutzeranmeldung (Login). Die FC-PH-Norm besteht überwiegend aus der Beschreibung dieser Schicht.

FC-3

definiert gemeinsam genutzte Dienste, die an verschiedenen Ports in einem Knoten verfügbar sein können. Für diese Schicht gibt es keine Norm.

FC-4

definiert das Mapping zwischen den unteren Fibre-Channel-Schichten und den Befehlsätzen, die Fibre Channel benutzen. Hier finden Sie SCSI, IPI-3, HIPPI und SBCS. Jeder dieser Befehlsätze erhält eine gesonderte Norm, da interessierte Dritte nicht unnötig mit systemfremden Informationen befasst werden sollen. Wenn Sie mit SCSI-3 arbeiten, sind Sie Abbildung 5 zeigt die interne Struktur eines Fibre Channel-Knotens mit einem N_Port. Zulässig sind auch mehrere N_Ports je Knoten. Hat ein Knoten mehr als einen N -Port, so werden die Schichten FC-0 und FC-2 für jeden N_Port reproduziert. Die Schichten FC-3 und FC-4 werden von mehreren N_Ports gemeinsam genutzt. Die Abbildung zeigt jede dieser Funktionsschichten. Die Schicht für die gemeinsam genutzten Dienste hat bisher keine definierten Komponenten. Im Verlauf der weiteren Entwicklungsarbeiten im Zusammenhang mit dieser Norm werden von dieser Schicht neue Funktionen aufgenommen.

Auf der Schicht FC-4 kann ein Knoten nicht alle von der Norm zugelassenen unterschiedlichen Optionen aufnehmen. Jeder Knoten kann einen oder mehrere Dienste implementieren. Auf der Schicht FC-0 kann lediglich eine Geschwindigkeits- und Medientyp-Option (Beschreibung folgt) in einem N_Port implementiert werden. Jeder einzelne Port in einem Knoten kann jedoch eine unterschiedliche Kombination von Geschwindigkeit und Medium implementieren. Die Schicht FC-2 unterstützt auch zahlreiche Optionen, aus denen ein bestimmter Hersteller gewählt werden muss. Einige





Industriegruppen arbeiten bereits daran, Profile zu definieren, die die Betriebsumgebung spezifizieren, die für einige Anwendungen erforderlich ist (z. B. SCSI, HIPPI, IPI-3 usw.). Auf der Schicht FC-1 gibt es keine Optionen.

Mehrere der FC-2, die derzeit definiert werden, sollen im Folgenden skizziert werden. Jede FC-4 wird als Einzelbestandteil der Norm in einem gesonderten Dokument entwickelt. Ein Hersteller kann sich genau auf das bzw. die FC-4 konzentrieren, für die er sich interessiert, und braucht sich nicht unnötig mit den Anforderungen für die anderen FC-4 zu befassen. Wenn bei der Entwicklung eines Produkts oder bei Beschaffungsplänen eine Erweiterungsoption vorgesehen ist, sollten anderen potenziellen FC-4 prüfen, so dass eine übergeordnete Port-Anforderungsliste vorhanden ist, wenn die Erweiterung realisiert wird. Ein Systemanbieter, der das IPI-3-Protokoll integriert und plant, später das Internet Protocol (IP) einzubauen, sollte sorgfältig beide FC-4 in Betracht ziehen, ehe er sich für ein FortDesign entscheidet, da die Anforderungen unterschiedlich sind.

HIPPI (High Performance Parallelinterface)

Eines der ursprünglichen Ziele von Fibre Channel bestand darin, HIPPI durch ein ursprüngliches Verkabelungssystem her, das aus zwei Sätzen paralleler Kabel bestand. Bei HIPPI handelt es sich um ein Vollduplex-Protokoll, das vorrangig dazu dienen sollte, große Datenmengen mit geringem oder keinem Systemverarbeitungsaufwand zu transportieren.

HIPPI hat keinen systemeigenen Befehlssatz. Es hat lediglich Quellen und Ziele, doch in der Regel wird IPI-3 verwendet, wenn ein Befehlssatz erforderlich ist. Weitere Informationen zu IPI-3 enthält der folgende Abschnitt. HIPPI arbeitet mit 100 MB/s in beiden Richtungen über kurze Parallelkabel. Zeitweise wurde an der Definition eines seriellen HIPPI gearbeitet, doch wurde diese Arbeit unterbrochen, als die Entwicklung von Fibre Channel begann.

IPI-3 (Intelligent Peripheral Interface-3)

In der Bezeichnung IPI-3 steht die Zahl 3 nicht für „Version 3“. IPI definiert - als Normenfamilie - verschiedene Schichten. Level 3 gilt als die geeignete Schicht für die Übertragung von Befehlen und Daten, wenn intelligente Geräte an das System angeschlossen sind. IPI-3 erlaubt auch die Datenübertragung über große Entfernungen, da während der Datenübertragung kein Takten erforderlich ist. Bei der Parallelversion von IPI-3 handelt es sich um ein Halbduplex-Protokoll. In der Fibre Channel-Version von IPI-3 bleibt dieser Halbduplex-Charakter erhalten. IPI-3 erlaubt zudem das Einreihen verschiedener vom Master kommender Befehle in eine Warteschlange im Slave. IPI-3 spezifiziert eine Geschwindigkeit von bis zu 100 MB/s auf kurzen, parallelen

Kupferkabeln. IPI-3 definiert Befehlssätze für jede von IPI-3 unterstützte Geräteklasse.

SBCS (Single Byte Command Set)

SBCS überträgt - wie es der Name schon sagt - Befehle, die nur ein einzelnes Informationsbyte haben. Es handelt sich hierbei um ein parallel arbeitendes Halbduplex-Protokoll, das viel von diesem Charakter in seiner Fibre-Channel-Implementierung beibehält. SBCS wurde vom IBM-Byte/Block-Multiplexerkanal abgeleitet, der seinen Ursprung in IBM-Systemen der 70er Jahre hat. Es ist auch heute noch beliebt, und es gibt eine IBM-spezifische Version namens ESCON, die mit Fasern und 8B/10B-Kodierung arbeitet und eine Geschwindigkeit von 20 MB/s in beiden Richtungen erreicht. ESCON besitzt zudem vordefinierte Schalter, die ähnlich wie der im nächsten Abschnitt beschriebene Class-1-Dienst funktionieren.

Der Befehlssatz ist bei SBCS nicht normiert; lediglich die Mechanismen zum Senden von Befehlen, Status- und Prüfdaten sind definiert. Jedes Produkt kann seine eigenen Befehle innerhalb der Klasse für Lesen, Schreiben, Lesewiederholkontrolle, Steuerung und Prüfung definieren.

Zusatz-Fibre-Channel-Arbitrated-Loop (FC-AL)

Eine abgespeckte Version des Fibre Channel ist der Fibre Channel-AL. AL bedeutet Arbitrated Loop und beschreibt die Topologie dieses für lokale Geräte und Disc Arrays entworfenen Fibre Channel-Typs. Die max. 127 Loop-Ports (NL-Ports) sind als Ring angeordnet. Der Datenaustausch ist nur als Point-to-Point-Verbindung möglich. Jedes Datenpaket gelangt zunächst über den Read-Port in das Device. Dieses prüft, ob es die Informationen bearbeiten soll. Wenn nicht, schickt es sie über den Write-Port wieder hinaus. Um diesen Datentransfer zu veranlassen, muss sich das Device zunächst um die Kontrolle über den Bus bemühen. Paralleler Datenaustausch mehrerer Geräte (wie bei der allgemeinen Fibre-Channel-Definition) ist nicht möglich.

Um Disk Arrays besser handhaben zu können, unterstützt der FC-AL neben der normalen Kabelverbindung auch die Backplane-Architektur. Die Festplatten werden über einen 40-poligen SCA (Single Connector Attachment)-Stecker, der sowohl Datenleitungen als auch Stromversorgung beinhaltet, an die Backplane angeschlossen. Steckt in einem Port kein Laufwerk, überbrückt die Backplanelogik den leeren Steckplatz, und der Kreis bleibt geschlossen. Eine weitere Aufgabe der Backplane ist die automatische Konfiguration des Laufwerks sowie die Sicherstellung der Hot-Plug-Funktion, also der Wechsel eines Laufwerks während des Betriebs.

Das gleiche Prinzip wird auch von Fibre-Channel-Hubs verwendet. Da bei einem FibreChannel-Loop der Ausfall eines Gerätes oder Defekt eines Kabels den Kreis unterbricht und so den ganzen Bus blockiert, überbrückt der Hub jeden Port, der



entweder ungenutzt ist, oder aber durch Störungen blockiert wird (s. Abbildung). Der Datenfluss zu den anderen Devices wird so nicht unterbrochen und der Bus arbeitet normal weiter.

FC-AL Produkte werden seit Herbst 1996 angeboten. Nachdem sie anfangs auf High-End RAID-Systeme beschränkt waren, spielen sie wegen des immer größeren Speicherbedarfs auch kleinerer Server eine immer größere Rolle. Nähere Informationen zu Produkten sind im Kapitel Fibre Channel (Seite 132) zu finden.

SSA

SSA (Serial Storage Architecture) ist eine High-Performance-Schnittstelle, die I/O-Devices aller Plattformen miteinander verbindet.

Diese serielle, busähnliche Schnittstelle wurde von IBM basierend auf der IBM-9333-Technologie entwickelt und dient vorwiegend zum Anschluss von Festplatten. Hiermit lassen sich bis zu 128 Geräte untereinander verbinden.

Wie der Fibre Channel ist die SSA eine Point-to-Point-Verbindung, wobei allerdings zwei Write- und zwei Read-Kanäle zur Verfügung stehen. Auf jedem Kanal (Write/Read) ist eine maximale Transferrate von 20 MB/s möglich, was einer kumulierten Transferrate von 80 MB/s entspricht. Diese kann aber nur erreicht werden, wenn das Schreib-Lese-Verhältnis 1:1 beträgt und der Hostadapter auf Daten zugreift, die sich auf mindestens vier Platten befinden.

Bei Entfernungen von bis zu 20 m zwischen zwei zu verbindenden Devices genügt ein normales Twisted-Pair-Kabel. Glasfaserkabel kommen bei Längen bis zu 680 m zum Einsatz. Nur 6% der über SSA beförderten Daten werden für Control- bzw. Routing

SSA wird jedoch nur von wenigen Herstellern (wie IBM, Siemens, Micropolis) unterstützt und wird im Laufe der nächsten Jahre wohl ganz durch die Fibre-Channel-Arbitrated-Loop-Technologie abgelöst werden.



4.1.4 Storage Area Network (SAN)

Das LAN ermöglicht den Zugriff auf lokale Systeme, die über Kommunikationsprotokolle wie TCP/IP, NFS, HTTP verfügen. LANs werden benutzt, um Daten zwischen verschiedenen Host-Systemen und um Benutzerzugriffe auf Systeme wie Workstations, Terminals und andere Geräte zu übertragen. LANs handhaben den Informationsfluss zwischen Host Systemen und Benutzer. Im Gegensatz hierzu ermöglicht SAN, den Informationsfluss mit der gesamten Umgebung zu teilen, das heißt zwischen den Rechnern und den Speichereinheiten und schließlich zwischen den Speichereinheiten selbst. So lassen sich Speichereinheiten von allen am SAN angeschlossenen Rechnern ansprechen. Ähnlich wie in LAN-Netzwerken (Ethernet, FDDI, ATM und Token Ring) gibt es auch beim SAN unterschiedliche Topologien, um so ein Storage Area Network aufzubauen.

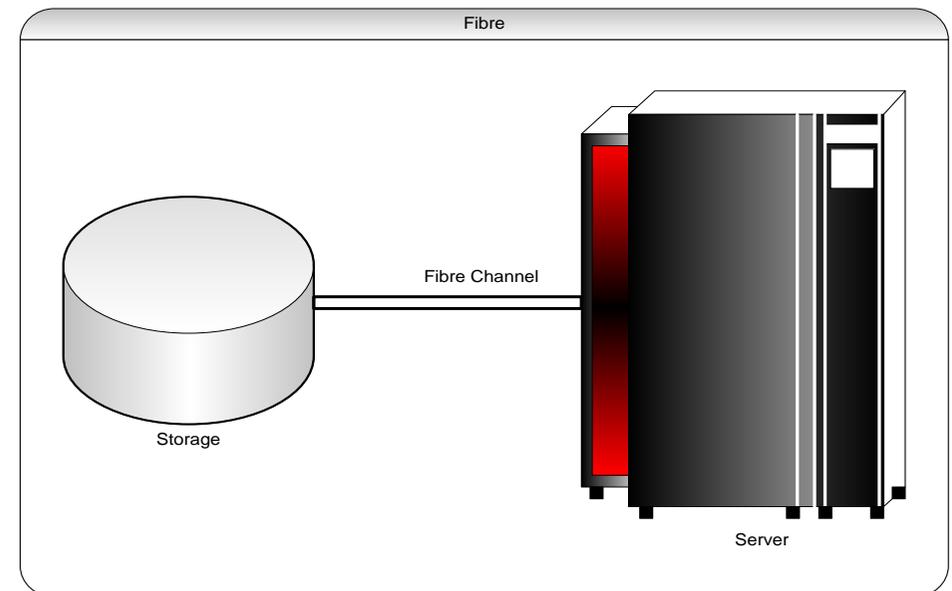
Storage Area Networks sind besondere Speichernetzwerke, die Server und Speichersysteme über Breitbandnetzwerke verbindet. In diesem Netzwerk spielt es zunächst prinzipiell keine Rolle, welches Betriebssystem auf einem Server installiert ist. Das heißt, es können mehrere unterschiedliche Server auf verschiedene Speicher-Subsysteme in einem Netzwerk zugreifen. Im Prinzip kann ein Storage Area Network mit einem einfachen oder mit zwei Kabeln aufgebaut werden. Die SCSI-Technologie ist die bekannteste Art, ein Storage Area Network in der einfachsten Form aufzubauen. Wegen der Großen Einschränkungen wie Geräteanzahl, Distanzen, Terminierung etc. ist die Fibre-Channel-Technologie das für SANS heute normalerweise eingesetzte Kommunikationsmedium. Durch die Eigenschaften von Fibre Channel eignet sie sich hervorragend als Medium. Die Anforderungen eines SANS sind eine garantierte Bandbreite (Netzwerkgeschwindigkeit) und geringe Fehlerraten (1 Fehler in 10 hoch 9, d. h. ein Fehler in der Sekunde)

Fibre Channel bietet Vorteile, wie:

- **400 MB/s Datendurchsatz**
- **2.0625 Gbit Bandbreite**
- **16 Millionen Geräte können angesprochen werden**
- **serielle Verbindung 8/10-bit-Encoding**
- **Hardware-basierendes Anschlussprotokoll zwischen den Schnittstellen**
- **flexible Kabelkonfiguration, Kupfer und Glasfaser, Distanz bis 10 km**
- **einfach anzuschließen, keine Terminierung**
- **Frame-gestützte Technologie basierend auf FDDI (FDDI-Prüfsummen)**

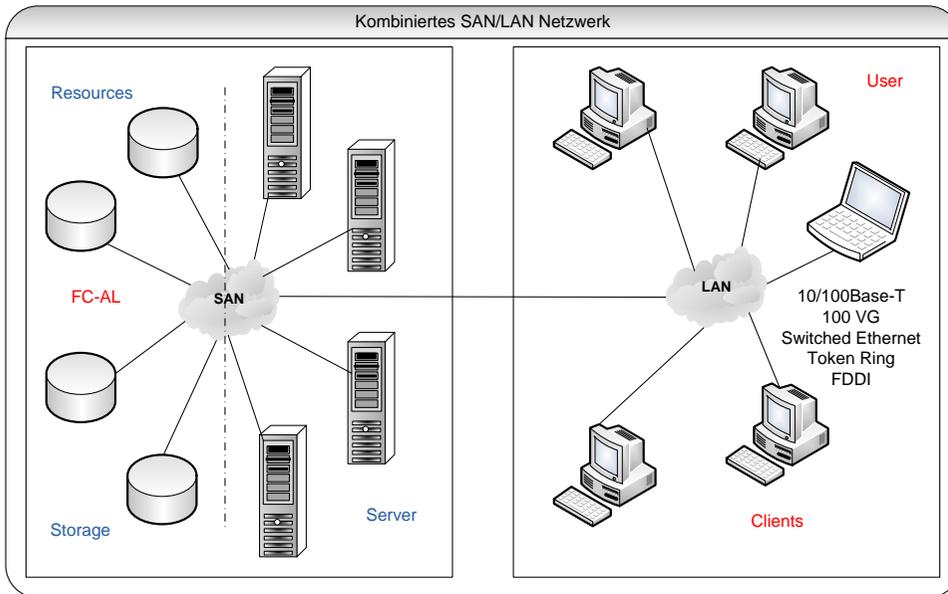
Im Moment wird an den Datentransferraten des Fibre Channels gearbeitet, so dass schon in naher Zukunft die Datentransferraten auf 2 GBaud und 4 GBaud gesteigert werden. Weitere Informationen können im Kapitel Fibre Channel nachgelesen werden.

Durch das SAN kann das LAN entlastet werden, da der gesamte Informationsaustausch in diesem Speichernetzwerk abgewickelt wird. Wenn man Backup-Laufwerke auch an das SAN und nicht an das LAN anschließt, kann man mit entsprechender Software eine weitere Entlastung erreichen. Dies ermöglicht eine einfachere Verwaltung der Systeme und höhere Datentransferraten. Ein Storage Area Network bietet die ideale Möglichkeit die gesamten Informationen zu zentralisieren.



Die unkomplizierteste Art, ein Storage Area Network aufzubauen, ist die Punkt-zu-Punkt-Verbindung über Fibre Channel. Sie verbindet zum Beispiel ein RAID-System mit einem Rechner. Man benötigt hierfür nur einen Hostadapter (HBA), ein Kabel und ein FibreChannel-Subsystem (RAID etc.) und als Abschluss einen Loopback Plug, der den internen Loop wieder schließt. Durch die einfache Kabelverbindung ist diese Installation wesentlich einfacher als SCSI.

Ein größeres System wird über Switches oder Hubs in Form der Ringtopologie aufgebaut. Diese Ringtopologie wird FC-AL genannt und verbindet mehrere Rechner mit mehreren Speichereinheiten. Der FC-AL (Fibre-Channel-Arbitrated-Loop) ermöglicht eine Zuteilung der Geräte, Leitungen und Benutzerzeiten. Fibre Channel benötigt nicht zwingend ein Lichtwellenleiter, sondern kann auch mit einem einfachen Kupferkabel realisiert werden. Der einzige Nachteil ist die geringere Distanz, die mit Kupfer überbrückt werden kann (ca. 30 m). Bisher wurde über die Hardware des SAN berichtet, um allerdings auch die Daten auf diesen Speichereinheiten teilen zu können, bedarf es einer speziellen SAN-Software. Diese Software benutzt die Speichernetzwerke und ermöglicht ein File-Sharing auf den Speicher Subsystemen. Jedes System, unabhängig vom Betriebssystem, kann somit zu jeder Zeit auf jede Speichereinheit zugreifen und die Daten abrufen. Man spricht deshalb von einem SAN Betriebssystem, das aber auf dem "normalen" Betriebssystem aufgesetzt ist. Firmen wie Veritas, Mercury oder SANergy bieten SAN-Software, die innerhalb des Speichernetzwerkes Spiegelungen erstellen, synchronisieren und im Fehlerfall die gespiegelte Speichereinheit aktivieren, während die Applikationen online sind.



Die Software ermöglicht ein unterbrechungsfreies, dynamisches Verändern des Applikationsvolumens. Des Weiteren erlaubt die Software eine Zuweisung von Speichereinheiten oder einer Gruppe von Speichereinheiten und einem Server. Einige SAN-Software-Applikationen unterstützen Clustering, um eine verbesserte Datenverfügbarkeit innerhalb des Speichernetzes zu gewährleisten. Bei Clustering sind die Speichereinheiten keinem Server explizit zugeordnet, außer wenn dies über Rechte

konfiguriert wurde, so dass bei einem Serverausfall die Speichereinheit über Backup-Pfade trotzdem erreichbar ist oder einem anderen Server zugeordnet wird. Die SAN-Software von Veritas unterstützt folgende Datenbanken

- - Oracle 8.x, 81
- - Sybase x.x
- - Informix x.x
- - SAP
- - Exchange, IIS, SQL
- - Lotus
- - Checkpoint Firewall -1

Es wird also nicht zwingend eine Software benötigt, um ein funktionierendes SAN-Netzwerk aufzubauen. In diesem Fall müssen nur die entsprechenden Verbindungen zwischen Rechnern und Speichereinheiten hergestellt werden. Die Speichereinheiten werden schließlich dem Rechner über das Betriebssystem zugewiesen. Dazu reichen die Standardwerkzeuge, die in den jeweiligen Betriebssystemen fest integriert sind, völlig aus. Weitergehende Funktionen erfordern eine zusätzliche Software. Firmen, die mit sehr hohen Datenkapazitäten zu tun haben oder in Planung sind, sollten sich auf jeden Fall mit dieser Thematik befassen, da für diese Technologie eine komplett neue Struktur notwendig ist.

4.1.5 DSSI-Schnittstelle

Die digitale DSSI-Schnittstelle ist in Bezug auf die Hardware der SCSI-1-Schnittstelle sehr ähnlich. Im Gegensatz zu SCSI sitzt aber noch mehr Intelligenz in dem ISE (Intelligent Storage Element) genannten Laufwerk. Sie wurde jedoch durch SCSI fast völlig verdrängt.





4.1.6 IDE-Schnittstelle

Im PC-Bereich ist die IDE-Schnittstelle (Integrated Drive Electronics) sehr weit verbreitet. Sie hat die älteren ST506-Schnittstellen inzwischen völlig abgelöst. Es lassen sich maximal zwei Festplatten pro IDE-Schnittstelle anschließen. Sollen zwei IDE-Festplatten betrieben werden, wird eine Festplatte als Master, die andere als Slave konfiguriert. Zu beachten ist, dass IDE-Festplatten standardmäßig immer als Master-Drive und nicht als Slave konfiguriert werden.

Bei der ursprünglichen IDE-Schnittstelle, auch AT-Bus oder ATA (AT-Attachment) genannt, konnten theoretisch maximal etwa 4,3 MB/s übertragen werden. In der Praxis werden jedoch nur circa 2 MB/s erreicht. Sie ist ausschließlich zum Anschluss von Festplattenlaufwerken vorgesehen und unterstützt somit keine anderen Peripheriegeräte. Um den gestiegenen Leistungsanforderungen gerecht zu werden, ist daher die IDE-Schnittstelle weiterentwickelt worden:

Fast-ATA und Enhanced IDE

Die Unterschiede der beiden Entwicklungen liegen primär in der Marketingstrategie; die Implementierungen und Funktionen sind weitgehend gleich. Sowohl Fast-ATA als auch Enhanced IDE bleiben kompatibel zu den älteren IDE-Adaptern und -Festplatten. Sie verwenden das gleiche 40-polige Kabel.

Für Enhanced IDE gibt es unter dem Namen ATAPI (AT Attachment Packed Interface) Erweiterungen, mit denen ähnlich wie bei SCSI der Anschluss von Peripheriegeräten wie CD-ROM, Bandlaufwerken, Scannern usw. möglich ist.

UltraATA

Bei UltraATA wird, ähnlich wie bei Ultra-SCSI, die Taktrate auf dem Bus der Fast-ATA Schnittstelle erhöht. Somit erhält man bei UltraATA eine Datenübertragungsrate von 33 MB/s auf dem Bus.

UltraATA/66 und UltraATA/100

Nach zwei weiteren Steigerungen ist die Rate mittlerweile bei 100 MHz angekommen. Die Anforderung an die Verkabelung ist wegen der hohen Taktrate aber seit ATA66 strenger: Es werden spezielle 80-polige Kabel benötigt. Da der Stecker aber unverändert bleibt, können ältere Platten und Controller mit den neuen Standards kombiniert werden, natürlich um den Preis der geringeren Performance.

4.1.7 USB-Schnittstelle

USB (Universal Serial Bus) ist ein neuer Schnittstellenstandard für den Anschluss externer Geräte (z. B. Drucker, Modems, Tastaturen, Monitore, digitale Kameras etc.) über ein Bussystem an PCs. Der Vorteil der USB-Schnittstelle ist die unproblematische Integration von zusätzlicher Peripherie. Der USB-Controller erkennt, ob weitere Peripherie angeschlossen wurde, installiert automatisch die benötigten Treiber und stellt die Betriebsbereitschaft her. Aufwendige Neukonfigurationen der PC-Systeme gehören der Vergangenheit an. Bis zu 127 externe Geräte können theoretisch an die USB-Schnittstelle angeschlossen werden. Ausführliche Informationen zu USB sind erhältlich unter www.usb.org.

4.1.8 FireWire 1394

FireWire (IEEE 1394) ist mit maximal 400 Mbit/s ein serieller High-Speed-Datenbus, der, ursprünglich von Apple verwendet, vor allem Multimedia-Geräte wie Camcorder und digitale Kameras mit dem Rechner verbinden soll. Der Standard wurde 1995 definiert. Der Bus ermöglicht reservierte Bandbreiten, was vor allem im Videobereich gefordert wird. 16 Devices können über eine Strecke von 72 m in Serie (4,5 m pro Link) verbunden werden. Allerdings sind auch Bridges definiert, die kaskadierend die Anzahl der Devices drastisch erhöhen (maximal 1023 Bridges sind erlaubt).

Als Verbindungsmedium benutzt der FireWire ein sechspoliges Spezialkabel, das aus zwei abgeschirmten Twisted-Pair-Leitungen und zwei zusätzlichen Leitungen für die Versorgungsspannung besteht.

Derzeit spielt FireWire noch keine sehr große Rolle. Ob er sich zwischen USB als der preisgünstigeren, langsameren Variante einerseits und dem universelleren Fibre Channel andererseits durchsetzen wird, ist offen.



4.2 Primär-Datenspeicher

4.2.1 Einführung

Darunter versteht man Massenspeicher, die Daten im Random Access (direkter Zugriff auf Informationsblöcke, z. B. Magnetplatte) verfügbar machen. Zu dieser Gruppe zählen Halbleiterspeicher und magnetische Festplattenlaufwerke. Sie sind die schnellsten, aber auch die teuersten verfügbaren Speicher.

4.2.2 Festplattenlaufwerke

Festplatten (auch Winchesterplatten oder Magnetplatten genannt) sind die für alle Standardanwendungen üblicherweise eingesetzten Massenspeicher. Sie arbeiten mit einem magnetischen Aufzeichnungsverfahren und lassen sich beliebig oft beschreiben und lesen. Die angebotenen Laufwerke unterscheiden sich äußerlich u. a. durch die Schnittstelle (nähere Informationen dazu im Abschnitt 4.1.2 Peripheriebusse in diesem Kapitel) und den Formfaktor.

Formfaktor

Der Formfaktor bezeichnet den Durchmesser des Datenträgers, also der Plattenscheibe(n) im Inneren der Laufwerksbox. Neben diesen Plattenscheiben enthält die Box außerdem die Schreib-/Leseköpfe, die Mechanik zum Bewegen der Köpfe (den Aktuator), den Spindelmotor und die Logik (Elektronik).

Derzeit werden Festplatten mit 2,5"-, 3,5"- und 5,25"- Formfaktor angeboten. Kleinere Platten mit 1,8"- bzw. 1,3"- Formfaktor sind ebenfalls entwickelt worden.

Nähere Informationen zu aktuellen Festplatten finden sich im Kapitel transtec Festplattensubsysteme.

Die Festplatten werden als Full Height (82 mm), Half Height (41 mm), Low Profile (25,4 mm = 1 ") und in Höhen von 19 und 12,5 mm angeboten. Die 3,5"-Versionen sind die derzeit wohl populärsten und erreichen Kapazitäten bis ca. 180 GB netto. Die größeren 5,25"-Laufwerke werden nicht mehr weiterentwickelt.

Kapazität

Die Kapazität von Massenspeichern wird in Megabyte gemessen. Man unterscheidet Brutto- und Nettokapazität. Die Bruttokapazität entspricht der theoretischen maximalen Kapazität des Laufwerks, die sich aus der Multiplikation von Bitdichte in der Spur mit

Spurlänge, Spurenzahl und Zahl der Plattenoberflächen ergibt. Die Nettokapazität gibt an, wie viel Platz tatsächlich auf einem Laufwerk nutzbar ist.

Die vom Hersteller angegebene Nettokapazität unterscheidet sich erheblich von der tatsächlich für den Anwender nutzbaren Nettokapazität. Dies liegt zum einen darin begründet, dass zwischen den Blöcken etwa 10 bis 20 Prozent der Kapazität für Fehlerkorrektur- und Adressinformationen belegt sind. Zum anderen jedoch sind sich Hersteller von Festplatten und Hersteller von Betriebssystemen über die Definition eines Megabytes uneinig: Plattenhersteller rechnen mit $1000 \times 1000 \text{ Byte} = 1 \text{ MB} (= 1.000.000 \text{ Bytes})$, während die meisten Betriebssysteme von $1024 \times 1024 \text{ Byte} = 1 \text{ MB} (1.048.576 \text{ Bytes oder Zeichen})$ ausgehen. Weiterhin benötigt das File-System einigen Platz für Verwaltungsdaten (z. B. SunOS reserviert darüber hinaus noch ca. 10 % eines File-Systems als stille Reserve und zeigt diese bei dem Kommando `df` dem Benutzer nicht an). Dazu ist die Nettokapazität abhängig von der Formatierung. Sie ist keine absolut feststehende Größe, sondern in gewissem Rahmen veränderbar.

Wie groß ein Massenspeicher dimensioniert werden muss, hängt von der Anwendung ab. Besonders bei Audio/Video (A/V) Anwendungen, Grafikprogrammen und Publishing Programmen fallen sehr große Datenmengen an. Aber auch das Betriebssystem selbst und die Anwendungsprogramme benötigen sehr viel Speicherplatz, sodass eine anfänglich groß erscheinende Festplatte sehr schnell mit Programmen und Daten gefüllt ist. Man rechnet derzeit mit einer jährlichen Verdoppelung des benötigten Speicherplatzes.

Grundsätzlich sollte die Festplattenkapazität großzügig geplant werden, da meist mehr Platz benötigt wird als ursprünglich angenommen. Ebenfalls ist zu berücksichtigen, dass die Performance bei allzu starker Ausnutzung der Kapazität leidet. Gegen eine viel zu große Dimensionierung spricht allerdings der ständige Preisverfall von Festplattenlaufwerken. Der Kauf eines Laufwerks mit geringen Platzreserven und der spätere Austausch gegen ein größeres Laufwerk kann insgesamt preiswerter sein als der sofortige Kauf eines größeren Laufwerks, allerdings nur, wenn der zeitliche Abstand zwischen Erstkauf und Austausch nicht zu kurz ist. Deshalb wird eine Festplatte empfohlen, die ausreichend groß für den Bedarf des nächsten Jahres ist.

Leider lassen sich nicht bei allen Betriebssystemen beliebig Große Platten verwenden. An HP9000 Workstations sind einige Einschränkungen zu beachten:

An den Modellen 7xx unter HP-UX 9.01 (mit Patch PHKL 3325) sowie HP-UX 9.03 - 9.05 können als Bootplatten nur Festplatten < 2.147 MB eingesetzt werden (genauer: es werden nur File-Systeme < 2 hoch 31 Bytes erkannt), als Datenplatte sind Festplatten bis 4.294 MB zulässig (< 2 hoch 32 Bytes).

Die Modelle HP9000/7xx ab HP-UX 10.xx und HP9000/8xx ab HP-UX 9.xx verfügen über einen LVM (Logical Volume Manager). Dieser ermöglicht Bootplatten bis zu 4.294 MB und unbegrenzt (bzw. nur limitiert durch die Anzahl der möglichen Filesysteme je SCSI-





ID) Große Datenplatten. Soll ein File-System > 4.294 MB angesprochen werden, zerlegt der LVM es einfach in mehrere logische Files und umgeht so die magische Grenze von 2 hoch 32 Bytes.

Bei den Modellen HP9000/3xx und 4xx unter HP-UX dürfen sowohl die Bootplatte wie auch die Datenplatte nicht grösser als 2.147 MB sein. Entsprechendes gilt unter DOMAIN-OS. Hier müssen die Festplatten zusätzlich auf SCSI-1 umgestellt werden.

Kapazitätseinschränkungen gibt es auch unter DOS, Win3.1, Win3.11 und Windows 95. Es kann jeweils nur eine primäre Partition auf einer Platte konfiguriert werden, wobei im Gesamtsystem nur eine Partition aktiv sein darf. Die aktive Partition ist normalerweise die Bootpartition. Die max. Partitionsgröße liegt leider immer noch bei 2 GB, die max.

Plattengröße bei 8 GB. Zu beachten ist, dass bei einer 2 GB Großen Partition die Blockgröße 32 KB beträgt, d. h., wenn eine Datei von 250 Byte abgelegt wird, belegt sie trotzdem einen Block von 32 KB. Dies ist nur zu umgehen, wenn eine Blockgröße von 8 KB konfiguriert wird, was bei einer Partitionsgröße von 500 MB automatisch der Fall ist. Bei Windows NT beträgt die maximale File-Systemgröße 16 Exabyte (16 Millionen Terabyte). Die maximale Plattengröße ist also nur vom entsprechenden SCSI-Controller abhängig. Die Partitionsgröße kann ohne Probleme bei 20 GB liegen.

Unter Sun Solaris1.x (nicht unter Solaris2.x) gibt es eine Beschränkung von File-Systemen auf 2 GB. Da maximal sieben Datenpartitionen angelegt werden können, ergibt das eine Plattenbeschränkung auf 14 GB.

Leistungsmerkmale

AIX 3.x von IBM hat ebenfalls eine Beschränkung bei File-Systemen auf 2 GB. Da aber AIX eine Festplatte mit dem LVM (Logical Volume Manager) fast beliebig einteilen kann, gibt es keine Beschränkung in der Plattengröße. AIX 4.x unterstützt File-Systeme bis max. 64 GB, so dass hier auch größere Platten bzw. RAID-Systeme als ein File-System angesprochen werden können.

Einige ältere Betriebssysteme (IBM AIX3.5, SGI IRIX5.x, Sun Solaris1.x) brechen die Formatierung von Festplatten über 8 GB mit einem Timeout ab. Vor Anschaffung einer größeren Festplatte sollte in diesen Fällen geprüft werden, ob ein entsprechender Patch vorliegt.

Neben der Geschwindigkeit des Prozessors selbst und natürlich auch der Größe des Hauptspeichers ist die Leistungsfähigkeit des Primär-Massenspeichers der wichtigste Faktor für die Reaktionszeiten des Rechners. Die Daten, die von der Festplatte übertragen werden, müssen auch an einem Stück in den Hauptspeicher passen, sonst muss nachgeladen werden. Mit der zunehmenden Datenmenge, die über den Bus

übertragen wird sollte auch der Hauptspeicher angepasst werden. Die Performance wird in erster Linie durch die Zugriffszeit auf die Daten und sekundär auch durch die Datenübertragungsrate bestimmt. Die Zugriffszeit errechnet sich aus der Zeit für mehrere einzelne, nacheinander ablaufende Vorgänge:

Will ein Programm Daten lesen oder schreiben, wird zunächst im Betriebssystem ein entsprechender Request erzeugt und dem Festplattencontroller übergeben. Die Zeit, die dieser Vorgang benötigt, nennt man Betriebssystem-Overhead. Der so erzeugte Request veranlasst das Laufwerk, die Schreib-/Leseköpfe auf einen bestimmten Punkt der Plattenoberfläche zu positionieren. Diese Zeit heißt Positionierzeit. Angegeben wird hier immer die mittlere Positionierzeit, d. h. die Zeit, die der Kopfmechanismus braucht, um 1/3 der Maximalpositionierstrecke zurückzulegen. Die Settling Time gibt an, wie lange der Kopfmechanismus braucht, um sich nach einer Kopfbewegung mechanisch zu beruhigen bzw. auszuschwingen. Bei modernen Laufwerken schließt die Positionierzeit die Settling Time bereits ein. Ist der Schreib-/Lesekopf über der entsprechenden Spur positioniert, muss er warten, bis der gewünschte Block unter ihm vorbeikommt.

Diese Wartezeit wird Latency oder auch Umdrehungswartezeit genannt. Angegeben wird hier immer die Zeit, welche die Festplatte für eine halbe Umdrehung benötigt. Diese Zeit ist ausschließlich drehzahlabhängig. So ergibt sich z. B. bei einer Drehzahl von 7200 U/min eine Latency von 4,17 ms. Dann erst werden die Daten selbst übertragen, und zwar zuerst von der Festplatte zum Festplatten-Controller. An dieser Stelle kommt nun die (interne) Transferrate der Festplatte ins Spiel. Sie gibt die Anzahl der übertragenen Bytes in einer Sekunde an. Manchmal wird hier auch eine Frequenz angegeben. Zur Umrechnung in die Transferrate ist diese durch 8 zu teilen. Je höher die Transferrate einer Platte ist, desto kleiner ist die zum Datentransfer benötigte Transferzeit. Sind die Daten beim Festplatten Controller angekommen, schickt dieser sie über den SCSI-Bus an den SCSI-Hostadapter. Die Transferraten über den SCSI-Bus betragen bis zu 320 MB/s. Näheres zu SCSI-Bussen steht im Kapitel Peripheriebusse.

Je kürzer die Gesamtzeit, desto besser die Systemleistung. Dies gilt insbesondere für Betriebssysteme, die während der Wartezeit keine anderen Aufgaben erledigen können, wie beispielsweise MS-DOS. Zu beachten ist, dass in der Regel bei Vergleichen der Transferraten von Festplatten in Tabellen meistens optimale Bedingungen angenommen werden, d. h., dass der Kopf schon positioniert ist, dass ein kompletter Zylinder gelesen werden kann und einiges mehr. Einfluss auf die Transferrate hat auch die Blockung der Platte, d. h., wie viele Bytes zu einem Sektor zusammengefasst werden. Allgemein üblich sind 512 Bytes/Sektor. Man kann aber die Platten auch mit bis zu 4096 Bytes/Sektor formatieren. In dem Fall ist auf der Platte mehr Platz für Benutzerdaten, weil weniger Platz für Formatinformationen notwendig ist. Dies wiederum führt zu einer höheren Nettotransferrate. Dies ist jedoch nicht bei allen Betriebssystemen möglich und nicht bei allen Anwendungen sinnvoll. Je kleiner die Files sind, die üblicherweise gelesen oder geschrieben werden, desto kleiner sollte auch die Sektorengröße sein (z. B. bei Datenbanken). Je grösser die Files sind, desto mehr Sinn machen auch Große Sektoren



(z. B. bei Bildverarbeitung).

Außerdem werden bei SCSI-Laufwerken oft die Übertragungsraten über den SCSI-Bus angegeben. Da in die SCSI-Laufwerke aber Pufferspeicher eingebaut sind, wird hier nur die Übertragungsrate vom Puffer der Platte in den Puffer des SCSI-Hostadapters angegeben. Die tatsächliche Übertragungsrate von der Plattenoberfläche bis in den Puffer des Hostadapters ist jedoch wesentlich geringer.

Da die meisten Anwendungen nur wenige Blöcke lesen und schreiben und somit geringe Datenmengen in einem Request übertragen, ist die Datentransferrate, mit der das Laufwerk die Daten zum Hostadapter überspielt, eher zweitrangig. Je gestückelter Daten auf der Festplatte gespeichert sind, desto mehr kurze Lesezugriffe erfolgen. Man muss aber darauf achten, dass in der Übertragungskette Festplatte - Festplatten-Controller - SCSI-Host-Controller - Rechner Hauptspeicher die Geschwindigkeiten aufeinander abgestimmt sind. Eine weitere Möglichkeit zur Leistungssteigerung ist der Einsatz von Controllern (auf der Festplatte wie auch beim SCSI-Hostadapter) mit Cache-Speichern.

Besonders vorteilhaft wirkt sich dabei ein Multisegment-Cache aus. Der Cache wird hierbei dynamisch verwaltet und in mehrere Bereiche aufgeteilt. Je nachdem, aus wie vielen Plattenbereichen Daten angefordert werden, werden diese in einem Bereich des Cache gespeichert. Beim Zugriff auf Daten im Cache entfallen die Zeiten für die mechanischen Komponenten.

Bei diesen Controllern wird jeder Schreib-Request wie von einem Controller ohne Cache abgearbeitet: Jeder zu schreibende Block wird zum angeschlossenen Laufwerk übertragen. Zusätzlich aber merkt sich der Controller die Adresse des Blocks und dessen Inhalt in einem internen Speicher, dem Cache. Der Vorteil liegt in den reduzierten Festplattenzugriffen.

Ein Festplattencontroller mit Cache-Speicher ist dann zu empfehlen, wenn folgende Bedingungen vorliegen: geringer oder gerade ausreichender Hauptspeicherausbau des Rechners, Festplattenlaufwerke mit einer hohen Zahl von Schreib-/Lese-Requests pro Zeiteinheit und Plattennutzung mit typisch kleiner Anzahl von Blöcken pro Request, zum Beispiel als Systemplatte, für Datenbanken und generell für Anwendungen, die oft im Wechsel auf denselben Files schreiben und lesen. Mit einem so gepufferten Controller sinken die durchschnittlichen Zugriffszeiten auf Werte unter einer Millisekunde.

Man unterscheidet hier Read-, Read-ahead- und Write-back-Cache. Bei einem Read-Zugriff auf einen Read-Cache wird der Speicher nach dem entsprechenden Block durchsucht. Wird dieser gefunden, wird er sofort übertragen. Die Wartezeit für Plattenpositionierung und Umdrehung entfällt. Steht der Block nicht im Cache, wird er vom Laufwerk geholt.

Beim Read-ahead-Cache werden die nachfolgenden Blöcke nach dem Lesen eines

Blocks auf der Platte im Voraus gelesen und im Cache gespeichert. Beim Write-back-Cache werden die zu schreibenden Blöcke im Cache zwischengespeichert und erst dann auf Platte geschrieben, wenn keine weiteren Schreib- oder Leseaufträge anliegen. Dadurch werden Schreibzugriffe für den Benutzer scheinbar schneller. Eine Gefahr besteht jedoch darin, dass bei Stromausfall die im Cache gespeicherten Daten verloren gehen. Beim Read-Cache ist das kein Problem, beim Write-Cache kann dadurch die Datenstruktur zerstört werden. Man sollte daher beim Einsatz eines Systems mit Write-Cache nicht auf eine unterbrechungsfreie Stromversorgungsanlage (USV) verzichten. Nähere Informationen dazu stehen im Kapitel USV.

Je nach Größe des Cache-Buffers, der Intelligenz des Cache-Algorithmus (d. h., welche Blöcke überschrieben werden, wenn der Cache-Speicher voll ist) und Art der Anwendungen lassen sich Trefferquoten (Hit-Rate) von über 90 Prozent erreichen - und damit eine gewaltige Durchsatzverbesserung.

Viele Betriebssysteme wie z. B. Windows NT, NetWare, Unix und OS/2 reservieren automatisch einen Teil des Hauptspeichers als Cache. Mehr Hauptspeicher kann somit die Performance des gesamten Systems enorm beschleunigen.

4.2.3 Halbleiterplattenspeicher

Reicht bei bestimmten Anwendungen die Geschwindigkeit, mit der ein Plattenlaufwerk die Daten liefern kann, nicht aus, so kann ein Halbleiterspeicher (RAM-Disk, Solid State Disk) eingesetzt werden. Bei der RAM-Disk-Lösung wird eine spezielle Software eingesetzt, die einen Teil des Hauptspeichers als Disk organisiert. Eine Solid State Disk ist eine Hardwarelösung, bestehend aus einem Bus-Interface mit Memory-Modulen.

Auf den Speicher kann in beiden Fällen so zugegriffen werden wie auf ein Plattenlaufwerk. Es können also Files wie auf einer richtigen Platte angelegt und wieder gelesen werden.

Vorteil: Die Positionierzeit und die Umdrehungswartezeit entfallen, so dass der Datentransfer mit maximal möglicher Geschwindigkeit erfolgt.

Nachteil: Ein solcher Speicher ist (auch bei Verwendung von Batterie-Backup) nicht als permanenter Datenspeicher geeignet. Auch ist er erheblich teurer als ein Plattenspeicher gleicher Größe. Ein Batterie-Backup für diesen Speicher ist normalerweise immer erforderlich, da sonst schon bei einem kurzen Stromausfall die Daten verloren gehen.





4.2.4 RAID

Bei CPUs und Hauptspeichern verdoppelt sich die Leistung etwa jedes Jahr. Massenspeicher verdoppeln ihre Kapazität nur etwa alle zwei Jahre, die Positionierzeit halbiert sich gar nur alle sieben Jahre. Plattenlaufwerke hinken also immer mehr der Technologiekurve der CPUs hinterher.

Man benötigt deshalb Techniken, die es auf Basis der sich langsamer entwickelnden Plattentechnologie dennoch schaffen, mit der Prozessorgeschwindigkeit und dem Datenhunger der heutigen Systeme Schritt zu halten - durch erhöhte Zugriffsgeschwindigkeit und erhöhte Kapazität.

Typische MTBF-Zeiten (MTBF = Mean Time Between Failure = durchschnittliche Zeit zwischen zwei Ausfällen) von Laufwerken liegen heute bei über 500.000 Stunden. Bei 100 Laufwerken an einem Rechner muss man mit einem Ausfall pro Halbjahr rechnen. Selbst wenn man davon ausgeht, dass die Zuverlässigkeit der Laufwerke in den nächsten Jahren weiter steigt, ist dieser Zustand nicht tragbar. Es werden also Systeme benötigt, die ausfallsicher sind.

Unter dem Oberbegriff RAID fasst man Technologien zusammen, die mehrere Laufwerke zu größeren, teilweise auch ausfallsicheren Gesamtsystemen zusammenpacken. RAID steht dabei für Redundant Array of Independent Disks, wobei oft statt „independent“ auch „inexpensive“ gelesen wird.

Redundant = ausfallsicher bedeutet, dass der Ausfall eines Einzellaufwerks weder zu einem Ausfall des Gesamtsystems noch zu Betriebsunterbrechung oder gar zu Datenverlust führt. RAID schließt oft verwendete Technologien wie Mirroring (d. h. Spiegelung von zwei oder mehreren Laufwerken an einem Controller), Duplexing (dito, aber mit zwei getrennten Controllern) und Striping (Zusammenfassen von mehreren Laufwerken als logische Einheit und blockweises Verteilen der Daten auf diese Laufwerke) ein.

Unterschiedliche Level von RAID werden in der Literatur diskutiert. Die Bezeichnung Level in der RAID-Bezeichnung ist eigentlich missverständlich, denn RAID-Level 1 baut keinesfalls auf RAID-Level 0 auf. Statt Level sollte man eigentlich besser Typ sagen.

Bevor auf die einzelnen RAID-Level genauer eingegangen wird, folgen einige grundlegende Überlegungen zu Plattenzugriffen, denn die Änderung der Performance beim Schritt vom Einzellaufwerk zu RAID ist stark abhängig von der Anwendung:

Wichtig ist der Mix zwischen Schreib- und Lesezugriffen und die durchschnittliche Länge

eines einzelnen Transfers.

Bei einem Einzelplattenlaufwerk ist ein Lesezugriff (Caches, Read-ahead-Buffer und andere Techniken zur Performance-Steigerung sollen vorläufig außer Betracht bleiben) gleich schnell wie ein Schreibzugriff. Dies ist bei Platten-Arrays keinesfalls so und auch von Level zu Level unterschiedlich.

Geschwindigkeitsunterschiede gibt es auch von kurzen (meist einer oder ganz wenige Blöcke) zu langen Requests (meist mehrere Hundert Blöcke). Der erste Typ kommt vor allem in Datenbank Anwendungen, Transaction Processing Systemen und kommerziellen Multiuser-Anwendungen vor. Der zweite Typ ist in der Regel bei Bildverarbeitung, Einsatz von Supercomputern oder technisch/wissenschaftlicher Datenerfassung zu finden. Jedes der weiter unten diskutierten RAID-Konzepte hat eine andere Charakteristik bei langen bzw. kurzen Requestlängen.

RAID ist keine Lösung für alle Arten von Problemen mit dem Plattendurchsatz. RAID ist keinesfalls immer schneller als der Einsatz von (konventionell genutzten) Einzellaufwerken. Auch beim Einsatz einer der nachfolgend beschriebenen RAID-Typen sollte man die Aufteilung der Daten optimieren. Aus der Regel, dass man auf wenige Daten sehr häufig und auf die meisten Daten sehr selten zugreift, folgt: Sinnvoll ist ein hierarchisches System mit Halbleiterspeicher (z. B. RAM-Disk) für ständig benutzte Daten, ein sehr schneller Massenspeicher (eventuell gespiegelt) für oft genutzte, einen durchschnittlich schnellen und Großen Massenspeicher (z. B. RAID) für weniger oft genutzte Daten und einen Archivspeicher (z. B. optische Platten mit automatischem Wechsler) für selten benutzte Daten.



RAID-Level 0

Dieser Typ von RAID steht für Striping. Bei diesem Verfahren werden mehrere kleinere Laufwerke zu einem Großen logischen Laufwerk zusammengefasst. Der Striping-Faktor sagt dabei aus, wie groß die Stücke sind, welche jeweils auf eines der Laufwerke geschrieben werden. Sind die Stücke sehr klein (typisch ein Byte), so erreicht man unabhängig von der Länge des Lese- oder Schreibrequests eine wesentliche Erhöhung der Transferrate, da alle Laufwerke in einem RAID-0-Set praktisch gleichzeitig transferieren.

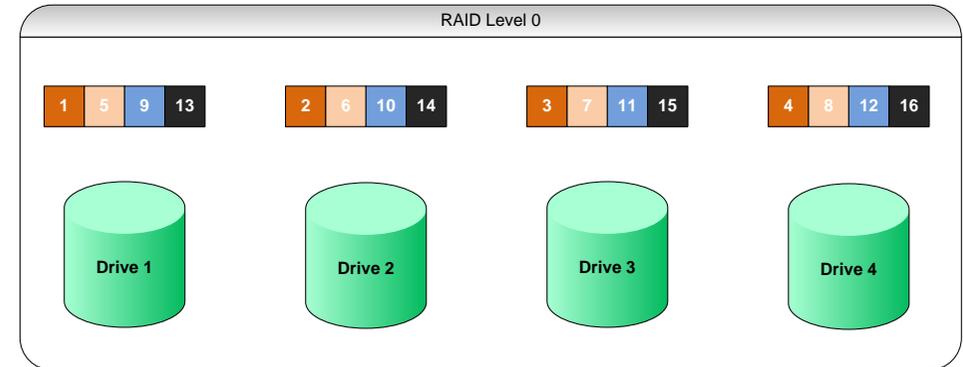
RAID-0 mit kleinem Striping-Faktor bietet den Vorteil der hohen Transferrate beim Schreiben und Lesen von langen Requests, hat aber wesentliche Nachteile in der Leistung bei kurzen Requests.

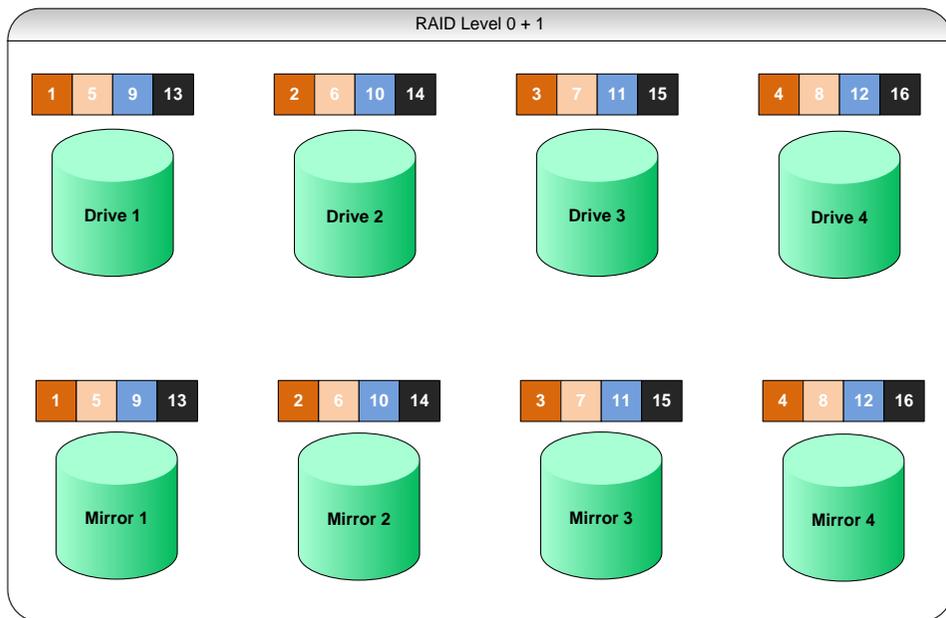
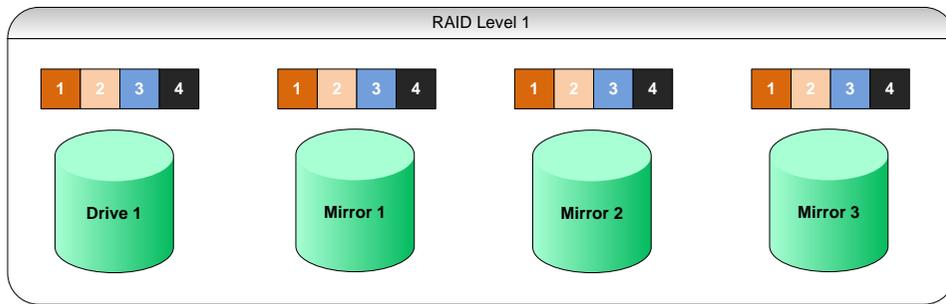
Vergleicht man RAID-0 nicht mit einem (entsprechend größeren) Einzellaufwerk, sondern mit mehreren kleineren Laufwerken, die ja kurze Requests überlappt abarbeiten können, wird der Nachteil von RAID-0 noch deutlicher.

Wählt man den Striping-Faktor nun groß (mehrere Blöcke), erreicht man, dass sowohl die Schreib- als auch die Lese-Performance bei kurzen Transfers mit der eines Einzelplattenlaufwerks vergleichbar bleibt. Auch ist es möglich, mehrere kurze Requests gleichzeitig auf unterschiedlichen Platten abzuarbeiten.

In beiden Fällen bleibt jedoch der Nachteil, dass bei Ausfall eines einzelnen Laufwerks auf die gesamten Daten nicht mehr zugegriffen werden kann. RAID-0 (Striping) ist eigentlich kein RAID (keine erhöhte Datensicherheit).

Host-based Striping gibt es bei vielen Betriebssystemen als Software-Lösung oder auch eingebaut im Platten-Controller. Da die Plattenlaufwerke vom Controller oftmals nur über einen Datenkanal angesprochen werden, kommt bei einer Controllerlösung meist der Vorteil der höheren möglichen Datenübertragung nicht zum Tragen, da die Requests auf den einzelnen Laufwerken doch sequenziell und nicht parallel abgearbeitet werden.





RAID-Level 1

RAID-1 bedeutet Mirroring. Hier werden alle Daten einer Platte auf alle weiteren Platten des RAID-Sets geschrieben. Vorteil: Bei Ausfall einer Platte bleiben die Daten weiter zugreifbar. Die Leistung beim Schreiben bleibt der einer Einzelplatte bzw. RAID-0 gleich (solange die Platten auf die Kanäle verteilt sind). Man geht man davon aus, dass die zusätzliche Rechnerbelastung durch doppeltes Schreiben nicht zählt.

Die Leseleistung verdoppelt sich im besten Fall, da jetzt die Requests auf zwei Plattenlaufwerke (bzw. zwei Sets) aufgeteilt werden können, die unabhängig voneinander lesen können. Allerdings sind die Kosten für RAID-1 hoch: Nur die Kapazität einer Festplatte des verfügbaren Platzes steht für die Originaldaten zur Verfügung; Der Rest wird durch redundante Daten verbraucht. Jedoch ist RAID-1 einfach zu implementieren.

Mirroring (von Einzelplatten) gibt es als Controller-Lösung oder als Software-Lösung für unterschiedliche Betriebssysteme.

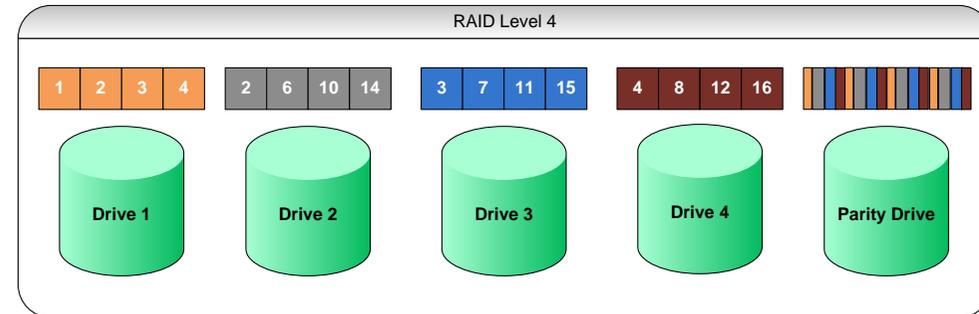
RAID-Level 0+1

RAID-0+1, manchmal auch RAID-10 genannt, vereinigt Mirroring und Striping. Hier wird tatsächlich die Hälfte der Gesamtkapazität gespiegelt, wobei sich die hohe Sicherheit der Spiegelung mit der Performance von RAID-0 verbindet. In den meisten Fällen ist dies die schnellste RAID-Lösung, aber natürlich gilt auch hier das Argument von RAID-1: Die Kosten sind, da doppelt so viele Platten verwendet werden, sehr hoch.



RAID-Level 4

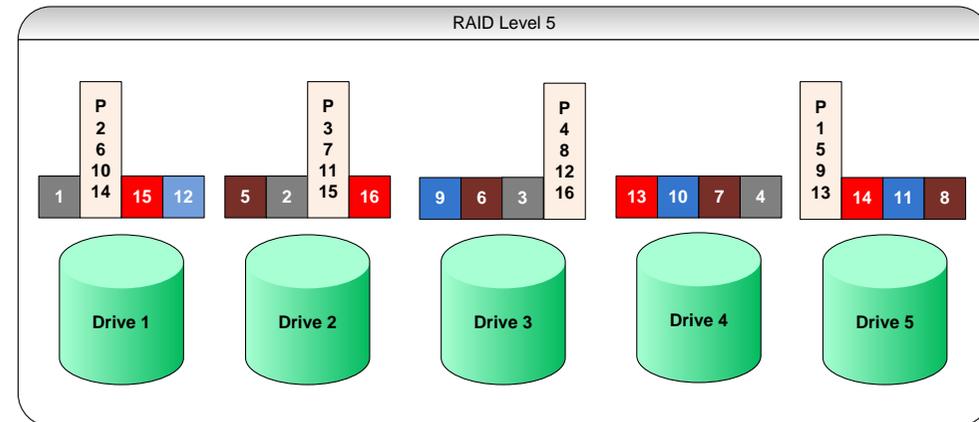
Während Ausfallsicherheit bei RAID-1 und 0+1 doppelte Plattenkapazität erfordert - und bei RAID-0 gar nicht gegeben ist - verwendet RAID-4 Parity, um die Daten zu sichern. Zu jeweils x Festplatten, die nach dem Striping-Verfahren beschrieben werden, kommt lediglich eine zusätzliche Parity-Platte, deren n-tes Bit jeweils das Parity-Bit zu den x n-ten bits der restlichen Platten enthält. Fällt eine Festplatte aus, kann aus dieser Parity-Platte zusammen mit den Daten der übrigen Platten Bit für Bit der Inhalt der defekten Platte rekonstruiert werden. Das Schreiben von Daten auf einer Platte erfordert allerdings immer auch das Ändern der Parity-Platte - beide Blöcke müssen zuerst gelesen und aus ihnen und den neuen Daten der neue Parity-Wert berechnet werden. So ist die Performance geringer als bei RAID-0 oder -1.



RAID-Level 5

Bei RAID 4 muss bei jedem Schreibzugriff auf die Parity-Disk zugegriffen werden. Dieses Laufwerk wird damit der Flaschenhals in diesem System. RAID-5 verteilt Parity und Daten blockbereichsweise auf alle Laufwerke. Jedes Laufwerk ist damit für einen bestimmten Blockbereich Parity-Laufwerk. Lesezugriffe werden etwas schneller, weil sie auf noch mehr Laufwerke verteilt werden können.

Bei kurzen Transfers ist aber auch RAID-5 auf der Basis von Zugriffen pro Zeiteinheit pro Megabyte einem Einzellaufwerk weit unterlegen.





Andere RAID-Level

Neben den oben genannten RAID-Leveln, die in einer Studie der Universität Berkeley erstmals beschrieben wurden und sich als Quasi-Standard etabliert haben, gibt es noch eine Reihe von herstellereigenspezifischen RAID-Leveln, die aber in der Regel nur Modifikationen der o. g. RAID-Level darstellen.

Wo wird RAID nun implementiert? Es gibt zwei Möglichkeiten: entweder in einem Controller, der zwischen dem Rechner und den Laufwerken sitzt (als Karte im Rechner oder in einer separaten Box) oder im Hostrechner selbst. Vorteil der ersten Lösung: keine zusätzliche Belastung des Rechners durch die Verwaltung von RAID. Vorteil der zweiten Lösung: Da in diesem Falle nicht alle Daten durch den Flaschenhals RAID-Controller zum Hostrechner müssen, kann eine höhere Datentransferrate durch die gleichzeitige Verwendung mehrerer Übertragungspfade erreicht werden.

Eine Reihe von Herstellern (sowohl Plattenlaufwerks- als auch Controller-Hersteller) bieten RAID-Implementierungen an. Diese Implementierungen unterscheiden sich in folgenden technischen Eigenschaften:

Einfachere Implementierungen schließen mehrere Laufwerke an einen SCSI-Bus an und fassen diese unter Verwendung von einem RAID- oder RAID-ähnlichen Konzept zusammen. Andere Implementierungen haben pro Plattenlaufwerk einen eigenen Controller. Sie erhöhen dadurch die Ausfallsicherheit, da selbst bei Ausfall des Controllers die Daten weiter zugreifbar bleiben.

Laufwerke können fest eingebaut werden. Es ist jedoch auf jeden Fall besser, wenn auch teurer, die einzelnen Laufwerke so einzubauen, dass sie im laufenden Betrieb ausgewechselt werden können und somit der Datenzugriff nicht unterbrochen werden muss (Hot Swap). Gute RAID-Systeme erlauben beim Austausch eines Laufwerks das Rekonstruieren der Daten für dieses Laufwerk während des normalen Betriebs.

Einen wichtigen Einfluss auf die Ausfallsicherheit von RAID-Systemen haben auch andere Elemente: Hängen alle Laufwerke an einem einzigen Power Supply, ist die Ausfallwahrscheinlichkeit (aber nicht notwendigerweise die Wahrscheinlichkeit des Datenverlustes) höher als bei getrennten Stromversorgungen für jedes einzelne Laufwerk oder einer anderen, redundanten Art der Stromversorgung. Natürlich sollten dann auch Kabel, Lüfter, Controller und Rechneranschlüsse doppelt ausgeführt werden, um den Single Point of Failure auszuschließen.

Und noch eine Warnung: Bei allen Betrachtungen von Ausfallhäufigkeiten und Ausfallwahrscheinlichkeiten geht man davon aus, dass Laufwerksausfälle statistisch unabhängig voneinander vorkommen. In der Praxis können externe Ereignisse (Blitzschlag, Stromspitzen) eintreten, die zu einer höheren punktuellen

Ausfallwahrscheinlichkeit - von mehr als einem Laufwerk - führen können, so dass die MTBF-Überlegungen für RAID-Systeme teilweise praxisfremd sind.

Und selbst bei einem RAID-System mit unendlich hoher durchschnittlicher Zeit zwischen zwei Ausfällen darf man das Backup nicht vergessen: Vor einem falschen Delete-Kommando oder einem Software-Fehler, der Daten zerstört, schützt auch RAID nicht. Und Würmer, Trojanische Pferde, Viren und Bomben werden wohl auch nicht aussterben oder Respekt gegenüber RAID entwickeln.

Fazit:

RAID-Systeme dienen der verbesserten Verfügbarkeit von Daten und nicht der Performance Verbesserung. Sie sind in der Regel bei der Geschwindigkeit Einzellaufwerken unterlegen. Sinnvoll ist der Einsatz von RAID-Level 0 bis 5 zum Speichern von großen Datenmengen, auf die entweder seltener oder nur mit langen Transfers zugegriffen wird. RAID bietet hier eine kostengünstige Möglichkeit, ausfallsichere Massenspeicher zu konfigurieren. Für häufiger benutzte Daten empfiehlt sich weiterhin der Einsatz von (gespiegelten) Einzellaufwerken, für extrem häufig verwendete Daten hingegen der Einsatz von RAM-Disks, die, vorausgesetzt die Anzahl der Schreibzugriffe ist nicht zu hoch, mit normalen Winchesterplatten gespiegelt werden können. Spiegeln sollte man wegen der geringeren Rechnerbelastung in der Regel im Controller bzw. Hostadapter. Braucht man die hohe Transferrate langer Transfers, sollte Striping mehrere Datenpfade zum Rechner zulassen und deswegen Hostbased sein. Hardware-RAID-Systeme werden in den Kapiteln Externe RAID-Systeme von transtec (Seite 141) und SCSI/IDE RAID-Systeme (Seite 142) angeboten. Interne Hardware RAID-Systeme mit PCI-Controllern sind in den Kapiteln PCI-RAID-Controller von ICP vortex (Seite 149) und Mega-RAID PCI-RAID-Controller von AMI (Seite 148) zu finden.

Auf jeden Fall sollte ein RAID (und der Rechner) an eine USV-Anlage (Näheres dazu im Kapitel USV (Seite 337) angeschlossen werden, da sonst im Fall eines Stromausfalls der eigentliche Sinn, die absolute Datenverfügbarkeit, nicht mehr erfüllt ist.

Software RAID

Windows NT, 2000 und XP bieten bereits standardmäßig die Möglichkeit, mehrere Plattenlaufwerke zu einem RAID-System zusammenzufassen. Hierbei brauchen lediglich die Festplatten an einen SCSI-Hostadapter intern oder extern angeschlossen zu werden. Die Konfiguration wird dann über Windows vorgenommen. Diese Lösung ist zwar preisgünstig und einfach einzurichten, hat jedoch auch Nachteile. Vor allem, wenn sehr große Datenmengen übertragen werden bzw. wenn Zugriffe parallel von mehreren Usern (beispielsweise in einem Netz) auf das RAID erfolgen, hat dies Auswirkungen auf die Performance des Windows-Rechners. Hierbei muss der gesamte Rechenaufwand (Verteilen der Daten auf die einzelnen Platten und Berechnen der Parity) von der CPU des Rechners aufgebracht werden. Des Weiteren wird das Betriebssystem des Rechners



über eine Bootplatte geladen, die nicht redundant sein kann, da die RAID-Konfiguration erst nach dem Laden des Betriebssystems zur Verfügung steht. Auf der Bootplatte befinden sich auch alle Konfigurationsdaten für den RAID-Verband. Fällt die Bootplatte aus, ist das RAID-System nicht mehr operabel. Diesem Nachteil beugen die folgenden Hardware-RAID-Lösungen mit separatem RAID-Controller.

Interne Hardware-RAID mit PCI-RAID-Controller

Hierbei übernimmt der RAID-Controller, wie bei den externen Hardware-RAIDS, die gesamte Rechenarbeit. Somit arbeiten die Controller, unabhängig von der CPU-Auslastung, mit konstanter Performance. Die RAID-Konfigurationsdaten befinden sich auf allen Festplatten des RAID-Systems und sind somit auch bei Ausfall einer Festplatte oder sogar des ganzen Controllers immer vorhanden. Bei Tausch des Controllers oder einer Festplatte werden die RAID Konfigurationsdaten eingelesen und der Rebuild gestartet.

RAID-Controller sind mit internen Anschlussbuchsen und einem externen Anschluss für SCSI-Festplatten versehen. Somit hat man die Möglichkeit, die Festplatten des RAID-Systems in den Rechner einzubauen oder aber extern anzuschließen. Weitere Informationen und detailliertere Angaben zu Anschlussmöglichkeiten von Festplatten sind in den Kapiteln PCI-RAID-Controller von ICP vortex und Mega-RAID PCI-RAID-Controller zu finden.

Externe Hardware-RAID

Die High-End-RAID-Lösung stellen die sog. Hardware-RAIDS dar. Hier sind der Controller und die Festplatten in einem separaten Gehäuse untergebracht. Das RAID-System wird mittels SCSI- oder FC-Kabel mit dem Hostadapter des Rechners verbunden.

Durch die Backplane, an der Controller und Festplatten direkt angeschlossen sind, erreicht man kürzeste Kabellängen und somit maximale Datensicherheit. Weitere Datensicherheit kann durch den Einsatz von redundanten Controllern erreicht werden. Hierbei wird bei Defekt des Controllers automatisch auf einen zweiten Controller im Gehäuse umgeschaltet, ohne Zeitverzögerung und Datenverlust. Der defekte Controller kann dann im laufenden System gegen einen neuen getauscht werden. Nähere Informationen hierzu stehen im Kapitel Externe RAID-Systeme von transtec.

Hardware-RAIDS arbeiten, wie PCI-RAID-Controller, immer mit konstanter Performance, unabhängig von der CPU-Auslastung. Hierbei werden die Daten vom Hostadapter des Rechners über den SCSI-Bus direkt zum RAID-Controller übertragen. Dort werden die gesamten Daten in den Cache eingelesen. Danach ist der SCSI-Bus nicht mehr belastet. Der Controller des Hardware-RAIDS verteilt dann die Daten auf die einzelnen Platten und berechnet die Parity, in Abhängigkeit vom gewählten RAID-Level. Währenddessen ist die CPU des Rechners nicht mit den Rechenoperationen des RAID-Systems belastet. Ein entsprechend groß gewählter Cache, der als Write-back-Cache konfiguriert ist, kann die

Schreib-Performance erheblich erhöhen. Das Lesen der Daten geschieht dann analog hierzu in umgekehrter Reihenfolge. Hardware-RAIDS können im Vergleich zu PCI-RAID-Controllern plattformübergreifend eingesetzt werden.





4.3 Sekundär-Datenspeicher

Informationsaufzeichnung ist heute mehr denn je eine Schlüsseltechnologie für große Bereiche in Wirtschaft und Technik, denn speziell Bereiche, die speicherplatzintensive Daten wie Multimedia-Anwendungen benötigen, verlangen nach schnellen, sicheren und kostengünstigen Massenspeichern. Ein anderer Aspekt ist die Datensicherheit, denn durch Hardwarefehler, vor allem aber durch Bedienungsfehler, können Daten in einem Rechner zerstört werden. Selbst wirklich erfahrene Benutzer können dies kaum vermeiden (auch Feuer und Wasser können Rechner und Daten zerstören). Deswegen ist es generell zu empfehlen, alle Daten regelmäßig auf einen Datenspeicher-Träger zu kopieren und diesen an einem sicheren Ort zu verwahren.

Plattenspiegelung (Mirroring) und andere Verfahren bieten zwar teilweise einen Schutz vor Datenverlust, besonders bei Hardwarefehlern. Sie schützen Benutzer jedoch nicht vor irrtümlichen Löschbefehlen oder anderen, durch Software veranlasste Datenzerstörungen, wie zum Beispiel durch Viren oder Programmfehler.

Für die Datensicherung gibt es eine Reihe wechselbarer Datenträger, und bei der Auswahl der Speichertechnologie sollten folgende Aspekte berücksichtigt werden:

- die Zeit, die bei regelmäßigem Backup anfällt
- die Zeit, die ein gelegentlicher Gesamtbackup benötigt
- die Zeit, die man zum Zurückholen einzelner Files braucht
- die Zeit, die bei einer Gesamtrestauration der Daten nötig ist
- Datensicherung als Archivierungslösung
- Preis des Datenträgers pro MB

4.3.1 Disketten-Laufwerke

Wichtig ist ebenso die Austauschbarkeit des Datenträgers mit anderen Systemen, um das Backup auch auf einem anderen Rechner lesen oder den Datenspeicher-Träger für den Datentransport verwenden zu können. Ein wichtiger Aspekt ist die Netzwerkfähigkeit eines Datenspeichersystems. Besitzt man ein lokales Netzwerk, kann es sinnvoll sein, mehrere Rechner über das Netzwerk mit einem Datenspeicherlaufwerk zu sichern.

Entsprechende Software ist auf dem Markt verfügbar. Der Vorteil liegt in geringeren Kosten und der einfachen, zentralen Bedienung.

Generell muss man zwei Arten von Backup-Datenträgern bzw. -Technologien unterscheiden:

diejenigen, bei denen man direkt auf die Daten zugreifen kann, zum Beispiel Wechselplatten und optische Platten, und solche, bei denen Daten vor der Bearbeitung erst auf die Festplatte umkopiert werden müssen, zum Beispiel Magnetbandkassetten (siehe Kapitel 4.4). Die einen bieten den Vorteil schneller und bequemer Handhabung, die anderen haben einen deutlich geringeren Preis pro MB.

Der in den letzten Jahren eingetretene enorme Anstieg der Speicherdaten erforderte eine Erweiterung der bestehenden bzw. die Einführung neuer Technologien. Die Angebotspalette ist in jüngster Zeit sehr umfangreich und damit auch etwas unübersichtlich geworden.

Bei Speicherkapazitäten von bis zu 2 GB pro Medium ist zwischen zwei grundsätzlich verschiedenen Technologien zu unterscheiden. Zum einen existieren Wechselplattensysteme und ZIP- bzw. JAZ-Laufwerke, bei denen ein Magnetkopf die Daten induktiv liest. Zum anderen werden optische Laufwerke angeboten, bei denen über einen Laser die Datenbits erzeugt und auch wieder gelesen werden können. Gemeinsam ist diesen Technologien allerdings die Art der Datenverwaltung, bei der direkter Zugriff auf die gespeicherten Daten besteht. Die Daten müssen vor dem Bearbeiten nicht erst auf eine Festplatte kopiert werden.

Die Technik von Disketten beruht auf einer wechselbaren, rotierenden magnetisierbaren Scheibe mit einer Zugriffszeit von etwa 150-250 ms. Sie haben den Vorteil der weiten Verbreitung für den Austausch mit anderen Systemen. Nachteilig war bisher die geringe Kapazität von 360 KB bis 2,88 MB. Diese reicht inzwischen, nachdem leistungsstarke PCs sowohl in den Unternehmen als auch für den privaten Gebrauch Einzug gehalten haben, nicht mehr aus.

Dieser Nachteil wurde durch das ZIP-Laufwerk von IOMEGA weitgehend aufgehoben. Mit 100/200 MB pro Speichermedium ist die Kapazität dieses Laufwerks auch für kleine bis mittlere Software-Pakete noch ausreichend. Außerdem überzeugt dieses Laufwerk durch ein faires Preis-Leistungs-Verhältnis.

Seit Mitte 1999 ist von Sony ein HiFD-Diskettenlaufwerk verfügbar, das mit 200 MB Speicherkapazität die bis jetzt gängigen Laufwerke ablösen könnte. Dieses ist kompatibel zu den momentan eingesetzten Laufwerken und kann die 1,44-MB-Disketten lesen.

Allerdings kann jedoch die geringe „Flughöhe“, mit der sich der Magnetkopf über der



Speicherplatte bewegt, zu einem so genannten „Head-Crash“ führen. Eine solche Berührung hat normalerweise den Verlust der dort gespeicherten Daten zur Folge. Dies kann auch bei den weiter unten beschriebenen Wechselpplatten-Laufwerken vorkommen.

4.3.2 Wechselpplatten-Laufwerke

Größere Datenmengen lassen sich mit Wechselpplatten verwalten, ohne dass durch Umkopieren Zeit verloren geht. Diese Technologie bietet sich besonders bei sicherheitskritischen Anwendungen an, wenn die Daten über Nacht in einen Tresor eingeschlossen werden.

Es gibt unterschiedliche Technologien, von IOMEGAs JAZ-Laufwerk mit 2 GB Medien über Wechselrahmen, in die normale Festplatten eingesetzt werden können, bis hin zu Syquest Laufwerken. Letztere haben den Nachteil, nicht stoßfest zu sein, so dass ein Transport nicht empfehlenswert ist.

Sinnvoll ist der Einsatz von Wechselpplatten nämlich auch bei ständig wechselndem Einsatzort, wenn z. B. ein Programmierer an mehreren Standorten tätig ist und stets Zugriff auf seine Projektdaten haben sollte. Da die Daten nach wie vor auf einem Plattenlaufwerk sind und damit auch die Gefahr des Datenverlustes bestehen bleibt, sollte man zusätzlich eine parallele Datensicherung auf einem anderen Medium vornehmen müssen.

4.3.3 Optische Laufwerke

Optische Platten haben mit der CD-ROM allgemeine Verbreitung gefunden. Technologien wie CD-R und CD-RW, aber auch die Vergrößerung der Kapazitäten durch DVD lassen diesen Markt weiter wachsen. In diesen Bereich fallen auch magneto-optische Technologien mit ebenfalls wachsenden Kapazitäten.

CD-ROM-Laufwerke

CD-ROMS sind wechselbare optische Platten, die nach dem Beschreiben mit Daten im Fertigungsprozess nur noch gelesen werden können. Dieses Medium eignet sich mit seinen ca. 650 MB ideal für die Massenverteilung von Daten, wie z. B. für die Softwaredistribution, da die Reproduktionskosten bei entsprechenden Stückzahlen sehr gering sind. Die Nachteile der CD-ROMs, die Nichtwiederbeschreibbarkeit und die relativ langsame Zugriffszeit (derzeit etwa 85-120 ms, je nach Laufwerk) spielen dort meist eine untergeordnete Rolle. Der Datenträger selbst ist überaus preiswert (maximal 0,01 bis

0,02 DM pro MB). Sinnvoll ist die Massenproduktion von CD-ROMS in der Regel ab einer Auflage von über 100 Stück. Dabei werden die Daten, ähnlich dem Herstellen einer Schallplatte, in das Trägermaterial gepresst.

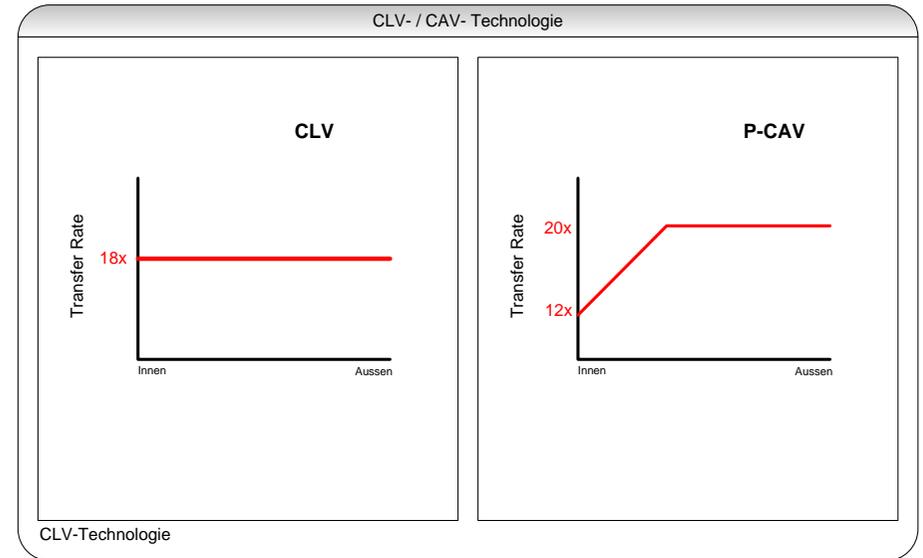


Abb. 15: CLV- / CAV- Technologie

Die Lesegeschwindigkeit der CD-ROM Laufwerke wird gemessen an der Übertragungsrate eines Audio-Laufwerks, die 150 KB/s beträgt. Ein 14x Laufwerk beispielsweise liest 2,05 MB/s. Die neuesten CD-ROM-Laufwerke jedoch arbeiten mit bis zu 52facher Geschwindigkeit und einer Datentransferrate von 7800 MB/s. Laufwerke mit Lesegeschwindigkeiten höher als 14fach basieren auf der Partial- CAV-Technologie (Constant Angular Velocity). Diese zeichnet sich durch eine variierende Datentransferrate bei gleich bleibender Umdrehungsgeschwindigkeit im Innenbereich der CD aus. Beim Lesen der äußeren Spuren einer CO wechselt das Laufwerk in das bisher bei den CD-ROM-Laufwerken übliche CLV (Constant Linear Velocity)-Verfahren, bei welchem die Umdrehungsgeschwindigkeit vor dem Lesen angepasst wird. Dadurch ergibt sich eine konstante Datentransferrate.

Des Weiteren bietet die neue Generation von CD-ROM-Laufwerken neben der obligatorischen Geschwindigkeitssteigerung ein neues Feature: Multiread. Dies bedeutet bei CDROM-Laufwerken, dass sie auch die wiederbeschreibbaren CD-RWs lesen können. Neben den normalen Einzellaufwerken werden auch CD-ROM-Wechsler angeboten. Die typische Wechslerzeit pro CO liegt bei ca. 3 bis 10 Sekunden. CD-ROM-Wechsler eignen sich vor allem für Anwendungen auf CD-ROM, bei denen größere



Datenmengen, auf die selten zugegriffen wird, im direkten Zugriff des Rechners sein sollten (z. B. Desktoppublishing oder Multimedia-Anwendungen). Auf dem Markt befindliche Wechsler-Systeme erlauben in einer einzigen Peripherieeinheit die Verwaltung von Datenmengen bis in den Terabyte-Bereich.

CD-R- und CD-RW-Laufwerke

Mit CD-Recordern (CD-R) können CD-Rohlinge (Write-once-CD) ohne großen Aufwand beschrieben werden. Dabei werden die Daten mit Hilfe eines Laserstrahls auf den CD-Rohling geschrieben. Durch diese Recorder ist auch die Herstellung von nur einer einzigen CD in wirtschaftlich relevante Dimensionen gerückt. So lassen sich kleine Auflagen von Produktkatalogen, Softwareprodukten oder Grafiksammlungen auf CD-ROM erstellen. Auch zur Langzeitarchivierung eignen sich die beschreibbaren CDs. Die Datenträger sind sehr sicher, aber eine nachträgliche Änderung der Daten ist nicht möglich.

Die mit einem CD-Recorder beschriebenen CDs lassen sich ebenso wie die in Großen Auflagen gepressten CDs mit jedem handelsüblichen CD-ROM-Laufwerk lesen. Mit Wechslern, die einen CD-Recorder enthalten, besteht die Möglichkeit, kostengünstig Archivierung und Backup in kleinen und mittleren Netzwerken durchzuführen.

Steht jedoch die Produktion bzw. das Kopieren von CDs im Vordergrund, so werden seit neuestem CD-Dupliziersysteme angeboten, die als Standalone-Geräte Möglichkeiten zur Duplikation von CDs bieten. Mehr Informationen zu den einzelnen Geräten sind im Kapitel CD-Duplizier- und Printsyste.

CD-Rewritable (CD-RW) ist eine Technologie, die es erlaubt, ein Medium wiederholt zu beschreiben. Dies kann bis zu 3000 Mal geschehen, allerdings muss derzeit noch jeweils die ganze CD am Stück gelöscht werden. Die Laufwerke beschreiben einmalig auch CDR-Medien. CD-RW-Medien können in bisher handelsüblichen CD-ROM-Laufwerken nicht gelesen werden, jedoch besitzen die seit kurzem im Handel angebotenen CD-ROM-Laufwerke die Multi read-Fähigkeit und können somit die CD-RWs lesen (zu Kompatibilitäten siehe Tabelle). Nähere Informationen zu Produkten sind im Kapitel CD-ROM-Subsysteme zu finden.

Medium	CD-ROM	CD-R	CD-RW	DVD-ROM	DVD-R	DVD-RAM	DVD-RW
CD-ROM	R						
CD-R	R	W / R	W / R	R		R	R
CD-RW	R	R	W / R	R		R	R
DVD-ROM				R	R	R	R
DVD-R				R	W / R	R	R
DVD-RAM						W / R	
DVD-RW							W / R

R = lesekompatibel
W = schreibkompatibel



CD-R & CD-RW-Laufwerke

Abb. 15

Abb. 16: CD-R- & CD-RW-Laufwerke

DVD-Laufwerke

Nachdem CD-ROM mit seiner Kapazität lange Zeit als ausreichend angesehen wurde, entstand auf Druck der Videoindustrie mit DVD (Digital Versatile Disk, ursprünglich: Digital Video Disk) eine neue optische Technologie, die die Kapazität der Medien auf 5,2 GB erweiterte. Durch Verwendung der Rückseite und den Einsatz einer zweiten Datenschicht soll diese Kapazität in Zukunft noch vervierfacht werden. Erreicht wurde diese Kapazitätserweiterung durch eine Verringerung der Mindestlänge für Pits und des Track Abstands der Windungen. Die DVD-Laufwerke können darüber hinaus alle herkömmlichen CD-Formate lesen.

Seit einiger Zeit sind DVD-R-Laufwerke (Recorder) auf dem Markt erhältlich. Allerdings, verfügen diese bis jetzt nur über eine Speicherkapazität von 4,7 GB/Seite.

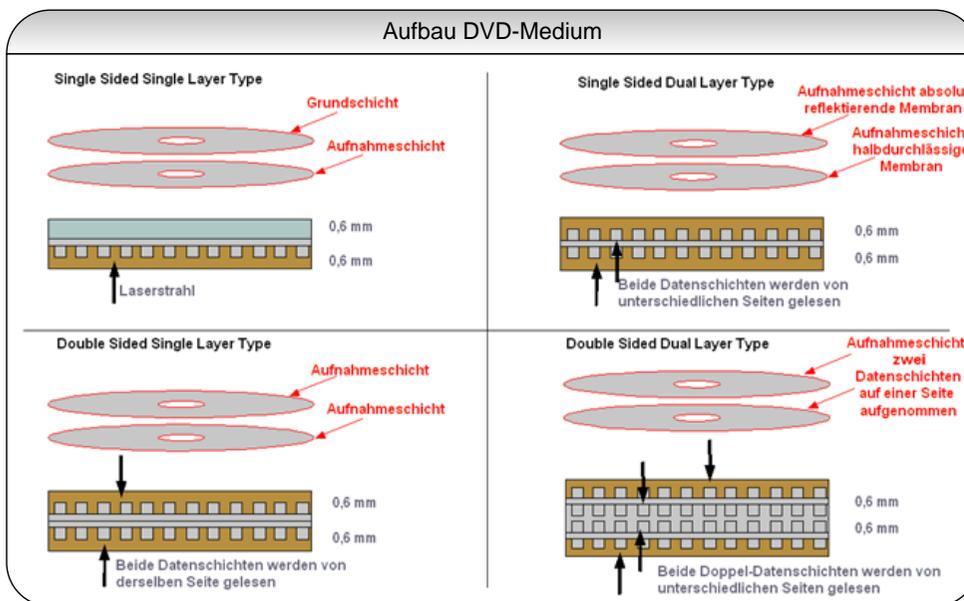


Abb. 17: Aufbau DVD-Medium

Der Siegeszug der DVD wurde jedoch dadurch unterbrochen, dass es keinen gemeinsamen Standard gibt. Toshiba, Hitachi und Panasonic entwickelten das DVD-RAM-Laufwerk mit 4,7GB Kapazität pro Seite, wobei dieses mit Caddy arbeitet und erste Laufwerke erhältlich sind. Sony, Philips und HP dagegen haben ein DVD-RW-Laufwerk entwickelt, welches 7,8 GB Kapazität bietet, ohne Caddy arbeitet und zudem in zukünftigen DVD-Laufwerken gelesen werden kann. Außerdem können die DVD-RW-

Laufwerke auch die Inhalte von CD-RWs lesen, was DVD-RAM-Laufwerke nicht können.

Noch ist nicht abzusehen, welcher Standard sich bei der wiederbeschreibbaren DVD durchsetzen wird.

Blu-ray Disc

Die Spezifikationen für die Blu-ray Disc wurden am 19. Februar 2002 durch die neun Unternehmen der *Blu-ray Group*, Panasonic, Pioneer, Philips, Sony, Thomson, LG Electronics, Hitachi, Sharp und Samsung, beschlossen; dieser Gruppierung schlossen sich Ende Januar 2004 zusätzlich noch Dell und Hewlett-Packard sowie Mitte März 2005 Apple und Acer an. Hewlett-Packard trat allerdings 2005 wieder aus dem Blu-ray-Konsortium aus, nachdem einige Verbesserungsvorschläge abgewiesen worden waren, und wechselte in das HD-DVD-Lager.

Die Blu-ray Disc gibt es in drei Varianten: als nur lesbare *BD-ROM* (vergleichbar mit DVD-ROM), als einmal beschreibbare Variante *BD-R* (vergleichbar mit DVD±R) und als wiederbeschreibbare *BD-RE* (vergleichbar mit DVD±RW).

Die Blu-ray Disc basiert auf einem tief-violetten Laser mit 405 nm Wellenlänge, die wiederbeschreibbare Blu-ray Disc arbeitet mit der Phase-Change-Technik.

Sie hat – genau wie CD und DVD – einen Durchmesser von 12 cm. Eine Blu-ray Disc fasst mit einer Lage bis zu 25 GB und mit zwei Lagen bis zu 50 GB an Daten. Alternative Quellen nennen als Bruttokapazität 21,7 GB. TDK ist es gelungen, auf einer sechslagigen Scheibe 200 GB unterzubringen, dabei wurde die Kapazität einer Lage auf 33,3 GB erhöht. Pioneer erklärte im Juli 2008, Prototypen mit 400 GB auf einer Scheibe mit 16 Lagen erzeugt zu haben; eine Entwicklung einer marktreifen Version war bis zum Jahr 2010 geplant. Stattdessen wurde 2010 die BDXL mit 100 GB Speicher veröffentlicht. Ebenfalls kündigte das Unternehmen für 2013 Versionen mit bis zu 1 TB Speicherkapazität an.

Des Weiteren soll die neue Phase-Change-Technik eine doppelt so hohe Übertragungsrate (Datentransferrate) von 72 Mbit/s beim Beschreiben anstatt der ursprünglich maximal spezifizierten einfachen 36 Mbit/s ermöglichen. Ein wichtiger Bestandteil der Spezifikation ist auch ein Kopierschutz in Form einer eindeutigen Identifikationsnummer. Außerdem eignen sich Blu-ray Discs besonders gut für Full-HD-Videos, die dank der hohen Auflösung eine bessere Qualität als die gängigen Systeme wie PAL und NTSC bieten, aber auch dementsprechend mehr Speicherplatz benötigen. BD-Spieler unterstützen in der Regel das zuerst von Panasonic und Sony eingeführte





hochauflösende AVCHD-Format.

In der Praxis sehen die technischen Spezifikationen für Blu-ray-Video-Discs folgendermaßen aus: Die Gesamt-Bandbreite ist auf 53,95 Mbit/s begrenzt. Davon sind 40,00 Mbit/s für den reinen Videostream (in Form von MPEG-2, VC-1 und AVC) reserviert, die verbleibenden 13,95 Mbit/s für die Tonspuren (in Form von Dolby Digital, Dolby Digital Plus, Dolby TrueHD, DTS, DTS-HD High Resolution Audio, DTS-HD Master Audio und Linear-PCM).

Eine weitere Neuerung gegenüber der DVD ist der verkleinerte Abstand des Lasers zum Datenträger sowie die geringere Wellenlänge (und daher andere Farbe) des Laserstrahls. Weiterhin ist die Schutzschicht auf der Laser-Seite mit 0,1 mm im Vergleich zu 0,6 mm der DVD deutlich kleiner. Aufgrund der daraus resultierenden größeren Anfälligkeit gegen Kratzer und Staub war zunächst geplant, die Blu-ray Disc nur in einer Art Kassette (Steckmodul oder Cartridge genannt) anzubieten, ähnlich wie seinerzeit die MiniDisc. Stattdessen wurde jedoch eine Beschichtung namens „Durabis“ entwickelt, die den Gebrauch eines Kassettengehäuses nicht mehr unbedingt notwendig macht.

Wegen des geringeren Abstandes zwischen Medium und Laseroptik sowie der dünneren Schutzschicht kann ein Objektiv mit günstigerer numerischer Apertur eingesetzt werden, das den Strahl effizienter bündeln kann. Somit werden Schreibfehler und stärkere Streuungen verringert und es ist möglich, eine Blu-ray Disc zum Beispiel aus Metall oder anderen stabilen, undurchsichtigen Materialien kombiniert mit einer dünnen durchsichtigen Trägerschicht zu bauen, die mit erheblich höheren Drehzahlen als eine Scheibe aus Polycarbonat betrieben werden können, woraus dann höhere Übertragungsraten resultieren. Zudem erlaubt die gegenüber der DVD kleinere Wellenlänge des Laserstrahls eine wesentlich höhere Datendichte und damit eine erhöhte Speicherkapazität.

Magneto-optische Laufwerke

Magneto-optische Datenspeicherung besitzt als Vertreter der optischen Speichertechnik diverse Vorteile gegenüber konkurrierenden Technologien. Magneto-optische Plattenlaufwerke zeichnen kontakt- und verschleißfrei mittels eines Lasers Daten durch Erhitzen und Anlegen eines Magnetfeldes auf der MO-Plattenoberfläche auf.

Die Datenträger können doppelseitig beschrieben werden, und das Lesen der Daten erfolgt durch den reflektierten Laserstrahl. In diesem sind die Informationen enthalten, die eindeutig die im Material vorliegende Magnetisierung wiedergibt. Das Beschreiben der MO geschah bisher sehr langsam. Der Grund dafür war, dass bei einem Schreibvorgang derselbe Block dreimal bearbeitet wurde: Beim ersten Vorgang wurde der Block gelöscht, bei der nächsten Umdrehung wurde der Block geschrieben und bei der darauf folgenden Umdrehung überprüft. Gegenüber einem Lese-Request dauerte also ein Schreib-

Request zwei volle Umdrehungen länger.

In der Zwischenzeit sind auch alle im Handel befindlichen Magneto-optischen Laufwerke LIMDOW-fähig (Laser Intensity Modulation Direct Overwrite) und können in diesen Modus umgestellt werden. LIMDOW bedeutet, dass es nun möglich ist, in einem einzigen Arbeitsgang - ohne einen zusätzlichen Löschyklus wie bisher üblich - alte gegen neue Daten auszutauschen, also eine alte Information mit einer neuen direkt zu überschreiben. Der Nachteil der geringeren Performance z. B. gegenüber konventionellen Winchesterplattenlaufwerken, der bisher das Bild der magneto-optischen Technologie etwas trübte, hat nun keine Berechtigung mehr.

Zusammengefasst stellen sich die Vorteile dieser Technologien wie folgt dar: Die Datenträger selbst sind klein, leicht und nicht allzu teuer. Die Laufwerke können vom Rechner wie ein normales Plattenlaufwerk genutzt werden, und es ist keine spezielle Filesystem-Software erforderlich.

Sinnvolle Einsatzgebiete für magneto-optische Plattenlaufwerke sind z. B. solche, bei denen der Datenträger aus dem Rechner entfernt werden soll (z. B. bei sicherheitskritischen Anwendungen) und die höhere Performance von Winchesterplatten in Wechselkassetten nicht benötigt wird bzw. man deren höheren Preis nicht zahlen möchte. Weiter kann man MO-Platten dort einsetzen, wo auf Backups schnell und ohne vorheriges Umkopieren auf einen anderen Datenträger zugegriffen werden soll. MO-Wechsler erlauben hier die Archivierung auch größerer Datenmengen. Diese werden allerdings in Zukunft an Bedeutung verlieren, da CD-RW- und CD-R-Jukeboxen an ihre Stelle treten.

WORM-Platten

WORM-Platten (Write Once Read Multiple) sind optische Platten, die nur einmal beschrieben, aber beliebig oft gelesen werden können. Diese Technologie spielt fast keine Rolle mehr seit der Einführung von CD-R.



4.3.4 Ausblick

Die CD-ROM hat sich sowohl im Audio- wie auch im Computerbereich einen festen Platz erkämpft. Durch die Entwicklung der CD-R (einmal beschreibbar) und neuerdings der CD-RW (mehrfach beschreibbar) werden sich diese Technologien - sicherlich zu unterschiedlichen Anteilen - einen Platz im Markt sichern können.

Etwas anders sieht es bei der DVD (Digital Versatile Disk) aus. Diese Technologie wird unter Umständen die CD-ROM aus einigen Bereichen verdrängen können, da die Kapazität einer Disk um ein Vielfaches höher liegt.

Parallel zu den Entwicklungen im DVD-Bereich, wird auch an der Entwicklung einer MOVideo-Platte gearbeitet. Diese so genannte MO-7 (ASMO) soll über eine Speicherkapazität von 6,1 GB verfügen. Gleichzeitig brachten Laufwerkhersteller wie Maxoptix ebenfalls Nachfolgeprodukte auf den Markt, die mit 5,2 GB eine Verdoppelung der momentanen Kapazität erreichten.

Die Entwicklung im optischen Datenspeichermarkt geht zurzeit mit großen Schritten voran. Die OSTA (Optical Storage Technology Association) hilft beim Verschaffen eines Überblicks über derzeitige und zukünftige Technologien: <http://www.osta.org>





4.4 Backup-Datenspeicher

Magnetband-Sicherungslösungen haben Netzwerkverwalter lange Zeit mit gemischten Gefühlen betrachtet. Aufgrund preiswerter Medien und wirtschaftlicher Hardware ist die Backup-Technologie auf Magnetbändern heute finanziell attraktiver als optische oder Festplattenspeicherung.

Zur Backup-Datenspeicherung werden Technologien gezählt, die sequenziell arbeiten. Es ist nicht - wie bei den Sekundärspeicherlösungen - möglich, direkt auf Daten zuzugreifen, da die Suche nach Informationsblöcken in der Reihenfolge stattfindet, in der sie auf den Datenträger geschrieben wurden.

4.4.1 Aktuelle Backup-Speicherlösungen

Das Magnetband ist noch immer das Medium, welches die höchsten Speicherkapazitäten bietet. Es hat bei den Bandspeichertechnologien ebenso wie im optischen Speicherbereich Weiterentwicklungen gegeben, wobei aber die optischen Speichersysteme der rasanten Entwicklung und dem Wachstum der Datenbestände nicht mithalten konnten, und Magnetbänder momentan das kostengünstigste Medium zur Sicherung größerer Datenmengen darstellen. Aktuelle, auf dem Markt erhältliche Bandlaufwerke können Datenmengen bis 220 GB auf einem Tape sichern, wobei sich die angebotenen Technologien durch das Aufzeichnungsverfahren unterscheiden.

Vorab aber noch einige generelle Erklärungen zu Speicherkapazitäten und wie diese für die Datenträger angegeben werden:

- Nur bei Verwendung von vorformatierten Datenträgern kann eine Nettokapazität angegeben werden.
- Die Speicherkapazität hängt sowohl von der zur Verfügung stehenden beschreibbaren Länge des Bandes als auch der Schreibdichte ab und wird in der Regel in bits/Inch angegeben. Auch das Aufzeichnungsformat selbst (Fehlerkorrektur, Filemarks, Steuerzeichen etc.) schmälert diese Kapazität.
- Bei Laufwerken mit Datenkompression kommt der Kompressionsfaktor hinzu, der zum einen vom verwendeten Kompressionsalgorithmus und zum anderen von der Redundanz der zu komprimierenden Daten abhängig ist.

4.4.2 DLT-Laufwerke

Die DLT-Technologie (Digital Linear Tape) zeichnet Daten serpentinartig linear auf, so dass die Spuren parallel zur Kante des Bandes liegen. Es werden 1/2"-Magnetbänder in kompakten Kassetten beschrieben. DLT-Laufwerke bieten zurzeit im Vergleich zu allen anderen Backup-Technologien mit die höchsten Speicherkapazitäten auf einer Kassette. Mit dem DLT4000 können bis zu 40 GB an Daten gespeichert werden, mit dem (mittlerweile nicht mehr verfügbaren) DLT7000 bis zu 70 GB und dem DLT8000 sogar bis zu 80 GB. Bisher wurden die Daten durch zwei im Lese-/Schreibkopf angebrachte Kanäle mit einer Dichte von 62500 bits/Zoll geschrieben, die Transferrate betrug 3 MB/s. In diesem Format bestand eine Dateneinheit aus 20 4-KB-Blöcken, wobei die einzelnen Datenblöcke mit verschiedenen Fehlererkennungsverfahren (Parity, Cyclic Redundancy Check CRC und Error Detection Check EDC) versehen wurden. Die letzten vier Blöcke jeder Einheit bestehen aus vier ECC-Blöcken (ECC error correction check). Beim neuen Verfahren werden die Daten von vier im Lese-/Schreibkopf angebrachten Kanälen mit einer Dichte von 86000 bits per Inch geschrieben. Dadurch konnte die Transferrate auf 5 MB/s erhöht werden. Hier besteht eine Dateneinheit aus 24 4-KB-Blöcken. Auch diese werden mit Fehlererkennungsverfahren versehen. Die letzten fünf Blöcke jeder Einheit sind ECC-Blöcke. Nach jedem Schreibvorgang führt der DLT-Controller einen Lesetest durch. Die geschriebenen Daten werden mit dem Pufferinhalt verglichen und im Fehlerfall korrigiert. Diese Sicherheitsmaßnahmen garantieren sehr hohe Datenintegrität.

Ein weiterer Vorteil dieser Technologie liegt darin, dass die Belastung von Bändern und Leseköpfen gering ist. Dies wird durch den Einsatz von stationären Magnetköpfen und einer einfachen Bandführung erreicht. So sind mit DLT-Laufwerken Banddurchläufe von bis zu 500.000 Zyklen pro Kassette möglich. Die Bänder DLTtape IV ermöglichen Banddurchläufe von mehr als 1 Mio. Zyklen durch Einsatz der neuen, oben beschriebenen Technologie.

Die Abrundung der DLT Produktlinien nach unten wurde im Jahr 2000 das DLT1 eingeführt, das 80 GB schreiben kann, aber nur mit einer Datendurchsatzrate von 6 MB/s. Es wird die DLT4000 Serie ablösen.

2001 kam Quantum mit dem ersten SuperDLT Laufwerken auf den Markt, die mit einer neuen Technologie 220 GB bei 22 MB/s (2:1 Kompression) erreichen. Sie brauchen dazu Tapes mit einer wesentlich besseren Beschichtung, aber gleicher Kassettengröße. Erste Systeme waren noch nicht lesekompatibel zu DLT8000, allerdings ist diese Kompatibilität das wichtigste Verkaufsargument für diese gegenüber LTO etwas teureren Produkte.

Jukeboxen und Libraries von verschiedenen Herstellern erhältlich und ermöglichen die Sicherung von sehr großen Datenbeständen.

Informationen zu Produkten sind im Kapitel DLT-Subsysteme und in den Kapiteln zu den

DLT-Libraries zu finden.

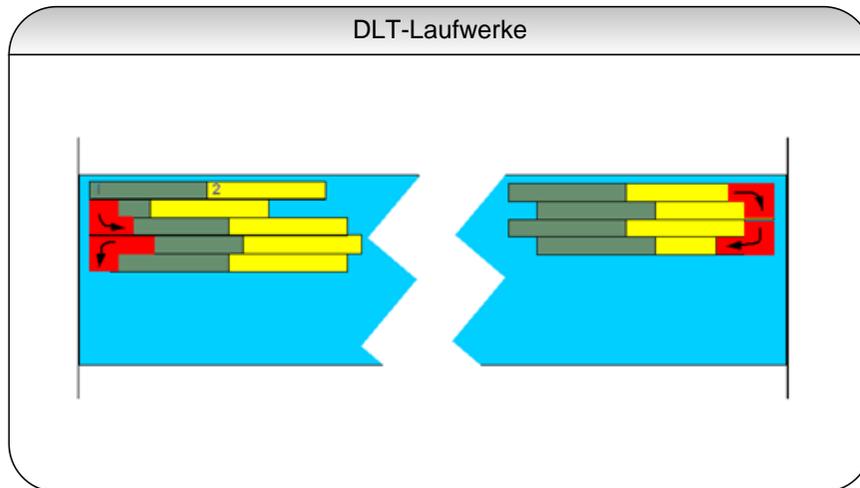


Abb. 18: DLT-Laufwerk

4.4.3 AIT-Laufwerke

Das 1997 von Sony auf den Markt gebrachte AIT (Advanced Intelligent Tape) beruht wie das Exabyte auf der 8-mm Helical-Scan-Technologie, ist aber zu dieser - schon durch ein anderes Kassettenformat - nicht kompatibel. Die maximale Kapazität liegt bei derzeit ca. 130 GB (unkomprimiert bei 50 GB), wobei die Chancen für einen guten Kompressionsfaktor (ca. 2,6) durch einen neuen Algorithmus (ALDC-Advanced Lossless Data Compression) gestiegen sind. Das Laufwerk passt außerdem wie DAT in einen 3,5"-Einbauplatz. Neu ist ein Selbstreinigungsmechanismus, der die Verwendung von Reinigungstapes in normalen Arbeitsumgebungen überflüssig macht.

Ab Sommer 2001 plant Sony, das neue AIT-3-Laufwerk anzubieten. Mit einer neuerlichen Verdoppelung der Kapazität auf bis zu 100/260GB (komprimiert) bei Verwendung der 230-m-Bänder und einer Transferrate von 11/28,6 MB/s liegt es in der Leistungsklasse von LTO-Laufwerken der ersten Generation.

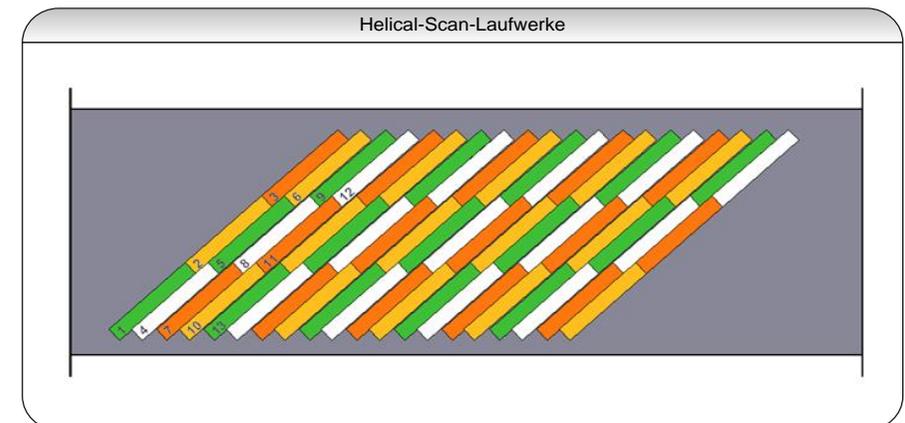
Bei schwerwiegenden Fehlern wird der interne Kopfreiniger automatisch aktiviert, wobei auch die AME-Medien entscheidend zur Reduzierung der Reinigungsintervalle beitragen. Eine interessante Neuerung ist aber auch die mögliche Verwendung eines Memory-Chips (MIC= Memory in Cassette, 16 Kbit bei 25/65 GB Medien, 64 Kbit bei allen anderen) in den Kassetten. Backup-Software kann auf ihm Informationen speichern, die bei herkömmlichen Technologien nur am Anfang des Bandes verzeichnet sind. Diese

Informationen erlauben eine Halbierung der durchschnittlichen Suchzeit auf einem Tape, die dann mit 27 Sekunden angegeben wird.

Inzwischen unterstützen auch alle gängigen Backup-Software-Hersteller das AIT-Laufwerk mit den oben beschriebenen Features. Nähere Informationen sind im Kapitel Backup Software zu finden.

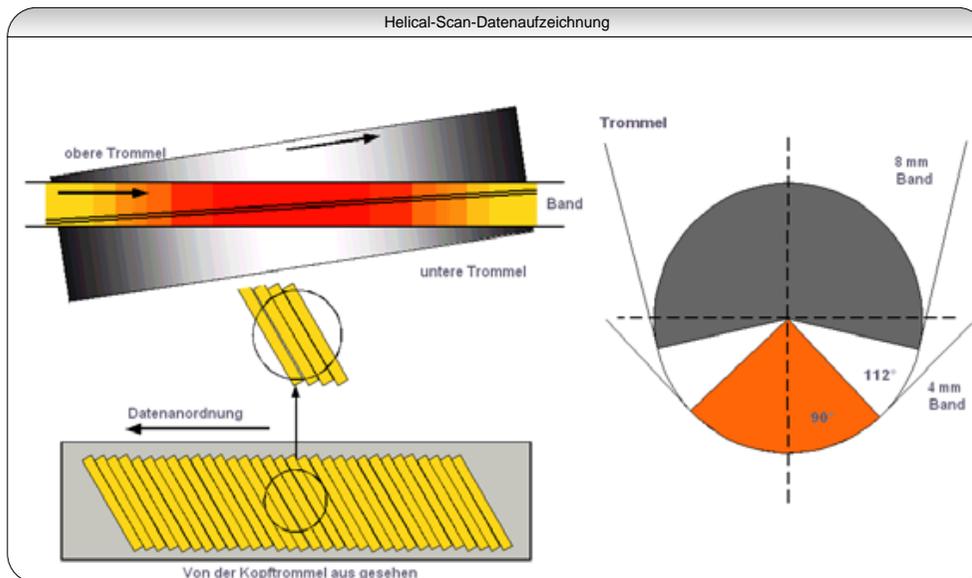
4.4.4 Exabyte-Laufwerke

Sehr hohe Datendichten werden mit Magnetbandgeräten aus dem Audio- und Videobereich, die das Helical-Scan-Verfahren verwenden, erreicht. Rotierende Kopftrommeln zeichnen die Daten dabei in schräg zur Laufrichtung des Bandes liegenden Spuren auf. Diese Spuren können mit einer hohen Datendichte beschrieben werden. Geräte, die auf dieser Technologie basieren und die auf die besonderen Bedürfnisse der Datensicherung angepasst wurden, haben Große Marktanteile im Bereich der Backup-Laufwerke erobert. Die Exabyte-Laufwerke sind aus der Video8-Technik hervorgegangen und wurden speziell für den Einsatz als Backup Geräte verbessert. Dabei wurde die Aufzeichnungstechnik verfeinert. Bei den Datenmengen, die mit diesen Laufwerken auf einer Kassette gesichert werden können (maximal 40 GB beim Exabyte Mammoth mit 170 m Band), sinkt der Datenträgerpreis pro GB, und auch der Platzbedarf einer Kassette ist minimal. Versand und Lagerung sind unproblematisch. Selbst Langzeitarchivierung ist mit Kassetten der neuesten Generation kein Problem. Die Hersteller (Exabyte, Sony) garantieren eine Archivierungszeit von 10 Jahren.



4.4.5 DAT-Laufwerke

Auch die DAT-Technologie ging aus dem Einsatz von digitalen Aufzeichnungsverfahren im Audiobereich hervor und zeichnet Daten im Helical-Scan-Verfahren auf ein Magnetband auf. Dieses ist jedoch im Vergleich zu Exabyte-Bändern (8 mm) nur 4 mm breit, und im Laufwerk selbst beträgt der Umschlingungswinkel des Bandes um die Kopftrommel nur 90 Grad im Vergleich zur Exabyte-Technologie, bei der der Umschlingungswinkel 112 Grad beträgt und somit das Band wie auch den Kopf des Laufwerks stärker belastet.



Das DDS-Format (Digital Data Storage) wurde von HP und Sony entwickelt und hat sich als Standard durchgesetzt. Die Entwicklungen im DAT-Bereich profitieren vom Wettbewerb unterschiedlicher Hersteller. Laufwerke entsprechend dem DDS-2 Standard speichern bis zu 8 GB (120 m Band) und erreichen Datentransferraten von bis zu 1 MB/s. Die Angabe von 8 GB Speicherkapazität stellt einen typischerweise mit Datenkompression (2:1) zu erreichenden Wert dar. Theoretisch könnten mit diesen Laufwerken bis zu 16 GB Daten gespeichert werden. In der Praxis erweisen sich diese rechnerisch ermittelten Maximalwerte aber als nicht realistisch.

Laufwerke, die im DDS-3-Format aufzeichnen, können mit einer Datentransferrate von 2 MB/s bis zu 24 GB auf einem 125 m Band aufzeichnen. Der DDS-4-Standard bietet mit

Kompression Kapazitäten von bis zu 40 GB (150 m Band) bei einer Datentransferrate von bis zu 6 MB/s. Die Schreib- und Lesekompatibilität zu DDS-2 und DDS-3 ist gewährleistet. Die DDS-3-Laufwerke verfügen über spezielle Features, die wesentliche Voraussetzungen für eine fehlerlose Sicherung darstellen.

Eine wesentliche Fehlerquelle ist die Verschmutzung der Kopftrommel. Der eingebaute Head Cleaner sorgt in 15-minütigem Abstand automatisch für die Reinigung der Köpfe. In Kombination mit einem Reinigungsband wird die Funktion des Laufwerks über Jahre gewährleistet.

Ist jedoch z. B. ein eingesetztes Band beschädigt, zu alt und nicht mehr zu gebrauchen oder ein Reinigungsband defekt, erhält der Netzwerkadministrator sofort eine Meldung. Dieses Feature heißt TapeAlert und ist eine neue von HP entwickelte Firmware, die Probleme bei Datenträgern netzwerkweit diagnostiziert. Außerdem überwacht TapeAlert permanent den Zustand des Laufwerks und der Medien während des Backups.

Mit Hilfe der Time-Tracking-Funktion wird der Lesekopf immer an der Mitte der Datenspur ausgerichtet. Dadurch wird gewährleistet, dass auch Bänder, die mit DAT-Laufwerken anderer Hersteller beschrieben wurden, zuverlässig gelesen werden können.

Ein neues Feature bei HP DAT-Laufwerken ist das One Button Disaster Recovery. Mittels geeigneter Software können bootfähige Kassetten erzeugt werden, mit welchen dann in Notfall das System ohne zusätzliche Floppies oder CD-ROMS wiederhergestellt werden kann.

Nähere Beschreibungen der Laufwerke und Bänder sind im Kapitel DAT-Subsysteme zu finden.

Stacker/Jukeboxen

Sowohl für LTO, DLT-, AIT-, Exabyte- als auch für DAT-Laufwerke gibt es automatische Kassettenwechsler. Die einfacheren Modelle erlauben nur ein sequenzielles Wechseln der Kassetten. Die teureren Random-Access-Modelle benötigen normalerweise spezielle Software zum Betrieb der so genannten Jukeboxen. Die kleinsten Jukeboxen bzw. Kassettenwechsler sind für sechs Kassetten geeignet, die größeren Modelle können über 100 Kassetten aufnehmen. Mit solchen Jukeboxen können ohne Operatoreingriff Daten gesichert werden. Alle angegebenen Größen bezüglich Speicherkapazität und Datentransferrate sind allerdings immer rechnerische Größen, da die meisten Laufwerke mit Datenkompression arbeiten. Nähere Informationen zu den Produkten finden sich in den Kapiteln DLT-Libraries und DAT-Subsysteme.

Es empfiehlt sich, ausschließlich solche Kassetten einzusetzen, die zur Datensicherung hergestellt wurden. Diese Kassetten sind z. B. mit dem DDS-Siegel bei DAT-Laufwerken



und bei Exabyte-Laufwerken mit dem D-Eight-Siegel gekennzeichnet.

Wie bei allen Magnetbandlaufwerken sollten die Schreib-/Leseköpfe regelmäßig gereinigt werden. Allerdings sollten nur die vom Hersteller empfohlenen Reinigungskits verwendet werden. Nicht geeignete Reinigungsbänder können eine Beschädigung der Mechanik zur Folge haben. Empfohlen wird meistens, einen Reinigungsvorgang nach 30 GB bzw. mindestens einmal im Monat vorzunehmen.

4.4.6 114"-Magnetbandkassetten-Laufwerke

Die 1/4"-Kassetten werden beim serpentinenförmigen Aufzeichnungsverfahren mit hoher Geschwindigkeit in mehreren Durchläufen auf jeweils einer Spur parallel zum Rand des Magnetbandes beschrieben. Diese Serpentine muss auch beim Lesen der Daten durchlaufen werden.

1/4"-Magnetbandkassetten-Laufwerke arbeiten im standardisierten QIC-Format (Quarter Inch Cartridge) und zeichnen im streaming Mode auf. Ist die Übertragungsgeschwindigkeit eines Systems grösser als die Aufzeichnungsrate des Streamers, wird das Magnetband ohne Lücken beschrieben (streaming) und voll ausgenutzt. Ist der Datenpuffer des Streamers leer, fordert er vom System weitere Daten an.

Um das Band auch bei Systemen mit langsamerer Transferrate voll auszunutzen, wird es bei einer Datenpause abgebremst und an das Aufzeichnungsende zurückgesetzt. Der nächste Datenblock kann so ohne Lücke aufgezeichnet werden.

Ein Vorteil der QIC-Technologie gegenüber dem Helical-Scan-Verfahren ist, dass das Tape immer in seiner Cartridge bleibt und dadurch bei weitem länger hält.

4.4.7 112"-Magnetbandlaufwerke

1/2"-Magnetbandlaufwerke sind heute eigentlich veraltet, werden aber wegen ihrer weiten Verbreitung weiterverwendet, insbesondere für den Datenaustausch mit Mainframes. In der Zukunft werden sie jedoch sicher an Bedeutung verlieren, da neuere Entwicklungen mit wesentlich kleineren und kostengünstigeren Datenträgern zur Verfügung stehen. Ein 1/2"-Magnetband wird in der Regel mit neun Spuren beschrieben.

Auf einer Großen Magnetspule (730 m) lassen sich bei einer Schreibdichte von 800 bpi 23 MB, bei 1600 bpi 46 MB, bei 3200 bpi 92 MB und bei 6250 bpi 180 MB speichern. Diese Speicherkapazitäten sind im Vergleich zu anderen Magnetbandkassetten-Systemen, die auf einer Kassette 10 GB und mehr speichern können, eher bescheiden. Nachteil, neben der geringen Kapazität, sind die bei 1/2"-Laufwerken die langen Backup- und Restore-Zeiten und der Große Platzbedarf des Magnetbandlaufwerkes und der

Magnetbänder.

4.4.8 LTO-Laufwerke

Die Linear-Tape-Open-Technologie (LTO) wurde von Seagate, HP und IBM entwickelt. Diese Hersteller werden auch die ersten sein, die entsprechende Laufwerke anbieten werden. Zahllose andere Hersteller haben diese Technologie bereits lizenziert und werden ebenfalls entsprechende Laufwerke anbieten. Aufgrund der breiten Herstellerunterstützung dürfte sich LTO sehr schnell am Markt durchsetzen.

Das Kernstück des LTO-Aufzeichnungsformats besteht aus mehreren linearen Kanälen, die serpentinartig verlaufen. Die Daten werden in Spuren geschrieben, welche die gesamte Länge des Bandes beanspruchen.

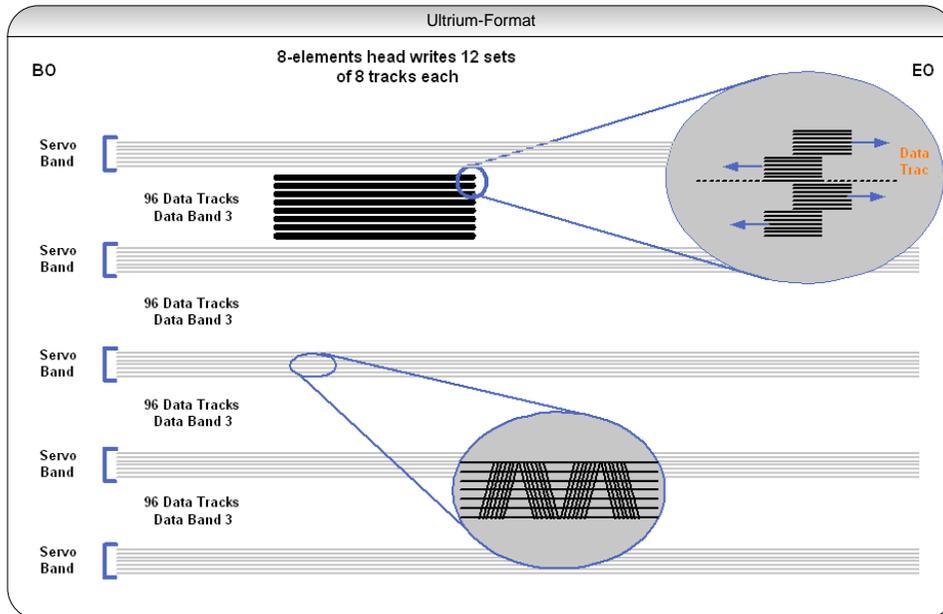
Es wurden zwei Standards entwickelt: Accelis und Ultrium. Von den beiden wurde allerdings nur Ultrium bisher produziert. Das Accelis-Format wurde für schnelle Zugriffe definiert. Das Accelis-Format benutzt zwei Bandrollen und beginnt in der Mitte des Bandes, auf Daten zuzugreifen, um die Zugriffszeit minimal zu halten.

Dadurch ist der Weg zum Anfang bzw. Ende des Bandes gleich. Der Vorteil dieses Prinzips kommt vor allem beim Schreiben oder Lesen von Teilen der Daten zum Tragen, beim Schreiben oder Lesen des kompletten Bandes ergibt sich kein Vorteil. Eine typische Anwendung ist HSM (Hierarchical Storage Management), wo sehr häufig nur einzelne Dateien vom Band gelesen werden müssen.

Beim Accelis-Format werden 256 Spuren in zwei Datenbereiche eingeteilt. Die erste Generation wird mit Datenkompression eine Kapazität von 50 GB mit einer Datentransferrate von maximal 40 MB/s bieten.

Das Ultrium-Format hingegen ist das optimale Medium für hohe Kapazitäten und mit einer hervorragender Betriebssicherheit in einem automatisierten oder Standalone-Umfeld; es verfügt über eine hervorragende Betriebssicherheit. Das Ultrium-Medium enthält eine Bandrolle und ist ideal für Backup-, Restore- und Archivierungsprogramme.





Das Ultrium-Format teilt 384 Spuren in vier Datenbereiche auf. Zwischen den Datenbereichen liegen die Servospuren für die Kopfpositionierung. Das Band wird serpetinenförmig mit jeweils acht Spuren parallel beschrieben. Die Daten werden von innen nach außen geschrieben, da die inneren Datenbereiche physikalisch am besten geschützt sind.

Die erste Generation wird mit Datenkompression eine Kapazität von 200 GB mit einer Datentransferrate von maximal 40 MB/s bieten.

Beide Kassettentypen enthalten ein kontaktloses Cartridge Memory (LTO-CM) mit 4 KB, in welchem Hersteller- und Benutzerinformationen abgespeichert werden. Für das Lesen bzw. Schreiben der Benutzerinformationen ist eine Unterstützung durch die Backupsoftware notwendig.

4.4.9 ADR_Laufwerke

Die ADR-Technologie (Advanced Digital Recording) wurde von Philips entwickelt und kommt in den Laufwerken von OnStream zum Einsatz. Die Daten werden in acht Spuren parallel aufgezeichnet. Zur genauen Positionierung des Kopfes befinden sich zwischen den Datenspuren Servo-Informationen.

Diese Servo-Informationen dienen gleichzeitig dazu, schlechte Bandstellen zu erkennen. ADR-Laufwerke haben eine variable Datenübertragungsrate von 0,5 bis 2 MB/s. Dadurch passt sich das Laufwerk der Datenrate des Systems an, und zeitintensive Neupositionierungen des Bandes können weitgehend vermieden werden. ADR-Laufwerke bieten mit Kompression eine Kapazität von bis zu 50 GB pro Kassette mit einer maximalen Datenübertragungsrate von 4 MB/s.

4.4.10 Ausblick

Wachsende Datenmengen und ein immer kleiner werdendes Zeitfenster für ein Backup kennzeichnen einen Teil der Anforderungen an die Backup-Technologie. Höhere Kapazitäten pro Band und immer schnellere Datentransferraten und Zugriffszeiten stehen im Vordergrund aller Neuentwicklungen.

Bei Unternehmen mit sehr hohen Datenmengen liegt die Entscheidung beim Anwender, ob er eine Library mit einem oder mehreren von den oben beschriebenen Laufwerken, die parallel Daten aufzeichnen, bevorzugt oder einem schnellen High-Speed-Device, wie z. B. dem neu entwickelten LTO.

Es wird auch in näherer Zukunft Neuentwicklungen im Bereich der Backup-Datenspeicher geben. Dabei kann es sich um Erweiterungen der Kapazität, der Datentransferraten oder um eine komplett neue Technologieentwicklung handeln. Ein Stillstand wird nicht eintreten, da die wachsenden Datenmengen diese Entwicklungen fordern.



4.5 Backup-Software

Ein Backup ist aufgrund des nicht anschließbaren Datenverlusts (menschliches Versagen, technisches Versagen, Sabotage oder Viren) unverzichtbar. Es ist zwar möglich, ein Backup ohne unterstützende Software zu fahren, jedoch ist dies bei größeren Datenmengen und bei Einsatz von Libraries fast nicht mehr realisierbar. Entsprechende Backup-Softwarepakete erleichtern den täglichen Backup und bieten viele Tools an, die auch eine sinnvolle Verwaltung der zu speichernden und gespeicherten Daten möglich machen (Archivierung und HSM).

Aus den geforderten Entwicklungen bei den Datenspeichern selbst resultiert auch eine ständige Überarbeitung und Erweiterung der unterschiedlichen Backup-Softwarepakete. Der Bedarf an Speicherkapazität wächst schneller als die Kapazität einzelner Medien. Da die Beschaffung von immer mehr Festplatten die Kosten explodieren lässt, muss immer mehr auf Archivierung - die Auslagerung von Daten auf preiswertere, aber langsamere Medien - zurückgegriffen werden. Dies führt andererseits zu einem hohen Administrationsaufwand.

HSM-Software (Hierarchical Storage Management) ist in der Lage, diese Administration selbständig zu leisten. Aufgrund von vorgegebenen Parametern wie Häufigkeit des Zugriffs, File-Größe, -Alter etc. werden Dateien gewichtet und nach Bedarf ausgelagert auf immer preiswertere/langsamere Medien, beispielsweise von Festplatten auf MO-Wechsler, von dort auf Tape-Libraries und weiter auf extern gelagerte Bänder. Im letzteren Fall wird bei Bedarf der Systemadministrator angewiesen, das entsprechende Band einzulegen.

Ein virtuelles File-System zeigt dem Anwender immer alle Dateien an, sowohl die tatsächlich auf der Festplatte vorhandenen als auch die ausgelagerten. Die virtuelle Kapazität ist dadurch unendlich. Beim Öffnen einer Datei wird diese zuerst auf die Festplatte zurückgeschrieben. Der Anwender bemerkt lediglich die entsprechend langsamere Zugriffszeit.

Mag diese langsamere Zugriffszeit manchen Anwender erschrecken - im schlimmsten Fall der Auslagerung auf externe Medien kann die Wartezeit eine halbe Stunde und mehr betragen - so mag die Überlegung trösten, dass auf 80 % aller Daten weniger als einmal pro Monat zugegriffen wird. Nicht einmal 5 % aller Daten werden öfter als einmal pro Woche verwendet.

4.6 Netzwerk-Storage-Server

Die Befriedigung des ständig wachsenden Speicherbedarfs in PC- und Workstation-Netzen erfordert den Einsatz von immer mehr File-Servern. Früher bedeutete das den Ankauf weiterer PCs und Workstations. Viel einfacher und auch preisgünstiger ist der Einsatz von Technologien, die als Network Attached Storage bezeichnet werden. Hier wird - ähnlich einem Communication- oder Print-Server - ein Netzwerk-Device speziell für eine einzige Aufgabe konstruiert, in diesem Fall für den Zugriff auf Speichermedien wie Festplatten und CD-ROM.

Die Vorteile dieser Technologie liegen auf der Hand:

Vereinfachung der Installation: Da der Netzwerk-Storage-Server nur als File-Server arbeitet, beschränkt sich die Verwaltung auf das Setzen von Netzwerkadressen und die Freigabe des Speicherplatzes für die Anwender. Dieser steht dann sofort allen autorisierten Benutzern im Netzwerk zur Verfügung.

Vereinfachung der Pflege: Da die Storage-Server mit standardisierten Protokollen arbeiten, gibt es keinen Aufwand beim Versionswechsel von Betriebssystemen.

Einfache Upgrades und Änderungen der Konfiguration: Durch den Einsatz weiterer Storage-Server kann der Speicherplatz problemlos erweitert oder umkonfiguriert werden. Flexibilität: Netzwerk-Storage-Server sind durch ihre Protokollvielfalt oft auch ideal für gemischte Netze, die beispielsweise zum Teil unter Windows NT laufen, zum Teil unter Unix oder gar NetWare.

Alle Daten sind in jeder der definierten Betriebssystemumgebungen verfügbar, als ob sie auf einem entsprechenden Server im Netz liegen würden. Der Zugriff auf die Daten erfolgt dabei mit den jeweils plattformtypischen Verfahren. Aus Anwendersicht sind alle Dateien dann verfügbar wie auf einem File-Server des eigenen Betriebssystems.

Nähere Informationen zu den Produkten sind im Kapitel transtec 3800 Netzwerk-Storage-Server zu finden.





5. Arbeitsspeicher

Nicht nur die Rechenleistung der CPU eines Rechners ist für die Performance ausschlaggebend, sondern auch der Arbeitsspeicher. Neue Technologien, schnellere Chips und verschiedene Bauarten machen es immer schwieriger, das richtige Speichermodul für den jeweiligen Rechner zu finden. Einige typische Begriffe sind in diesem Kapitel beschrieben.

5.1 Speichertechnologien

Prinzipiell kann man zwischen statischen, dynamischen und nicht flüchtigen Speichertechnologien unterscheiden.

5.1.1 Nicht flüchtige Speicher

Allen nicht flüchtigen Speichern ist gemeinsam, dass sie ihren Inhalt, also die abgespeicherten Daten, auch dann behalten, wenn die Betriebsspannung abgeschaltet wird. Als Beispiele seien hier EEPROMs und die zu dieser Gruppe gehörenden Flash-Speicher genannt. EEPROM, EIPROM: Electrically Erasable Programmable Read- Only Memory

Als EEPROM werden sämtliche nicht flüchtigen Speicher bezeichnet, deren Inhalt auf elektrischem Wege (und nicht z.B. durch Bestrahlung mit UV-Licht wie bei seinem Vorgänger, dem EPROM) verändert bzw. gelöscht werden kann. Es gibt mehrere Architekturen, die sich durch unterschiedliche elektrische Eigenschaften unterscheiden. EEPROMs finden sich z.B. auf diversen Speichermodulen, wo die jeweiligen Moduleigenschaften (Betriebsspannung, Zugriffszeiten, Bauaufbau, Fehlerkorrektur usw. bis hin zum Hersteller) in codierter Form abgespeichert sind. (z.B. SPDs auf SDRAM DIMMs)

Flash Memory

Flash-Speicher sind dadurch gekennzeichnet, dass einzelne Bytes adressiert und ausgelesen, Schreib- und Löschvorgänge aber nur blockweise erfolgen können. Die Lese-Zugriffszeiten betragen etwa das Doppelte von dynamischen Speichern und liegen derzeit bei etwa 100ns. Die Anzahl der Programmier- und Löschzyklen ist begrenzt und liegt etwa bei 100.000.

Im Allgemeinen wird ein Datenerhalt über einen Zeitraum von 10 Jahren garantiert. Flash Memory ist u.a. als SIMM, PC-Card (PCMCIA), Compact Flash (CF) Card, Miniature Card (MC) und Solid State Floppy Disc Card (SSFDC) erhältlich. Unabhängig vom Äußeren gibt es zwei Haupttypen von Flash-Speichermodulen: Linear Flash und ATA Flash. Linear

Flash Module besitzen einen „linearen“ Adressraum, wobei jede beliebige Adresse von außen direkt angesprochen werden kann. Im Gegensatz hierzu findet bei ATA-Flashkarten intern eine Adressumsetzung statt, so dass diese Variante mehr wie eine Festplatte angesprochen werden kann, was u.U. die Treiberprogrammierung vereinfacht. Flash-Module werden z.B. in Notebooks, Network-Routern, Druckern, PDAs und Digitalkameras als Massen- oder Programmspeicher verwendet.

5.1.2 Dynamische Speicher

DRAM: Dynamic Random Access Memory DRAM ist ein dynamischer Speicher mit wahlfreiem Zugriff. Dieser Speichertyp wird im Allgemeinen als Hauptspeicher eingesetzt. Dynamische Speicher sind gekennzeichnet durch die Speicherung der Information in einem Kondensator, der ähnlich wie ein Akku Energie aufnehmen und eine gewisse Zeit halten kann. Soll z.B. eine logische Eins gespeichert werden, wird dieser Kondensator aufgeladen, bei einer logischen Null entladen. Die Kondensatoren sind in einer Matrix aus Reihen und Spalten angeordnet. Um die Chips mechanisch klein zu halten und um Anschlüsse und damit Kosten zu sparen, erfolgt die elektrische Ansteuerung dieser Bausteine in zwei Stufen: Die Adresse eines Datums wird entsprechend der Matrix aufgeteilt in eine Reihen(Row-) Adresse und eine Spalten- (Column-) Adresse, die nacheinander über die gleichen Anschlüsse am Chip übermittelt werden. Der Vorteil dieser Technologie ist, dass sie relativ preiswert und mit Großen Dichten hergestellt werden kann. Der Nachteil ist, dass der Kondensator nicht ideal produziert werden kann: Wiederum ähnlich einem Akku, der lange Zeit nicht benutzt wird, entlädt sich dieser Kondensator. Um zu verhindern, dass die Daten unbrauchbar werden, müssen sie in regelmäßigen Abständen aufgefrischt werden (Refresh). Es gibt mehrere Weiterentwicklungen dieser grundlegenden Architektur, die kurz angesprochen werden sollen:

FPM: Fast Page Mode

Speicherbausteine mit Fast Page Mode sind eine Weiterentwicklung der „Standard“-DRAM Speicher, die durch eine besondere Ansteuermöglichkeit die technologiebedingten Verzögerungszeiten bei bestimmten Anwendungen beschleunigen. Meistens werden innerhalb von Computerprogrammen zusammenhängende Speicherinhalte vom Prozessor bearbeitet. Bei einem Zugriff auf eine Speicherbank wird normalerweise zuerst die Reihen und dann die Spaltenadresse übertragen. Bei aufeinander folgenden Speicheradressen ändert sich hingegen nur die Spaltenadresse, weil die aufeinander folgenden Daten in der gleichen Reihe (in der gleichen „page“) liegen: Ein erneutes Übertragen der nicht veränderten Reihenadresse ist eigentlich unnötig. Diesen Umstand macht sich der Fast Page Mode zunutze. Dabei werden nur beim ersten Zugriff die Reihen- und die Spaltenadressen übertragen, bei den darauf folgenden Zugriffen nur noch die Spaltenadressen, so dass die Zykluszeit bis zum Anlegen der Daten an den Ausgängen der Speicherbank verkürzt wird. Dieser Modus



muss natürlich vom verwendeten System und dessen Chipsatz unterstützt werden.

EDO: Extended Data Output

Speicherbausteine mit EDO stellen eine Weiterentwicklung gegenüber den FPM-Speichern dar, wo ebenfalls durch bestimmte Ansteuertechniken der Speicherzugriff beschleunigt wird. Bei FPM-Speichern wird das elektrische Signal der Datenleitungen gelöscht (nicht zu verwechseln mit dem Inhalt der Speicherzelle, dieser bleibt erhalten!), wenn eine neue Adressinformation angelegt wird. Da die Weiterverarbeitung der Daten eine gewisse Zeitspanne in Anspruch nimmt, gibt es einen Zeitraum, in dem der Speicher „stillgehalten“ werden muss, damit die an den Datenleitungen anliegenden elektrischen Signale aufgenommen und weiterverarbeitet werden können. Bei EDO-Speichern ist die Ausgangsstufe so gestaltet, dass anliegende Informationen auch dann beibehalten werden, wenn eine neue Adresse übertragen wird. Auf diese Weise kann simultan das anliegende Datenwort verarbeitet und die nächste angeforderte Adresse in den Speicherbaustein geladen werden. Auch hierdurch werden die Zykluszeiten verkürzt.

BEDO: Burst Extended Data Output

Als eine Weiterentwicklung der EDO Speichermodule gilt der BEDO als der letzter asynchrone DRAM. Durch sein zeitgleiches Erscheinen mit den SDRAM Modulen hatte er nie eine Gelegenheit, sich auf dem Markt durchzusetzen. Er ist durch einen zusätzlichen BurstModus gekennzeichnet. Nach einer Adressübermittlung gibt das Modul den Zelleninhalt wie bei einem EDO-RAM aus, hängt aber die folgenden drei Zelleninhalte mit einem Taktzyklus von einem Takt pro Wert an.

SDRAM: Synchronous Dynamic Random Access Memory

Ähnlich wie FPM und EDO stellt die SDRAM-Technologie eine Weiterentwicklung bereits vorhandener Speicherarchitekturen bzw. deren Zugriffsmodi dar. Anders als bei FPM oder EDO ist die SDRAM-Technologie allerdings nicht rückwärtskompatibel, d.h. SDRAM-Speicher können nur in solchen Rechnersystemen eingesetzt werden, die diese Technologie auch ausdrücklich unterstützen. Die Weiterentwicklung bei SDRAM stellt nichts anderes dar als die Verlagerung eines Teils des Memory-Controllers auf den Speicherchip. Dieser Schritt ist in etwa vergleichbar mit der Einführung von IDE-Festplatten (SCSI Platten sind hier vielleicht ein besseres Beispiel), die ja auch den auf ihre speziellen Bedürfnisse zugeschnittenen Controller mit im Gehäuse eingebaut haben. Wie auch die FPM- oder EDO-Zugriffsarten kann die SDRAM-Technologie ihre Stärken bei im Adressraum aufeinander folgenden Daten ausspielen. Der typische SDRAM-Zugriff erfolgt, wie bei allen DRAM-Typen, mit der aufeinander folgenden Übermittlung der Reihen- und der Spaltenadresse. Anders als bei bisherigen Technologien erfolgt während dieser Adressierung auch eine „Befehlsübermittlung“ an das SDRAM, wobei auf dem Speicherchip je nach Befehl festgelegte Abläufe in Gang gesetzt werden. Ein typischer Befehl könnte z.B. etwa lauten: Auslesen der Adresse X und der drei darauf

folgenden Adressen. In diesem Fall wird mit dem Befehl zusammen der Wert für die Startadresse X übermittelt und ohne weiteres Zutun werden die Inhalte der vier aufeinander folgenden Adressen übermittelt. Da der Zeitpunkt, zu dem die angeforderten Daten Gültigkeit besitzen, feststehen muss, werden SDRAM-Bausteine mit einem Taktsignal versorgt, mit dem alle Vorgänge synchronisiert werden. Die Verwendung von SDRAM-Speichern bringt dann Geschwindigkeitsvorteile, wenn große Datenmengen blockweise übertragen werden müssen, z.B. bei Großen Grafiken.

DDR SDRAM: Double Data Rate SDRAM

Der DDR SDRAM, meist auch SDRAM II genannt, ist eine schnellere Version des SDRAMs. Er wurde dahingehend weiterentwickelt, dass er Daten auf der steigenden und auf der abfallenden Flanke der System-Clock lesen kann und somit die Transferrate des Speichers verdoppelt. Die maximale Transferrate dieser Technologie liegt bei 1 GB/s.

Statische Speicher werden aufgrund ihrer Schnelligkeit als Cache-Speicher eingesetzt. Im Gegensatz zu den dynamischen Speichern brauchen sie keinen Refresh (Auffrischung) des Speicherinhaltes. Ein statischer Speicher arbeitet pro Speicherzelle mit einer aus mehreren Bauelementen bestehenden Schaltung, die - ausgehend vom zu speichernden Datum - einen bestimmten Zustand einnimmt und sich dann selbst verriegelt, so dass eine Zustandsänderung nur von außen vorgenommen werden kann. Ein statischer Speicher verliert seinen Dateninhalt erst, wenn die Versorgungsspannung zusammenbricht.

RDRAM: Rambus DRAM

Aufgrund des komplexeren Aufbaus der Speicherzelle können statische Speicher nur mit geringeren Dichten gebaut werden als dynamische Speicher. Außerdem sind sie - bei vergleichbarer Speicherkapazität - wesentlich teurer als dynamische Speicher.

Rambus DRAM basiert auf einer von der Firma Rambus Inc. entwickelten komplett neuen Technologie. Durch die grundlegende Überarbeitung und Neudefinition seiner inneren Struktur wie Leiterbahnlängen, Pin-Kapazitäten und Spannungsschwankungen ist der RDRAM in der Lage, sehr hohen Leistungsansprüchen gerecht zu werden. Der Speicher wird auf der steigenden und auf der abfallenden Flanke der System-Clock angesprochen. Ein Einkanal-Rambus-Speicher liefert mit 1,6 GB/s eine um den Faktor 3 höhere Leistung als ein 64-bit-100-MHz-SDRAM-Modul. Der Hauptvorteil der Rambus-Technologie liegt darin, dass 2 Rambus Kanäle (demnächst auch 4 Kanäle) parallel genutzt werden können. Somit sind mit 2 Kanälen eine Bandbreite von 3,2 GB/s und mit 4 Kanälen eine Bandbreite von 6,4 GB/s erreichbar.





5.2 Modulbauformen

Warum Module? Moderne Rechnersysteme verlangen nach Speichergrößen, die in Datenbreite (also der Anzahl der verwendeten Datenbits) und Adressraumtiefe (also der Anzahl der Datenwörter, die im Speicher untergebracht werden können) nicht mit einem einzelnen Speicherchip realisiert werden können. Daher werden aus einzelnen Speicherchips Module gebaut, die elektrisch quasi wie ein großer Chip angesteuert werden können. Man unterscheidet zwischen folgenden verbreitet eingesetzten Bauformen:

SIMM: Single Inline Memory Module

SIMMs haben auf beiden Seiten der Platine Kontaktflächen, die jedoch miteinander verbunden sind. Demnach hat ein 72-Pin-SIMM 144 Kontaktflächen, von denen jedoch nur 72 elektrisch relevant sind.

DIMM: Dual Inline Memory Module

Ein DIMM hat auf beiden Seiten der Platine Kontaktflächen, wobei hier allerdings gegenüberliegende Kontakte elektrisch voneinander isoliert sind. Dadurch steht bei gleicher Modulgröße eine größere Anzahl von elektrischen Anschlüssen (= doppelt so viele wie bei einem vergleichbaren SIMM) zur Verfügung, so dass auch eine größere Anzahl von Datenbits oder ein größerer Adressraum angesprochen werden kann. Darüber hinaus wird die Anzahl von Anschlüssen für Betriebsspannungen und Steuersignalen vergrößert, was Vorteile hinsichtlich des Designs der Platine und somit der elektrischen Eigenschaften des Modules mit sich bringt. DIM-Module sind mittlerweile Standard im PC- und Workstation Bereich.

PC-100

Die ersten verfügbaren SDRAM Chips und -Module wurden mit einer Taktfrequenz von 66 MHz betrieben - eine Geschwindigkeit, bei der EDO Speicher in etwa auch betrieben werden können. Von Intel wurden allerdings bald Versuche unternommen, diese Taktfrequenz und damit die Zugriffsgeschwindigkeit zu erhöhen. Diese Versuche resultierten in der sog. PC-100-Norm, die von einer Memory-Taktfrequenz von 100 MHz ausgeht, und mit der Intel Spezifikationen hinsichtlich der zu verwendenden Speicherchips, des Aufbaus der Platine, der Topologie der Leiterbahnen usw. veröffentlichte.

Die geringfügige Erhöhung der Taktfrequenz um den Faktor 1,5 verursacht allerdings eine weitaus größere Zunahme der technologischen Probleme, die dieser Frequenzbereich mit sich bringt. So müssen PC-100 taugliche Speichermodule mit einer

vielfach größeren Genauigkeit entwickelt und gefertigt werden als vergleichbare bisherige Modelle. Mittlerweile sind von mehreren Herstellern Chipsätze auf dem Markt, die 100 MHz Bustakt unterstützen. In diesem Zusammenhang ist jedoch wichtig, dass auch die verwendeten Prozessoren dafür ausgelegt sein müssen.

PC-133

Wie auch in der Prozessorweiterentwicklung immer höhere Taktraten erzielt werden, bleibt die Speicherentwicklung auch nicht stehen. Kontinuierliche qualitative Verbesserungen haben es ermöglicht, die PC-133-Norm zu verabschieden. Die Speicher haben die gleiche Bauform wie die PC-100-Module, werden jedoch mit 133 MHz Takt betrieben.

5.3 Begriffe rund um den Speicher

Cache

Ein Cache ist ein relativ kleiner Hochgeschwindigkeitsspeicher, üblicherweise SRAM, der häufig benötigte Daten zwischen der CPU und dem Hauptspeicher puffert. Die CPU kann auf Daten im Cache sehr viel schneller zugreifen als auf Daten aus dem Hauptspeicher. Ein kleiner Cache-Speicher kann daher die Performance eines Computers ohne Große zusätzliche Kosten erheblich verbessern.

Bei Cache wird -je nach Position des Speichers im Datenstrom - zwischen verschiedenen Levels unterschieden.

Level 0 Cache: Entkoppelt den Datenstrom der unterschiedlichen Recheneinheiten innerhalb der CPU. Seine Größe liegt bei etwa 1 Byte bis 128 Byte.

Level 1 Cache: Entkoppelt den Datenstrom innerhalb der CPU von der Außenwelt, Größe von wenigen Bytes (128) bis zu mehreren KBs.

Level 2 Cache: Entkoppelt den Datenstrom der CPU vom Memory Bus, an dem der Hauptspeicher angeschlossen ist. Größe von 256 KBs bis zu mehreren MBs.

Level 3 Cache: Entkoppelt bei Mehrprozessorsystemen den separaten Systembus vom Memory Bus.

Parity/Non-Parity

Durch äußere Einflüsse (elektromagnetische Felder, Spannungsschwankungen, radioaktive Strahlung (natürliche Höhenstrahlung, etc.) können einzelne Datenbits



„umkippen“: Aus einer logischen Null wird eine Eins und umgekehrt. Dadurch werden die gespeicherten Daten verändert.

Non-Parity-Module speichern nur Daten und bieten keine Fehlerfeststellung. Parity-Module hingegen speichern Daten- und Prüfsummen-Informationen. Dies geschieht derart, dass bei einer geraden Anzahl von gesetzten bits das Parity-Bit ebenfalls gesetzt ist: Bei einer ungeraden Anzahl von gesetzten bits ist es gelöscht.

Mit Hilfe der Parity Technik werden Ein-bit-Fehler erkannt. Da keine Fehlerkorrektur stattfindet, werden die meisten Systeme beim Auftreten eines Parity-Fehlers mit einer Fehlermeldung angehalten. Normalerweise wird ein Parity-Bit pro Byte (8 Bit) Daten gespeichert. Vorsicht: Wenn durch äußere Einflüsse zwei bits in einem Datenwort ihren Inhalt geändert haben, bleibt die Prüfsumme gleich und der Fehler bleibt unbemerkt! Die Gefahr, dass so etwas passiert, ist allerdings sehr gering.

ECC: Error Checking and Correcting

Das ECC-Verfahren ermöglicht, Ein- und Zwei-Bit-Fehler zu erkennen. Ein-Bit-Fehler können darüber hinaus sogar korrigiert werden. Gelegentlich wird das zugrunde liegende Verfahren auch als EDC, Error Detection and Correction, bezeichnet. Mit Hilfe entsprechender Algorithmen werden blockweise Prüfsummen (ähnlich wie beim CRC-Verfahren) gebildet und in eigenen Speicherbereichen abgelegt. Anhand dieser Prüfsummen können einzelne Bitfehler erkannt und korrigiert werden. Der Software-Anwender merkt wie bei der Fehlerkorrektur der Audio-CD nichts von diesem Vorgang.

Memorybus

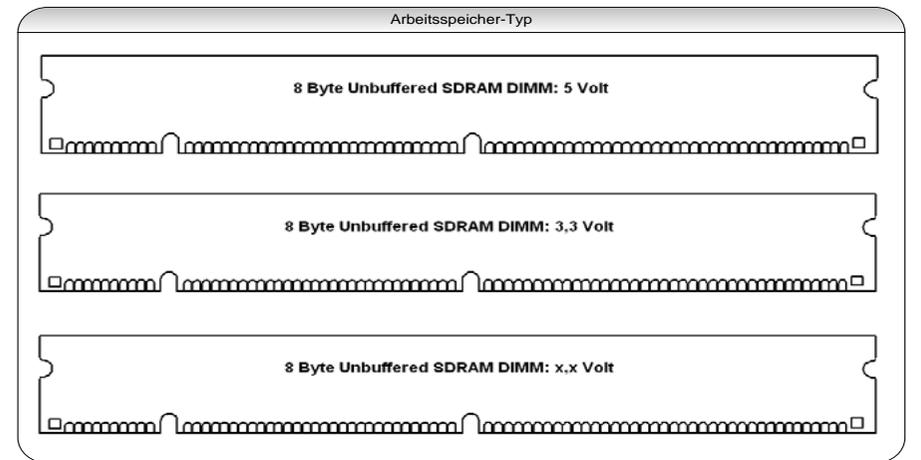
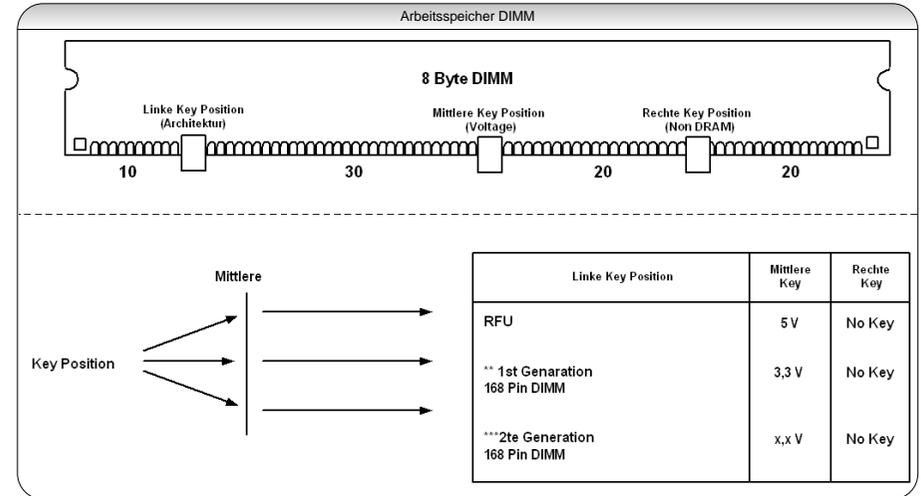
Der Memorybus ist der Systembus zwischen I/O und CPU, der mit Hilfe des Chipsets den Hauptspeicher (Memory) ansteuert. Er besteht aus dem Adressbus und dem Datenbus.

SOJ: Small Outline J-Lead (Chip).

TSOP: Thin Small Outline Package (Chips).

Welcher Speichertyp für welchen Rechner?

Prinzipiell kommen die Vorgaben, welchen Speichertyp man verwenden kann, vom Hardwarehersteller, der den Speicher anhand seiner System-Spezifikationen festlegt. Server sollten nach Möglichkeit immer mit ECC ausgestattet sein.



Innerhalb einer Speicherbank müssen die Module identisch sein. Die verschiedenen Bänke können jedoch je nach Systemvorgaben im Allgemeinen mit Speichermodulen unterschiedlicher Kapazität und Hersteller bestückt werden. Im Zweifelsfall sollte allerdings das Handbuch des Systems zu Rate gezogen werden.





6. Netzwerke LAN

Grundlagen Netzwerke

Um Daten zwischen Rechnersystemen zu transportieren, braucht man Hardware und Software. Zuerst müssen die beteiligten Systeme durch ein Datentransportmedium, in der Regel ein Kabel, miteinander verbunden sein. Doch das passende Kabel allein genügt keinesfalls. Es muss auch definiert sein, wie die Rechner miteinander kommunizieren. Beispielsweise welche elektrische Spannung am Kabel welchem Signal entspricht, wie Daten zu Paketen zusammengefasst werden, wie sichergestellt wird, dass alle Pakete richtig beim Empfänger ankommen und im Fehlerfall neu gesendet werden, wie auf Basis dieser Pakete dann Files transferiert werden und wie Anwendungen auf anderen Rechnern auch genutzt werden können.

6.1 ISO/OSI-Modell

Das ISO/OSI (International Standardization Organisation/ Open Systems Interconnection) 7-Schichten-Modell, mit dem die OSI-Protokolle spezifiziert werden, wird sehr häufig herangezogen, um den Aufbau von Netzwerksystemen und die darin verwendeten Netzwerkprotokolle zu beschreiben. Das liegt zum einen an dem klaren Aufbau der Funktionen in sieben Schichten, zum anderen ist es ein offizieller Standard, der auch für zukünftige Entwicklungen offen ist. In diesem Zusammenhang soll das ISO/OSI-Modell hier kurz erläutert werden.

Das ISO-7-Schichten-Modell (siehe Schaubild) definiert in jeder Schicht das Protokoll, mit dem beteiligte Rechner kommunizieren.

Dabei greifen Dienste der höheren Schicht jeweils auf die nächstniedrigere zurück. Die Schichten sind:

- **Schicht 1: Bit-Übertragungsschicht (unterste Schicht)**
Transparente Übertragung von Bit-Sequenzen über ein beliebiges Medium, Unterstützung unterschiedlicher Übertragungsarten, keine explizite Fehlerbehandlung.
- **Schicht 2: Sicherungsschicht**
Aufbau einer fehlerfreien Verbindung zwischen Endsystem und Netzzugang, Zusammenfassung der Daten in Pakete, Paketsynchronisation, Fehlererkennung und Korrektur.
- **Schicht 3: Vermittlungsschicht**
Anwahl und Steuerung des Transportnetzes, Wegewahl (Routing),

Vermittlung, Kopplung unterschiedlicher Transportnetze, Multiplexing eines physischen Netzzuganges.

- **Schicht 4: Transportschicht**
Aufbau und Unterhaltung einer (virtuellen) Verbindung zwischen zwei Endsystemen (end-to-end), Bereitstellung eines netzunabhängigen Transportmechanismus, Adressierung eines Endteilnehmers.
- **Schicht 5. Kommunikationssteuerungsschicht**
Einrichtung und Steuerung von Sitzungen, Zugangskontrolle, Definition von Aufsetzpunkten.
- **Schicht 6: Darstellungsschicht**
Globale einheitliche Informationsdarstellung und Interpretation, Verschlüsselung, Datenkompression.
- **Schicht 7: Anwendungsschicht**
Spezifische Anwendungen (Dateitransfer, Jobtransfer, Nachrichtensysteme, verteilte Datenbanken etc.).



6.2 Topologien

Die Topologie eines Netzwerkes beschreibt die physikalische Verbindung von Netzwerkknoten. In der Regel unterscheidet man zwischen vier Grundtypen.

Netzwerke sind jedoch nicht auf eine Topologie begrenzt: Je grösser ein Netz ist, desto wahrscheinlicher ist es, dass mehrere Topologien miteinander verbunden sind.

Bus:

Bei der Bustopologie kommunizieren die Netzwerkstationen über ein gemeinsames Kabel. Ein typischer Vertreter dieser Topologie ist das ThickWire-Kabel, das vor allem früher bei Ethernet-Netzen zum Einsatz kam.

Stern:

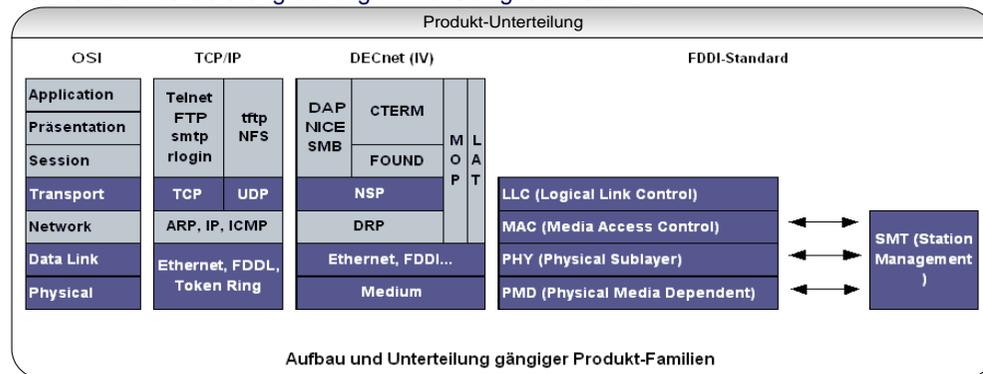
Von einer Sterntopologie spricht man, wenn von einem zentralen Punkt (Hub, Konzentrator) aus eine Punkt-zu-Punkt-Verbindung mit den einzelnen Netzwerkknoten besteht. Als Beispiel kann hier ein Ethernet TwistedPair Hub aufgeführt werden, an dem alle Netzwerkknoten angeschlossen sind.

Ring:

Wie der Name schon sagt, ist bei dieser Topologie die Verkabelung, mit der die einzelnen Netzwerkknoten miteinander verbunden werden, als Ring ausgeführt. Typische Vertreter dieser Topologie sind TokenRing- und FDDI-Netze.

Baum:

Eine Baumstruktur wird z.B. erreicht, indem einzelne Hubs oder Konzentratoren über Punkt-zu-Punkt-Verbindungen kaskadiert werden. Die Netzwerkknoten werden dabei an nicht für die Kaskadierung benötigten Ports angeschlossen.





6.3 Netzwerkprotokolle

Es gibt eine Vielzahl von Netzwerkprotokollen, die die unterschiedlichsten Aufgaben in der Kommunikation zwischen Netzwerkknoten übernehmen. Wenn von Netzwerkprotokollen die Rede ist, wird im Allgemeinen eine ganze Protokollfamilie angesprochen und nicht ein einzelnes Protokoll. Eine Auswahl der verbreitetsten Protokolle soll hier aus der Fülle von Netzwerkprotokollen aufgeführt werden.

Netzwerkprotokolle können in routbare und nicht routbare eingeteilt werden. Um ein Netzwerkprotokoll routen zu können, muss es über eine Layer 3-Netzwerkadresse verfügen. Zu den routbaren Protokollen gehören z.B. IP, IPX, OSI, AppleTalk und DECnet. Nicht routbar sind z.B. LAT, NetBEUI und NetBIOS.

6.3.1 TCP/IP

Das vom amerikanischen Verteidigungsministerium definierte TCP/IP (Transmission Control Protocol/ Internet Protocol) ist ein Protokoll, das auf jeder wichtigen Rechnerplattform verfügbar ist. Es wurde nicht für ein spezielles Nachrichtentransportsystem konzipiert wie z.B. ein LAN-Protokoll, sondern für den Einsatz auf unterschiedlichen Medien und Rechnern. Damit ist TCP/IP das Netzwerkprotokoll zur Vernetzung von heterogenen Systemen. Es lassen sich z.B. Rechner vernetzen, die als Betriebssystem Unix (bzw. seine Varianten SunOS, Digital UNIX, HP-UX, AIX, Linux), OpenVMS, DOS oder Windows einsetzen. Auf das TCP/IP-Protokoll setzen eine Reihe von Applikationen auf, die normalerweise unter dem Obertitel des Protokolls gemeint werden: z.B. ftp für den Filetransfer, telnet und rlogin für Remote Control bzw. Remote Login, electronic Mail, Webbrowser etc.

6.3.2 OSI

Als Alternative zu TCP/IP gibt es das standardisierte Netzwerkprotokoll OSI (Open Systems Interconnection) zur Vernetzung von heterogenen Netzwerken. OSI ist nicht sehr verbreitet. Dies liegt daran, dass TCP/IP schon lange auf den meisten Rechnerplattformen zur Verfügung steht und daher sehr stabil läuft. Außerdem sind wenige Anwender bereit, die zeitaufwendige und teure Umstellung auf ein anderes Netzwerkprotokoll zu riskieren. Auch ist die Zahl der verfügbaren OSI-Anwendungen noch unbefriedigend.

Wie TCP/IP besteht auch OSI aus mehreren Protokollen. OSI hat sich als Netzwerkprotokoll nicht durchgesetzt, obwohl es von einigen wenigen Herstellern noch unterstützt wird. Einzelne Teile des OSI-Stacks, wie beispielsweise X.400 Mailing und X.500 Directory Services, sind inzwischen recht weit verbreitet, greifen aber auf den unteren Schichten meist auf Protokolle des TCP/IP-Stacks zurück.

6.3.3 IPX/SPX

IPX (Internetwork Packet eXchange) ist das klassische Netzwerkprotokoll des Netzwerkbetriebssystems NetWare von NOVELL. Das Protokoll ist routbar und wird daher auch von vielen Multiprotokoll-Routern unterstützt. Mit den NetWare-Versionen ab 4.x und IntranetWare hat NOVELL den Wandel zu IP als Default-Protokoll vollzogen.

6.3.4 NetBIOS

NetBIOS ist ein von IBM entwickeltes Netzwerkprotokoll zur Peer-to-Peer-Kommunikation zwischen PCs. Der OS/2 LAN Server unterstützt z.B. dieses Protokoll. NetBIOS-Netze sind einfach zu managen, solange sie auf Workgroupgröße begrenzt bleiben. Da NetBIOS viele Broadcasts generiert, führt es zu einer erheblichen Reduzierung der Bandbreite, wenn über WAN-Verbindungen kommuniziert wird. NetBIOS kann nicht geroutet werden, da es keinen Netzwerklayer hat, auf dem ein Router aufsetzen könnte.

6.3.5 NetBEUI

NetBEUI (NetBIOS Enhanced User Interface) ist ein Standardprotokoll zwischen PCs, das von einigen Netzwerkbetriebssystemen verwendet wird, um Point-to-Point-LANS aufzubauen. Dieses Protokoll sollte nur verwendet werden, wenn wenige PCs miteinander vernetzt werden sollen, da der administrative Aufwand erheblich ist. Denn jeder PC im Netz muss individuell konfiguriert werden bezüglich Zugriffsrechten und Diensten, die der Server zur Verfügung stellt. Domain Name Service (DNS), wie sie z.B. unter TCP/IP unterstützt werden, stehen nicht zur Verfügung. Windows 98 und Windows NT verwenden NetBEUI als Netzwerkprotokoll. In größeren Netzen sollte jedoch TCP/IP verwendet werden, das ebenfalls standardmäßig von Windows 98 und Windows NT unterstützt wird. Hier ist der Verwaltungsaufwand geringer, und wenn Internetanwendungen (E-Mail, Webbrowser) eingesetzt werden sollen, ist TCP/IP zwingend erforderlich.

6.3.6 DECnet

DECnet ist eine Familie von Hard- und Softwareprodukten, die die Kommunikation zwischen Digital-Rechnern ermöglicht. DECnet ist nicht nur auf Digital-Rechner begrenzt, auch PCs können ins DECnet integriert werden. Da DECnet ein routbares Protokoll ist, ist der Anschluss an öffentliche Netzwerke ebenso möglich wie der Aufbau einer SNA-Verbindung. Interessant bei DECnet ist die Möglichkeit, verschiedene Verbindungen zu nutzen wie z.B. Ethernet und X.25. DECnet ist in seiner Leistungsfähigkeit vergleichbar mit TCP/IP. DECnet hat sich in Phasen entwickelt. Mit jeder neuen Phase kamen neue Features hinzu. Derzeit ist man bei Phase V angelangt. DECnet ist nach der DNA Architektur (Digital Network Architektur) aufgebaut und steht sehr nah am ISO/OSI-



Modell.

Digital's Versuch, DECnet auch zukünftig als Netzwerkprotokoll am Leben zu erhalten, indem alle DECnet-Produkte ISO/OSI-kompatibel gemacht werden, muss bezweifelt werden. Die wenigsten Anwender werden auf ISO/OSI umstellen, da praktisch keine Akzeptanz für dieses Protokoll am Markt vorhanden ist.

6.3.7 LAT

Das LAT-Protokoll (Local Area Transport-Protokoll) ist ein auf die Kommunikation zwischen Terminalserver und Digital-Rechner spezialisiertes Protokoll. Es bietet eine sehr effiziente Einbindung von Terminals und Druckern in eine Ethernet/Digital-Umgebung. Das Protokoll ist allerdings nicht routbar, daher ist der Einsatz in der Regel nur innerhalb eines LANS möglich.

6.3.8 AppleTalk

AppleTalk ist ein spezielles Protokoll, das zur Kommunikation insbesondere zwischen Macintosh-Rechnern und Peripheriegeräten, die dieses routbare Protokoll unterstützen, verwendet wird.

7. Ethernet

7.1 10 Mbit/s Ethernet

7.1.1 Zugriffsverfahren

Standard Ethernet, Fast Ethernet und Gigabit Ethernet verwenden das gleiche Zugriffsverfahren, daher ist die Migration vom Standard Ethernet zu den schnelleren Technologien sehr einfach zu realisieren, da nur wenige Änderungen beachtet werden müssen. Die Besonderheit vom Ethernet-Standard IEEE 802.3 ist die Nutzung eines einzelnen Kommunikationskanals durch viele Stationen, ohne dass eine einzelne Station den Zugang kontrolliert. Sobald eine Station Daten übertragen möchte, prüft sie, ob der Übertragungskanal frei ist (CS = Carrier Sense). Ist dies der Fall, beginnt die Station mit der Datenübertragung. Gleichzeitig hört die Station auf das Signal im Kabel. Hat eine andere Station (fast) gleichzeitig (MA = Multiple Access) mit dem Übertragen begonnen, wird eine Kollision von der sendenden Station festgestellt (CD = Collision Detect). Daraufhin werden von der sendenden Station für einen kurzen Zeitraum so genannte Jam-Signale übertragen, damit die anderen Stationen über die Kollision ebenfalls informiert werden und wissen, dass die übertragenen Daten ungültig sind. In einem solchen Fall warten die sendewilligen Stationen eine zufällige Zeitperiode ab und versuchen dann die Übertragung erneut. Dieses Zugangsverfahren wird mit CSMA/CD

bezeichnet.

7.1.2 Kabel

Kategorie	Anwendung	max. Kabellänge (m)	max. Datenrate (Mbit/s)	Bauart AWG24	Leiterwiderstand = 93,8 Ohm Wellenwiderstand (Ohm/- 15%)	max. Dämpfung (dB/km)	min. NEXT (dB)	Kategorie
1*	Telekommunikation							
2*	Low Speed LAN							
3	LAN zB. 10 BASE-T	100	10		100	22,3	54	bei 512 kHz
						25,6	43	bei 722 kHz
						55,8	41	bei 1 MHz
						85,3	32	bei 4 MHz
						98,4	26	bei 10 MHz
						131,2	23	bei 16 MHz
4	LAN zB. 16 Mbit / s Token-Ring	100	16		100	18,7	58	bei 722 kHz
						21,3	56	bei 1 MHz
						42,7	47	bei 4 MHz
						72,2	41	bei 10 MHz
						88,6	38	bei 16 MHz
						101,7	36	bei 20 MHz
5	Verlustarmes High Speed LAN zB. 100 BASE-T FDDI (TP-PMD)	100	100		100	18,1	64	bei 722 kHz
						20,7	62	bei 1 MHz
						42,7	53	bei 4 MHz
						65,5	47	bei 10 MHz
						82	44	bei 16 MHz
						91	42	bei 20 MHz
						118,1	40	bei 31,25 MHz
						170,1	35	bei 62,5 MHz
						219,8	32	bei 100 MHz

 = Standard

* = nicht mehr in TSB 36
spezifiziert





7.1.3 10BASE5, ThickWire

Das dicke gelbe ThickWire-Kabel ist der Urtyp des Ethernet-Kabels. Signale und Übertragungsgeschwindigkeit sind bei allen Kabeltypen prinzipiell gleich, die Konfigurationsregeln sind allerdings unterschiedlich.

Beim ThickWire-Kabel wird im einfachsten Konfigurationsfall die AUI-Buchse (Attachment Unit Interface) jeder Station mit einem Transceiver-Kabel und einem Transceiver an dieses gelbe Kabel angeschlossen.

Maximal 500 m darf ein solches Ethernet-Kabel lang sein, maximal 100 Transceiver können angeschlossen werden. Der Abstand zwischen zwei Transceivern muss 2,5 m oder ein Vielfaches davon betragen. Beim Anschluss eines Transceivers wird das ThickWire-Kabel nicht aufgetrennt. Das Kabel wird angebohrt und der Transceiver über einen Dorn mit der Innenader des Koax-Kabels elektrisch verbunden. Da bei der Installation eines Transceivers das Kabel nicht unterbrochen werden muss, wird der Netzbetrieb nicht gestört.

Ein Transceiver (Transmitter-Receiver) enthält Sende- und Empfangslogik. Er sichert eine regenerationsfreie Datenübertragung bis zu 500 m Kabellänge, führt die Kollisionserkennung durch und übernimmt das Carrier Sensing sowie die Generierung der Präambel (Synchronisationssignal).

Eine weitere Aufgabe ist die elektrische Isolation zwischen der Station und dem ThickWire-Kabel. Der Transceiver wird über das Transceiver-Kabel von der Station mit Strom versorgt. Neben den Einfach-Transceivern kann man auch Zwei- und Vierfach-Transceiver einsetzen, die pro Anschluss preiswerter sind. Sie zählen, je nach Modell, nur als ein Transceiver bei der 100-Transceiver-pro-Segment-Regel.

Zwei, vier oder acht Stationen lassen sich an so genannte FAN-Out-Units anschließen, die wiederum mittels einer AUI-Buchse an einen Transceiver angeschlossen werden können. Das ThickWire-Kabel kann aus mehreren Kabelteilen bestehen, die durch entsprechende Verbinderstecker aneinandergeschlossen werden. Die maximale Länge ist immer 500 m, egal aus wie vielen Teilen das Segment besteht. An beiden Enden muss das Kabel mit einem 50-Ohm-Terminator elektrisch abgeschlossen werden. Das Kabel muss immer an genau einem Ende (nicht an beiden Enden) geerdet werden.

Mehrere ThickWire-Segmente lassen sich mit Repeatern und Bridges (siehe weiter unten) zu einem größeren Netz zusammenfassen.

7.1.4 10BASE2, ThinWire, Cheapernet

Diese Variante von Ethernet entspricht der 10BASE2-Norm und arbeitet im Prinzip wie das normale ThickWire-Ethernet. Sie verwendet jedoch ein wesentlich dünneres, flexibleres und preiswerteres Koax-Kabel und wird daher auch Cheapernet genannt.

ThinWire hat Vor- und Nachteile. Viele Stationen (Workstations, Terminalserver, PCs) werden zusätzlich zu der flexibel einsetzbaren AUI-Buchse mit einem Direktanschluss für ThinWire geliefert. Verwendet man diesen Anschluss, spart man Transceiver-Kabel und Transceiver. Stationen mit AUI-Buchse lassen sich mit Transceiver-Kabel und ThinWire-Transceiver (oft Station-Adapter genannt) anschließen.

ThinWire-Minitransceiver können direkt auf die AUI-Buchse einer Station gesteckt werden, ein Transceiver-Kabel ist dann nicht erforderlich. Nachteil von ThinWire ist die Beschränkung auf eine Gesamtkabellänge von 185 m und auf 30 Stationen (Mindestabstand zwischen den Stationen 0,5 m). Ein weiterer Nachteil ist, dass das ThinWire-Kabel zur Installation einer Station aufgetrennt werden muss. Der Station-Adapter wird über ein T-Stück mit den beiden aufgetrennten Teilen des Koax-Kabels verbunden. Das T-Stück muss direkt auf dem Station-Adapter sitzen und darf nicht mit einem Koax-Kabel verlängert werden. Deswegen muss das Koax-Kabel bei Stationen mit eingebautem ThinWire-Adapter in einer Schleife zur Station geführt werden.

Die Enden des ThinWire-Kabels müssen mit 50 Ohm terminiert werden (wie auch bei anderen Kabeltypen ist keine Kommunikation auf dem Kabel möglich, wenn es nicht auf beiden Seiten terminiert ist). Wird das Kabel (beispielsweise bei der Installation einer weiteren Station oder auch versehentlich) aufgetrennt, kommt der Datenverkehr im Netz zum Stillstand. Die Suche nach der Fehlerursache ist oft zeitaufwendig.

Der Einsatz von Repeatern erlaubt die Eingrenzung von Fehlern auf einzelne und die Erweiterung auf mehrere Segmente. Wie man mehrere ThinWire-Segmente untereinander oder auch mit anderen Kabeltypen verbindet, wird weiter unten beschrieben.



7.1.5 10BASE-T, TwistedPair

TwistedPair-Verkabelung kommt eine besondere Bedeutung zu, da die herkömmlichen Koax-Kabel nicht mehr den heutigen Anforderungen gerecht werden. Entsprechend nimmt die Zahl der Koax-Installationen ab und die Verwendung von TwistedPair-Kabel zu. Zudem eignen sich hochwertige TwistedPair-Kabel auch für die Übertragung schnellerer Signale (z.B. Fast Ethernet, Gigabit Ethernet, FDDI und ATM), so dass beim Wechsel der Endgeräte die vorhandene Kabelinfrastruktur beibehalten werden kann.

Beim Auf- und Ausbau der Infrastruktur eines Netzwerks, d.h. der Verkabelung als physikalischer Basis für die Kommunikation zwischen den einzelnen aktiven Komponenten, müssen heute verschiedene Aspekte berücksichtigt werden. In der Vergangenheit hat sich gezeigt, dass die herkömmliche Vorgehensweise, je nach aktuellem Bedarf unterschiedliche Topologien, Übertragungsmedien und Anschlusstechniken einzusetzen, in der Regel hohe Folgekosten verursacht, wenn nachträgliche Änderungen oder Erweiterungen der vorhandenen Struktur notwendig werden. Darüber hinaus erweisen sich Kabel, deren Übertragungsverhalten Transferraten von 10 oder 16 Mbit/s problemlos ermöglicht, inzwischen häufig als ungeeignet für den Einsatz neuerer Technologien wie Fast Ethernet, Gigabit Ethernet, FDDI, oder ATM.

Der Leistungsfähigkeit dieser und zukünftiger Technologien müssen deshalb Leistungsreserven einer neu vorzunehmenden Verkabelung gegenüberstehen, die sowohl eine flexible und universelle Nutzung als auch hohe Bandbreiten zulassen.

Ein weiterer Aspekt bei der Planung einer zukunftssicheren Investition in die Infrastruktur eines Netzwerks ergibt sich aus der seit 1996 verbindlichen europäischen Gesetzgebung zur elektromagnetischen Verträglichkeit (EMV) informationstechnischer Installationen, der die Hersteller durch Abgabe der sog. CE-Konformitätserklärung nachkommen. Zu beachten ist in diesem Zusammenhang allerdings, dass sich die angesprochenen Vorschriften auf Gesamtsysteme aus aktiven und passiven Komponenten beziehen. Nichtsdestoweniger ist aber die Auswahl eines geeigneten Verkabelungssystems eine Grundvoraussetzung für die Einhaltung dieser Vorschriften.

Eine Möglichkeit, den dargestellten Gesichtspunkten und Anforderungen Rechnung zu tragen, bietet das Konzept der strukturierten Verkabelung, das zwischen Primär-, Sekundär und Tertiärverkabelung unterscheidet. Während für die als Primärverkabelung bezeichnete Verbindung von Gebäuden in der Regel Lichtleiterkabel zu empfehlen sind, lassen sich im Sekundärbereich, d. h. für die Verbindung verschiedener Etagen eines Gebäudes, und vor allem im Tertiärbereich, also auf Stockwerkebene, preisgünstige UTP- (Unshielded TwistedPair) bzw. SUTP-Kabel (Screened Unshielded TwistedPair) einsetzen, die den im EIA/TIA 568 TSB-36 (Technical System Bulletin) festgelegten Spezifikationen der Kategorie 5, z. B. bezüglich Nahnebensprechen (auch als Near End

Cross Talk oder NEXT bezeichnet), Dämpfung und Wellenwiderstand, entsprechen.

Die hohe Übertragungssicherheit des SUTP-Kabels kann nur genutzt werden, wenn auch der für die 10/100BASE-T-Verkabelung spezifizierte RJ45-Stecker geschirmt ist und die angeschlossenen Geräte diesen Kabeltyp unterstützen. Die Konsequenz aus den oben aufgeführten Aspekten ist, dass bei der Auswahl eines TwistedPair-Kabels für den Einsatz in Ethernet-Netzen nicht nur die Spezifikation der Kategorie 5 erfüllt sein sollte, es sollte auch aus acht Adern bestehen, damit es beim Umstieg auf andere High Speed Technologien weiterverwendet werden kann.

Beim Einsatz von vorhandenen Kabeln muss sichergestellt sein, dass diese mindestens der Kategorie 3 entsprechen. Nicht jedes Telefonkabel erfüllt diese Spezifikation.

Nicht erst bei der Erweiterung kommen die Vorteile einer TwistedPair-Verkabelung zum Tragen. Da jede Station ihr eigenes Segment (Punkt-zu-Punkt) hat, werden Störungen aufgrund der dazwischen geschalteten Repeater nicht auf andere Segmente übertragen. Außerdem lassen sich durch LEDs, wie sie die meisten Repeater und Hubs haben, Fehlersituationen leicht optisch erkennen. Weitere Informationen zu TwistedPair-Kabeln, wie sie im EIA/TIA 568 TSB-36 spezifiziert werden, können der Tabelle entnommen werden. 10BASE-T-TwistedPair wird als Punkt-zu-Punkt-Verbindung geschaltet. Üblicherweise ist an einem Ende des maximal 100 m langen Kabels ein 10BASE-T-Multiport-Repeater, auch Hub genannt, am anderen Ende entweder ein 10BASE-T-Transceiver mit einem einzelnen Gerät oder aber ein Umsetzer auf einen anderen Kabeltyp.

Bei der TwistedPair-Verkabelung wird unterschieden zwischen Send- und Receiverleitungspaaren. Dieser Sachverhalt muss z.B. bei der Kaskadierung von Repeatern berücksichtigt werden, denn entweder muss ein Kabel eingesetzt werden, bei dem die Send- und Receiverleitung gekreuzt sind, oder es lässt sich am Repeaterport die Send- und Receiverleitung umschalten. Dieser Umschalter ist meist mit MDI/MDIX gekennzeichnet, wobei MDI für Media Dependant Interface und das X für Crossed steht.



7.1.6 10BASE-F, Lichtleiter

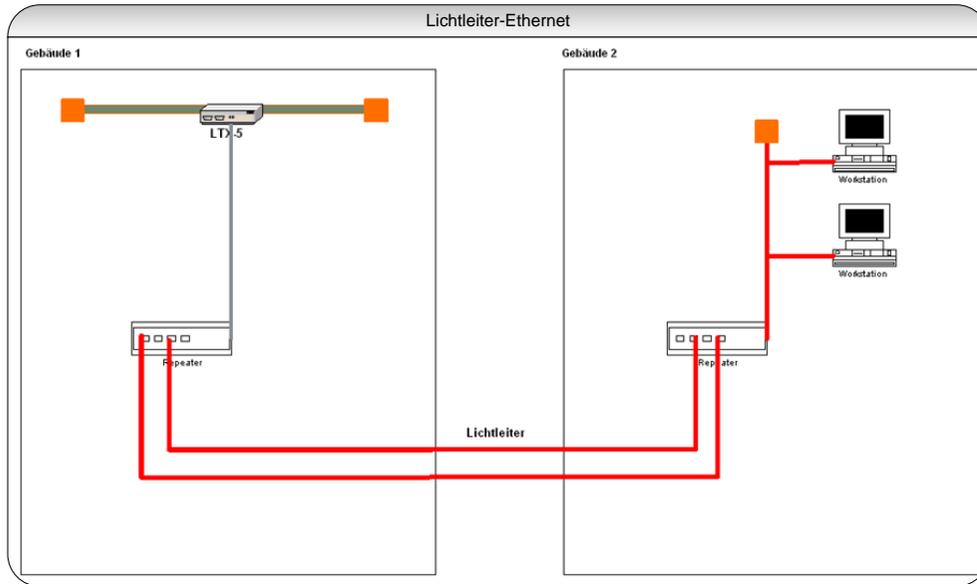


Abb. 23: Lichtleiter-Ethernet

Lichtleiter können wie TwistedPair auch im Ethernet-Verkehr nur für Punkt-zu-Punkt-Verbindungen eingesetzt werden. Lichtleiter werden zwischen Bridges, Switches und/oder Repeatern, einem Repeater und einer einzelnen Station mit Transceiver oder zwischen zwei Stationen mit Transceivern verwendet.

Als Industriestandard für Lichtleiterprodukte hatte sich ursprünglich FOIRL (Fiber Optic Inter Repeater Link) durchgesetzt. Inzwischen wurde FOIRL vom offiziellen IEEE 802.3 10BASE-FL-Standard abgelöst, daher sollte man heute nur noch 10BASE-FL konforme Geräte einsetzen. An einem FOIRL-Segment kann ein FOIRL-kompatibles Gerät mit einem 10BASE-FL-Transceiver gemischt werden. In diesem Fall gelten jedoch die strengeren FOIRL-Regeln. Normalerweise ist das eingesetzte LWL-Kabel ein Multimode (MMF) Kabel mit ST- oder SC-Steckern. Die maximale Länge des Kabels ist 2000 m beim Einsatz von 10BASE-FL- Komponenten, 1000 m bei FOIRL.

Lichtleiter sind auch für die schnelleren Übertragungstechnologien Fast Ethernet, Gigabit Ethernet, FDDI und ATM spezifiziert, die weiter unten näher beschrieben sind. Wählt man passende Kabel, so lassen sich Lichtleiter in einer ersten Phase für Ethernet und später

dann für Fast Ethernet, Gigabit Ethernet, FDDI bzw. ATM nutzen. Allerdings müssen in der Regel andere Stecker oder passende Adapter verwendet werden.

7.1.7 Interfaces

Es gibt Ethernet-Stationen unterschiedlichster Art: zunächst die diversen Rechner, die jeweils mit einem Ethernet-Interface ausgestattet sein müssen. Der 10BASE-T-Port ist heute Standard, alternativ werden meist noch AUI- und/oder 10BASE2-Port angeboten. Muss man einen Rechner erst mit einer Netzwerkkarte aufrüsten, so ist zu beachten, ob der benötigte Bus (inklusive Treiber) zur Verfügung steht. Alternativ dazu stehen Netzwerkkarten mit

SC- und ST-Stecker für Lichtleiter-Verbindungen ebenfalls zur Verfügung. Haben Stationen nicht den gleichen Anschluss wie das vorhandene Kabel, so kann der Anschluss relativ preisgünstig über Medienkonverter oder Multiport- Repeater realisiert werden.

Weitere Arten von Stationen sind Terminals (z.B. X-Window-Terminals), Terminal-/ Printserver, Bridges oder Router zur Verbindung mit anderen Netzsegmenten.

Hat eine Station eine AUI-Buchse (DB 15-Buchse), so können mit entsprechenden Transceivern verschiedene Medien (ThickWire, ThinWire, TwistedPair, Lichtleiter) angeschlossen werden. Sollen PCs ins Netzwerk integriert werden, so empfiehlt sich der Einsatz von PCI-Bus Netzwerkkarten mit automatischer Geschwindigkeitsanpassung (10BASE-T Ethernet und 100BASE-T Fast Ethernet). PC-Netzwerkadapter der neuesten Generation unterstützen Remote Wake Up. Diese Funktion erlaubt, ausgeschaltete PCs über das Netz zu booten,

so dass System-Upgrades außerhalb der Kernarbeitszeit durchgeführt werden können. Um diese Funktion nutzen zu können, müssen folgende Voraussetzungen vorhanden sein: Das Motherboard (ATX) muss über einen 3-Pin Remote Wake up Stecker verfügen, an den mittels Kabel die Netzwerkkarte angeschlossen werden kann. Das BIOS des Rechners muss diese Funktion unterstützen sowie ein Netzteil (ATX) vorhanden sein, das die „soft power on“ Funktion ermöglicht.



7.1.8 Repeater

Mehrere Ethernet-Segmente -ThinWire, ThickWire und auch anderer Kabeltypen - lassen sich mit Repeatern oder auch mit Bridges und Bridge/Routern zusammenschalten. Repeater werden zum einen eingesetzt, wenn ein Segment das Limit seiner physikalisch erlaubten Ausdehnung (500 m bei 10BASE5, 185 m bei 10BASE2, 100 m bei 10BASE-T) erreicht hat, aber erweitert werden soll, und zum andern aus Gründen der Verfügbarkeit des Netzes, wenn es in mehrere Segmente unterteilt werden soll. Repeater verhindern dann, dass fehlerhafte elektrische Signale von einem Segment auf ein anderes übertragen werden.

Ein Repeater ist ein Signalregenerator, der mehrere (mindestens zwei) Netzwerkanschlüsse hat. Er arbeitet auf der Ebene 1 des OSI-Modells. Sobald er auf einem seiner Eingänge die ersten Bits eines übertragenen Pakets empfängt, schickt er ihn auf allen Ausgängen fast ohne Zeitverzögerung weiter. Eine Modifikation der Daten erfolgt nicht. Repeater mit zwei AUI-Buchsen verbinden über Transceiver zwei Segmente. Diese Repeater lassen sich flexibel für beliebige Medien wie z.B. Lichtleiter oder ThinWire einsetzen. Häufig eingesetzt werden Multiport Repeater mit acht 10BASE2-Ports und einer AUIBuchse. Hierbei werden die einzelnen Segmente, wie im Abschnitt 10BASE2 beschrieben, aufgebaut, jedoch bleibt ein Ende ohne Terminator. Dieses unterminierte Ende wird direkt an einen Repeaterport, welcher intern terminiert ist, angeschlossen. Es gibt auch Repeater, bei denen sich die interne Terminierung zumindest an einem Port abschalten lässt. Wird die interne Terminierung abgeschaltet, kann der Repeater an einer beliebigen Stelle des Segments mittels T-Stück installiert werden.

Unbenutzte Ports sollten extern terminiert werden, auch wenn die automatische Erkennung von fehlerhaften Segmenten den Port mit nicht angeschlossenem Segment abschalten würde. Der Anschluss eines Repeaters an ein Segment zählt übrigens bei den Konfigurationsregeln für dieses Segment als normaler Anschluss. Mit einem Repeater reduziert sich also die Anzahl der weiteren Stationen in einem ThinWire-Segment auf 29.

Multiport Repeater für 10BASE-T, auch Hubs genannt, verfügen meistens über acht, 16 oder mehr Ports (R145) sowie über mindestens einen zusätzlichen Port zum Anschluss eines weiteren Segments.

Stackable Multiport Repeater lassen sich über spezielle Ports zu einem Großen Repeaterstack verbinden. Bei der Verbindung der Repeater muss man zwischen zwei Methoden unterscheiden:

Bei der ersten Methode werden die Repeater über ThinWire-Kabel verbunden, da sie als Backbone-Anschluss standardmäßig über einen 10BASE2-Anschluss verfügen. In diesem Fall zählt jeder Repeater als ein Repeater im Sinne der Repeaterregel (siehe

weiter unten). Vorteil dieser Lösung ist, dass die Repeater räumlich nicht unmittelbar beieinander stehen müssen.

Bei der zweiten Methode werden die Repeater über spezielle Busports und in der Regel sehr kurze Buskabel verbunden. Vorteil dieser herstellereigenen Kaskadierung ist, dass alle so verbundenen Repeater als ein Repeater bezüglich der Repeaterregel zählen. Gemeinsamer Vorteil beider Lösungen ist, dass die in einem Stack zusammengefassten Repeater über ein gemeinsames Management-Modul über SNMP verwaltet werden können.

Beachten muss man in allen Fällen, dass es zwischen zwei Stationen nur genau einen Weg durch das Ethernet geben darf. Ring- oder Schleifenkonfigurationen sind also nicht erlaubt. Eine Ausnahme ist nur mit Bridges und Switches möglich, welche den Spanning Tree Algorithmus unterstützen. Und noch eine weitere Einschränkung gibt es: die Repeater Regel, auch als 5-4-3-Repeater-Regel bezeichnet. Maximal zwei Repeaterpaare dürfen im Übertragungsweg zwischen zwei beliebigen Stationen sein, sofern sie nicht durch Bridges, Switches oder Router getrennt sind. Ein Übertragungsweg kann aus maximal fünf Segmenten und vier Repeater-Sets (zwei Repeater-Paaren) bestehen. Dabei können bis zu drei Segmente Koax-Segmente sein, an denen die Stationen angeschlossen sind, die restlichen Segmente müssen Punkt-zu-Punkt-Verbindungen sein, die auch als IRL-Verbindung (Inter Repeater Link) bezeichnet werden.

Maximal sind 1024 Stationen (Knoten) in solch einem ungebrückten Netz möglich. Wichtigster Grund für die Limitierung der Kabellänge in den einzelnen Segmenten sind die elektrischen Eigenschaften der Kabel und der Transceiver sowie die dadurch entstehende Signallaufzeit. Es muss sichergestellt sein, dass Kollisionen auch dann erkannt werden, wenn zwei Rechner am entgegengesetzten Ende des Netzes praktisch gleichzeitig mit der Datenübertragung beginnen.

7.1.9 Terminal- und Printserver

Umsetzer wie der LTX-C von Lantronix sind keine Repeater im eigentlichen Sinn, da sie keine Signalregenerierung durchführen. Was aber die durch sie verursachte Verzögerung angeht, verhalten sie sich ähnlich wie Repeater. Diese Verzögerung ist kleiner als bei einem Standardrepeater, daher sollte der LTX-C ungefähr als ein halber Repeater bei der Netzwerkkonfiguration berücksichtigt werden. Die Verwendung mehrerer solcher Produkte in einem Pfad kann zu Laufzeitproblemen führen, wenn man sie mit Repeatern kombiniert. Terminal- und Printserver bieten eine flexible und preiswerte Möglichkeit, Terminals und Drucker in ein Netzwerk zu integrieren. Aber auch Modems und andere Geräte mit serieller oder paralleler Schnittstelle lassen sich mittels Terminal-/Printservern





einbinden.

Terminal- und Printserver gibt es in einer Vielzahl von Varianten. Sie unterscheiden sich in der Anzahl und Ausführung der Ports (seriell, parallel, volle Modem Control), der Anzahl der unterstützten Netzwerkprotokolle und anderen Funktionen wie etwa dem Management. Terminal-/Printserver, die mehr als ein Netzwerkprotokoll unterstützen, eignen sich gut für den Einsatz in heterogenen Netzwerken.

Manche Multiprotokoll-Terminal- und -Printserver (z.B. von Lantronix) unterstützen alle gängigen Netzwerkprotokolle wie TCP/IP für Unix-Systeme, LAT für Digital-Systeme, IPX für Netware, AppleTalk für Macintosh-Systeme und NetBIOS/NetBEUI für Anwendungen unter DOS bzw. Windows. Damit können angeschlossene Drucker von allen Protokollen gleichzeitig angesprochen werden. Ein Drucker kann also mit den verschiedensten Systemen (wie z.B. Sun, HP, Digital, IBM, Windows, NOVELL oder Macintosh) gleichzeitig genutzt werden. Dies kann in heterogenen Netzwerken die Anzahl der Drucker erheblich reduzieren, da nicht mehr für jedes System bzw. für jede Systemarchitektur eigene Drucker notwendig sind. Außerdem werden die Drucker effektiver genutzt und können flexibler eingesetzt werden.

Die Ansteuerung der Drucker unter TCP/IP erfolgt in der Regel über remote lpr. Sollen Drucker unter LAT eingebunden werden, müssen die Terminal- und Printserver die LAT Services und Reverse-LAT beherrschen.

Terminals werden bei Unix-Systemen via TCP/IP und bei Digital-Systemen mit LAT eingebunden. Manche Terminalserver bieten auch die Möglichkeit der Protokollumsetzung von TCP/IP auf LAT und umgekehrt. Das heißt, ein Benutzer kann sich von einem Digital System mit LAT auf einem Server einloggen und von hier aus mit TCP/IP (telnet oder rlogin) auf Unix-Systeme zugreifen oder umgekehrt. Durch dieses Feature kann in vielen Netzwerken zusätzliche Software auf der Digital- oder Unix-Seite eingespart werden. Bei den meisten Terminalservern können pro Terminal bis zu acht Sessions, auch mit unterschiedlichen Rechnern und Protokollen, aufgebaut werden. Zwischen diesen Sessions kann mittels einfacher Tastenkombinationen beliebig umgeschaltet werden. Mit MultiSession-Terminals wie z.B. dem VT525 können zwei Sessions auch gleichzeitig auf dem Bildschirm dargestellt werden und vier Sessions, sofern der Terminalserver SSU unterstützt. Der Anschluss von Terminals erfolgt seriell, Drucker können entweder seriell, bei den Printservern auch parallel angeschlossen werden. Die parallele Schnittstelle ist standardmäßig Centronics- und je nach Modell auch noch HP-bitronics-kompatibel.

Das Management der meisten Server kann mittels SNMP (TCP/IP) oder TSM, NCP (Digital) unterstützenden Softwarepaketen erfolgen. Diese Softwarepakete sind aber keine Voraussetzung für das Management der Server. Sie können auch mittels telnet oder eines direkt angeschlossenen Terminals verwaltet werden. Neuere Terminalserver lassen sich sehr einfach über einen Webbrowser managen, sofern diese Funktion

implementiert ist.

Je nach Hersteller werden für das Laden des Betriebssystems der Server verschiedene Möglichkeiten angeboten. Die wohl am häufigsten anzutreffende Form ist das Laden des Serverbetriebssystems über das Netz von einem Laderechner aus (MOP Protokoll bei OpenVMS-, TFTP oder BOOTP bei Unix-Systemen).

Bei größeren Netzwerken mit vielen Servern kann das aber, z.B. nach einem Stromausfall, sehr lange dauern. Deshalb ist es hier sinnvoller, Server einzusetzen, die entweder die Software von einem Flash PROM oder von einer Flash Card (z.B. PCMCIA Speicherkarte) laden. Neue Softwareversionen werden einfach über das Netz in die Server geladen und dort im Flash PROM abgelegt.

Nähere Produktinformationen lassen sich dem Kapitel Ethernet Printserver von Lantronix (Seite 235) und dem Kapitel Device Server von Lantronix (Seite 236) entnehmen.

7.1.10 Bridges

Eine Bridge erweitert das Netzwerk über die für ein 802.3-Ethernet-LAN spezifizierte Begrenzung hinaus (Anzahl Knoten, maximale Entfernung usw.), durch Trennung der Collision Domains. Eine Bridge arbeitet auf OSI Layer 2. Sie erhöht die Ausfallsicherheit, da Störungen von der einen Seite einer Bridge nicht auf die andere Seite gelangen. Sie verbessert die Datensicherheit, da Informationen, die zwischen Knoten auf einer Seite der Bridge ausgetauscht werden, nicht auf der anderen Seite der Bridge abgehört werden können - man denke nur an die Benutzerpasswörter, die über das Netz zwischen Rechner und Servern übertragen werden.

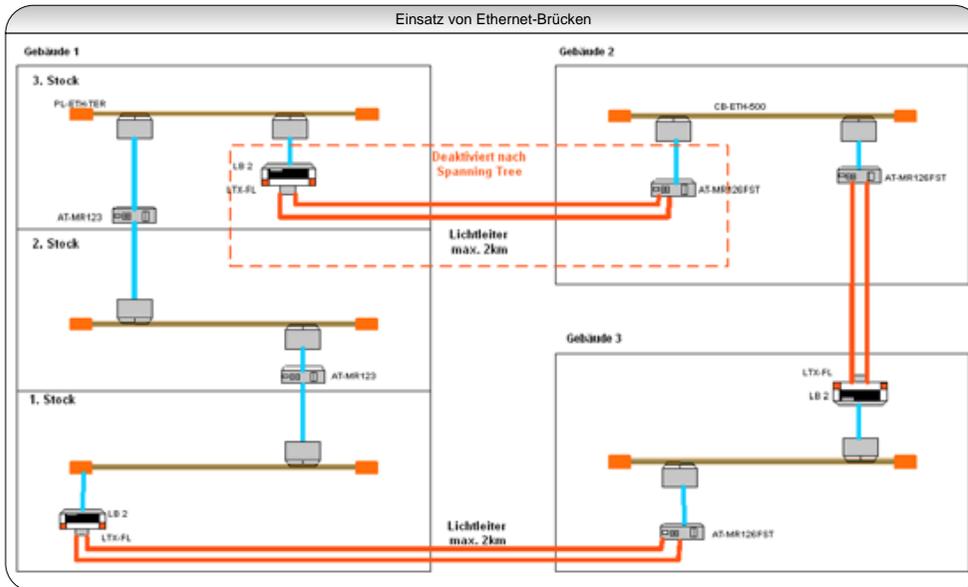
Und schließlich optimiert sie den Durchsatz, denn in durch Bridges getrennten Segmenten können jeweils unterschiedliche Blöcke gleichzeitig transferiert werden. Allerdings erzeugen Brücken dadurch, dass sie die Blöcke zwischenspeichern eine zusätzliche Verzögerung und können deswegen bei kaum ausgelasteten Netzen die Performance sogar verschlechtern.

Bridges können Ethernet-Segmente auch über synchrone Standleitungen, Satellitenverbindungen, Funkverbindungen, öffentliche Paketvermittlungsnetze und schnelle Lichtleiternetze (z.B. FDDI) verbinden. In der Regel müssen solche Bridges immer paarweise eingesetzt werden. Bridges sind komplette, relativ leistungsfähige Rechner mit Speicher und mindestens zwei Netzwerkanschlüssen. Sie sind unabhängig von höheren Protokollen (funktionieren also z.B. mit TCP/IP, DECnet, IPX, LAT, MOP etc. gleichzeitig) und erfordern bei normalem Einsatz keine zusätzliche Software oder



Programmierung.

Die Local Bridge hat zwei AUI-Buchsen. Manche Bridges haben außer den AUI-Buchsen auch noch alternativ nutzbare 10BASE2-Ports (BNC). Remote Bridges, die an Lichtleiter angeschlossen werden, haben in der Regel eine AUI-Buchse und einen Anschluss für Lichtleiterkabel. Die Funktion von Remote Bridges mit WAN-Anschluss wird heute von Routern übernommen. Die Router der jüngsten Generation sind leistungsfähiger, flexibler einsetzbar und preislich attraktiver als die alten Remote Bridges.



Die Bridge empfängt von beiden Netzsegmenten, mit denen sie wie jede normale Station verbunden ist, alle Blöcke und analysiert die Absender- und Empfängeradressen. Steht die Absenderadresse nicht in der brückeninternen Adresstabelle, so wird sie vermerkt. Die Bridge lernt und speichert so die Information, auf welcher Seite der Bridge der Rechner mit dieser Adresse angeschlossen ist. Ist die Empfängeradresse bekannt und der Empfänger auf derselben Seite wie der Absender, so verwirft die Bridge das Paket (filtert es). Ist der Empfänger auf der anderen Seite oder nicht in der Tabelle, wird das Paket weitergeschickt. Die intelligente Bridge lernt so selbständig, welche Pakete weitergeschickt werden müssen und welche nicht. Bei managbaren Bridges können zusätzliche Adress-Filter gesetzt werden, die regeln, an welche Adressen die Bridge Informationen immer weiterschicken muss oder nie weiterschicken darf. So kann man erreichen, dass vertrauliche Daten sich nicht auf der anderen Seite der Bridge ausbreiten können und dort von einem „Spion“ (d.h. einem Rechner, der nicht für ihn bestimmte

Pakete empfängt) aufgenommen werden können.

Bei durchschnittlich belasteten Netzen kann durch den Einsatz von Bridges die Leistung des Gesamtnetzwerks erhöht werden, weil auf jedem Netzwerkteil nicht alle Pakete des Gesamtnetzes übertragen werden müssen. Die Leistungsverbesserung ist umso grösser, je sinnvoller die Bridges eingesetzt werden. Man sollte also Rechnergruppen, die viel miteinander kommunizieren, durch Bridges vom Gesamtnetz trennen.

Müssen jedoch fast alle Pakete von der Bridge weitergeschickt werden, kann sich durch die brückenbedingte Verzögerung sogar eine Durchsatzverschlechterung des Netzes ergeben. In solchen Fällen sollten leistungsfähige Switches eingesetzt werden, die im nächsten Abschnitt erläutert werden.

Da eine Bridge von jedem der beiden angeschlossenen Netze wie eine Station behandelt wird, muss man nur sicherstellen, dass die 802.3-Spezifikationen jeweils getrennt auf jeder Seite der Bridge eingehalten werden, nicht jedoch in der Summe beider Seiten. Das ist der Grund, weshalb mehr Stationen und größere Entfernungen erlaubt sind als bei einem Netz ohne Bridges.

7.1.11 Switches

Bridges gibt es in einer Vielzahl von Varianten. Sie können sich in folgenden Features unterscheiden:

An eine Standard-Bridge lassen sich zwei Segmente anschließen. Können mehr als zwei Segmente angeschlossen werden, so wird aus dem Begriff Multipart-Bridges der Begriff Switch.

Die Größe der Adresstabelle gibt an, wie viele Adressen (Knoten) insgesamt in der Bridge gespeichert werden können.

Die Filtrierate gibt an, wie viele Pakete pro Sekunde (packets per second, pps) eine Bridge maximal empfangen kann. Bei voller Last und minimaler Paketlänge können in einem Ethernet-Segment theoretisch bis zu 14.880 Pakete pro Sekunde auftreten. Auf beiden Ports hat eine 2-Port-Bridge also insgesamt maximal 29.760 Pakete pro Sekunde zu filtern. Alle modernen Bridges erreichen diese theoretisch möglichen Maximalwerte.

Die Transferrate gibt an, wie viel Pakete pro Sekunde die Bridge auf die andere Seite weiterleiten kann. Der Maximalwert ist hier 14.880 pps, da bei dieser Transferrate beide Segmente voll ausgelastet sind.





Netzwerke können mit vielen Bridges aufgebaut werden. Bei 802.3 und Ethernet muss man normalerweise sicherstellen, dass es zwischen zwei Rechnern jeweils nur einen Datenpfad gibt. Im Gegensatz zu anderen „dummen“ Ethernet-Boxen wie Repeatern kann man jedoch mit Bridges auch redundante Verbindungen aufbauen.

Ethernet überträgt mit einer Geschwindigkeit von 10 Mbit/s. Noch vor einigen Jahren schien diese Geschwindigkeit auch für größere Netze auszureichen. Durch den gestiegenen Bedarf an Kommunikation erreicht man die Leistungsgrenze von Ethernet inzwischen sehr schnell.

Die Bridges innerhalb eines Netzes kommunizieren miteinander und stellen redundante Mehrfachverbindungen selbst fest. Sie stellen über den so genannten Spanning Tree Algorithmus sicher, dass bei mehreren physikalischen Verbindungen immer nur eine aktiv ist.

Um Performanceprobleme zu vermeiden, sollte man versuchen, Teilnetze mit hohem internen Verkehrsanteil, typischerweise Workgroups, durch Bridges vom Hauptnetz abzutrennen und somit das übrige Netz zu entlasten. Diese Strategie funktioniert jedoch nur dann, wenn zum einen die Bridge schnell genug für den Verkehr zwischen Workgroup und Backbone ist, zum anderen weder das Backbone-Ethernet noch das Workgroup-Ethernet zu langsam für den dort anfallenden Verkehr ist.

Mischt man Bridges unterschiedlicher Hersteller in einem Netz, muss man sicherstellen, dass alle den gleichen Spanning Tree Algorithmus verwenden. Alle neueren Bridges arbeiten mit dem in der IEEE-802.1d-Norm definierten Algorithmus, manche ältere Modelle nach einem Vorläuferstandard.

Reicht die Bandbreite für Ethernet nicht, braucht man ein schnelleres zentrales Medium als Backbone. Mehrere Strategien gibt es: entweder setzt man FDDI, ATM, Fast Ethernet oder Gigabit Ethernet als Backbone-Technologie ein und verbindet die Ethernet-Segmente über Bridges mit dem schnellen Backbone oder aber man verwendet einen Ethernet-Switch oder eine Multiport Bridge mit einem schnellen internen Bus als Backbone (collapsed Backbone).

Eine weitere Regel ist zu beachten: Maximal sieben Bridges dürfen zwischen zwei beliebigen Knoten installiert werden. Nur dann liegt die maximale Übertragungsdauer unterhalb der von unterschiedlichen Protokollen erwarteten Grenze. Warum? Bei Überlastung eines Segments kann es vorkommen, dass die zu übertragenden Daten nicht schnell genug auf diesem Segment weitergesendet werden können, und Pakete dürfen vernichtet werden, wenn sie zu lange in der Bridge auf Weiterversand warten. Diese Regel ist allerdings abhängig vom eingesetzten Protokoll. Es gibt Protokolle, die längere Verzögerungen und damit mehr als sieben Bridges erlauben.

Beide Möglichkeiten haben ihre Vor- und Nachteile: FDDI oder ATM erlauben es, den schnellen Backbone geographisch auszudehnen und damit auch Große Netze zu konfigurieren. Auch lassen sich an diese Netze Rechner mit hohem Datenverkehr (z.B. Fileserver) direkt anschließen. So kann man die Limitierung von 10 Mbit/s bei Ethernet für Einzelrechner auch noch umgehen. Collapsed-Backbone-Systeme kosten wesentlich weniger als FDDI- oder ATM-Lösungen. Sie begrenzen jedoch die geographische Ausdehnung, da die Ethernet-Segmente zu dem zentralen Switch geführt werden müssen. Sofern diese Geräte über keinen Uplink-Port zu den schnelleren Technologien (Fast Ethernet, Gigabit Ethernet, FDDI, ATM) verfügen, sind sie später nur schlecht erweiterbar.

An ein Lichtleitersegment kann man sowohl zwei Bridges als auch eine Bridge und einen Repeater anschließen. Bei Verwendung eines Repeaters zählt das Lichtleitersegment zum Netz, muss also bei den Konfigurationsregeln berücksichtigt werden.

Eine weitere Möglichkeit, höhere Performance in Großen Netzen zu erreichen, ist die Aufteilung in mehrere Subnetze und der Einsatz von Routern zwischen diesen Subnetzen. Im Gegensatz zu Lösungen mit Bridges dürfen dann mehrere aktive Pfade zwischen zwei Stationen bestehen. Allerdings ist der Managementaufwand solcher Netze erheblich höher. Auch verliert man dann an Flexibilität, weil eine Station nicht mehr einfach von einer Stelle im Netz zu einer anderen umgehängt werden kann, ohne dass z.B. IP-Adressen geändert werden müssen.

Multiport-Bridges haben mehr als zwei Netzwerkports. Diese Bridges werden von den Herstellern oft auch als Switches bezeichnet. Hier gibt es wieder zwei Typen: solche, die an einem Segment nur eine geringe Anzahl von Rechnern erlauben, und andere, die eine große Zahl von Adressen speichern können. Der erste Typ ist sinnvoll, wenn man einzelne Systeme mit einem privaten Ethernet ausstatten will. Sie sind ungeeignet und verlangsamen ein Netz, wenn man mehr als die vorgesehene Zahl von Rechnern an einen Port anschließt. Manche Hersteller bezeichnen solche Multiport-Bridges auch als Switching-Hubs oder Switches. Durch die rasante Weiterentwicklung der Elektronik der Switches sind diese Geräte preislich so attraktiv geworden, dass Bridges im herkömmlichen Sinn nur noch eine untergeordnete Rolle spielen.

Was ist nun der Unterschied zwischen einem Switch und einer Multiport-Bridge? Technisch sind Switch und Bridge identisch, üblicherweise wird ein Layer-2-Gerät mit zwei Ports Bridge genannt und ein Layer-2-Gerät mit mehr als zwei Ports Switch.

Switches brechen die Ethernet-Busstruktur in eine Bus-/Sternstruktur auf. Teilsegmente mit Busstruktur werden sternförmig über je einen Port des Switches gekoppelt. Zwischen den einzelnen Ports können Pakete mit maximaler Ethernet-Geschwindigkeit übertragen werden. Wesentlich ist die Fähigkeit von Switches, mehrere Übertragungen zwischen unterschiedlichen Segmenten gleichzeitig durchzuführen. Dadurch erhöht sich die



Bandbreite des gesamten Netzes entsprechend.

Die volle Leistungsfähigkeit von Switches kann nur dann genutzt werden, wenn eine geeignete Netzwerktopologie vorhanden ist bzw. geschaffen werden kann. Die Datenlast sollte nach Möglichkeit gleichmäßig über die Ports verteilt werden. Systeme, die viele Daten übertragen, müssen unter Umständen an einen eigenen Switch Port angeschlossen werden. Dies bezeichnet man dann als PrivateEthernet. Außerdem sollte man versuchen, Systeme, die viel miteinander kommunizieren, an einen gemeinsamen Port des Switches anzuschließen, um so die Datenmengen, die mehr als ein Segment durchlaufen müssen, zu reduzieren.

Kaskadierung von Standalone-Switches

Die Performance eines Netzes kann man auf Basis vorhandener Standalone-Switches erhöhen, indem zusätzliche Switches über die Ethernetports kaskadiert werden.

Die Hersteller Cisco und 3Com bieten eine Lösung mit einem weiteren Vorteil. Diese Ethernet Switches haben gegenüber Bridges eine geringere Verzögerungszeit (latency). Die dafür benötigte Technik basiert auf einer so genannten Cross-Point Switch Matrix und wird On-the-Fly Switching genannt. Der Ethernet Switch wartet im Gegensatz zu normalen Bridges nicht, bis er das vollständige Paket gelesen hat, sondern er überträgt das ankommende Paket nach Empfang der 6-Byte-Destination-Adresse. Da nicht das gesamte Paket bearbeitet werden muss, tritt eine Zeitverzögerung von nur etwa 40 Mikrosekunden ein. Sollte das Zielsegment bei der Übertragung gerade belegt sein, speichert der Ethernet Switch das Paket entsprechend zwischen.

Alle Switches erlauben die Kaskadierung über einen einzelnen Ethernet-Port mit einer maximalen Transferrate von 10 Mbit/s (bzw. 100 Mbit/s bei Fast Ethernet Switches). Kann man das Netz in Teilnetze unterteilen, zwischen denen diese Transferrate ausreicht, ist dies eine sinnvolle Lösung. Doch meistens ist das nicht der Fall.

Bei den Switches werden, im Gegensatz zu Bridges, mit Ausnahme von short frames (Pakete, die kleiner als die minimal zulässigen 64 Bytes sind), fehlerhafte Pakete auch auf das andere Segment übertragen. Grund hierfür ist, dass die CRC-Prüfung (Cyclic Redundancy Check) erst bei vollständig gelesenen Paket durchgeführt werden kann. Solange der Prozentsatz von fehlerhaften Paketen im Netz gering ist, entstehen keine Probleme. Sobald aber (z.B. aufgrund eines Konfigurationsfehlers, fehlerhafter Hardware oder extrem hoher Netzlast bei gleichzeitig langen Segmenten mit mehreren Repeatern) der Prozentsatz der Kollisionen steigt, können Switches auch dazu führen, dass die Leistung des Gesamtnetzes deutlich sinkt.

Unterstützen die Switches Full Duplex Ethernet, können Geräte mit maximal 20 Mbit/s (bzw. 200 Mbit/s bei Fast Ethernet Switches) kaskadiert werden. Diese kollisionsfreie Switch-zu-Switch-Verbindung ist nur über 10BASE-T- und 10BASE-F-Verbindungen

möglich.

Ein anderer Ansatz neben dem geschwindigkeitsoptimierten On-the-Fly Switching von Cisco ist die Store-and-Forward-Technik, die der IEEE-Norm für Bridges entspricht. Bei Produkten, welche diese Bridging-Funktionalität implementiert haben, wird nicht nur die 6-Byte-Destination-Adresse gelesen, sondern das ganze Paket wird einer kompletten Fehlerprüfung unterzogen und erst dann weiter übertragen, wenn es vollständig und richtig empfangen wurde. Einerseits hat dies den Nachteil der größeren Verzögerung beim Weiterschicken des Paketes, andererseits werden keinerlei fehlerhafte Pakete auf das andere Segment übertragen.

Full Duplex kann weiterhin auch zum Anschluss von einzelnen Stationen verwendet werden, sofern diese einen Full Duplex Ethernet-Anschluss haben. Die meisten aktuellen Ethernet-Netzwerkkarten mit TwistedPair- oder Lichtleiteranschluss unterstützen den Full Duplex Betrieb. Zu beachten ist, dass Full Duplex nur bei einer Switch-zu-Switch- bzw. Switch-zu-Rechner-Verbindung möglich ist.

Wann sollte nun welche Technologie eingesetzt werden?

On the fly Switching bietet dann einen Vorteil, wenn man sehr geringe Verzögerungen bei der Übertragung zwischen einzelnen Knoten benötigt. Diese Technologie sollte also eingesetzt werden, wenn es darum geht, in relativ kleinen Netzen eine große Anzahl Daten zwischen wenigen Knoten zu übertragen.

Die Store and Forward-Lösung ist bei größeren Netzen mit vielen Knoten und Kommunikationsbeziehungen besser, weil nicht einzelne fehlerhafte Segmente durch Kollisionen das ganze Netz belasten können. Bei diesen Anwendungen ist die Gesamttransferrate entscheidend, die Verzögerung wirkt sich hier kaum aus.

Inzwischen sind Switching-Produkte (z.B. von 3Com, Cisco oder Allied Telesyn) am Markt, die beide Technologien unterstützen. Dies geschieht entweder per Konfiguration (Software) oder automatisch anhand der CRC-Fehler-Häufigkeit. Wird eine vorgegebene Anzahl von fehlerhaften Paketen überschritten, schaltet der Switch automatisch von „On the fly“ auf „Store and Forward“ um.

Switches mit Highspeed-Backbone

Die dritte und wohl beste Möglichkeit der Kopplung von Switches ist der Einsatz von Produkten, die den Anschluss an einen High Speed Backbone erlauben. Im Gegensatz zu kaskadierten Standalone-Switches können weitere Geräte an den Backbone gehängt werden, ohne dass Ports für die Switch-zu-Switch-Verbindung verlorengehen.

Eine Backbone-Lösung ist nicht nur schneller und flexibler, sondern für Große Netze





auch kostengünstiger. Man muss unterscheiden zwischen Lösungen, die eine herstellereigene Verbindung benutzen (proprietär) und solchen, die auf einen Standard wie Fast Ethernet, Gigabit Ethernet, FDDI oder ATM setzen. Die herstellereigene Lösung sind heute meist preisgünstiger, schränken jedoch die spätere Erweiterung ein. Auch erlauben sie meist nur kurze Entfernungen zwischen den Switches.

FDDI-Lösungen mit einer Backbone-Transferrate von bis zu 100 Mbit/s sind typischerweise etwas teurer, jedoch ist die Technologie ausgereift. Produkte unterschiedlicher Hersteller können gemeinsam an einem FDDI-Ring eingesetzt werden. Auch ist die Kommunikation mit Stationen möglich, die mit einem FDDI-Interface ausgestattet sind. ATM-Lösungen für bis zu 155 Mbit/s auf dem Backbone sind heute auch erhältlich. Die Normierung ist aber immer noch nicht endgültig abgeschlossen. Deshalb sollte man vor dem Kauf die Kompatibilität der ATM Produkte klären, sofern Produkte unterschiedlicher Hersteller eingesetzt werden sollen. 100BASE-T Fast Ethernet ist inzwischen quasi Standard für die Verbindung zwischen Switches. Für alle größeren Switches stehen inzwischen 1000BASE-T Gigabit Ethernet Anschlüsse zur Verfügung, die den Aufbau von HighSpeed Backbones ermöglichen.

Layer 3 Switching

Layer 3 Switching ist eine neue Technologie. Sie kombiniert leistungsfähiges Switching (Layer 2) mit skalierbarem Routing (Layer 3). Herkömmliche Switches verwenden die MAC-Adresse der Ethernet-Frames zur Entscheidung, wohin die Frames transportiert werden, sollen, während Router Datenpakete anhand von Routingtabellen und Accesslisten auf Layer 3 weitervermitteln. Router sind in vielen Installationen als reine LAN-to-LAN-Router im Einsatz, um Subnetze zu verbinden und die Nebeneffekte von rein geschichteten Netzen, wie z.B. Broadcast-Stürme, fehlendes Subnetting etc. zu verhindern. Router, die auf der Transportebene arbeiten, müssen jedes IP-Paket aus den Ethernet-Frames zusammenbauen und vielfältige Operationen an IP-Paketen durchführen. Dies führt zu einer Großen Verzögerungszeit und, im Vergleich zu Switches, geringerem Datendurchsatz. In reinen IP-Netzen kann das Layer 3 Switching, auch Fast IP genannt, diese LAN-to-LAN-Router ersetzen.

Der Layer 3 Switch liest beim ersten IP-Paket sämtliche Frames dieses Paketes, analysiert die Absender- und Empfänger-IP-Adressen und leitet das IP-Paket weiter. Alle nachfolgenden Frames dieses Absenders an diesen Adressaten können daraufhin anhand der MAC-Adresse weitergeleitet werden. Der Layer 3 Switch behandelt IP-Pakete beim ersten Mal wie ein Router, nachfolgende Daten können auf Frame-Ebene geschickt werden. Nicht-IP-Daten, wie z.B. IPX-Pakete, werden vom Layer 3 Switch auf Layer 2 geschickt.

Das Konzept des Layer 3 Switching bedingt eine Erweiterung des Ethernet-Frameformats und ist bisher nur proprietär implementiert. Die Erweiterung des Layer 3 Switching auf andere Layer 3 Protokolle wie z.B. IPX ist geplant. Es ist anzunehmen, dass die

herstellereigene Implementationen in einen gemeinsamen Standard münden. Bis dahin empfiehlt es sich, ausschließlich Netzkomponenten eines einzigen Herstellers einzusetzen. Mit den Superstock 11 1100/3300 Switches von 3Com befinden sich solche Layer 3 Switches im Produktspektrum.

Power over Ethernet

Immer mehr kleine Geräte mit externer Stromversorgung (z.B. Web-Kameras, Printserver, serielle Server) werden ans Netzwerk angeschlossen. Bei diesen Geräten ist die Stromversorgung oft grösser als das Gerät selbst und stellt außerdem einen wesentlichen Kostenfaktor dar. Um diese Geräte direkt über das Ethernet-Kabel mit Strom zu versorgen, wird bei der IEEE die Norm 802.3af vorbereitet. Dabei werden bei Twisted Pair Verkabelung zwei unbenutzte Adernpaare für die Stromversorgung verwendet. Mehr Informationen zu dieser Norm sind auf der Homepage von IEEE 802.3af zu finden unter <http://grouper.ieee.org/groups/802/3/af/index.html>.

7.1.12 Router

Router verbinden, im Gegensatz zu Bridges, in OSI-Schicht 3 auch Netze unterschiedlicher Topologien. Sie sind Dreh- und Angelpunkt in strukturiert aufgebauten LAN- und WAN-Netzen. Mit der Fähigkeit, unterschiedliche Netztypen sowie unterschiedliche Protokolle zu routen, ist eine optimale Verkehrslenkung und Netzauslastung möglich. Routing wird erst dann erforderlich, wenn Kommunikation zwischen Stationen in unterschiedlichen Subnetzen erfolgen soll.

Sie sind nicht protokolltransparent, sondern müssen in der Lage sein, alle verwendeten Protokolle zu erkennen, da sie Informationsblöcke protokollspezifisch umsetzen. Das heißt, die verwendeten Protokolle müssen routbar sein oder entsprechend umgesetzt bzw. in andere Protokolle eingepackt werden. Da nicht alle Protokolle geroutet werden können, sind die meisten Router auch in der Lage, Pakete zu bridgen, deshalb ist die Bezeichnung Bridge/Router für solche Geräte präziser.

Gegenüber Bridges gewährleisten Router eine bessere Isolation des Datenverkehrs, da sie Broadcasts zum Beispiel nicht standardmäßig weiterleiten. Allerdings verlangsamen Router den Datentransfer in der Regel. In verzweigten Netzverbunden, insbesondere in WANS, führen sie Daten jedoch effektiver zum Ziel. Router sind andererseits meist teurer als Bridges. Deswegen muss im Bedarfsfall analysiert werden, was sinnvoller ist.

Die logischen Adressen in einem Netzwerk können von Routern ausgewertet werden, um mit Hilfe anzulegender interner Routing-Tabellen den optimalen Weg (Route) vom Sender zum Empfänger zu finden. Router passen die Paketlänge der Daten der in einem



Netzwerksegment maximal möglichen an, verändern die Paketlänge also beispielsweise beim Übergang von Ethernet zu Token-Ring oder X.25. Aber nicht nur Paketlängen werden von Routern verändert, Router führen vor allem beim Übergang vom LAN zum WAN eine Geschwindigkeitsanpassung durch. Dafür benötigen sie einen entsprechend Großen Puffer. Router gibt es in den verschiedensten Ausprägungen. So gibt es lokale Router, die vor allem aus Sicherheitsgründen eingesetzt werden, wenn z.B. im LAN nur zwischen bestimmten Knoten die Kommunikation erlaubt werden soll.

Die wohl größte installierte Basis haben die seriellen Bridge/Router für die LAN-zu-LAN-Kopplung.

Durch die große Zahl an verfügbaren ISDN-Anschlüssen und die attraktive Gebührenstruktur von ISDN werden immer mehr ISDN-Router für kurze, temporäre Verbindungen eingesetzt. Im Abschnitt ISDN wird näher auf ISDN-Router eingegangen.

Die bisher beschriebenen Routertypen basieren alle auf einer Kombination aus Soft- und Hardware, aber es gibt auch reine Software-Lösungen, die auf Servern, Workstations oder PCs laufen. Man muss im Einzelfall abwägen, welche Lösung für die jeweilige Anwendung die geeignetste ist.

Grundlegende Komponenten und technische Eigenschaften von Routern sollen im Folgenden erläutert werden.

LAN Interfaces

Die meisten Router haben ein oder mehrere LAN-Interfaces, je nach Topologie für TokenRing, Ethernet, 10BASE-T Fast Ethernet, FDDI oder auch ATM. Für den Anschluss entsprechender Medien sind entweder alternativ nutzbare Ports (z.B. Ethernet AUI, BNC, RJ45) vorhanden oder der Anschluss ist als Einschub realisiert und kann daher den Erfordernissen angepasst werden.

WAN Interfaces

WAN-Leitungen werden von unterschiedlichen Anbietern mit unterschiedlichen Geschwindigkeiten angeboten. Entsprechend variieren die Kosten und die Schnittstellen.

Für kleinere Anbindungen (z.B. Workgroups) werden Verbindungen mit einer Übertragungsgeschwindigkeit von 64 Kbit/s empfohlen. Es gibt natürlich Applikationen, wo eine geringere Übertragungsrate ausreicht. Werden höhere Übertragungsraten benötigt, so bietet sich die in Europa übliche E1-Verbindung (im Prinzip ein ISDN Primärmultiplexanschluss) mit einer Übertragungsrate von 2048 kbit/s an.

Router haben einen oder mehrere WAN-Ports, die entweder fest eingebaut sind oder bei

modularen Modellen mit entsprechenden Schnittstellenmodulen aufgerüstet werden können. Übliche physikalische Schnittstellen für Synchronbetrieb sind RS449, V35 und X.21, für asynchronen Betrieb das RS232-Interface. Für den Anschluss an ISDN wird die SO-Schnittstelle verwendet.

Netzwerkprotokolle

Router routen ein oder mehrere Netzwerkprotokolle. Die am häufigsten von Routern unterstützten Netzwerkprotokolle sind IP und IPX. Durch die Verbreitung heterogener Netze bieten die meisten Router auch Multiprotokoll-Fähigkeit. Außer IP und IPX werden je nach Router und Ausstattung auch DECnet, AppleTalk, OSI, XNS, VINES und Apollo Domain unterstützt. Alle nicht routbaren Protokolle wie z.B. LAT und NetBIOS werden, sofern der Router auch die Bridge-Funktion unterstützt, gebridged.

Routing-Protokolle

Mit welcher Effizienz ein Router Daten ans Ziel übermittelt, hängt wesentlich vom verwendeten Routing-Protokoll ab. Über einen protokollabhängigen Algorithmus wird vom Router der optimale Datenpfad zwischen Sender und Empfänger berechnet, wofür unterschiedliche Netzwerkparameter ausgewertet werden. Das IGRP-Protokoll (Interior Gateway Routing Protocol) beispielsweise, das von Cisco entwickelt wurde, berechnet durch Verknüpfung der wichtigsten Faktoren wie durchschnittliche Übertragungsdauer, Last und Bandbreite eine Messgröße, die als qualitative Bewertung des zugehörigen Datenweges verstanden werden kann. Jeder der aufgeführten Parameter geht hierbei mit einer durch den Netzwerkmanager konfigurierbaren Gewichtung in die Entscheidung über die Wegewahl mit ein. Durch dieses Verfahren wird sichergestellt, dass der Router die einzelnen Pakete zielgerichtet und unter Berücksichtigung des dynamischen Netzwerkzustands zum vorgesehenen Empfänger lenkt. Die kontinuierlich via Routing-Protokoll ermittelten Informationen werden in den Routing Tabellen gespeichert. Die gängigsten Router-Protokolle sind außer dem oben erwähnten IGRP das erweiterte EIGRP (Enhanced IGRP), OSPF (Open Shortest Path First), NLSP (NetWare Link State Protokoll), RIP (Router Information Protokoll), IS-IS (Intermediate System to Intermediate System), BGP, EGP, ES-IS und RTMR. Bei den Routingprotokollen unterscheidet man zwischen Distance-Vektorprotokollen, wie etwa dem weit verbreiteten RIP und Link State Protokollen wie NLSP. Letztere sind schneller und effizienter.

Aus Kompatibilitätsgründen unterstützen viele Router mehrere Routing-Protokolle, allerdings ist die Verwendung des gleichen Routing-Protokolls keine Gewähr dafür, dass Router unterschiedlicher Hersteller auch uneingeschränkt miteinander kommunizieren können. Ursache hierfür sind herstellereigene Funktionen, für die es keinen verbindlichen Standard gibt.





Verbindungs-Protokolle

Da die Pakete über die WAN-Verbindung anders transportiert werden als im LAN, werden Verbindungsprotokolle benötigt, die den sicheren Transport auf der WAN-Verbindung übernehmen. Mindestens eines, meistens aber mehrere der folgenden Verbindungsprotokolle sind in Routern implementiert: PPP, HDLC, Frame Relay, ISDN, SMDS, X.25.

PPP kommt eine besondere Bedeutung zu, da über dieses standardisierte Protokoll (vorausgesetzt, es handelt sich um kompatible PPP-Versionen) Router von verschiedenen Herstellern untereinander Verbindungen aufbauen können.

Management

Das Management erfolgt entweder über SNMP, das inzwischen alle Router der jüngsten Generation unterstützen, oder über die von den Herstellern implementierten eigenen Managementfunktionen.

Für die Konfiguration eines Routers muss mit einem höheren Managementaufwand gerechnet werden als für die Konfiguration der Plug & Play-Bridges. Dieser Umstand verursacht nicht nur Probleme, sondern auch Kosten. Man stelle sich ein Unternehmen mit 100 Außenstellen vor, bei denen die Routersoftware upgedatet werden muss. Jeder Router müsste aufgesucht werden, da es vor Ort keinen Mitarbeiter gibt, der den Router updaten und konfigurieren kann. Daher sollten die Router vollständig von einer zentralen Stelle aus konfiguriert, upgedatet und gemanaged werden können.

Was das Softwareupdate von einer zentralen Stelle aus angeht, so reicht die Palette je nach Hersteller von „nicht möglich“ bis „problemlos“. Manche Hersteller erlauben zwar das Update über die WAN-Leitung, wenn aber eine Störung bzw. ein Fehler bei der Übertragung auftritt, geht nichts mehr, da die alte Softwareversion bereits aus dem Flash PROM entfernt wurde. Andere Hersteller begegnen diesem Problem, indem im Router so viel Speicher vorhanden ist, dass gleichzeitig zwei Softwareversionen gespeichert werden können. Wiederum andere bieten die Möglichkeit, alternativ mittels Modem auf den Router zuzugreifen.

7.1.13 Spezielle Features

Immer mehr Router Hersteller bieten die Funktion der Datenkompression an, um die meistens knappe Bandbreite kostengünstig zu erhöhen.

Da Kompressionsraten immer von der zu komprimierenden Datenstruktur abhängen, schwanken die Angaben je nach Hersteller sehr stark. Ein Kompressionsfaktor von 2:1

bis 4:1 kann als realistisch angesehen werden.

Bietet ein Router das Feature Dial on Demand, ermöglicht dies den automatischen Aufbau einer Wählverbindung, wobei je nach Leitungstyp ein Modem oder ein ISDN-Terminaladapter einsetzbar ist. Bei manchen Routern ist ein ISDN-Terminaladapter bereits integriert. Diese Funktion wird vor allem als Backupfunktion eingesetzt für den Fall, dass die Standardleitung ausfallen sollte.

Software

Gespeichert wird die Routersoftware im Allgemeinen in Flash PROMs, die den Vorteil des einfachen Upgrades bieten. Beim Booten des Routers wird dann die Software in das RAM geladen und ausgeführt. Was den Softwareumfang angeht, verfolgen die Hersteller unterschiedliche Strategien. Entweder wird mit dem Router eine Basisversion mitgeliefert, die dann später nach Bedarf erweitert werden kann, oder es wird gleich die gesamte Software mitgeliefert.

Konzentratoren

Mit zunehmender Größe eines Netzwerkes nimmt auch die Schwierigkeit zu, solche Netze zu betreuen. Da ein Netz nie ein starres Gebilde ist, kann der Überblick sehr schnell verloren gehen, wenn zum Beispiel häufig umgezogen oder öfters erweitert wird. Auch Probleme bezüglich Netzlast und Fehler werden dadurch grösser. Im Gegensatz dazu darf das Netz nie ausfallen.

Mit Konzentratoren können größere Netze effizient konfiguriert, überwacht und verwaltet werden. Konzentratoren sind Informationsgeber für das Management von lokalen Netzen, da alles in einem Knotenpunkt zusammenkommt. Vor allem die Betriebskosten in Großen Netzen dürfen nicht außer Acht gelassen werden, da sie oft die Anschaffungskosten erheblich übersteigen. Die Verfügbarkeit des Netzes ist von erheblicher Bedeutung für ein Unternehmen. Konzentratoren sind aufgrund ihrer räumlichen Verteilung im Netz in der Lage, besonders effektiv Störungen und Totalausfälle zu vermeiden. Mit entsprechender Managementsoftware können Engpässe frühzeitig erkannt werden. Für die in der Regel modularen Konzentratoren gibt es eine Vielzahl von Modulen wie Repeater, Terminalserver, Bridges, Router, Switches und Multiplexer.

Größere Konzentratoren machen heute nur noch Sinn, wenn sie über eine sehr schnelle Backplane verfügen, da z.B. mit stackablen Lösungen vergleichbare Lösungen zur Verfügung stehen.



7.1.14 Gateways

Gateways decken alle sieben Schichten des OSI-Referenzmodells ab und bewirken eine Umsetzung aller Schichten zwischen zwei unterschiedlichen Systemen. Sie sind notwendig für die Anpassung bzw. für den Übergang von einem Netztyp auf einen anderen, wenn Netze mit unterschiedlichen Protokollen gekoppelt werden. Beispielsweise werden Gateways benutzt, wenn TCP/IP-Systeme mit DECnet-Hosts oder SNA-Hosts Daten austauschen müssen.

Gateways müssen nicht unbedingt reine Hardwarelösungen sein, es gibt auch Softwaremodule mit Gatewayfunktion. Zu den Aufgaben eines Gateways gehören: Adressierung über die Grenzen eines Netzwerks hinaus, Adressabbildung, Wegewahl und Protokollkonvertierung. Ein typisches Einsatzgebiet von Gateways ist der Zugang eines LANs auf einen Telekommunikationsdienst, beispielsweise die X.25-Gateways für Datex-P bzw. Telepac und Datanet 1, oder auch der Austausch von Electronic Mail zwischen zwei Rechnern in unterschiedlichen Netzen mittels Mail-Gateway.





7.2 100 Mbit/s Fast Ethernet

Aufgrund der gravierenden Änderungen im Netzwerkbereich, vor allem hervorgerufen durch die Anzahl der vernetzten Rechner und der damit verbundenen Netzlast, hat Ethernet mit seinen 10 Mbit/s inzwischen in vielen Netzen seine Leistungsgrenze erreicht.

Ethernet Switches eignen sich sehr gut, um Netzwerküberlastungen zu reduzieren, können jedoch maximal 10 Mbit/s an Durchsatz pro Port liefern. Wird Full Duplex unterstützt, kann zwischen zwei Knoten ein Durchsatz von max. 20 Mbit/s erreicht werden. Für Anwendungen, die mehr als 20 Mbit/s an Durchsatz benötigen, kommt das teure FDDI in Frage, das vor allem für den Backbone-Bereich zu empfehlen ist, oder der 100 Mbit/s Fast Ethernet Standard. ATM ist ebenfalls wegen der hohen Kosten nur für wenige Einsatzbereiche zu empfehlen. Produkte für Gigabit Ethernet sind vorhanden, haben ihren Platz aber derzeit hauptsächlich im Backbone-Bereich.

Das Ziel der Initiatoren von Fast Ethernet war es, ein möglichst kostengünstiges Hochgeschwindigkeitsnetz anbieten zu können, welches außerdem einen problemlosen Migrationspfad von bestehenden Netzen aus ermöglichen sollte. Das Ergebnis dieser Bemühungen waren die zwei konkurrierenden Systeme für ein 100 Mbit/s LAN und zwar das vom IEEE-Gremium IEEE802.3u standardisierte 100BASE-T und das als IEEE803.12 standardisierte 100VG-AnyLAN.

Aus diesem Konkurrenzkampf ist ganz klar der 100BASE-T Fast Ethernet Standard als Sieger hervorgegangen. Ein entscheidender Pluspunkt für die Akzeptanz war sicher die einfache Migration von Ethernet zu Fast Ethernet, da 100BASE-T direkt auf dem Ethernet Standard aufsetzt. Es muss also keine völlig neue Technologie erlernt werden, da das Zugriffsverfahren, Adressierung, Frameformat, Installation etc. quasi identisch sind. Hinzu kommen lediglich die Fast Ethernet spezifischen Erweiterungen, die sich im Wesentlichen auf die Spezifikationen von Kabel, Kabellängen und Repeatern bezieht. Außerdem unterstützen fast alle namhaften Hersteller von Netzwerkprodukten diesen Standard. Unter dem Aspekt der Kosten hat Fast Ethernet ganz klar die Nase vorn. Geht die Preisentwicklung in diesem Tempo weiter, wird innerhalb kurzer Zeit die Preisdifferenz zwischen Ethernet- und Fast Ethernet-Komponenten unbedeutend sein.

Was ist eigentlich 100BASE-T?

Vereinfacht ausgedrückt ist es Ethernet, nur zehn Mal schneller. Deshalb wird in den folgenden Abschnitten im Wesentlichen auf die Unterschiede von 100BASE-T zu Ethernet eingegangen. Detaillierte Informationen zum 10 Mbit/s Ethernet sind unter dem Kapitel Ethernet (Seite 304) zu finden.

7.2.1 100BASE-T Zugriffsverfahren

100BASE-T benutzt ebenso wie 10BASE-T das Kollisionsprotokoll CSMA/CD als Zugriffsverfahren. Der stochastische Netzzugriff erlaubt keine dedizierte Zuordnung von Bandbreite. Aus diesem Grund ist 100BASE-T für Anwendungen, die, wie etwa Multimedia-Anwendungen, eine zugesicherte Bandbreite brauchen, weniger geeignet.

Auf der physical Layer 1 (PHY) ist das physikalische Interface definiert. Bei 10 Mbit/s Ethernet ist dies das Attachment Unit Interface (AUI), bei 100 Mbit/s Fast Ethernet wird dieses Interface Medium Independent Interface (MII) genannt. Allerdings ergeben sich in der Praxis teilweise Inkompatibilitäten zwischen MII-Interfaces und MII-Transceivern. Wenn nicht wichtige Gründe dagegen sprechen, sollte man Geräte mit fest eingebauter Schnittstelle einer MII-Transceiver-Lösung vorziehen.

7.2.2 100BASE-T Network Interface Card (NIC)

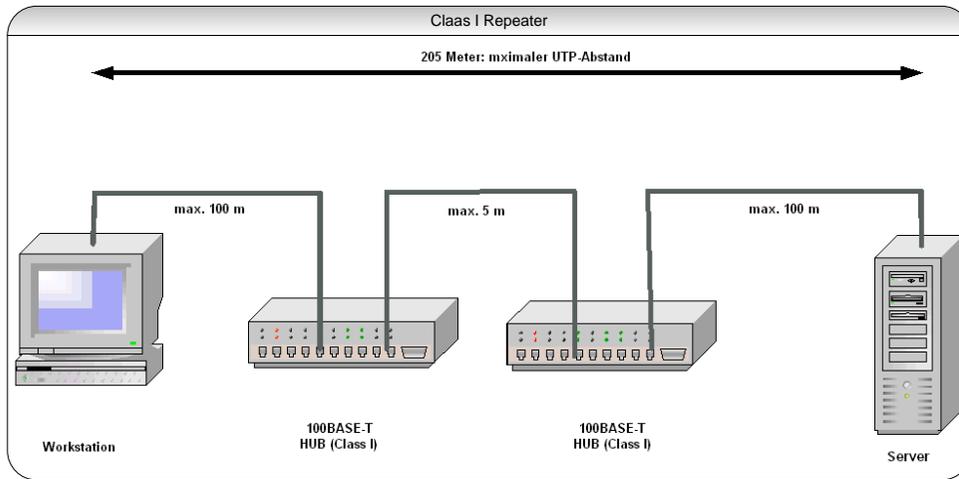
Wie beim 10 Mbit/s Ethernet wird auch bei 100 Mbit/s Fast Ethernet zum Anschluss von Geräten (Server/Clients etc.) ans Netzwerk ein Netzwerkadapter, oder auch Network Interface Card (NIC) genannt, benötigt.

Die Netzwerkadapter, die sowohl 10 Mbit/s und auch 100 Mbit/s unterstützen, haben sich als De-Facto-Standard durchgesetzt. Aufgrund der Auto-Negotiation-Funktion erkennen diese Adapter automatisch den richtigen Übertragungsmodus. Der Übertragungsmodus wird mit dem nWay Protokoll auf der physikalischen Ebene ermittelt. Das nWay Protokoll ermöglicht Fast-Ethernet-Adaptoren und Switch-Ports die automatische Einstellung der Geschwindigkeit und des Übertragungsmodus, d.h. ob 10 Mbit/s oder 100 Mbit/s, ob Full oder Half Duplex, vorausgesetzt auf beiden Seiten ist das nWay Protokoll implementiert. Beim Kauf eines 10/100 Mbit/s Netzwerkadapters sollten folgende Fragen geklärt sein: - An welchen Kabeltyp soll der Adapter angeschlossen werden (UTP-Kabel Kategorie 3, 4, 5 oder Lichtleiter)?

- Welcher Bustyp hat der Rechner (PCI, EISA, ISA, PC-Card)?
- Gibt es passende Treiber für das eingesetzte Betriebssystem?

7.2.3 100BASE-T Repeater

100 Mbit/s Fast Ethernet Repeater arbeiten genau wie 10 Mbit/s Ethernet Repeater, nur mit dem Unterschied, dass die Übertragungsgeschwindigkeit höher ist. Der Ethernet Standard definiert einen maximalen Round Trip Delay in einer Collision Domain von 576 Bitperioden. Bei 100 Mbit/s entspricht dies 5,76 Mikrosekunden, bei 10 Mbit/s sind es 57,6 Mikrosekunden. Dieser Wert bestimmt, welche max. geographische Ausdehnung ein

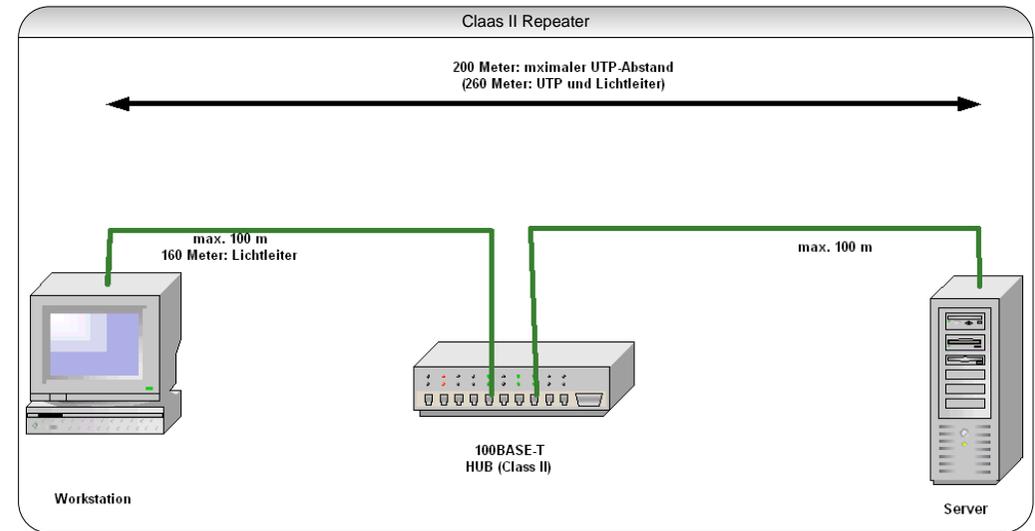


Netzwerk innerhalb einer Collision Domain haben darf. Überschreitet die Signallaufzeit (Laufzeit des Signals auf den Kabeln plus Verzögerungszeiten in Repeatern, NICs) diesen Wert, versagt die Kollisionserkennung. Aus diesem Grund verringert sich der geographische Durchmesser einer Collision Domain von 2500 m bei 10 Mbit/s Ethernet auf 205 m bei 100 Mbit/s Fast Ethernet, wenn kein Lichtleiterkabel zum Einsatz kommt und Class-II-Repeater verwendet werden. Da die Übertragungszeit für einen Block bei Fast Ethernet zehn Mal kürzer ist, kann die 5-4-3-Repeater-Regel, die beim 10 Mbit/s Ethernet beachtet werden muss (siehe auch Abschnitt Ethernet Repeater), nicht angewendet werden. Es mussten neue Repeater-Regeln definiert werden.

Der 100BASE-T-Standard unterscheidet zwei Repeaterklassen: Class-I- und Class-II-Repeater.

Class-I-Repeater weisen höhere Verzögerungszeiten (0,7 Mikrosekunden) oder geringer) als Class-II-Repeater auf. Zwischen zwei Endgeräten darf deshalb bei Ausnutzung der maximalen Kabellänge zwischen Node und Repeater von 100 m nur ein Class-I-Repeater dazwischengeschaltet sein. Class-I-Repeater stammen aus der Anfangszeit von Fast Ethernet. Inzwischen werden fast nur noch Class-II-Repeater hergestellt, da sie wesentlich flexibler eingesetzt werden können und kein wesentlicher Kostenfaktor zwischen Class-I und Class-II-Repeatern besteht.

Class-II-Repeater haben eine Verzögerungszeit von 0,46 Mikrosekunden und darunter. Unter Ausnutzung der maximalen Kabellängen zwischen Repeater und Node von 100 m dürfen zwei Class-II-Repeater zwischen den Endgeräten liegen. Dabei darf der Interrepeaterlink zwischen den beiden Repeatern max. 5 m betragen.



Die bisher genannten Angaben bezüglich der erlaubten Kabellängen bezogen sich auf TwistedPair Kabel. Welche Längen mit Lichtleiterkabel zulässig sind, kann der Tabelle entnommen werden.

Auf den ersten Blick scheinen die Restriktionen bezüglich Repeatern und der maximalen Kabellängen eine Einschränkung für die Konfiguration von Fast Ethernet Netzen darzustellen. Aber näher betrachtet ist dem nicht so. Zum Beispiel lässt sich mittels Repeatern, die über einen internen Bus kaskadiert werden können, die Portzahl erhöhen, ohne die Repeaterregel zu verletzen, da die Repeater in einem "Stack" als ein Repeater zählen. Mit Lichtleiter-Komponenten können größere Distanzen überbrückt werden und mit Switches lassen sich problemlos neue Collision Domains aufbauen, also das Netz erweitern. Aufgrund ihrer Eigenschaften sollten Switches generell vermehrt in heutigen Netzen eingesetzt werden. Die Preise für Switches bewegen sich stark nach unten, sodass die Entscheidung für den Kauf eines Switches von der Kostenseite aus betrachtet einfacher ist.



7.2.4 100BASE-T Switches

Wie bei den Repeatern gilt auch bei den 100BASE-T Switches die gleiche Aussage, nämlich dass sie prinzipiell wie ihre Pendants aus dem 10 Mbit/s Ethernet arbeiten (mehr zur Funktionsweise von Switches ist im Abschnitt Ethernet Switches zu finden). Sie müssen nur mit einer zehnmal höheren Datenrate fertig werden. Dies wird durch den Einsatz von leistungsfähigen Prozessoren und mehr Speicher erreicht, was allerdings auch höhere Kosten nach sich zieht.

Switches sind ein fundamentales Element für die Konfiguration von Fast Ethernet Netzen, da über sie der Übergang von 10 Mbit/s auf 100 Mbit/s erfolgt und man ja normalerweise nicht alle Knoten im Netz gleichzeitig auf 100 Mbit/s umstellen kann oder möchte. Etliche Hersteller haben mittlerweile Fast Ethernet Switches im Programm, die sich, auf einem oder auch mehreren Ports, mittels nWay-Protokoll auf die Übertragungseigenschaften der Gegenstelle (Full oder Halbduplex, 10 oder 100 Mbit/s) einstellen können. Aufgrund der Restriktionen bezüglich Kabellängen und Repeatern sind sie auch bei der

Erweiterung von Fast Ethernet Netzen unentbehrlich, da durch den Einsatz eines Switches auch eine neue Collision Domain entsteht. Mit einem Fast Ethernet Extender kann vor allem eine sehr kostengünstige Distanzenerweiterung erfolgen. Ein Extender ist in seiner Funktion eigentlich ein Switch, allerdings mit nur zwei Ports. Der Extender kann ebenfalls die

Geschwindigkeitsanpassung von 10 Mbit/s auf 100 Mbit/s durchführen oder trennt auch nur die beiden anschließbaren Segmente in eigene Collision Domains. Nicht zu vergessen: Auch im Fast Ethernet gilt natürlich, dass mit Switches die Bandbreite im Netz erhöht wird.

Mit Dual Speed Hubs können 10BASE-T und 100BASE-TX Netze kostengünstig verbunden werden. Ein Dual Speed Hub ist eine Kombination aus 10/100BASE-T Switch und Repeater: An jedem Port kann ein Ethernet oder Fast Ethernet Gerät angeschlossen werden, im Dual Speed Hub erfolgt die Geschwindigkeitsanpassung. Ein Dual Speed Hub kann also die Migration von Ethernet nach Fast Ethernet erleichtern. Im Gegensatz zu einem 10/100BASE-T Switch leitet ein Dual Speed Hub Kollisionen weiter und erlaubt nur eine Datenübertragung zu einem Zeitpunkt. Ansonsten erfüllt ein Dual Speed Hub alle üblichen Repeaterfunktionen (Signalaufbereitung, Restaurierung der Präambel, Isolierung fehlerhafter Ports etc.).

Verbindung	Kupfer (Twisted pair)	Kupfer (Lichtleiter)	Lichtleiter (Multi-Mode)
Endgerät zu Endgerät	100 m		412 m (Half Duplex)
(Switch to Switch)	AMD Palomino > 1,4 GHz	AMD Morgan > 800 MHz	2000 m (Full Duplex)
Ein Class-I-Repeater	200 m	260 m	272 m
Ein Class-II-Repeater	200 m	308 m	320 m
Zwei Class-II-Repeater	205 m	216 m	228 m

7.2.5 Verkabelung

100BASE-T IEEE802.3u basiert ebenso wie 10BASE-T oder 10BASE-F auf reinen Punkt-zu-Punkt-Verbindungen. Zu beachten ist, dass kein Koaxial-Kabel unterstützt wird. Das hat zur Folge, dass die Entscheidung für Fast Ethernet in viele Fällen mit einer Neuverkabelung verbunden ist, da in Europa ThinWire immer noch sehr verbreitet ist. Aber auch jede andere schnelle Netzwerktechnologie wie CDDI, ATM oder Gigabit Ethernet setzt eine strukturierte Verkabelung voraus.

100BASE-T unterstützt drei „physical layers“, zwei davon definieren TwistedPair Kabel mit einer max. Länge von 100 m und die dritte multimode (412 m, 2000 m im Full Duplex Mode) oder singlemode Lichtleiter (10000 m oder mehr).

100BASE-TX: Setzt aufgrund der höheren Frequenz 2-paariges UTP Kategorie 5 oder IBM STP Typ 1 Kabel voraus. Die Signalfrequenz beträgt 125 MHz, sie wird mittels des Multi-Level Transmission-3 (MLT-3) Verfahren reduziert, so dass über das Kabel nur Signale mit einer Frequenz von 41,6 MHz gehen. Im Vergleich dazu ist bei 10BASE-T diese Signalfrequenz 20 MHz, was den Einsatz von Kategorie 3 UTP Kabel ermöglicht.

Mit einer 4-paarigen UTP-5 Verkabelung ist optional Full Duplex-Betrieb (200 Mbit/s) möglich, sofern beide Seiten dies unterstützen. Full Duplex ist zwischen Endstationen und Switch bzw. Switch-zu-Switch-Verbindungen möglich. Die maximale Länge eines TwistedPair-

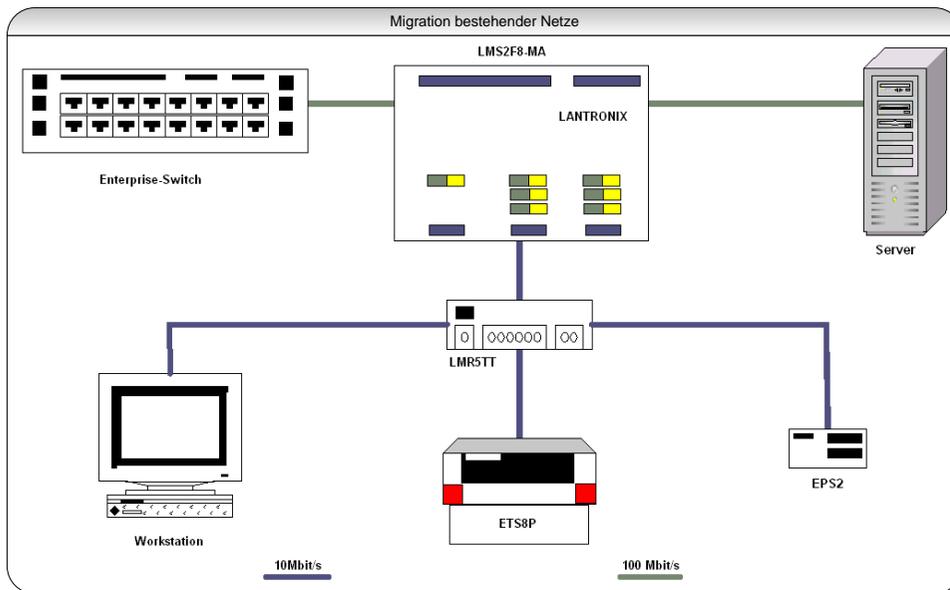
Segments beträgt aufgrund der maximal zulässigen Dämpfung 100 m. Für 100BASE-TX wurde der achtpolige RJ45-Stecker von 10BASE-T übernommen. 100BASE-T4: 100BASE-T4 ist eigentlich der einzig neue PHY Standard, der für 100BASE-T Fast Ethernet definiert werden musste, da 1 OOBASE-TX und 1 OOBASE-FX dem ANSI FDDI entnommen wurde. 100BASE-T4 wurde aufgrund der Großen in Nordamerika installierten Basis an UTP Kabel der Kategorie 3 entwickelt.

100BASE-T4 unterstützt 4-paarige ungeschirmte TwistedPair Kabel (UTP) der Kategorie 3, 4 und 5. Damit Kategorie 3 Kabel eingesetzt werden kann, erfolgt bei 100BASE-T4 die Übertragung der Signale über drei Datenleitungen. Dadurch wird erreicht, dass die Übertragungsfrequenz maximal 25 MHz beträgt. Die vierte Leitung wird für die Kollisionserkennung verwendet. Bei 100BASE-T4 ist kein Full Duplex möglich, da keine getrennte Sende- und Empfangsleitung wie bei 100BASE-TX/FX vorhanden ist. Die maximale Länge eines TwistedPair-Segments beträgt aufgrund der maximal zulässigen Dämpfung 100 m. Auch bei 100BASE-T4 kommt der gleiche RJ45 Stecker zum Einsatz wie bei 10BASE-T und 100BASE-TX.

100BASE-FX: 100BASE-FX spezifiziert einpaarige Lichtleiterkabel (multimode oder singlemode). Die maximale Länge von Lichtleiter-Segmenten variiert je nach eingesetzten Komponenten.

Für eine Switch zu Switch- oder Switch zu Adapter-Verbindung sind maximal 412 m über ein Multimode-Kabel erlaubt. Ist Full Duplex möglich, kann die Distanz bis zu 2000 m erhöht werden. Mit singlemode Kabel können im Full Duplex Modus bis zu 10000 m überbrückt werden. Da wie oben schon erwähnt der 100BASE-FX Standard dem ANSI FDDI entspricht, können sowohl der MIC/FDDI und der ST-Stecker eingesetzt werden. Empfohlen wird aber der kostengünstigere SC-Stecker, der bei ATM und inzwischen auch bei FDDI Verwendung findet.

7.2.6 Migration bestehender Netze



MII:

Das Media Independent Interface ist das Gegenstück zur AUI- Schnittstelle bei 10 Mbit/s Ethernet. MII-Transceiver stellen die Verbindung her zwischen der 40poligen MII-Buchse und einem beliebigen Fast Ethernet Kabelmedium, also Twisted Pair (T4 und Kategorie 5

STP) bzw. Lichtleiter (SC und ST Anschluss). Der Anwender hat also die Option, Fast Ethernet Geräte mit MII-Buchse mit seinem bevorzugten Kabelmedium zu verbinden. Die Migration zu 100BASE-T kann in mehreren Stufen erfolgen, dadurch kann sie individuell den topologischen, finanziellen und zeitlichen Gegebenheiten sehr gut angepasst werden. Nachfolgend werden exemplarisch einige mögliche Migrationspfade aufgezeigt. Die ersten Überlegungen müssen der Verkabelung gewidmet werden, denn 100BASE-T setzt Punkt-zu-Punkt Verbindungen voraus. Sofern noch keine TwistedPair Verkabelung (Kategorie 3, 4, oder 5) vorhanden ist, muss neu verkabelt werden, was je nach Umfang mit erhebliche Kosten verbunden sein kann. Die Empfehlung lautet ganz klar: Strukturierte Verkabelung mit UTP Kabel der Kategorie 5, wenn es um die Verkabelung bis zum Endgerät geht, da diese Kabel auch für Gigabit Ethernet, FDDI und ATM eingesetzt werden können. Bei längeren Distanzen oder im Backbone-Bereich sollte Lichtleiterkabel eingesetzt werden da, auch dieses für Gigabit, FDDI und ATM geeignet ist.

Ist die Entscheidung für 100BASE-TX gefallen, so könnte ein erster Migrationsschritt wie folgt aussehen:

Alle neu ins Netz zu integrierenden Rechner werden über UTP Kabel der Kategorie 5 ins bestehende Netz integriert. In den Rechnern werden 10/100 Mbit/s NICs installiert, die in der ersten Phase noch unter 10 Mbit/s betrieben werden und in der zweiten dann unter 100 Mbit/s. Dabei ist die Umstellung denkbar einfach, denn der Rechner muss nur an einen 100BASE-TX-Repeater, besser noch -Switch angeschlossen werden. Weder bei den Treibern noch bei der Software müssen Änderungen vorgenommen werden, selbst vorhandene Netzwerkmanagementapplikationen können weiterhin ohne Änderung genutzt werden. Auch die Einstellung des richtigen Übertragungsmodus wird von der vorhanden Auto-Negotiation-Funktion übernommen.

Heutige Rechner sind aufgrund ihrer Bus-Architektur (z.B. PCI) in der Lage, so viele Pakete zu verschicken, dass Ethernet mit seinen 10 Mbit/s nicht mehr ausreicht. Mit Full Duplex sind zwar theoretisch 20 Mbit/s möglich, dies ist aber bei Servern nicht so effizient, da in der Regel die Masse des Datentransfers vom Server zum Client erfolgt. Allerdings sind die Mehrkosten für Full Duplex bei einer solchen Anwendung gering. Es liegt also nahe, dass bei Servern, auf die eventuell Hunderte von Clients zugreifen, das vorhandene, hohe Leistungspotential auch ausgenutzt wird, indem die Server über 100BASE-T in das bestehende 10 Mbit/s Netz eingebunden werden. Eine weitere Stufe der Leistungssteigerung ist denkbar, indem im Server mehrere Netzwerkadapter installiert werden.

Umgesetzt werden kann die Servereinbindung z.B. mittels eines Workgroup-Switches. Ein Workgroup-Switch hat typischerweise mehrere switched 10BASE-T Ports und einen oder mehrere 100 Mbit/s Ports, über die die Geschwindigkeitsanpassung von 10 Mbit/s zu 100 Mbit/s erfolgt. Die 100 Mbit/s Ports sind entweder fix mit einem Interface (100BASE-TX, 100BASE-T4, 100Base-FX) bestückt oder aber modular aufgebaut, so dass zwischen den drei Interfacetypen ausgewählt werden kann. Es gibt auch Switches





mit MII-Schnittstelle. Vorteil dieser Lösung ist die Flexibilität, die dieser Anschluss bietet. Mittels kostengünstiger MII-Transceiver kann der Switch an das gewünschte Medium angeschlossen werden. Auch ein nachträglicher Medienwechsel ist so einfach zu realisieren. Zu beachten ist bei der Auswahl von Workgroup-Switches, dass je nach Modell die Zahl der zu speichernden Adressen pro Port von einer bis über 1000 gehen kann. Die meisten Switches haben heute eine Shared Address Table. Man sollte darauf achten, dass die Address Table auch für spätere Netzerweiterungen groß genug ist, da es keinen Sinn macht, an einen Port, der nur wenige Adressen speichern kann, ein ganzes Segment mit vielen Knoten anzuschließen. Der Server, in dem ein 100BASE-TX Netzwerkadapter eingebaut ist, wird direkt an einen Port des Workgroup-Switches angeschlossen. Sollen weitere Server über 100 Mbit/s eingebunden werden, kann an einen 100BASE-TX Port des Switches ein 100BASE-TX Repeater angeschlossen werden: Wenn möglich ein Class-II Repeater, um bei weiteren Erweiterungen flexibler zu sein. Werden nur Server an diesen Repeater angeschlossen (ist aber kein muss), so spricht man auch von einer sogenannten Server-Farm. Soll die Portzahl weiter erhöht werden, um z.B. eine komplette Arbeitsgruppe in ein 100 Mbit/s Fast Ethernet einzubinden, kann dies mittels eines weiteren Class-II Repeaters erfolgen. Reichen die Ports dann immer noch nicht aus, so kann die Portzahl via Repeater, die über einen internen Bus kaskadierbar sind, weiter erhöht werden. Voraussetzung hierfür ist, wenigstens einer der beiden Class-II Repeater verfügt über einen Bus, über den weitere Repeater kaskadiert werden können. Besser und kostengünstiger ist es, gleich einen Switch einzusetzen: Mit ihm beginnt wegen der neuen Collision Domain die Rechnung bezüglich der Repeaterregel und der Kabellängen von neuem.

Bei größeren Netzen ist der Einsatz von Backbone-Switches zu empfehlen. In der Switchfunktion besteht kein Unterschied zwischen einem Workgroup-Switch und einem Backbone-Switch. Die Switches unterscheiden sich in der Regel in der Anzahl der Ports, der Adress- und Speichergröße und der Prozessorleistung.



7.3 1000 Mbit/s Gigabit Ethernet

Alle für den Aufbau oder die Einbindung in ein bestehendes Netz benötigten 100BASE-T Produkte werden von transtec angeboten. Detailliertere Produktbeschreibungen dazu sind in den Kapiteln für Fast Ethernet-Adapter, -Switches und -Hubs zu finden.

Nachdem Fast Ethernet Produkte vom Markt sehr gut aufgenommen werden und in vielen Installationen Fast Ethernet bis zum Desktop reicht, haben manche Netzwerkbetreiber Bedarf nach einer schnelleren Backbone-Technologie, die einfach zu implementieren und auch noch kostengünstig ist. Bisher war ATM die einzige Möglichkeit, um ein noch schnelleres Backbone aufzubauen. Der Einsatz von ATM erfordert jedoch einen erheblichen Aufwand bei der Hardware und Software, denn ATM ist eine grundlegend andere Technologie als Ethernet. Im Mai 1996 hat sich eine Gigabit Ethernet-Allianz (GEA) zusammengefunden: Unter den Gründungsmitgliedern sind namhafte Hersteller wie 3Com, Cisco, Sun Microsystems, Bay Networks und Intel. Mittlerweile haben sich über 100 Hersteller in der GEA zusammengeschlossen. Ziel der GEA ist es, in Zusammenarbeit mit der IEEE einen Gigabit Ethernet Standard unter dem Namen IEEE 802.3z zu entwickeln. Die Standardisierungsphase von 1000BASE-x über Lichtwellenleiter ist abgeschlossen ebenso die für 1000BASE-TX, also Gigabit Ethernet über Cat5 TwistedPair Kabel. Die Anzahl an Gigabit Ethernet Produkte nimmt sprunghaft zu, sodass sich Gigabit Ethernet auch in naher Zukunft im High-Speed Backbonebereich als Standardtechnologie durchsetzen wird. Neben der höheren Bandbreite bei Gigabit Ethernet ergeben sich für den Anwender noch weitere Vorteile: Da der Aufbau der Datenpakete und das Zugriffsverfahren identisch mit Ethernet bzw. Fast Ethernet ist, sind praktisch keine Änderungen an Management-Software, Netzwerktriebssystem und Anwendungsprogrammen erforderlich. Dadurch reduziert sich auch der Umstellungs- und Schulungsaufwand erheblich.

7.3.1 1000BASE Zugriffsverfahren

Wie auch bei den bestehenden Ethernet-Standards IEEE 802.3 (10 Mbit/s) und IEEE 802.3u (100 Mbit/s) kommt bei IEEE 802.3z und IEEE802.3ab Gigabit Ethernet das Kollisionsprotokoll CSMA/CD zum Einsatz. Allerdings ist geplant, über die Protokollerweiterung RSVP (Resource Reservation Protocol) die Quality of Service Eigenschaft von ATM nachzubilden, so dass für zeitkritische Übertragungen (z.B. im Multimediabereich) dediziert Bandbreite zur Verfügung gestellt werden kann.

7.3.2 Migrationswege für bestehende Netze

Gigabit Ethernet findet zunächst als schnelles Backbone in Großen Installationen sein Einsatzgebiet, um Bandbreite zwischen Switches, Hubs, und Routern zur Verfügung zu stellen. Beispielsweise also Verbindungen vom Switch zum Router, Switch zu Switch, Switch zu Server und Switch zu Hub. Die Anbindung des Desktops wird vorerst weiterhin „klassisch“ über Ethernet oder Fast Ethernet vorgenommen, es ist aber ein Ziel der GEA,

Server bzw. High-End-Workstations über entsprechende Netzwerkkarten direkt an Gigabit Ethernet anzuschließen. Beispiele:

- Anbindung eines oder mehrerer Server an einen 100/1000-Switch, - Kopplung von 100/1000-Switches über 1000Mbit/s-Leitungen,
- Ersatz/Erweiterung von FDDI-Backbones mittels Gigabit Ethernet Switches bzw. Gigabit Ethernet Repeatern.

7.3.3 Gerätearten

Nachdem Gigabit Ethernet auf allen relevanten ISO/OSI-Leveln identisch ist mit Ethernet bzw. Fast Ethernet, werden alle entsprechenden Geräte auch für Gigabit Ethernet entwickelt. Nähere Produktinformationen finden sich im Kapitel SuperStack von 3Com.

7.3.4 Verkabelung

Ziel der GEA ist es, Gigabit Ethernet soweit wie möglich auf bereits installiertem Kabel (UTP/Fibre) einzusetzen. Allerdings gibt es Einschränkungen bezüglich der Kabellängen. Wie auch bei Fast Ethernet basiert die Verkabelung auf Punkt-zu-Punkt-Verbindungen. Auf der physikalischen Schicht gibt es zwei unterschiedliche Kabelmedien:

Multi- und Singlemode Lichtleiter:

Als Lichtleiter kommen sowohl Singlemodekabel wie auch Multimodekabel zum Einsatz. Die maximalen Längen sind 3000 m für Singlemode- und 550 m für Multimodekabel. 1000BASE-SW verwendet Low-cost Multimodekabel, das in horizontalen, kurzen Backboneverbindungen zum Einsatz kommen soll. 1000BASE-SX bietet maximale Längen von 525 m (50 micron LWL) und 260 m (62,5 micron LWL). 1000BASE-LX verwendet hochwertigere Lichtleiterkabel und erreicht mit Singlemode-LWL 5000 m, mit Multimodekabel sind Entfernungen von 550 m (50 micron LWL) bzw. 440 m (62,5 micron LWL) überbrückbar. 1000BASE-LX eignet sich somit für längere Multimode-Backbones und Singlemode Campus Backbones.

Kupferbasierende Kabelverbindungen:

1000BASE-CX definiert Verbindungen über ein IBM STP Typ 1 Kabel. Durch die Beschränkung auf max. 25 m eignet es sich zum Überbrücken kurzer Entfernungen, also etwa zum Verbinden von Endgeräten oder in Schalträumen. 1000BASE-T verwendet Kategorie 5 Twisted Pair Kabel und überbrückt Entfernungen von bis zu 100 m. Der große Vorteil von 1000BASE-T ist, dass bereits vorhandene Kabelinfrastruktur, soweit sie den Anforderungen von Kategorie 5 erfüllt, für Gigabit Ethernet weiterverwendet werden kann. Die Übertragung soll über die vier Paare des Kategorie 5 Twisted Pair Kabel





erfolgen. Die Entwicklung von 1000BASE-T ist noch nicht abgeschlossen.

Eine Spezifikation für eine medienunabhängige Schnittstelle (GMII= Gigabit Media Independent Interface) ist geplant. Damit ist es möglich, Gigabit Geräte in eine heterogene Infrastruktur einzubinden.

Standard	Kupferkabeltyp	Fiber Type (Multi/Mode)	Durchmesser (Micron)	max. Kabellänge (m)
1000 BASE-SX	V.22	MM	62,5	220
1200 bps Vollduplexbetrieb über Wählleitung. Standard in USA und Kanada		MM	50	500
1000 BASE-LX	V.24	MM	62,5	550
75/1200 bps Halbduplexbetrieb über Wählleitung		MM	50	550
Bell 201	2400 bps, Halbduplexbetrieb über Wählleitungen oder Vollduplexbetrieb	SM	9	5000
1000 BASE-CX	IBM Typ 1			25
1000 BASE-T	Cat 5 UTP			100

Kupferkabeltyp



8. Token-Ring

Token-Ring ist eine von IBM entwickelte Netzwerktechnologie. Das Wort Token bezieht sich auf das Zugriffs-verfahren. Die Bezeichnung Ring beschreibt die Topologie in Form eines physikalischen Rings.

Ein Token-Ring-Netzwerk ist vor allem dann zu empfehlen, wenn Systeme auch gleichzeitig Zugang zu IBM-Rechnern erhalten sollen.

8.1 Zugriffsverfahren

Token-Ring arbeitet nach dem Token-Passing-Verfahren. Die Zugriffskontrolle ist grundlegend anders als bei Ethernet: Eine Station kann erst dann senden, wenn sie dazu die Berechtigung erhält. Diese Berechtigung wird von einem im Ring kreisenden Datenpaket erteilt, dem so genannten Token (die beste deutsche Übersetzung ist wohl Münze, Pfand oder Freizeichen). Der Adapter, der zuerst eingeschaltet wurde, übernimmt die Generierung (Monitorfunktion) des Token. Sobald weitere Stationen im Netz hinzukommen, empfangen sie das Token, verstärken es und senden es weiter. Eine sendebereite Station erkennt am Token, ob das Netz frei ist. In diesem Fall wird das Token als belegt markiert und die Daten werden mit Absende- und Zieladresse angehängt.

Die Empfangsstation bestätigt den Empfang im Token und schickt es weiter. Kommt es wieder beim Sender an, wird es als Frei-Token an die nächste Station weitergegeben. Das Zeitverhalten des Netzes wird durch die Länge des Rings und die Anzahl der Stationen bestimmt.

Bei diesem so genannten deterministischen Zugriffsverfahren kann es im Gegensatz zu Ethernet nicht vorkommen, dass bei hoher Netzbelastung einzelne Stationen unbestimmt lange warten müssen, bis sie senden können. Token-Ring bietet eine bestimmbar maximale Wartezeit. Allerdings muss auch bei geringer Belastung immer auf ein freies Token gewartet werden, woraus sich Zeitnachteile gegenüber Ethernet ergeben können.

8.2 Verkabelung

Wie bei jeder Netzwerktopologie müssen auch bei Token-Ring Konfigurationsregeln bezüglich Kabel und Netzwerkadapter eingehalten werden. Die maximale Ringlänge ist abhängig von dem verwendeten Kabel sowie der Anzahl der Stationen und der MAUs (Media Access Unit).

Für Token-Ring gibt es unterschiedliche Kabeltypen und -anschlüsse. In der Regel wird ein STP-Kabel (Shielded TwistedPair) verwendet. Die Verkabelung erfolgt zwar sternförmig, wegen der doppelten Leitungsführung (Hin- und Rückleitung) entsteht jedoch

ein physikalischer Ring.

Wird das Token-Ring-Netzwerk als physikalischer Doppelring ausgeführt, erhöht sich die Betriebssicherheit des Netzes. Erweiterungen im laufenden Netzbetrieb und das Lokalisieren auftretender Fehler sind sehr einfach.

8.3 Komponenten

Es gibt zwei Typen von Token-Ring- Adaptern, die sich in der Übertragungsgeschwindigkeit unterscheiden: 4 und 16 Mbit/s. Alle im Netz befindlichen Adapter müssen mit der gleichen Übertragungsgeschwindigkeit arbeiten. Das hat zur Folge, dass der gesamte Verkehr im Netz mit 4 Mbit/s läuft, wenn auch nur eine Station 16 Mbit/s nicht unterstützt. Zwar werden fast nur noch Adapter für 16 Mbit/s produziert, aber tatsächlich sind noch viele Token-Ring-Netze auf 4 Mbit/s ausgelegt.

Über Multi-Station Access Units (MAUs) werden die einzelnen Stationen sternförmig angeschlossen. Die Zuführungskabel besitzen aber zwei getrennte Leiter für den Transport der Signale zu und von der Station, so dass ein physikalischer Ring realisiert wird.

Mit einem einzelnen MAU kann ein funktionsfähiges Netzwerk aufgebaut werden. Für größere Netzwerke werden mehrere MAUs eingebunden.

8.4 Zukunft von Token-Ring

Token-Ring kann mit seiner maximalen Übertragungsrate von 16 Mbit/s inzwischen nicht mehr zu den schnelleren Netzwerktechnologien gerechnet werden. Wir rechnen nicht damit, dass Token-Ring sich weiter verbreiten wird. Die High Speed Token-Ring Alliance hat sich zum Ziel gesetzt, Datenraten von 100 Mbit/s bis 1 Gbit/s über Token-basierte Zugriffstechnik zu standardisieren. Zu den Gründungsmitgliedern gehören u.a. Madge, Olicom, Cisco, 3Com und Cabletron. Erste Produkte sind bereits vorgestellt worden.





9. FDDI

FDDI (Fiber Distributed Data Interface) ist eine Möglichkeit zur Erhöhung der Bandbreite in einem Netzwerk, wenn die 10 Mbit/s von Standard Ethernet nicht mehr ausreichen bzw. wenn es sich um räumlich ausgedehnte Netzwerke handelt, die mit Fast Ethernet schwierig aufzubauen wären.

Durch seinen hohen Durchsatz und aufgrund seiner Großen Zuverlässigkeit wird FDDI oft als zentrales High-Speed Backbone, z.B. zur Kopplung von Ethernet-Segmenten eingesetzt. Für den FDDI-Ethernet-Übergang werden entsprechende Produkte angeboten. Bandbreiten-intensive Stationen, wie z.B. zentrale Server, können unter Umgehung des Ethernet-Flaschenhalses direkt in den FDDI-Ring eingebunden werden.

Die Vorteile von FDDI sind die relativ hohe Nettodatenübertragungsrate, die Fehlertoleranz aufgrund der Doppelring-Topologie und die elektromagnetische Unempfindlichkeit bei Verwendung von Lichtleiter als Übertragungsmedium. Aufgrund seines MAC-Protokolls bietet FDDI eine faire und flexible Aufteilung der Bandbreite unter den Stationen. Im Gegensatz zu Ethernet ist FDDI auch für laufzeitabhängige Multimedia-Anwendungen geeignet, da es eine maximale Verzögerungszeit garantiert.

Durch die Erweiterung von FDDI auch für die Verwendung von TwistedPair-Kupferkabel neben den Multimode- und Singlemode-Lichtleitern ist FDDI eigentlich eine irreführende Bezeichnung. Bei FDDI über TwistedPair-Kupferkabel spricht man deshalb auch von CDDI (Copper Distributed Data Interface).

9.1 FDDI-ANSI-Standard

Schon 1982 wurde von ANSI die Arbeitsgruppe X3T9.5 mit der Entwicklung von Hochgeschwindigkeitsnetzen beauftragt, und 1989 wurde der FDDI-Standard definiert. Der Standard ist aus vier Teilen modular aufgebaut.

Im ISO/OSI-Modell umfasst FDDI die Ebenen 1 und 2. Die Spezifikationen für die physikalische Schicht sind in den PMD- (Physical Medium Dependend) und PHY- (Physical Layer Protocol) Dokumenten festgelegt. Das Zugriffsverfahren ist im MAC- (Media Access Control) und das FDDI-Management im SMT- (Station Management) Dokument spezifiziert. Im PMD-Dokument sind die medienabhängigen Eigenschaften der Stecker und Lichtwellenleiter beschrieben. Im ersten PMD-Standard wurde das Medium Lichtleiterkabel als Multimode-Gradientenfaser mit maximal 2 km Abstand zwischen zwei Stationen festgelegt. Der Einsatz von Monomode-, bzw. Singlemode-Lichtleiter ist auch normiert, es ist eine maximale Entfernung zwischen zwei Stationen von 40 km möglich.

1994 wurde der TP-PMD Standard verabschiedet, der die Verwendung von Unshielded

TwistedPair Kabel (UTP) in FDDI-Netzen regelt. Der TP-PMD Standard basiert auf dem MLT-3 Kodierungsverfahren und nicht, wie im ursprünglichen Antrag aufgeführt, auf dem nicht so zuverlässigen NRZ Verfahren. Die erlaubte maximale Länge beträgt 100 m mit einem Kabel der Kategorie 5. Damit haben nun Netzwerkmanager die Möglichkeit, kostengünstig einzelne Stationen in ein FDDI-Netz einzubinden.

9.2 Zugriffsverfahren

Das Zugriffsverfahren auf das Medium ist im MAC(Media Access Control)-Dokument definiert. FDDI arbeitet nicht wie Ethernet stochastisch mit CSMA/CD als Zugriffsverfahren, sondern deterministisch nach dem Token-Passing-Prinzip.

Stationen dürfen nicht zu beliebigen Zeitpunkten senden, sondern nur wenn sie im Besitz des Tokens sind. Das Token ist ein spezieller Frame, der die Sende-Erlaubnis repräsentiert. Um die Sendedauer und damit die zur Verfügung stehende Bandbreite fair aufteilen zu können, darf eine Station ein empfangenes Token nur für eine bestimmte Zeit (Token Holding Time THT) behalten. Während dieser Zeit kann die Station ihre Datenframes auf den Ring senden.

Bei Empfang eines Tokens nimmt eine Station dieses vom Ring und sendet stattdessen ihre Datenframes. Ein ausgesendeter Datenframe kreist auf dem Ring und wird von der Empfängerstation in ihren internen Puffer kopiert. Der Frame kreist weiter auf dem Ring und wird dann von der Sendestation vom Ring genommen (Stripping). Ist die THT erreicht, wird das Token wieder freigegeben, indem es direkt nach dem letzten Datenframe wieder ausgesendet wird (Early Token Release). Damit besitzt die nächste sendewillige Station sofort die Sendeerlaubnis und muss nicht die Leerlaufzeit abwarten, bis die vorherige Station den letzten kreisenden Datenframe vom Ring genommen hat.

Um eine maximale Verzögerungszeit garantieren zu können, limitiert das MAC-Protokoll die maximale Umlaufzeit des Tokens (TargetToken Rotation Time, TTRT). Der TTRT-Wert wird bei der Initialisierung des FDDI-Rings vom SMT für alle Stationen festgelegt. Jede Station misst während des Tokenumlaufs die tatsächliche Umlaufzeit (Token Rotation Time) seit dem letzten Empfang des Tokens. Nach dem nächsten Empfang des Tokens wird dann die verbleibende Sendezeit (THT) als Differenz aus nomineller Umlaufzeit und tatsächlicher Umlaufzeit ($THT = TTRT - TRT$) benutzt.

Weiterhin unterscheidet das MAC-Protokoll von FDDI zwischen synchronem und asynchronem Verkehr. Unter synchronem Verkehr versteht man die Übertragung von zeitkritischen Daten wie z.B. Audio- und Video-Daten von Multimedia-Anwendungen. Daher wird synchroner Verkehr von FDDI priorisiert, indem dieser von jeder Station zuerst übertragen wird. Erst wenn eine Station keine synchronen Daten mehr zu senden hat, ermittelt sie die verbleibende Sendezeit THT, in der sie den anstehenden asynchronen Verkehr übertragen kann. Der asynchrone Verkehr kann zusätzlich in bis zu



acht Prioritätsklassen unterteilt werden.

9.3 Topologie

FDDI basiert meist auf Lichtleitern als Übertragungsmedium. Die Übertragungsrates ist 100 Mbit/s. Anders als Ethernet ist FDDI keine Bus-Topologie, sondern eine Doppel-Ring-Topologie.

Die Maximalanzahl der Anschlüsse ist 1000, also 500 Stationen mit Doppelanschluss (DAS) oder einer geringeren Anzahl von Stationen (abhängig von der Anzahl der anderen FDDI-Knoten) mit Einfachanschluss (SAS), da diese zwar nur einen einzelnen eigenen Anschluss haben, aber immer auch einen Anschluss an einen Konzentrator erfordern. Der Maximalabstand zwischen zwei Stationen liegt bei 2 km, die maximal erlaubte Länge (Umfang) eines Rings beträgt 100 km. Im Normalfall werden die Daten auf dem Primärring übertragen. Bei einer Unterbrechung dieses primären Rings bemerkt die Station vor der Unterbrechung den Fehler und überträgt den Datenblock auf den Anschluss des sekundären Rings. Der Ausgang des sekundären Rings ist nicht mit derselben Station verbunden wie der primäre, sondern mit der jeweils letzten Station rückwärts, also in der Gegenrichtung.

Das Datenpaket läuft so Station für Station durch den Ring zurück (unbearbeitet), bis es die andere Seite der Unterbrechungsstelle erreicht. Die Station dort hat ebenso die Unterbrechung erkannt und setzt das Paket wieder in der ursprünglichen Richtung auf den primären Ring auf. Die unterbrochene Stelle wird auf diese Weise überbrückt. Das Auftrennen des Rings an einer einzelnen Stelle führt also nicht zu einer Unterbrechung des Netzes. Gleiches gilt beim Totalausfall einer Station, die von den beiden benachbarten Stationen überbrückt wird. Fällt gleichzeitig eine zweite Station aus, so zerfällt der Ring in zwei Teilringe. Diese Fehlersituation kann durch optische Bypass-Relais verhindert werden, wobei jedoch auf die maximal zulässigen Distanzen zwischen den Stationen geachtet werden muss. Doch ein Ring kann nicht nur aus einzelnen Stationen, sondern auch aus Bäumen von Stationen (Baumtopologie) gebildet werden.

Alle neueren FDDI-Geräte unterstützen auch Dual Homing. Beim Dual Homing hat ein FDDI-Gerät je eine Verbindung zu zwei FDDI-Konzentratoren auf der nächsthöheren Ebene des Baumes. Es ist jedoch nur eine Verbindung aktiv, die andere ist im Stand-by-Mode.

9.4 Kabel

Wie oben schon erwähnt, sind für FDDI drei Kabeltypen spezifiziert: Multimode-, Singlemode-Lichtleiter und TwistedPair. Letzteres Kabel ist näher im Abschnitt 10BASE-T beschrieben. Aus Zeiten, als es noch keinen TP-PMD-Standard gab, stammen noch Produkte und Installationen, bei denen als proprietäre Lösungen auch ThinWire- und

Shielded TwistedPair- (STP) Kabel eingesetzt wurden.

Der Unterschied zwischen Singlemode- und Multimode-Lichtleiter besteht im Durchmesser der lichtführenden Faser. Bei Singlemode beträgt er 8 - 10 Micron, bei Multimode sind 62,5 Micron üblich, kann aber je nach Anwendung zwischen 50 und 200 Micron betragen. Um den Kern herum befindet sich in der Regel ein Mantel von 125 Micron.

Die Kosten der beiden Kabeltypen selbst unterscheiden sich nur unwesentlich. Singlemode Anschlusskomponenten sind aber deutlich teurer als Multimode-Anschlusskomponenten. Mit Singlemode kann man dafür aber größere Entfernungen überbrücken (max. 40 km) und hat eine höhere Bandbreite zur Verfügung.

Warum sind Singlemodekomponenten teurer als Multimodekomponenten? Bei den Anschlüssen wird bei Singlemode nur eine Toleranz von 1 - 2 Micron, bei Multimode dagegen von 10 Micron akzeptiert. Bei der Generierung des Lichts müssen bei Singlemode teure 1300 bis 1550 nm Laser eingesetzt werden, bei Multimode reichen 650 bis 1300 nm LEDs. Die beschriebenen Netzkabel finden sich im Kapitel Netzkabel (Seite 270).

9.5 Stationen

Bei FDDI gibt es zwei Arten von Stationen: DAS- (Dual Attachment Station) und SAS(Single Attachment Station) Stationen.

DAS-Stationen können direkt miteinander zu einem Ring verbunden werden. Jede dieser Stationen hat zwei Ports, A und B genannt. Port A ist dabei der Anschluss für den Eingang des primären und den Ausgang des sekundären Rings, Port B derjenige für den Ausgang des primären und den Eingang des sekundären Rings. Die MIC-Stecker (Media Interface Connector) des Lichtleiter-Kabels sind codiert, um ein Verwechseln zu vermeiden. DAS wird mittlerweile aber auch über Kupferkabel (UTP) implementiert.

SAS-Stationen verfügen nur über einen Port, sie werden nie direkt mit dem Doppelring verbunden, sondern immer über einen Konzentrator (nähere Beschreibung siehe unten).

Workstations und kleinere Rechner wird man wegen der geringeren Kosten meist als SAS-Stationen anschließen. Zum Anschluss von SAS-Stationen gibt es zwei Porttypen: S (Slave) ist der Port an einer SAS. Er wird mit dem M (Master) Gegenport an einem Konzentrator verbunden. Der M-Port wiederum kann auch mit dem Port B eines weiteren (kaskadierten) Konzentrators verbunden werden.



9.6 Konzentratoren

Konzentratoren sind die Schlüsselgeräte in der Doppelring-Topologie. Es handelt sich dabei um intelligente Hubs zum Anschluss von SAS-Stationen.

Konzentratoren sind oft modular aufgebaut, sie bestehen aus einem Gehäuse mit Einbauplätzen für unterschiedliche Port-Module. Bei neueren Konzentratoren lassen sich einige Ports per Software als M-Ports zum Anschluss von SAS-Stationen oder als A- und B-Ports zum Anschluss von DAS-Stationen konfigurieren.

Multimode-Lichtleiter werden über ANSI-MIC-Stecker, Singlemode-Lichtleiter über ST-Stecker und UTP-Kabel über RJ45-Buchsen angeschlossen. Digital bietet für seine FDDI-Produkte sogenannte ModPMDs (Modular Physical Media Depent Card) an, über die der Kabelanschluss erfolgt. Mit diesen Modulen lassen sich die einzelnen Ports sehr flexibel bestücken, was die Wahl des Kabeltyps betrifft.

Konzentratoren können auch kaskadiert werden, so lässt sich eine baumartige Struktur aufbauen. Es ist auch nicht unbedingt notwendig, einen solchen Baum mit einem Ring zu verbinden. Ein FDDI-Netzwerk kann auch lediglich als Stern aus einem Konzentrator mit daran angeschlossenen Stationen konfiguriert werden.

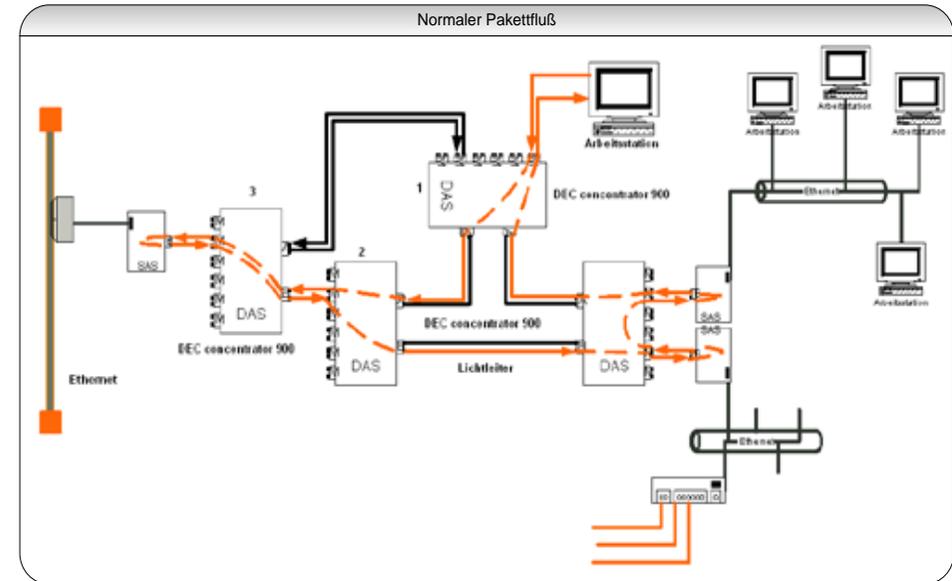
9.7 FDDI/Ethernet Bridges/Switches

Als Bindeglied zwischen Ethernet und FDDI werden FDDI/Ethernet Bridges/Switches eingesetzt. Um unabhängig von einem bestimmten Hersteller zu sein, sollten Translating Bridges verwendet werden, die nach dem IEEE 802.1d, 802.3 und ANSI-FDDI-Standard arbeiten. Sie sind protokollunabhängig und erlauben die Kommunikation zwischen Rechnern am FDDI und Rechnern am Ethernet.

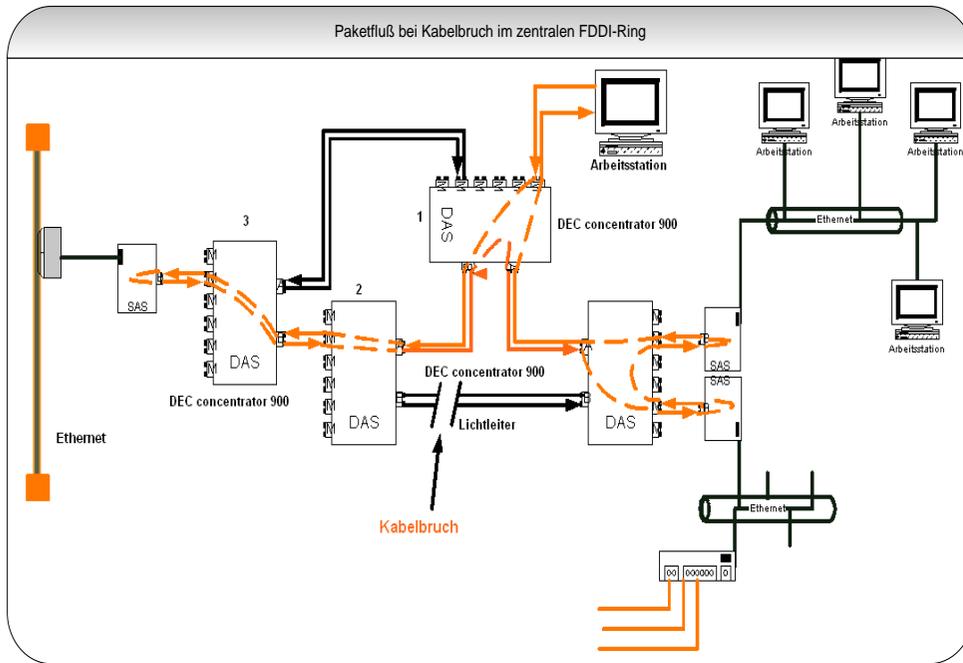
Auch FDDI/Ethernet Bridges/Switches können als SAS oder DAS ins Netz eingebunden werden.

FDDI-Konzentratoren und -Bridges können entweder Out-of-Band oder mittels SMT oder SNMP konfiguriert und überwacht werden.

9.8 Einsatzmöglichkeiten



FDDI ist ideal als schnelles Backbone-Netz. Ethernet-Segmente können über Bridges mit FDDI verbunden werden. Mit Hilfe von Translation-Bridges können auch Rechner am Ethernet mit Rechnern am FDDI direkt kommunizieren. Ebenso natürlich auch mit Rechnern der über FDDI miteinander verbundenen Ethernet-Segmente. Bei Verwendung von Encapsulation-Bridges dient der FDDI-Ring lediglich dem schnellen Durchschleusen von Frames zwischen den Ethernet-Segmenten. Rechner an Ethernet-Segmenten können nicht mit Rechnern direkt am FDDI kommunizieren. FDDI wird Ethernet in den nächsten Jahren nicht ersetzen, sondern vor allem im Backbone-Bereich ergänzen. FDDI-Komponenten sind teurer als Ethernet-Komponenten vergleichbarer Funktion, ihr Durchsatz ist jedoch höher als bei Fast Ethernet Komponenten.



9.9 Zukunft von FDDI

Wer ein sehr zuverlässiges Backbone-Netz mit einer hohen Durchsatzrate benötigt, ist mit FDDI gut beraten. Für bestimmte Applikationen werden höhere Datenübertragungsraten erforderlich sein, hier kommen dann Technologien wie ATM oder Gigabit Ethernet zum Einsatz. In Konkurrenz tritt FDDI zunehmend mit anderen HighSpeed Netzwerktechnologien; vor allem zum 100 Mbit/s Fast Ethernet, da diese Technologie doch erhebliche Preisvorteile hat und sich inzwischen im Markt etabliert hat.





10. ATM

ATM steht als Abkürzung für Asynchronous Transfer Mode. Hinter diesem Begriff verbirgt sich ein extrem schnelles Übertragungsverfahren für Netzwerke, das in jüngster Zeit sehr viel Aufmerksamkeit erfahren hat. ATM gilt heute als Schlüsseltechnologie der Zukunft zur Implementierung universeller HighSpeed-Netze; zumal auch die Einbindung in WAN-Topologien problemlos ist, da alle großen Netzwerkprovider ATM unterstützen.

10.1 Nutzen

In der Regel ist es unerheblich, ob ein Filetransfer eine Sekunde länger oder kürzer dauert. Anders ist dies bei zeitbasierten Daten wie Audio und bewegten Bildern. Schon eine kleine Verzögerung im Audio-Datenstrom bewirkt ein hörbares Aussetzen oder Knacken und bei Videoinformation ist ein ungleichmäßiger Bildablauf das unweigerliche Ergebnis. Sollen also multimediale Daten in das Netzwerk integriert werden, so müssen sämtliche beteiligten Hardware- und Softwarekomponenten ein berechenbares Echtzeitverhalten aufweisen. ATM bietet diesen Service und ist damit die vielversprechendste Technologie für Multimedia-Anwendungen. Der Schlüssel zu ATM liegt allerdings in der Übertragungsgeschwindigkeit, die bis hinauf in den Gigabit-Bereich reicht. Netzwerkmanager drängen bereits heute ihre Lieferanten und Systemintegratoren zu Lösungen für Ihre Bandbreitenprobleme im Backbone. Hier stellt ATM eine zukunftssträchtige Investition dar und wird sich weiter von einer HighEnd-Technologie zur alltäglichen Lösung hinbewegen. Unternehmen sollten sich schon jetzt über den Markt informieren und Migrationswege ausloten, die den Anwender zu ATM hinführen.

Zur Geschwindigkeit kommt die Skalierbarkeit von ATM, worunter man die Möglichkeit der flexiblen Bereitstellung der jeweils erforderlichen Bandbreite versteht. Die heutige Generation von ATM-Switches etwa unterstützt typischerweise 16 Ports zu je 155 Mbit/s beziehungsweise 24 Ports mit 100 Mbit/s, was einer Gesamtbandbreite von 2,4 Gbit/s entspricht. Switches mit 622 Mbit/s Ports befinden sich bereits in Entwicklung. Aber auch dies ist noch längst nicht die Obergrenze: Im Gespräch sind bis zu 2,4 Gbit/s Fortgeschwindigkeit für Switches der Zukunft. ATM ist außerdem die erste Netzwerktechnik, die LANs und WANs nahtlos integrieren kann. Zum ersten Mal in der Geschichte der Datenübertragung macht dies zusätzliche Gateways überflüssig, die von LAN- auf WAN-Protokolle umsetzen. Dadurch ist es äußerst wahrscheinlich, dass sich ATM zu einer Massenmarkt-Technologie entwickelt, die nach technischen und wirtschaftlichen Gesichtspunkten lange Zeit wettbewerbsfähig bleiben wird. Entsprechend groß ist daher auch das allgemeine Interesse an ATM.

10.2 Technologie

Bei ATM werden alle Arten von Informationen, also Audio, Video und Daten in Paketen mit fester Länge (53 Bytes) befördert, die als Zellen bezeichnet werden (cell relay). Der

Protokoll-Overhead dieser Zellen beträgt ca. 10%. 48 Bytes stehen für Nutzdaten zur Verfügung, 5 Bytes sind für Kontrollinformationen reserviert. Aus dieser Datenstruktur resultieren einige wesentliche Eigenschaften von ATM. Durch die einheitliche Länge aller Zellen entsteht eine kalkulierbare Verzögerung bei der Übertragung beliebiger Informationen, wodurch auch bei mehreren konkurrierenden Datenströmen für die einzelnen Anwendungen garantierte Bandbreiten vergeben werden können. Das von anderen Topologien bekannte Problem längerer Pakete, die z.B. bei Filetransfers auftreten und andere Anwendungen blockieren, tritt durch die Zellstruktur bei ATM nicht auf. Sehr kurze Blöcke eignen sich besser für die Sprachübertragung, lange Blöcke für den Transfer von Daten und bewegten Bildern. Mit der Zellgröße bei ATM hat das ATM-Forum einen salomonischen Kompromiss gefunden, der prinzipiell für alle Dienste geeignet ist. Da nun die meisten Informationen nicht in einer einzelnen ATM-Zelle unterzubringen sind, werden die unterschiedlich langen Pakete höherer Netzwerkschichten mit dem Anpassungsmechanismus SAR (Segmentation and Reassembly) des sendenden ATM-Adapters auf ATM-Zellen aufgeteilt und am Ziel wieder zusammengesetzt.

ATM Dienstkategorie	Eigenschaft
CBR Constant Bit Rate	feste Übertragungsrate spezifiziert
ABR Available Bit Rate	Spitzenrate spezifiziert
VBR Variable Bit Rate	Spitzenrate und Minimumrate mit QoS Garantie
UBR Unspecified Bit Rate	keine Übertragungsrate spezifiziert

ATM Dienstkategorie

Die Übertragung selbst beruht auf dem Prinzip der virtuellen Verbindung, das auch paketvermittelnden Netzen wie X.25 zugrunde liegt. Bei diesem Prinzip werden keine festen Kanäle zwischen den beteiligten Endeinrichtungen geschaltet. Vielmehr werden die Zellen einer bestimmten Verbindung dann, wenn sie erzeugt werden, auf einem vorher festgelegten Weg durch das Netz transportiert. Dadurch können die Betriebsmittel in den Netzelementen effizient für mehrere Verbindungen eingesetzt werden. ATM kennt sowohl Festverbindungen (PVCs, Permanent Virtual Circuits) als auch geschaltete Verbindungen (SVCs, Switched Virtual Circuits). Dabei kann es sich wiederum um virtuelle Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Verbindungen handeln.

Verbindungen können mit einer gewissen Betriebsgüte QoS (Quality of Service) aufgebaut werden. Bei konventionellen LANs ist dies nicht der Fall. Die Bandbreiten von Ethernet (10 Mbit/s), Token-Ring (16 Mbit/s) und FDDI (100 Mbit/s) werden von allen angeschlossenen Geräten gemeinsam genutzt, müssen also entsprechend aufgeteilt werden. Bei Private Ethernet ist jedem Endgerät eine fixe Bandbreite von 10 oder 20 Mbit/s zugeordnet, bei Fast Ethernet eine Bandbreite von 100 oder 200 Mbit/s. ATM geht noch einen Schritt weiter. Jedem an ATM angeschlossenen Gerät kann durch die



erwähnten PVCs oder SVCs statisch oder dynamisch die benötigte Bandbreite zugeordnet werden, wobei diese nur durch die Kapazität der ATM-Hardware begrenzt ist. Nach erfolgtem Verbindungsaufbau hat man die Gewissheit, die Bandbreite des angeforderten Übertragungskanal alleine nutzen zu können, ohne von anderen sendewilligen Stationen gestört oder sogar unterbrochen zu werden.

Dabei wird versucht, den jeweiligen Anforderungen bestmöglich gerecht zu werden. Grundsätzlich bietet ATM hier drei verschiedene Kategorien von Diensten an: Garantierte Dienste, vorhersagbare Dienste oder Dienste, die eine jeweils verfügbare Bitrate bestmöglich nutzen. Eine garantierte Verbindung wird für die Unterstützung konstanter Bitraten (CBR, Constant Bit Rate) benötigt, bei der alle Zellen zuverlässig mit nur geringfügiger Zeitabweichung an den Bestimmungsort übertragen werden müssen, wie etwa bei Sprachinformation. Es existieren aber auch Anwendungen mit variablen Bitraten, beispielsweise Filetransfer und E-Mail, für die ein Service, der die verfügbaren Bitraten bestmöglich nutzt, ausreichend ist. Dabei gibt es keine festen Garantien. Die Zellen werden vielmehr einfach auf der Bandbreite, die Verbindungen mit höherer Priorität noch übrig lassen, bestmöglich übertragen. In der Spezifikation des ATM-Forums sind diese Dienste unter dem Begriff Traffic Management subsummiert. Die Tabelle gibt Auskunft über alle relevanten Einzelheiten.

10.3 Schnittstellen

Eine entscheidende Rolle bei ATM spielen die Schnittstellen. Zur Auswahl stehen unter anderem die vom ATM-Forum akzeptierten SONET-Schnittstellen (Synchronous Optical Network) mit 622 Mbit/s und 155 Mbit/s für Glasfaser und UTP-Kabel, TAXI mit 100 Mbit/s für Lichtleiterkabel und 52 Mbit/s für UTP. Die verbreitete 100-Mbit/s-TAXI-Schnittstelle kann von einigen Herstellern auch umschaltbar mit 140 Mbit/s betrieben werden; diese Lösung ist aber nirgendwo standardisiert. Die ATM-Schnittstellen und die unterstützten Kabeltypen sind in der Tabelle zusammengefasst. Zusätzliche Schnittstellen wie SONET STS48c (2,4 Gbit/s) befinden sich noch im Standardisierungsprozess oder werden nur von einzelnen Herstellern unterstützt.

10.4 Verfügbarkeit und Standardisierung

Der Motor für die Standardisierung von ATM ist das bereits erwähnte ATM-Forum: eine Interessenvereinigung von ATM-Herstellern, die die zögerliche ITU (früher CCITT) mit Vorschlägen versorgen. Die Definition der Zellen ist seit längerem abgeschlossen. Es ist festgelegt, wie die Hardware von ATM-Systemen zu funktionieren hat, weiter ist beschrieben, wie Verbindungen aufgebaut und kontrolliert werden und welche logischen Interfaces dabei vonnöten sind. ATM umfasst aber noch weitere Spezifikationen, die noch nicht oder in recht unterschiedlichem Umfang implementiert sind. Als besonders kritisch erweist sich vor allem der Übergang von ATM auf konventionelle Topologien wie Ethernet, FDDI oder Token-Ring.

Schnittstelle	Datenrate (Mbit/s)	Multimode Fibre (MMF)	Singlemode Fibre (SMF)	Coaxial Cable	UTP-5	UTP-3
DS1	1,5					
E1	2					
E3	34					
DS3	45					
STS-1	52					
Taxi 4B/5B	100					
SONET 8B/10B	155					
SONET STM-1/STS3C	155					
SONET STM-2/STS12C	622					

Schnittstellen-Kabeltyp

Für die Verwendung von IP über ATM wurden verschiedene RFCs (Request for Comments) herausgegeben, die es Stationen mit IP-Stock erlauben, ATM als Transportmedium zu verwenden. Davon haben sich die beiden konkurrierenden Ansätze RFC 1483 (Multiprotocol Encapsulation) und RFC 1577 (Classical IP-over-ATM) durchgesetzt. In der Realität ist

die Normierung inzwischen immerhin soweit fortgeschritten, dass nach Angaben der Hersteller die Produkte mittels Firmwareupgrade problemlos an zukünftige Standards angepasst werden können. Dadurch ist bei Produkten des gleichen Herstellers auch die Konformität mit zukünftigen Spezifikationen des ATM-Forums gewährleistet. Sollen ATM-Produkte mehrerer Hersteller zusammen eingesetzt werden muss die Kompatibilität der eingesetzten Produkte zueinander erwiesen sein.

10.5 Migration in bestehende Netze

Die Großen Unterschiede zu bisherigen Netzwerken machen eine flexible Einbindung von ATM-Produkten in vorhandene Netzwerke nötig, um bestehende Investitionen weiter nutzen zu können. Diese länger dauernden Anpassungen bezeichnet man als Migration. Die Migration von ATM wird in mehreren Schritten verlaufen. ATM-Switches können in Großen Netzen als Collapsed Backbone eingesetzt werden. Bisher verlegte ring- oder busförmige Backbone-Kabel fallen dann punktförmig auf den ATM-Switch zusammen, über den alle Segmente und Geräte des Netzes sternförmig verbunden werden. An ATM-Switches können weitere ATM-Switches oder Endgeräte mit ATM-Adaptern angeschlossen werden. Die Anbindung vorhandener Netzwerk-Topologien an zentrale ATM-Switches erfolgt heute vor allem mit Hilfe von ATM-Lösungen, die auf Routern basieren. Auch die meisten Hersteller von Großen Netzwerk-Konzentratoren bieten





Module für ATM-Verbindungen an.

Damit wird eine Kommunikation zwischen konventionellem LAN und ATM möglich.

Als letzter Schritt wird die durchgehende Verbindung zu den Endgeräten anstehen. Es ist zu erwarten, dass dieser Prozess die summierten Pro-Port-Kosten von ATM-Vernetzungen noch weiter sinken lassen wird. Für Anwendungen wie Hochleistungs-Workstations, Server, Bildübertragung oder Virtual Reality ist ATM jetzt schon eine interessante Alternative zu Topologien wie FDDI.

Wie soll man nun aber bestehende Anwendungen in ein ATM-Netz integrieren? Die einfachste Möglichkeit bestünde in dem Austausch des existierenden LAN-Interfaces eines Rechners gegen eine ATM-Karte und der Installation des ATM-Treibers. So leicht ist es aber leider nicht, denn ATM fehlt eine Eigenschaft, die konventionelle LANs aufweisen: die Unterstützung von Broadcasts, Multicasts und die Benutzung von MAC-Adressen. Das allerdings sind grundlegende Voraussetzungen für den Einsatz der meisten Netzwerkprotokolle wie TCP/IP oder IPX.

Die vom ATM-Forum verabschiedete Lösung für diese Problematik heißt LAN Emulation LANE 1.0. LANE besteht aus vier Softwarekomponenten in einem Netz aus ATM und herkömmlichen LAN-Technologien. Die aus drei Komponenten bestehenden LAN-Emulation-Services (LESs) werden auf einem oder mehreren an das ATM-Netz angeschlossenen Rechnern als ATM-Applikationen oder als integrierter Bestandteil eines ATM-Switches bereitgestellt. Der LAN-Emulation-Client (LEC) als vierte Komponente wird auf den Endgeräten installiert.

LAN-Emulation-Services:

Der LAN Emulation Confirmation Server LECS koordiniert alle LESs und LECs. Der LAN Emulation Server LES übersetzt MAC- in ATM-Adressen und umgekehrt.

Der Broadcast and Unknown Server BUS leitet Broadcast- und Multicastpakete mit Hilfe von ATM-Point-to-Multipoint-Verbindungen und Pakete an unbekannte Rechner weiter, bis die Zieladresse gefunden ist. Zu Beginn einer Übertragung kontaktiert der LEC den LECS unter Verwendung einer einheitlichen Netzwerkadresse, um allgemeine LANE-Informationen auszutauschen. Dabei gibt der LECS dem Client die Adresse des für ihn zuständigen LES. Der LEC nimmt danach Verbindung mit dem LES auf. Dann werden ATM-Adresse, MAC-Adresse, Frame-Größe und LAN-Typ vereinbart. Broadcasts und Pakete mit unbekanntem Ziel werden vom LEC an den BUS übergeben, der die Weiterleitung übernimmt.

Die fehlenden MAC-Level-Eigenschaften werden also für die Clients emuliert, für die sich ATM dann z.B. als 802.3 (Ethernet) oder 802.5 (Token-Ring) Netzwerk darstellt.



11. Drahtlose Datenübertragung

11.1 Infrarot

Bei Notebooks und anderen mobilen Kommunikationsgeräten (PDAs, Handhelds, Mobiltelefonen) haben sich die Infrarotschnittstellen IrDA (max. 115,2 kbit/s) bzw. FastIrDA (max. 4 Mbit/s) etabliert. IrDA stellt eine reine Punkt-zu-Punkt-Verbindung mit einem eigenen Protokoll her. Durch die vergleichsweise geringe Geschwindigkeit liegt der Einsatzbereich bei der Übertragung kleiner Datenmengen, z.B. drahtloses Drucken, das Überspielen von Bildern einer Digitalkamera oder mobiler Datenfunk über Notebooks. Eine weitere Einschränkung ist die maximale Distanz von ca. 30 cm zwischen zwei IrDA-Geräten in direkter Linie. Die Zahl IrDA-fähiger Geräte (insbesondere Notebooks und Mobiltelefone) steigt stetig.

11.2 Laser

Optischer Richtfunk über LEDs bzw. Laser erreicht Geschwindigkeiten bis zu 622 Mbit/s und Reichweiten von bis zu 5 km. Auch der optische Richtfunk ist eine Punkt-zu-Punkt-Verbindung und setzt Sichtverbindung voraus. Optischer Richtfunk ist zwar schnell, abhörsicher und wartungsfrei, die Verfügbarkeit ist allerdings wetterabhängig (Nebel). Bedingt durch den hohen Installationsaufwand ist optischer Richtfunk eine Nischenlösung.

11.3 Bluetooth

Der Funk-Standard Bluetooth überträgt Daten mit bis zu 1 Mbit/s im lizenzfreien 2,4 GHz Band. Der Einsatzbereich für Bluetooth ist die Kommunikation mit Peripheriegeräten und der Datenaustausch. Eine Sichtverbindung wird nicht benötigt, je nach Sendeleistung können Entfernungen zwischen 10 und 100 m überbrückt werden. Bluetooth eröffnet ein weites Anwendungsgebiet, von drahtlosen Peripheriegeräten (Tastatur, Maus, Drucker, Modem/ISDN) über Bluetooth-fähige Mobiltelefone, Organizer und PDAs. Es können zwar Daten zwischen bis zu 8 Geräten zugleich ausgetauscht werden, Bluetooth ist jedoch kein LAN-Netzwerk.

11.4 HomeRF

HomeRF verwendet ebenfalls das lizenzfreie 2,4 GHz-Band zur Datenübertragung mit 1 und 2 Mbit/s über Distanzen bis ca. 50 m. Im Unterschied zu Bluetooth ist HomeRF kompatibel zum Datenfunk nach IEEE 802.11 sowie DECT und kann TCP/IP-Daten übertragen. HomeRF soll sämtliche Kommunikationsgeräte im Consumer-Bereich miteinander kommunizieren lassen, die gemeinsame Nutzung von Peripheriegeräten ermöglichen und außerdem Sprachübertragung ermöglichen. Ob sich Bluetooth oder HomeRF am Markt durchsetzen werden, hängt von Verfügbarkeit, Preis und

Kompatibilität der Geräte ab.

11.5 Datenfunk nach IEEE 802.11

Ursprünglich für militärische Zwecke entwickelt, hat sich diese Technik im zivilen Bereich erfolgreich bewährt. Im Frequenzbereich von 2,4 GHz werden je nach Geräte- und Antennentechnik Übertragungsraten bis zu 11 Mbit/s erreicht und Entfernungen bis 10 km überbrückt. In Gebäuden liegt die typische Entfernung bei ca. 30 - 50 m, also etwa entsprechend einem DECT Handy.

Beim Einsatz wird unterschieden zwischen mobilen Clients in einem Netzwerk (Wireless LAN) und der Verbindung von Netzwerken über Funk (Wireless Bridging). Die Abhörsicherheit entspricht der von kabelgebundenem Ethernet und wird durch die WEP (Wired Equivalent Privacy) Verschlüsselung sichergestellt. Im Gegensatz zu früheren, proprietären Lösungen können IEEE 802.11 kompatible Geräte verschiedener Hersteller problemlos zusammen eingesetzt werden.

Um die Kompatibilität der Geräte zu gewährleisten, haben die führenden Hersteller in diesem Bereich die WECA (Wireless Ethernet Compatibility Alliance) gegründet. WECA garantiert mit umfangreichen Tests die Kompatibilität der Geräte und vergibt für getestete und kompatible Geräte das Wi-Fi Logo. Mehr Information über WECA und das Wi-Fi Logo finden sich auf der WECA-Homepage unter www.wirelessethernet.com.

11.5.1 Wireless LAN

In einem Wireless LAN wird jeder Netzwerkclient mit einem Funkadapter ausgestattet, je nach Geräteart als PCI-, ISA- oder PC-Card. Der Zugang zum kabelgebundenen Netzwerk stellt ein so genannter Access Point oder Funkhub her. Der Access Point bildet eine Funkzelle aus und versorgt ein begrenztes Gebiet mit Funkinformationen. Weitere Funkzellen können durch das Aufstellen zusätzlicher Access Points aufgebaut werden. Die mobilen Clients können sich frei innerhalb dieser Zellen bewegen (transparentes und unterbrechungsfreies Roaming), während die Access Points über Kabel an das Ethernet Netzwerk angeschlossen werden. Um das Roaming zu gewährleisten, müssen die Access Points innerhalb des gleichen Subnetzes liegen. Mit sogenannten Workgroup Bridges lassen sich über einen Hub mehrere Geräte mit normalem Ethernet Anschluss in ein Wireless LAN einbinden. Ein Wireless LAN eignet sich hervorragend für Umgebungen, in denen eine klassische Kabelinstallation nur schwer realisierbar ist (z.B. in historische Gebäuden) oder ein ad-hoc Netzwerk aufgebaut werden muss.

11.5.2 Wireless Bridging

Beim Wireless Bridging werden Datennetze über Funkbridges miteinander verbunden. Die Bridges verhalten sich wie herkömmliche LAN-Bridges und filtern Frames anhand der





MAC-Adresse. An die Funkbridge können je nach Datenrate und zu überbrückender Entfernung unterschiedliche Antennensysteme angeschlossen werden, sowohl Rund- wie auch Richtstrahlantennen. Damit ergibt sich die Möglichkeit, nicht nur Punkt-zu-Punkt-Verbindungen aufzubauen, sondern auch Punkt-zu-Multipunkt. Grundvoraussetzung ist in jedem Fall eine direkte ununterbrochene Sichtverbindung zwischen den Antennensystemen sowie ein Freiraum ober- und unterhalb der Verbindungslinie (Fresnelzone).

Hier genauere Angaben über die erreichbaren Entfernungen zu machen, ist aufgrund der vielfältigen Parameter wie Antennengröße, -ausrichtung, Kabelqualität und vielen anderen mehr, unmöglich. Hersteller wie Cisco bieten jedoch Tools an, die bei der Auswahl der passenden Komponenten für bestimmte Anforderungen helfen. Sie enthalten auch Hinweise auf evtl. zu beachtende spezielle Konfigurationsrichtlinien.



12. Weitbereichsnetze WAN

Ein Netz, das aus mehreren Local Area Networks (LANs) oder Einzelsystemen über Remote Verbindungen (z. B. ISDN, X.25, Internet oder VPN über Internet) zusammengeschlossen ist, bezeichnet man als Wide Area Network (WAN).

12.1 Analoge Wählleitungen

Das wohl umfangreichste und jedem bekannte WAN ist das öffentliche Telefonnetz. Über Wählverbindungen wird in diesem Netz vor allem die Sprachkommunikation abgewickelt. Die Nutzung dieses Netzes zum Übertragen von Daten mittels Modem oder in Form von Fax-Transfer wird auch weiterhin seine Bedeutung haben.

12.1.1 Telex und Teletex

Der Fernschreiber war über 50 Jahre lang der einzige Textkommunikationsdienst, der auf der ganzen Welt verbreitet war. Auch heute wird der Telex Dienst noch genutzt.

Im Gegensatz zum Telex Dienst, bei dem der Fernschreiber ausschließlich als Kommunikationsgerät dient, ist beim Teletextdienst das Endgerät eine Kombination aus Kommunikationsgerät und lokalem Textsystem. Texte werden in der so genannten Teletex-Box zwischengespeichert und können editiert, langfristig gespeichert, versendet und empfangen werden. Telex und Teletex spielen heute kaum noch eine Rolle.

12.1.2 Modems

Modems werden für die Datenübertragung im analogen Telefonnetz eingesetzt. Solange die Mehrzahl der weltweit installierten Anschlüsse nicht direkt auf das ISDN-Netz, sondern mit dem Endgerät auf das analoge Telefonnetz zugreift, werden Modems ihre Bedeutung für die Datenübertragung behalten.

Die Bezeichnung Modem ist ein Kunstwort, das aus den ursprünglichen Funktionen Modulation und Demodulation entstand. Heute erfüllen Modems noch weitere Funktionen wie zum Beispiel Fehlerkorrektur, Datenkompression und - in Verbindung mit entsprechender Kommunikationssoftware auf dem angeschlossenen PC - Faxfunktion und Anrufbeantworterfunktion.

Ein Modem empfängt Daten vom Rechner in digitaler Form und wandelt sie in analoge Signale um, damit sie über die Telefonleitung transportiert und am anderen Ende von einem zweiten Modem demoduliert werden können, und somit wieder in digitaler Form zur Verfügung stehen. Beim Anschluss eines Modems unterscheidet man zwischen jenen, die vorwiegend bei PCs als Steckkarten eingebaut werden, und externen Modems,

die über die serielle RS-232-Schnittstelle angeschlossen werden. Alternativ hierzu sind mittlerweile auch Modems mit PC-Card-Schnittstelle (PCMCIA) sehr verbreitet, da nahezu alle modernen tragbaren Personal Computer über diesen Anschluss verfügen.

Die Fähigkeit heutiger Modems, auch Faxe versenden und empfangen zu können, hat spezielle Faxkarten vom Markt verdrängt.

Für das Konfigurieren und Steuern von Modems hat sich der Hayes-kompatible Befehlssatz durchgesetzt. Er wird auch AT-Befehlssatz genannt, da die Kommandos mit AT beginnen.

Übertragungsmodi

Die Vielzahl der verschiedenen auf dem Markt befindlichen Modems unterscheidet Übertragungsgeschwindigkeit.

Asynchrone Übertragungen arbeiten zeichenweise. Jedem zu übertragenden Zeichen wird ein zusätzliches Startbit und ein oder zwei Stoppbits hinzugefügt. Bei synchroner Übertragung werden alle Datenbits direkt aufeinander folgend gesendet. Die Synchronisation erfolgt durch separate Taktleitungen. Allerdings braucht man für Synchronmodems auch entsprechende synchrone Anschlüsse mit entsprechenden Protokollen, sodass man normalerweise asynchrone Modems einsetzt.

Die Übertragungsrate eines Gerätes wird in der Einheit Bit/s gemessen. Die Einheit Baud gibt die Schrittgeschwindigkeit auf der Übertragungsstrecke an. Da bei neueren Übertragungsverfahren die Information nicht nur in der Frequenz, sondern auch in Amplitude und Phase kodiert sind, können pro Baud mehrere Bit übertragen werden.

Für das Übertragen großer Datenmengen können Modems nie schnell genug sein. Die höheren Anschaffungskosten für schnellere Modems amortisieren sich schon bald durch die geringeren Betriebskosten.

Mit dem Übertragungsstandard V34+, der eine Brutto-Übertragungsrate von 33600 Bit/s spezifiziert, ist immer noch nicht die maximale Kapazität einer Telefonleitung ausgereizt, auch wenn Experten dies schon für 28800 Bit/s prognostiziert hatten. Die neue Geschwindigkeitskategorie 56000 Bit/s ist als V90 standardisiert. Mit V90 können in Downloadrichtung bis zu 56 kbit/s übertragen werden. Voraussetzung hierfür ist ein so genannter 56k-Host. Erreicht werden die höheren Übertragungsraten dadurch, dass zwischen dem 56k-Host und der digitalen Vermittlungsstelle auf eine Analogkonvertierung des Signals verzichtet wird. Lediglich auf der Benutzerseite bleibt der analoge Anschluss bestehen. Der V.90-Standard beinhaltet Komponenten der Vorläufer X2 (US Robotics/3Com) und K56flex (Rockwell/Lucent/Conexant) und ist kompatibel zu diesen proprietären Technologien. Ältere herstellerspezifische Protokolle wie PEP, HST, V.32terbo oder VFast haben inzwischen ihre Bedeutung verloren, da mit





dem V34+ Standard all diese Protokolle in der Übertragungsgeschwindigkeit übertroffen werden.

Die V-Normen der ITU-TSS (früher CCITT) sind inzwischen internationaler Standard. Die Bell-Normen für die USA haben in Europa keine Bedeutung mehr. Eine Übersicht über diese Standards kann der Tabelle entnommen werden.

12.2 ISDN

ISDN (Integrated Services Digital Network) ist in Europa auf dem unaufhaltsamen Vormarsch. ISDN vereinigt die Nutzung von Sprache, Text, Bildern und Daten in einem einzigen Netz. Mit nur einem ISDN-Anschluss können somit verschiedene Telekommunikationsdienste genutzt werden wie z. B. Telefon, Fax, Dateitransfer etc. Die hohe Übertragungsgeschwindigkeit, die störungsfreie Datenübertragung, der schnelle Verbindungsaufbau und die wachsende Verbreitung machen ISDN nicht nur für Neueinsteiger im Bereich der Datenkommunikation interessant, sondern auch für Anwender, die bisher auf analoge Modemlösungen angewiesen waren.

ISDN verwendet die bereits verlegten Telefonleitungen zum Endgerät. Der wesentliche Unterschied zum bisherigen Telefonnetz besteht darin, dass Signale bis zum Teilnehmer durchgehend digital übertragen werden. Der Datenverkehr zwischen den Hauptvermittlungsstellen und den Ortsvermittlungsstellen ist bereits vollständig digital.

12.2.1 ISDN-Anschlüsse

Der Anschluss an das ISDN-Netz erfolgt in der Regel über den ISDN-Basisanschluss, im Englischen als BRI (Basic Rate Interface) bezeichnet. Er stellt auf der Teilnehmerseite den so genannten SO-Bus mit SO-Schnittstelle (Vierdrahtschnittstelle) für bis zu acht Endgeräte zur Verfügung, von denen zwei gleichzeitig betrieben werden können. Der Bus hat zwei Nutzkanäle mit je 64 kbit/s (B-Kanäle) Übertragungsrate und einen Steuerkanal mit 16 kbit/s (D-Kanal).

Bei analogen Endgeräten ist für die Nutzung von ISDN ein externer ISDN-Terminaladapter oder ein ISDN-Controller mit integriertem a/b-Wandler notwendig. Auch analoge Endgeräte wie Fax oder Modem können an einem ISDN-Anschluss weiterverwendet werden. Serielle Geräte können über einen TA (Terminaladapter, fälschlicherweise auch ISDN-Modem genannt) direkt an das ISDN-Netz angeschlossen werden. Mehr dazu weiter unten in diesem Kapitel.

Neben dem ISDN-Basisanschluss gibt es den Primärmultiplexanschluss (PMx). Die englische Bezeichnung ist PRI steht für Primary Rate Interface. Der PMx hat 30 B-Kanäle mit jeweils 64 kbit/s und einen D-Kanal mit ebenfalls 64 kbit/s. Teilnehmerseitig hat er die Vierdrahtschnittstelle S2M. Der PMx eignet sich besonders aus Kostengründen für den

Anschluss von Großen TK-Anlagen, Datenservern oder für die Kopplung mehrerer lokaler Netze. Auch hier ist es wie bei einem BRI möglich, jeden einzelnen der 30 B-Kanäle für einen anderen Kommunikationspfad zu nutzen oder mehrere Kanäle zu bündeln. Bei Kanalbündelung kommt bei IP-Übertragungen das Protokoll Multilink-PPP zum Einsatz, ansonsten werden proprietäre Protokolle verwendet (z. B. bei Bildtelefonie).

12.2.2 Kompatibilität

Wird eine Verbindung zwischen zwei ISDN-Endgeräten hergestellt, so werden dazu zunächst Steuerinformationen im D-Kanal übertragen. Darin enthalten ist zum Beispiel die Nummer des Anrufers, die dann bei einem ISDN-Telefon im Display angezeigt wird, sowie Informationen über die Art des gewünschten Dienstes (z. B. Sprache oder Fax) und weitere Angaben, die zum Aufbau der Verbindung zwischen den beiden ISDN-Stellen nötig sind. Nach der Einführung von ISDN entwickelten sich unterschiedliche Standards für die Protokolle, die bei der Übertragung der Steuerinformationen im D-Kanal verwendet werden. Dies führte zum Beispiel dazu, dass in Deutschland heute zwei D-Kanal-Protokolle im ISDN vorhanden sind: zum einen die nationale Lösung 1TR6 und zum anderen das europäische Protokoll DSS1 oder auch E-DSS1. Man spricht hier vom Euro-ISDN-Protokoll, obwohl es mittlerweile auch in vielen nichteuropäischen Ländern eingesetzt wird. Weltweit ist die Zahl der Netzbetreiber, die Euro-ISDN anbieten, auf über 30 angewachsen, davon 20 in Europa. Während man beim Telefonieren keinerlei Probleme zu erwarten hat, wenn die D-Kanal-Protokolle der Standorte unterschiedlich sind, gibt es unter Umständen Probleme, wenn Daten übertragen werden sollen oder wenn bestimmte Dienstmerkmale oder Leitungstypen im ISDN benötigt werden, die jedoch nur national verfügbar sind. Mittlerweile hat sich Euro-ISDN in vielen Ländern durchgesetzt, sodass bei Neuinstallationen nach Möglichkeit dieser Verbindungstyp eingesetzt werden sollte.

12.2.3 Verbindungstypen

Innerhalb von ISDN kann man zwischen drei Verbindungstypen unterscheiden.

Bei der ISDN-Wählverbindung wird ein B-Kanal für einen ISDN-Dienst durch den Wählvorgang zu einem beliebigen ISDN-Teilnehmer bereitgestellt. Wählverbindungen sind auch zu anderen Netzen möglich (analoges Telefonnetz, Mobilfunk, X.25).

Digitale Festverbindungen stellen permanent geschaltete digitale 64-kbit/s-Kanäle bereit. Es können maximal 30 B-Kanäle (PRI) pro Anschluss bereitgestellt werden. Diese exklusiven Festverbindungen können sowohl mit Steuerkanal als auch ohne genutzt werden.



X.25 über ISDN

Ein Anfang 1995 im Euro-ISDN implementierter Dienst eröffnet nun auch die Möglichkeit des Transports von X.25-Paketen im ISDN. Die Integration von X.25 in ISDN ist in der Norm CCITT X.31 Case D und Case B standardisiert. Für Basisanschlüsse werden sowohl der D-Kanal- als auch der B-Kanal-Zugang angeboten. Dagegen wird beim Primärmultiplexanschluss nur der D-Kanal-Zugang unterstützt.

Die Übertragung der Pakete erfolgt im X.25-Format. ISDN übernimmt dabei nur die reinen Transportfunktionen, d.h. eine Vermittlung der Datenpakete findet nicht statt. Diese erfolgt in den Vermittlungsknoten des jeweiligen X.25-Netzes. Der Übergang vom ISDN zum X.25-Netz findet in so genannten ISDN-Vermittlungsstellen statt, die mit speziellen Packet Handlern (PH) und Frame Handlern (FH) ausgestattet sind. Welches X.25-Netz benutzt wird und welche Funktionen es haben soll, wird mit dem X.25-Netzbetreiber ausgehandelt und als individuelles Nutzerprofil im Packet Handler unter einer ganz bestimmten ISDN-Rufnummer gespeichert.

Die physikalische Anbindung erfolgt über einen SP-Anschluss (Spezialanschluss für Paketdaten). Dieser nach dem X.75-Standard arbeitende Anschluss kann Daten in beiden Richtungen (Voll duplex- Betrieb) mit 64 kbit/s übertragen. Pro SP-Anschluss können bis zu 350 virtuelle Verbindungen gleichzeitig verwaltet werden. Über den SP-Anschluss lassen sich sowohl Verbindungen zwischen zwei Euro-ISDN-Anschlüssen mit den entsprechenden Leistungsmerkmalen als auch Verbindungen von und zu X.25-Anschlüssen aufbauen.

Im D-Kanal werden die Daten mit einer Geschwindigkeit von 9.6 kbit/s und im B-Kanal mit 64 kbit/s übertragen. Entsprechend der unterschiedlichen Bandbreite sind auch die Kosten für den B-Kanal entsprechend höher.

Genutzt werden kann dieser Dienst nur, wenn entsprechende Endgeräte die Funktion eines X.25-PADs (Packet Assembler Disassembler) übernehmen können. Bei einem PAD handelt es sich um eine Einrichtung, die ISDN-Hardware oder asynchrone Endgeräte wie PCs mit Modem an das synchron arbeitende, paketvermittelnde X.25-Netz anpasst. In den meisten universellen Remote Bridge-Routern ist diese Funktion heute integriert. Vorteil des X.25Dienstes ist, dass sich je nach Anwendung Kosten sparen lassen und der ISDN-Anschluss auch für andere Anwendungen genutzt werden kann. Zusätzlich ist auch die Kommunikation mit Ländern realisierbar, die noch nicht flächendeckend über ISDN verfügen, sondern nur ein X.25-Netz bereitstellen.

12.2.4 ISDN-Terminaladapter mit serieller Schnittstelle

Die Kommunikation bestehender Anwendungen ist in der Regel auf serielle Analogmodems abgestimmt, die den Hayes-AT-Befehlssatz beherrschen. Möchte man trotzdem ISDN nutzen, empfiehlt sich der Einsatz eines ISDN-Terminaladapters mit

serieller Schnittstelle. Da es sich um ein externes Gerät mit serielltem Anschluss nach RS-232-Norm handelt, kann es direkt anstelle eines analogen Modems eingesetzt werden. Die Steuerung erfolgt, wie vom analogen Modem bekannt, über die erweiterten AT-Befehle. Daher eignen sich ISDN-Terminaladapter prinzipiell überall dort, wo Daten von der seriellen Schnittstelle über ISDN übertragen werden sollen. Einsatzbeispiele sind Workstations, für die kein interner ISDN-Controller zur Verfügung steht, sowie Remote Bridges und Router mit serieller Schnittstelle. Auch in Verbindung mit seriellen Communication-Servern eignen sich ISDN-Terminaladapter zum Aufbau von leistungsfähigen Remote-Access-Anwendungen über ISDN. Zu beachten ist, dass nicht jede serielle Schnittstelle für die hohe Übertragungsrate von 64000 Bit/s (bis zu 256000 Bit/s oder mehr bei Kanalbündelung / Datenkompression) im ISDN geeignet ist. Näheres ist den technischen Spezifikationen der Schnittstelle zu entnehmen. In jedem Fall ist eine serielle Schnittstelle mit eingebautem Datenpuffer (UART 16550-kompatible Schnittstellen) von Vorteil.

Ergänzend sollte erwähnt werden, dass die meisten ISDN-Terminaladapter zusätzlich zum AT-Befehlssatz auch wahlweise über eine CAPI-Schnittstelle bedient werden können. Weitere Informationen zu CAPI sind im Abschnitt CAPI zu finden.

12.2.5 ISDN-Adapter mit a/b-Schnittstelle

Herkömmliche Telefone, Anrufbeantworter, Faxgeräte der Gruppe 3 und Modems sind analoge Endgeräte und können nicht direkt am ISDN-Anschluss betrieben werden. Abhilfe schafft hier ein ISDN-Terminaladapter mit a/b-Schnittstelle, über den die vorhandenen analogen Endgeräte auch mit ISDN weiter benutzt werden können. Kleine ISDN-Nebenstellenanlagen mit bis zu 16 analogen Nebenstellenanschlüssen entsprechen im Prinzip einem 16fach-Terminaladapter. Die Qualität und die nutzbare Übertragungsgeschwindigkeit werden durch die geringere Leistungsfähigkeit der analogen Verbindung bestimmt.

12.2.6 ISDN-Controller

ISDN-Controller bieten mittlerweile die einfachste und preisgünstigste Möglichkeit, Datenkommunikation im ISDN zu nutzen. Sie sind für die meisten Bussysteme und Hardwareplattformen erhältlich. Die gebräuchlichste Form sind jedoch ISA-Steckkarten für PCs.

Die Geschwindigkeit im ISDN ist wesentlich geringer als die Geschwindigkeit heutiger Bussysteme. Daher sind PC-Steckkarten für den aus heutiger Sicht langsamen ISA-Bus bei weitem ausreichend. Allerdings bieten Karten für den PCI-Bus einen weitaus höheren Installationskomfort.

Der Einsatz von ISDN-Karten hängt davon ab, ob die Datenkommunikation vollständig digital zwischen zwei ISDN-Endgeräten stattfindet oder ob eines der beiden Endgeräte





an das analoge Telefonnetz angeschlossen ist. Daher wird nachfolgend auf beide Anwendungen getrennt eingegangen.

Kommunikation mit digitalen Gegenstellen

Befindet sich auf der Gegenseite ein digitales Endgerät wie zum Beispiel ein PC mit ISDN-Karte oder ein digitales Faxgerät (Fax Gruppe 4) oder handelt es sich um einen ISDN-Zugang zu einem Netzwerk oder zu einem Dienstleistungsanbieter (Datex-JDienst, CompuServe, Internet-Provider), so erfolgt der Datenaustausch im ISDN-B-Kanal gewöhnlich entweder nach X.75- oder V 110-Norm. Das X.75-Protokoll nutzt die Bandbreite des ISDN voll aus, dabei beträgt die Datenübertragungsrate 64000 Bit/s pro ISDN-B-Kanal. Handelt es sich um eine Gegenstelle, die weniger als 64000 Bit/s zulässt, zum Beispiel der CompuServe-Dienst über ISDN, so muss die Datenrate angepasst werden. Man spricht daher von der Bitratenadaption. Dabei werden zwischen der benötigten Bitrate und den 64000 Bit/s Maximaldatenübertragung Füllbits eingefügt. Dieses Verfahren ist in der Norm V 110 für 2400 bis 38400 Bit/s definiert und kann nur mit ISDN-Karten genutzt werden, die diesen Standard unterstützen. Wer flexibel in der Anwendung sein will, sollte sich daher für einen Adapter entscheiden, der beide Normen erfüllt.

CAPI

CAPI steht für Common ISDN Application Interface und wurde mit dem Ziel entwickelt, eine einheitliche Schnittstelle zwischen der Anwendungssoftware und dem ISDN-Endgerät (z. B. ISDN-Karte) zu schaffen. CAPI ermöglicht prinzipiell die Nutzung jeder ISDN-Karte mit CAPI-Unterstützung mit jeder ISDN-Anwendungssoftware, die ebenfalls CAPI unterstützt. federführend bei der Entwicklung von CAPI waren hauptsächlich deutsche Firmen der ISDN-Branche und die Deutsche Telekom.

In der Praxis kommen momentan zwei CAPI-Versionen zum Einsatz. CAPI-Version 1.0 und 1.1 ist auf PC-basierende ISDN-Lösungen zugeschnitten und wird von nahezu allen PC basierenden ISDN-Karten unterstützt; die neuere Version CAPI 2.0 bringt als wesentliche Verbesserung die Unterstützung beliebiger Plattformen und hat daher gute Chancen, sich auch im UNIX-Umfeld zu etablieren. Die Plattformunabhängigkeit ist mit ein Grund, warum Windows NT in den Remote Access Services (RAS) CAPI 2.0 verwendet. Kommunikation mit analogen Gegenstellen.

Falls sich die Gegenstelle im analogen Telefonnetz befindet, etwa wenn es sich um ein analoges Modem oder um einen analogen Zugang zu einem Netzwerk handelt, so gestaltet sich die Datenkommunikation wesentlich schwieriger. Die Verbindung mit analogen Gegenstellen funktioniert nur, wenn dies vom ISDN-Endgerät unterstützt wird. Einige ISDN-Karten oder ISDN-Terminaladapter haben daher einen eingebauten analogen Modemchip oder digitalen Signalprozessor (DSP), der eine Nutzung wie ein

analoges Modem gestattet. Die Kommunikation mit analogen Faxgeräten ist jedoch auch mit ISDN-Karten möglich, die keinen Modemchip besitzen, wenn eine entsprechende Faxsoftware für diese Karte verfügbar ist. Diese Software bereitet dann die digitalen Daten für das analoge Faxgerät auf. Allerdings ist diese Methode aufwendig und kann unter Umständen zu Fehlern in der Faxübertragung führen.

12.2.7 Aktive/passive ISDN-Karten

Beim Kauf einer ISDN-Karte kann man sich zwischen einer preiswerten passiven ISDN-Karte oder einer leistungsfähigeren aktiven Karte entscheiden. Für Einzelplatzanwendungen, die nur gelegentlich ISDN-Dienste nutzen, reicht gewöhnlich eine passive Karte aus. Diese verfügen über keinen eigenen Prozessor. Daher muss die Abwicklung der ISDN-Kommunikation von der Kommunikationssoftware übernommen werden, die auf dem Prozessor des PCs abläuft. Dies führt während der Datenübertragung zu einer höheren Rechnerbelastung. Hier haben aktive Karten, die einen eigenen leistungsfähigen Prozessor besitzen, einen wesentlichen Vorteil. Wer die ISDN-Kommunikation im Hintergrund betreiben will oder wer datenintensive Anwendungen zum Beispiel beim Einsatz einer oder mehrerer ISDN-Karten in einem Netzwerk-Fileserver zur LAN-LAN-Kopplung oder für Remote Access einsetzt, sollte unbedingt eine aktive Karte verwenden.

Alternativ zu den aktiven Karten gibt es auch ISDN-Karten, die zwar über keinen Speicher auf der Karte verfügen, aber trotzdem einen eigenen Prozessor besitzen. Man bezeichnet diese Karten daher als semi-aktiv. Im Gegensatz zu passiven Karten ergibt sich eine geringere Rechnerbelastung und eine größere Sicherheit in der Datenübertragung. ISDN-Karten liegen preislich zwischen den passiven und den aktiven Karten.

12.2.8 ISDN Bridge/Router

Auf die grundlegenden Eigenschaften von Bridges und Bridge/Routern wurde im Abschnitt Bridges und Router bereits näher eingegangen. ISDN-Bridge/Router unterscheiden sich von seriellen Routern vor allem durch die integrierte ISDN-Schnittstelle und zusätzliche Features, die bei der LAN-LAN-Kopplung über Wählverbindungen erforderlich sind.

Spoofting und Filtering

Warum werden von ISDN Bridge/Routern Funktionen wie Spoofting und die Unterstützung von umfassenden Filtern gefordert? Man stelle sich folgendes Szenario vor: Es werden zwei größere NetWare LANs über zwei ISDN Bridge/Router gekoppelt. Über die ISDN-Verbindung sollen insbesondere Datenbankdaten einmal pro Tag aktualisiert werden. Die Rechnung aber, die am Monatsende kommt, übersteigt bei weitem das, was anhand der



kalkulierten Übertragungszeit zu erwarten wäre. Ursache dafür sind regelmäßige Broadcasts, die zwischen Clients und Servern auftreten. Bei einem LAN werden im Sekundentakt Pakete über den Zustand des Netzes und der angeschlossenen Stationen verschickt. Diese Broadcast- und Statusinformationen führen dazu, dass die Verbindung zu einem remote angeschlossenen LAN entweder gar nicht erst ab- oder ständig neu aufgebaut wird.

Daher sollten für die effiziente Kopplung von Netzen über Wählleitungen, also dort, wo die Kosten nach Verbindungsdauer anfallen, Bridges und Bridge/Router eingesetzt werden, welche Spoofing implementiert haben. Spoofing ermöglicht es, Broadcasts zu unterdrücken und, wenn erforderlich, auf der Gegenseite zu emulieren. Statusinformationen oder SAP-Pakete, die nicht benötigt werden, werden einfach herausgefiltert. Spoofing ist damit zumindest in der Theorie eine elegante Lösung, um unnötige Pakete von einer WAN-Verbindung fernzuhalten. Doch wie Spoofing von den Herstellern in den Produkten implementiert wird, ist durchaus unterschiedlich. Es ist zwar einfach, z. B. Service Frames auf der einen Seite zu filtern und auf der Gegenseite zu emulieren. Allerdings muss auch beim Spoofing dafür Sorge getragen werden, dass der Transport wichtiger Informationen (z. B. Änderungen in den Routertabellen, die für die Aufrechterhaltung des Netzbetriebs notwendig sind) weiterhin erfolgt. Deswegen gibt es für die Aktualisierung von netzwerkrelevanten Daten über eine ISDN-Verbindung drei verschiedene Techniken.

Timed updates

Bei dieser Methode ist der Netzwerkmanager in der Lage, Zeitintervalle festzulegen, in denen RIP- (Router Information Protocol) und SAP- (Service Advertising Protocol) Pakete als Broadcasts über den WAN-Port von Bridge oder Router geschickt werden. Bei Netzen, in denen nur wenige Änderungen auftreten, ist diese Methode eine adäquate Lösung. Triggered updates.

Der Router öffnet hier immer dann die ISDN-Verbindung, wenn er Änderungen in den Routing- oder SAP-Tabellen feststellt. Vorteil dieser Methode ist, dass Änderungen quasi online an alle im Netz befindlichen Knoten mitgeteilt werden. In einem sehr großen Netz (das sich bezüglich Änderungen mehr oder weniger dynamisch verhält) kann dieses Verfahren teuer werden, da bei jeder Änderung die WAN-Verbindung aufgebaut wird. Hinzu kommt, dass viele Änderungen für die meisten anderen Subnetze uninteressant sind. Piggyback updates

Diese Technik aktualisiert die Routing- und SAP-Tabellen immer dann, wenn sowieso eine ISDN-Verbindung aufgebaut wird, um Daten zu übertragen. Da dieses Update nur erfolgt, wenn auch die Leitung hergestellt ist, kann dies dazu führen, dass die Tabellen nicht mehr aktuell sind, nachdem längere Zeit keine Daten übertragen wurden. Die Folge können Verbindungsprobleme im Netz sein. Diese Methode ist am effizientesten in Netzwerken einzusetzen, in denen die ISDN-Leitungen regelmäßig genutzt werden. Bei regelmäßigen oder sogar permanenten Verbindungen kann der Einsatz eines virtuellen

privaten Netzwerks über das Internet die kostengünstigere Alternative zu ISDN sein.

Remote Maintenance

Der Wettbewerbsdruck zwingt Unternehmen heute verstärkt zur Rationalisierung in allen betrieblichen Bereichen. Fernwartung etwa erlaubt es dem Benutzer, Remote Bridges und Router vom zentralen Netz aus zu betreuen, wodurch ein zusätzlicher Netzwerkadministrator in den Außenstellen entfällt. Interessante Möglichkeiten eröffnet hier die Dual Flash RAM Technologie. Ein Dual Flash Filesystem erlaubt es dem Anwender, neue Betriebssoftware oder Konfigurationsdateien zu laden, ohne den bisherigen Speicherinhalt von Bridge oder Router überschreiben zu müssen. Dieses Feature birgt eine Reihe von Vorteilen, die für den störungsfreien Netzwerkbetrieb wesentlich sind. Zum einen besteht die Möglichkeit, beim Bootvorgang des Routers automatisch die Sicherungskopie der Betriebssoftware zu aktivieren, sollte beim Laden des primären Software-Images ein Fehler auftreten. Weiterhin kann der Netzwerkmanager beim Testen neuer Konfigurationen jederzeit problemlos zum Ausgangspunkt zurückkehren. Selbst das Aufspielen neuer Software vom zentralen Netz auf die extern installierten Bridge/Router kann ohne Risiko durchgeführt werden. Die Gefahr des Überschreibens später wieder benötigter Files wird mit der Dual Flash-Technologie wirksam beseitigt.

Produktauswahl

Generell sind bei der Auswahl von ISDN-Produkten nicht nur die einmaligen Anschaffungskosten, sondern vor allem auch die laufenden Kosten ins Kalkül mit einzubeziehen. Über die Lebensdauer des Produkts hinweg fallen Leitungskosten an, die typischerweise in der Summe deutlich höher sind als der reine Anschaffungspreis. Aus diesem Grund zahlt sich ein vermeintlich teureres Produkt mit effizientem Verbindungsmanagement und hohem Datendurchsatz wegen der geringeren laufenden Kosten in der Regel auch finanziell aus. Zwar ist der Datendurchsatz zunächst durch den Leitungstyp begrenzt; es wird aber oftmals nicht bedacht, dass die effektive Ausnutzung dieser Verbindung für die Übertragung von Nutzdaten bei den am Markt erhältlichen Produkten sehr unterschiedlich sein kann. Neutrale Testergebnisse können hier recht hilfreich sein. Vor der Entscheidung für ein solches Produkt müssen in jedem Fall die Anforderungen klar definiert sein, damit ein in der Anschaffung günstigeres Gerät nicht doch langfristig teuer kommt. Um unangenehme Überraschungen bei der Gebührenabrechnung auch im Ortsbereich zu vermeiden, muss unbedingt die Anzahl der Verbindungsaufbauten und die gesamte Verbindungszeit kontrolliert werden.





12.3 xDSL - Digital Subscriber Lines

Die xDSL-Technik (Digital Subscriber Lines) ist ein neues Übertragungsverfahren auf einer analogen 2-Draht-Leitung. Dabei kann, skalierbar in 64 kbit/s-Schritten, eine Übertragungsgeschwindigkeit von bis zu 2 Mbit/s erreicht werden. Die maximale Entfernung zwischen zwei Punkten beträgt 6 km. Auf beiden Seiten ist je ein so genanntes Megabit- bzw. xDSL-Modem nötig. Unterschieden wird zwischen den folgenden Standards: ADSL (Asymmetric DSL), HDSL (High-Bit-Rate DSL), RADSL (Rate Adaptive DSL), SDSL (Symmetric High-Bit-Rate DSL) und VDSL (Very High-Bit-Rate DSL). xDSL ist eine an und für sich viel versprechende Technologie, die auch recht preisgünstig zu implementieren ist. Derzeit wird von der Deutschen Telekom und anderen Telefongesellschaften ADSL in Ballungsräumen angeboten, die Gebühren liegen jedoch drastisch über den ca. 50 Euro, die ADSL-Dienste volumenunabhängig in den USA kosten.

12.4 Kabelmodems

In den USA sind die Feldversuche zu High Speed Internet und Telefonie via TV-Kabelnetz erfolgreich abgeschlossen und zur Marktreife gelangt. Dabei erfolgt der Zugang zum Netz über ein spezielles High Speed Kabel Modem, welches in der Regel über das Netzwerk mit dem Computer verbunden wird. In Download-Richtung können diese Modems Daten mit bis zu 10 Mbit/s zum Kabelkunden übertragen. Eine separate Telefonleitung wird nicht mehr benötigt, da die TV-Kabelnetze, mit Verstärkern für die Gegenrichtung ausgerüstet, breitbandig rückkanalfähig sind. Der Empfang von Fernsehprogrammen wird durch die zusätzliche Verwendung des TV-Kabelnetzes für die Internet-Nutzung nicht beeinträchtigt. Ein Einsatz dieser Technik auch in Europa scheitert derzeit in erster Linie noch an politischen Blockaden. Es gibt zwar auch einen ersten Feldversuch in Deutschland („Infocity NRW“). Die Deutsche Telecom favorisiert allerdings die ADSL-Technik. Sollten die derzeit bestehenden Hemmnisse abgebaut werden können, ist mittelfristig mit einem Marktvolumen von mehreren Milliarden Euro zu rechnen. Netzwerk- und PC-Anbieter wie Cisco, 3Com, Bay Networks, NEC und Toshiba wollen einen Kabelmodem-Standard für den nordamerikanischen Markt entwickeln. In Europa arbeiten insbesondere Siemens und Motorola bereits jetzt gemeinsam an der Weiterentwicklung der nötigen Hardware.

12.5 X.25

Zum Zweck der Datenübertragung gibt es eigene Datennetze, z. B. Datex-P in Deutschland, Telepac in der Schweiz oder Datenet 1 in den Niederlanden.

Diese öffentlichen Wählnetze basieren auf dem international standardisierten Paketvermittlungsprotokoll X.25. Sie ermöglichen den Zugang zu allen anderen weltweit

vorhandenen nationalen X.25-Paketvermittlungsdiensten.

X.25-Dienste eignen sich insbesondere für die Kopplung lokaler Netze mit X.25-fähigen Remote Routern. Gegenüber dem Fernsprechnet liegen die wesentlichen Vorteile in der kürzeren Verbindungsaufbauzeit von einer Sekunde und der besseren Übertragungsqualität. Übertragungsgeschwindigkeiten von 300 bis 64000 Bit/s sind möglich.

X.25 ist heute weitgehend durch Frame Relay ersetzt.

12.6 Frame Relay

Frame Relay ist ein X.25-ähnliches Übertragungsverfahren, das sich durch einen vergleichsweise geringen Protokoll-Overhead auszeichnet. Im Gegensatz zu X.25 arbeitet Frame Relay nur auf den Ebenen 1 und 2 des ISO/OSI-Modells. Das Protokoll kümmert sich damit nicht mehr selbst um die korrekte Zustellung von Datenpaketen, sondern legt die Verantwortung hierfür in die Hände der Endgeräte.

Die von X.25 bekannten Probleme der Effizienz werden somit durch die Verlagerung der Fehlerkorrektur auf obere Protokollschichten umgangen. Es werden auch bedeutend höhere Datenraten als bei X.25 ermöglicht. Damit eignet sich Frame Relay sehr gut, um den Durchsatz im WAN zu verbessern. Im Vergleich zu Standleitungen bringt Frame Relay immer dann wirtschaftliche Vorteile, wenn die Punkt-zu-Punkt-Verbindung nur ungenügend ausgelastet ist. Je nach Land kann die Frame-Relay-Technik in unterschiedlichen privaten oder öffentlichen Netzen eingesetzt werden, so z. B. im Datex-M-Dienst der Deutschen Telekom. Für den Netzzugang wird das SNI (Subscriber Network Interface) als Netzwerkabschluss eingesetzt. Der Small-Entry-Anschluss beginnt bei 64 kbit/s, die nächste Kategorie bei 2 Mbit/s (E1). Die Standardschnittstelle zu Router oder Bridge ist in solchen Fällen X.21. Die höchste Geschwindigkeitsklasse erreicht derzeit 34 Mbit/s nach dem Standard E3. Hier kommt als Anschluss die von Cisco Systems entwickelte HSSI-Schnittstelle (High Speed Serial Interface) zum Einsatz.

Obwohl Frame Relay deutliche Vorteile gegenüber X.25 bietet, ist diese Technik für die Unterstützung zeitkritischer Anwendungen wie Sprach- und Videoübertragung weniger geeignet. Noch bis vor einigen Jahren stellte dies kein Problem dar, da Sprach-, Bild- und Datennetze ohnehin getrennt errichtet wurden. Seit jedoch Multimedia-Anwendungen wie Videoconferencing und Videodistribution sowohl in LAN- als auch in WAN-Netzwerken immer häufiger genutzt werden, ist die Integration von Audio- und Videoinformation in das bislang nur für Datenübertragungen verwendete Netzwerk erforderlich. Hier kommt vor allem das jüngste paketvermittelnde Übertragungsverfahren ins Spiel – der



Asynchrone Transfer Modus ATM.

Inzwischen bieten einige Anbieter Frame Relay Verbindungen an. Diese Anbieter unterscheiden sich deutlich im Preis, aber teilweise noch deutlicher in der Leistung. Es ist in diesem Markt keinesfalls üblich, dass zugesagte CIRs (Committed Information Rate) auch wirklich zur Verfügung gestellt werden oder dass Round Trip Delays in vernünftigen Bereichen liegen. Ehe man sich für einen Frame Relay Anbieter entscheidet, sollte man genau prüfen, wie gut dessen Netz ist, und sich vertraglich zusichern lassen, was bei Nichteinhaltung zugesicherter Eigenschaften passiert.

12.7 Datenübertragung über das Stromnetz

Das Stromnetz ist das bei weitem dichteste Netz und erreicht praktisch jeden Haushalt. Schon seit Jahrzehnten wird das Stromnetz zur Übertragung langsamer Datenströme (ein bis fünf Bit pro Sekunde) an Steuerungsanlagen genutzt. Durch den Fortschritt der Datenübertragungstechnik können mittlerweile bis zu 1 Mbit/s bidirektional übertragen werden. Dabei werden die Daten in der Umspannstation eingekoppelt und über Niederspannungsleitungen zum Nutzer übertragen. Die Auskopplung der Daten erfolgt am Stromzähler, der Rechner wird über ein so genanntes Powerline Modem über USB oder Ethernet angeschlossen. Erste Pilotprojekte werden von einigen Stromnetzbetreibern betreut.

12.8 Remote Access

Unter Remote Access versteht man den Fernzugriff auf Anwendungen oder Daten von Rechnern von einem System aus, das nicht direkt über ein LAN mit diesen Rechnern verbunden ist.

Voraussetzung für den erfolgreichen Zugriff sind eine Reihe von Faktoren, welche im Einzelnen nachfolgend beschrieben werden.

Erste Voraussetzung ist eine Netzwerkverbindung zwischen dem zugreifenden Rechner und dem System, auf dem sich die Daten oder Applikationen befinden. Im einfachsten Fall erfolgt die Verbindung über Modems, die jeweils an eine serielle Schnittstelle beider Systeme angeschlossen werden. Es können aber auch Communication Server (siehe Punkt 12.7.5) mit daran angeschlossenen Modems eingesetzt werden. Wird ISDN als Übertragungsdienst gewählt, kommen interne ISDN-Controller oder seriell anschließbare ISDN-Terminaladapter zum Einsatz. Prinzipiell sind auch alle anderen Verbindungstypen wie GSM, X.25 oder Frame Relay, die in den vorhergehenden Abschnitten bereits beschrieben wurden, einsetzbar.

Mehr und mehr gewinnt das Internet an Bedeutung als kostengünstiges Transportmedium für Verbindungen über das von Microsoft entwickelte Point to Point

Tunneling Protokoll (PPTP). PPTP erlaubt die Einrichtung gesicherter Tunnels für so genannte Virtual Private Dial-Up-Networks (VPDN). Unter Punkt 12.8.4 wird hierauf näher eingegangen.

Zweite Voraussetzung ist ein Kommunikationsprotokoll mit dem die Daten zwischen den Systemen oder auch über das Netzwerk transportiert werden. Die größte Bedeutung kommt hier dem Point-to-Point Protokoll (PPP) zu. PPP ist ein spezielles Leitungsprotokoll für WAN-Verbindungen über serielle Leitungen. Es ermöglicht die Übertragung von LAN-Protokollen wie TCP/IP, IPX oder DECnet im asynchronen oder synchronen Verfahren. Auf die Funktionsweise und den Aufbau von PPP wird weiter unten im Punkt 12.7.2 näher eingegangen. Die älteren Protokolle SLIP und CSLIP (Compressed Serial Line Internet Protocol) haben heute kaum mehr Bedeutung. Für X-Window-basierende Systeme wurde das so genannte Low Bandwidth X Protocol (LBX) entwickelt. Dieses Protokoll sorgt durch Datenkompression für eine Beschleunigung der Datenübertragung, wenn, wie bei seriellen Verbindungen, nur eine geringe Bandbreite zur Verfügung steht.

Typischerweise teilt man Remote Access Anwendungen in die folgenden drei Hauptgruppen: Remote Control, Remote Node und Datentransfer. Zwar sind alle diese Anwendungen mit sehr unterschiedlichen Systemen auf beiden Seiten denkbar; da jedoch bei den weitaus meisten Szenarien das zugreifende System unter einem Windows-Betriebssystem läuft, wird im Folgenden jeweils nur hierauf näher eingegangen. Das Gesagte lässt sich prinzipiell auch auf beliebige andere Systeme übertragen.

12.8.1 Remote Control

Unter Remote Control versteht man die Fernbedienung eines Rechners durch einen zweiten Rechner, der von außen über die WAN-Verbindung zugreift. Beim fernbedienten Rechner kann es sich entweder um ein Standalone-Gerät handeln oder auch um eine Arbeitsstation in einem lokalen Netzwerk. Je nachdem, ob es sich bei dem fernbedienten Rechner um ein Single-User-System oder ein Multi-User-System handelt, ist die Fernbedienung exklusiv (z. B. bei Windows 9x) oder kann parallel erfolgen (z. B. bei Unix).

Da sich die Datenübertragung auf Tastatur- und Bildschirminformationen beschränkt, ermöglicht die Remote-Control-Technik eine relativ hohe Arbeitsgeschwindigkeit, sofern man nicht mit Anwendungen arbeitet, die sehr häufig den Bildschirm komplett neu aufbauen oder Große Mengen an Grafiken verwenden. Ein wichtiger Anwendungsbereich von Remote Control liegt in der Wartung eines einzelnen Rechners oder eines LANs über die WAN-Verbindung. So lassen sich Software-Probleme sehr einfach und preisgünstig beheben, die teure Anfahrt eines Spezialisten wird in vielen Fällen vermieden.

Remote Control von Windows 9x- und Windows NT Systemen benötigt auf beiden Seiten eine spezielle Kommunikationssoftware, die für die Übertragung und Darstellung der





Daten sorgt. Die am weitesten verbreiteten Software sind hier pcAnywhere von Symantec, ReachOut von Stac und Carbon Copy von Dr. Neuhaus. Die Datenverbindung zwischen den Systemen kann über Modem, ISDN, Internet, aber auch LAN (TCP/IP, IPX, NetBEUI etc.) vorgenommen werden.

Remote Control bei Windows 2000 Servern ist dank der enthaltenen Terminal Services sehr einfach. Die Terminal Services erlauben im Administrations-Modus die Verwaltung des Servers sowohl über Intranet als auch Internet von jedem unterstützten Client aus.

Beim Remote-Control-Zugriff auf ein Unix-Netz kommt auf der PC-Seite eine Terminalemulation (wie zum Beispiel das Hyperterminal in Windows 9x) zum Einsatz. In der Praxis reicht diese aber häufig nicht aus. Deshalb werden meistens gesonderte Terminalprogramme wie KEA! von Attachmate oder der Host Explorer von Hummingbird verwendet, insbesondere wenn auf besondere Tastaturzuordnungen Rücksicht genommen werden muss. Der Anwender macht über die Terminalemulation einen remote Login und erhält dieselbe Arbeitsumgebung, die er auch bei einem direkten Login über ein ASCII-Terminal oder innerhalb eines Shell-Fensters in einer grafischen Unix-Oberfläche hat. Sollen grafische Anwendungen wie zum Beispiel ein Kalender-Manager oder ein grafisches Mailprogramm bedient werden, muss auf der Client-Seite eine PC X-Server-Software installiert werden. Für serielle Übertragungen des X-Protokolls haben die Anbieter dieser Software proprietäre Lösungen (wie zum Beispiel Xremote von NCD oder Xpress-Host von Tektronix) entwickelt. Mit Einführung von X.11 Release 6 (X11 R6) werden diese inzwischen durch den einheitlichen Standard Low Bandwidth X (LBX) abgelöst. Dabei wird ein Proxyserver zwischen X-Client und X-Server geschaltet. Dieser Proxy-Server übernimmt Datenkompressions- und Cache-Funktionen für die in der Regel langsame WAN-Strecke zwischen Client und Proxy. Neueste PC X-Server wie Exceed Version 6 von Hummingbird unterstützen LBX bereits. Da LBX im Gegensatz zu den vorherigen Lösungen auf TCP/IP beziehungsweise auf einer PPP-Verbindung basiert, handelt es sich dabei nicht mehr um Remote Control im eigentlichen Sinne.

12.8.2 Remote Node

Bei einer Remote-Node-Lösung wird der Remote-PC zu einem Knoten des Netzwerks in welches er sich einwählt. Die Kommunikation erfolgt, wie im LAN, über das Netzwerkprotokoll, das mittels eines Trägerprotokoll über die Wählleitung betrieben wird. Der Remote-PC besitzt daher, wie ein direkter Knoten im Netz, eine eigene Netzwerkadresse. Diese wird entweder bei der Einwahl zugewiesen oder vorher fest vergeben.

Bei Remote Node laufen alle Anwendungen auf dem zugreifenden Rechner. Damit die Anwendungsprogramme nicht immer über die vergleichsweise langsame Leitung geladen werden müssen, ist es sinnvoll, wenn sie auch dort lokal vorhanden sind.

Da LAN-Protokolle wie TCP/IP, IPX oder DECnet nicht direkt über eine serielle Leitung

übertragen werden können, ist ein spezielles Kommunikations- bzw. Trägerprotokoll nötig. Das mit Abstand am häufigsten verwendete Protokoll ist das Point-to-Point-Protokoll (PPP). Die Aufgabe von PPP ist somit, Daten mit dem LAN-Protokoll zu transportieren. PPP ist folglich kein weiteres Protokoll im Sinne der LAN-Protokolle, sondern in der Hauptsache ein Trägerprotokoll für die vorhandenen LAN-Protokolle. Beim Transport übernimmt PPP verschiedenste Aufgaben, wie Aushandlung der Verbindungsparameter, Kompression, Festlegung der Blockgröße, Ausblenden von Steuerzeichen, Überwachung der Leitungsqualität oder Passwortvalidierung über PAP (Password Authentication) und CHAP (Challenge Handshake Authentication). Über PPP können verschiedene Netzwerkprotokolle wie TCP/IP, IPX oder AppleTalk auch gleichzeitig benutzt werden. Ebenso ist es möglich, über eine PPP-Verbindung parallel mehrere Tasks laufen zu lassen, etwa ein telnet-Fenster für ein Unix-System plus einen Web-Browser über TCP/IP.

Der Remote Node Zugang bei Windows NT läuft über den in Windows NT direkt enthaltenen RAS (Remote Access Service). Der einwählende PC verbindet sich mit dem RAS Server und kann über diesen auf das Netzwerk zugreifen. Als Transportprotokoll wird PPP oder SLIP verwendet, für Verbindungen über TCP/IP, IPX/SPX oder NetBEUI. Der RAS-Server muss in jedem Fall ein NT-Server sein, da nur im Server-Betriebssystem die RAS-Server-Funktionalität enthalten ist. Einwählen können sich RAS-Clients sowie Remote-Clients, auf denen Microsoft DFÜ-Netzwerk ausgeführt wird, aber auch prinzipiell jeder andere PPP-Client. Jeder RAS-Client kann Dienste wie Internet-Zugang, Datei- und Druckerfreigabe, E-Mail, Terminplanung und SQL-Datenbankzugriff nutzen. Über einen RAS-Server sind bis zu 256 Verbindungen gleichzeitig möglich.

Durch den vollwertigen IP-Stock in den aktuellen Windows-Versionen können auch Remote Node Verbindungen zu Unix-Netzwerken aufgebaut werden. Auch hier erfolgt eine PPP-Verbindung, und der Remote Rechner erhält eine eigene IP-Adresse. Für den Filezugriff auf Unix-Laufwerke muss allerdings eine zusätzliche NFS-Clientsoftware auf dem PC vorhanden sein (siehe auch NFSunter Punkt 6.4.1).

Für Remote Node unter NetWare/IntranetWare gibt es von NOVELL spezielle Softwarepakete. Auf dem einwählenden Rechner wird NetWare-Connect installiert. Im Netz wird auf einem NetWare-Server entweder auch NetWare-Connect oder die NetWare Multiprotokoll-Routersoftware installiert. Die Verbindung zwischen Client und Netz läuft auch hier über PPP, wobei als Netzwerkprotokoll sowohl IPX als auch TCP/IP gewählt werden kann. Verschiedene Hersteller von ISDN-Controllern (z. B. AVM) bieten spezielle Versionen von NetWare-Connect und der NetWare Multiprotokoll-Routersoftware an, welche auf die CAPI-Schnittstelle und damit auf interne ISDN-Controller aufsetzen.

12.8.3 Datentransfer und Datenkopierprotokolle

Neben Remote Control und Remote Node gibt es eine Reihe von Anwendungen, bei denen Dateien, Mails oder HTML-Dokumente übertragen werden. Wie Remote Node



basieren diese Protokolle auf einem Netzwerkprotokoll, vorrangig TCP/IP. Im Gegensatz zu Remote Control und Remote Node ist hier die logische Verbindung nur solange aktiv, bis ein bestimmter Dienst (z. B. ein Dateitransfer) ausgeführt wurde. Von besonderem Interesse für Internet- und Internet-Anwendungen sind folgende Protokolle:

- HTTP (Hyper Text Transmission Protocol) und Netscapes Erweiterung HTTPS (Hyper Text Transmission Protocol, Secure) zum Datenaustausch zwischen Web-Browsern und Web-Servern im World Wide Web
- FTP (File Transfer Protocol) zur Übertragung von Dateien und Dateigruppen zwischen Rechnersystemen, die per IP miteinander verbunden sind.
- POP3 (Post Office Protocol Version 3) und IMAP4 (Internet Message Access Protocol Version 4) zum Mailaustausch mit einem Mailserver und zum Verwalten eines Mailservers
- SMTP (Simple Mail Transfer Protocol) zum Austausch von Mails zwischen Mail-Hosts in einem TCP/IP-basierenden Kommunikationsnetz, typischerweise im Internet.

12.8.4 PPTP und Virtual Private Networks (VPN)

Das Point-to-Point Tunneling Protocol (PPTP) ist ein von Microsoft entwickeltes Protokoll, mit dem der Datenverkehr zwischen zwei Stationen verschlüsselt übertragen werden kann. Es erlaubt den Aufbau von Virtual Private Networks (VPN) beziehungsweise Virtual Private Dial-Up Networks (VPDN). PPTP schafft einen sicheren Daten-Tunnel, innerhalb dessen insbesondere auch Passwörter verschlüsselt übertragen werden, und erlaubt so die Nutzung ungesicherter Medien wie Internet oder das Netz eines beliebigen Carriers für den Aufbau einer gesicherten Dial-Up-Verbindung oder sogar eines standortübergreifenden Intranets über öffentliche und somit nicht firmeneigene Leitungen.

PPTP ist Bestandteil von RaRAS (Routing and Remote Access Service), welches fester Bestandteil von Windows NT 5.0 sein wird. Ausführliche Informationen zu RaRAS finden sich unter Netzwerkdienste von Windows NT (Seite 281).

Derzeit unterstützen noch nicht alle ISPs und Carrier die Nutzung von PPTP-Verbindungen. Es ist jedoch abzusehen, dass sich PPTP als Standard durchsetzen wird. Dann ist auch mit einem flächendeckenden Angebot zu rechnen.

12.8.5 Communication Server

Communication Server sind Standalone Systeme für den Aufbau von Remote Access Lösungen mit hoher Portdichte.

Der Hardwareaufbau eines typischen Communication Servers entspricht dem eines Terminalservers. Das Gerät besitzt einen Ethernet-Port und mehrere serielle Schnittstellen für den Anschluss von Modems oder ISDN-Terminaladaptern. Neuere Modelle sind inzwischen bereits mit ISDN-Ports für den direkten Anschluss des Communication Servers an einen Basis- oder Primärmultiplexanschluss ausgestattet.

Im Gegensatz zu einem Terminalserver bietet ein Communication Server jedoch eine Reihe zusätzlicher Funktionalitäten. Communication Server unterstützen Kommunikationsprotokolle wie PPP oder SLIP/CSLIP und sind damit in der Lage, mehrere logische Datenströme über einen physikalischen Port zu leiten und somit mehrere Rechner über diese eine Verbindung zu bedienen. Die integrierte Routingfunktionalität ermöglicht es sogar komplette Netze über einen Port des Communication Servers zu verbinden.

Weitere Unterscheidungsmerkmale zu Terminalservern sind die höhere bidirektionale Geschwindigkeit der seriellen Ports (bis zu 230 kbit/s) sowie die Unterstützung von Security Funktionen wie Username/Password und Dialback sowie spezieller Security-Systeme wie RADIUS, Kerberos oder SecurID (siehe Punkt 9.4 Netzwerk-Security). Der Einsatz eines Communication Servers erübrigt einen zusätzlichen Rechner mit seriellen Schnittstellen oder ISDN-Controllern, der eigens für Remote Access Aufgaben abgestellt werden muss. Speziell auf die Kommunikationsaufgaben abgestimmte Konfigurations- und Managementtools erleichtern zudem die Einrichtung und Wartung der Remote-Verbindungen. Da die Anzahl der im Netz installierten Communication Server nur durch die Netzperformance beschränkt ist, können selbst komplexe Lösungen mit mehreren Hundert Ports realisiert werden. Bei einer Dial-up-Konfiguration mit einem Communication Server kann auf der Client-Seite beliebige Kommunikations-Hardware zum Einsatz kommen. Unabhängig davon, ob Modem, ISDN-Controller, Router oder wiederum Communication Server - wichtig ist lediglich die Unterstützung des verwendeten Kommunikationsprotokolles (PPP, SLIP/CSLIP etc.).

12.8.6 Datenübertragung via GSM

Es ist nicht möglich, ohne weiteres Daten oder Faxe über Mobiltelefone zu versenden, indem man seinen Laptop mit einer PCMCIA-Karte ausstattet und mit seinem Handy verbindet. Der Grund hierfür liegt in dem verlustbehafteten Datenkompressionsverfahren, dass in GSM-Netzen Anwendung findet. Dieses stellt zwar sicher, dass Sprache mit kaum wahrnehmbaren Veränderungen übertragen wird, für die fehlerfreie Übermittlung von Modemsignalen ist es aber ungeeignet. Wer dennoch auf die Nutzung der Fax- und Datendienste Wert legt, muss sich von seinem Provider entsprechende zusätzliche Mobilfunk-Rufnummern freischalten lassen, über die eine transparente Datenverbindung gefahren werden kann. Ebenfalls notwendig ist ein entsprechendes Adapterkit, bestehend aus PCMCIA Karte und Kabel, für den Anschluss des Mobiltelefons an den Computer. Alternativ kann auf dem verwendeten PC ein so genanntes Softmodem installiert werden. Dieses Softmodem emuliert ein Modem auf dem PC, der Anschluss des Handys wird über ein Spezialkabel zur RS-232-Schnittstelle des Computers





herbeigeführt.

Die dritte Variante, die PC/GSM Connection via IrDA-kompatibler Infrarotschnittstelle, bietet sich bei Handys an, die den kompletten IrDA-Befehlssatz unterstützen. Entsprechende Geräte von Ericsson (z. B. Ericsson 6130) sind bereits auf dem Markt, andere Hersteller wie z. B. Nokia werden in Kürze ebenfalls solche Geräte anbieten.

Eine Neuentwicklung ist die Kombination aus PCMCIA-Karte und GSM900 Telefon. Diese eignen sich insbesondere für Geschäftsleute, deren Handy nicht datentauglich ist oder für Reisende, die für Sprachverbindungen ein separates Telefon bevorzugen.

Derartige Kombigeräte gibt es derzeit von Nokia (CardPhone) und Ericsson (Mobile Office). Die Karten werden im Standard-PCMCIA-Slot eines Laptops betrieben. Die jeweils mitgelieferte Software wird per Setup aufgespielt und bietet Schnittstellen zu zahlreichen MS Windows-Applikationen. Aus diesen lassen sich E-Mails, Faxe oder auch SMS-Messages senden und empfangen.

Hardwareseitig bestehen die PCMCIA-GSM-Telefone aus einem GSM-Modem, das seine Leistung über die PCMCIA-Schnittstelle des PC bezieht, einem integrierten Mobiltelefon mit zwei Watt starker GSM-Antenne und einem SIM-Kartenleser.

12.9 Nutzung des Internets

Das Internet stellt dem Anwender eine Vielzahl interessanter Dienste zur Verfügung, das World Wide Web und Electronic Mail als bekannteste Dienste, Filetransfer über FTP, Fernzugriff mittels TELNET und vieles mehr. Allein in Deutschland sind über 1,25 Millionen Internet-Domänen registriert (Stand Ende 1999).

Die Nutzung des Internets kann grob in drei Bereiche eingeteilt werden:

- Abruf von Informationen
- Bereitstellung von Informationen
- Datenaustausch zwischen Standorten über das Internet

Grundvoraussetzung für den Abruf von Informationen aus dem Internet ist ein Internet-Terminal (z. B. PC mit entsprechender Softwareausstattung wie Webbrowser, E-Mail-Programm sowie Modem oder ISDN-Karte/Terminaladapter). Damit kann eine Datenverbindung ins Internet über einen Internet-Service-Provider (ISP) hergestellt

werden.

Über die unterschiedlichen Dienste im Internet kann der Anwender nun gezielt auf Informationen zugreifen: Treiberdateien und Software von Hersteller-FTP-Servern laden, WWW-Dienste wie Auskunfts-, Support-, Onlinebanking- und E-Commerce-Systeme nutzen, elektronische Post empfangen und senden und vieles mehr.

Die Kosten des Internetzugangs hängen ab von Parametern wie z. B. Dauer des Zugangs, übertragenes Datenvolumen und Geschwindigkeit des Zugangs. Neben dem „klassischen“ Modell einer monatlichen Grundgebühr zuzüglich der Kosten für die Online-Zeit gibt es das so genannte Internet-by-Call, bei dem analog zum Call-by-Call ausschließlich Verbindungskosten ohne Grundgebühr und Vertragsbindung anfallen. Welches der beiden Modelle am kostengünstigsten ist, hängt vom individuellen Online-Verhalten ab. Das Internet-by-Call stellt eine einfache Möglichkeit dar, das eigene Online-Verhalten zu beobachten und hilft, die einzelnen Angebote preislich abzuwägen.

Bei der Bereitstellung von Informationen (z. B. WWW-Server, E-Commerce-Anwendungen) erwartet der Anwender, dass diese Dienste rund um die Uhr zur Verfügung stehen. Das bedeutet, dass der Dienst entweder von einem ISP betreut wird (z. B. Webhosting), der ISP hält also bei sich vor Ort die Infrastruktur vor; die Administration erfolgt über gesicherte Verbindungen zwischen Anbieter und „seinem“ Server. Alternativ dazu kann der Anbieter das Serversystem lokal betreuen, benötigt dann aber eine Festverbindung (vorzugsweise über ISDN) zu seinem ISP, um die permanente Erreichbarkeit des Angebots sicherzustellen. Der Datenaustausch zwischen Standorten über das Internet ist eine kostengünstige Alternative zu den klassischen Routing- oder Festverbindungen über ISDN, X.25 und FrameRelay. Wird die Anbindung zum ISP zudem über eine der neuen Anschlusstechniken wie ADSL oder Cable Modem realisiert, kann die Datenübertragung zu noch günstigeren Preisen ermöglicht werden. Um die Daten abhör- und fälschungssicher zwischen den Standorten auszutauschen, wird zwischen den Standorten ein virtuelles privates Netzwerk (VPN) aufgebaut. Dabei werden die Daten verschlüsselt und über eine so gesicherte Verbindung wie durch einen Tunnel zwischen den Endpunkten des VPN hindurchgeleitet. Die Verschlüsselung umfasst die Daten, der Schlüssel wird regelmäßig geändert, so dass Unbefugte praktisch keinen Zugriff auf diese Daten haben. Die Implementierung kann entweder so erfolgen, dass jeder Standort der Endpunkt des VPN ist, also bereits die Verbindung zum ISP gesichert ist, oder aber über eine unsichere Verbindung zum ISP (und dieser bildet einen Endpunkt des VPN) in Abhängigkeit von dem Sicherheitsbedürfnis des Anwenders und den technischen Möglichkeiten seines ISPs.

Zur Realisierung eines VPN auf Anwenderseite steht VPN-Hardware und VPN-Software zur Verfügung. Router Hersteller wie z. B. BinTec und Cisco bieten VPN-fähige ISDN-Router an. Softwarebasierte VPN-Lösungen für Einzelplatz- bzw. Gatewayrechner werden z. B. von Check Point und F-Secure angeboten.



Ein VPN kann also so aufgebaut werden: Eine Tunnel-Software wird in einem Router oder Firewall-Rechner an jedem Standort einzeln installiert, somit wird jeglicher Datenverkehr zwischen den Standorten gesichert durch den VPN-Tunnel geleitet. Alternativ dazu wird die Tunnel-Software auf dem Endgerät installiert (zum Beispiel auf dem Notebook eines Außendienst Mitarbeiters oder auf einem Heimarbeitsplatz). Auf dem Communication Server bzw. Router in der Zentrale muss ebenfalls eine Tunnel-Software installiert sein, dann kann eine gesicherte Wählverbindung (analog, ISDN, GSM) zwischen Zentrale und Außenstelle aufgebaut werden. Trotz aller Normierungsbemühungen ist Tunnel-Software untereinander nicht generell kompatibel. Daher ist bei der Auswahl darauf zu achten, entweder das gesamte VPN-Netz mit der Lösung eines Herstellers aufzubauen oder Hersteller miterwiesener Kompatibilität auszuwählen.





13. Netzwerkmanagement

13.1 Netzwerkmanagementwerkzeuge

Auch ohne den Einsatz von speziellen Tools oder Programmen kann man bereits einfachstes Netzwerkmanagement betreiben. Dazu gehört die richtige Beschriftung der Geräte und ein stets aktueller Plan bzw. eine Dokumentation der eingesetzten Kabel und Geräte. Nächste Stufe ist der Einsatz von Testgeräten, mit denen die verlegten Kabel überprüft werden können, und von Netzwerkmonitoren, mit denen der Datenverkehr auf dem Netz beobachtet und analysiert werden kann.

Eine weitere Möglichkeit des Netzwerkmanagements bietet die Verwendung von Managementsystemen, die auf bestimmten Netzmanagementstandards, herstellerspezifisch oder herstellerneutral, basieren. Zu beachten ist, dass solche Systeme immer auch zusätzliche Last auf dem Netz erzeugen.

Heterogene Netze erfordern ein herstellerübergreifendes Netzwerkmanagementsystem. Aufgrund der weiten Verbreitung von TCP/IP hat sich SNMP (Simple Network Management Protocol) als Quasi-Standard durchgesetzt. SNMP stammt von der Internet Engineering Task Force, einer Gruppe aus dem Internet Activities Board (IAB).

SNMP wurde bereits 1988 von der IAB als Netzwerkmanagementstandardprotokoll für TCP/IP-Netze eingeführt. Es handelt sich dabei um ein asynchrones Request-/ResponseProtokoll.

Ziele bei der Entwicklung von SNMP waren: einfache Konzeption, wachstumsfähige Architektur, kurze Antwortzeiten und geringe Belastung des Netzwerks. SNMP besteht im Wesentlichen aus drei Teilen: einer NMS (Network Management Station), den Managed Nodes mit den Agents und dem eigentlichen SNMP-Protokoll, das zur Kommunikation zwischen NMS und Agent verwendet wird. Als Transportprotokoll wird meist UDP (User Datagram Protocol) verwendet.

Ein Agent ist ein Softwareteil in einem Gerät (beispielsweise einem Switch oder einem Terminalserver) im Netzwerk. Die NMS ist ein Rechner im Netz mit dem Programm, das Informationen bei den Agents anfragt, auswertet und anzeigt. Grundlage des Informationsaustausches ist die SMI (Structure and Identification of Management Information) und die daraus abgeleitete MIB (Management Information Base) mit der Beschreibung der einzelnen Objekte.

Im SNMP ist festgelegt, welche Informationen in der MIB stehen. Leider haben einige Hersteller von SNMP-Produkten die vorgesehenen Private-Fields ausgenutzt und zusätzlich ihre eigenen Informationstypen definiert, so dass es zu

Kompatibilitätsproblemen kommen kann.

Es ist nicht auszuschließen, dass sich aus diesem Grund in Zukunft CMIP (Common Management Information Protocol), der ISO-Standard für Netzwerkmanagement, durchsetzen wird.

Ein weiterer Vorteil von CMIP ist, dass es alle sieben Ebenen des ISO-Modells berücksichtigt. Allerdings ist dafür auch mehr Speicher in den einzelnen Geräten erforderlich.

Den Anwendern von Netzwerk-Management-Systemen ist zu empfehlen, ein System einzusetzen, das SNMP bzw. RMON (mehr zu RMON siehe Abschnitt 12.3) und CMIP unterstützt.

13.2 Kabeltester und Analytoren

Netzwerkanalyse gewinnt vor dem Hintergrund expandierender Netze immer mehr an Bedeutung. Je weiter Netzwerke in sensible Bereiche der Unternehmen vordringen, desto mehr wächst die wirtschaftliche Abhängigkeit von diesem Informationssystem und desto wichtiger werden vorbeugende Maßnahmen zur Aufrechterhaltung des Netzbetriebes. Zwei Dinge werden von Netzwerkbetreuern am meisten gefürchtet: der plötzliche LAN-Stillstand und die mehr oder weniger schleichende LAN-Verlangsamung. Obwohl diese beiden Störungen unterschiedlichen Mechanismen gehorchen, ist ihre Ursache sehr häufig in der Verkabelung zu finden (man schätzt zwischen 50 und 70 Prozent).

Neben echten Kabelunterbrechungen, die für den erwähnten Stillstand sorgen, gibt es zahlreiche Faktoren, die das Netz unnötig verlangsamen. Dazu gehören zum Beispiel: Überschreitung von maximal zulässigen Segmentlängen, schlechte Verbindungsqualität an Stecker-/Kabelübergängen, Abweichung der Kabelqualität von normierten Toleranzgrenzen, Mischung von Kabeln unterschiedlicher Impedanz, Kabelverzweigungen, zu hohe Dämpfung aufgrund zu vieler Stoßstellen (z. B. Stationen) etc. Die Konsequenz aus den oben aufgeführten Erkenntnissen sollte sein, dass jeder Netzwerkmanager sein Netz via Kabeltester prüft oder zumindest im Fehlerfall einen solchen Tester zur Verfügung hat. Voraussetzung für ein gut funktionierendes Netzwerk ist eine qualitativ hochwertige Verkabelung, besonders beim Einsatz von TwistedPair-Kabel. Normen und Empfehlungen befinden sich im Abschnitt 10BASE-T des Kapitels Netzwerke LAN.

Für die Güte von Kabelverbindungen gibt es eine Reihe von Kennzahlen, die im Folgenden diskutiert werden sollen.



Abnahmemessungen an Verkabelungssystemen

Kabellänge

Die Länge eines bereits verlegten Kabels wird über die Time-Domain-Reflektor (TDR) Methode bestimmt. Eine am Ausgang offene oder kurzgeschlossene Leitung ist maximal fehlangepasst und reflektiert einen am Eingang eingespeisten sehr kurzen Impuls annähernd zu 100%. Der Impuls benötigt für den Hin- und Rücklauf eine messbare Zeit, aus der sich bei bekannter Ausbreitungsgeschwindigkeit NVP (Nominal Velocity of Propagation) die zurückgelegte Wegstrecke ermitteln lässt. NVP ist hierbei der springende Punkt, da die Ausbreitungsgeschwindigkeit nur in der Theorie der Lichtgeschwindigkeit entspricht, in der Praxis ist sie abhängig vom Übertragungsmedium. Aus diesem Grund müssen sehr exakte Messgeräte die Möglichkeit vorsehen, über eine Referenzmessung an einem Kabel einer bekannten Länge eine Kalibrierung vorzunehmen.

Wellenwiderstand

Der Wellenwiderstand ist zusammen mit der Frequenz des Signals für die Dämpfung des Signals verantwortlich. Er muss sich in bestimmten Toleranzen um einen vorgegebenen Wert bewegen, damit am fernen Ende des Kabels ankommende Signale noch eindeutig interpretierbar sind. Da der Wellenwiderstand per Definition für ein absolut homogenes Medium festgelegt ist, das keine Anfangsreflexionen erzeugt, sollte im Zusammenhang mit nichtidealen Kabeln besser von einer Eingangsimpedanz gesprochen werden.

Nahnebensprechen

Das Nahnebensprechen (NEXT, Near End Cross Talk) ist ein Effekt bei TwistedPair-Kabeln, der durch kapazitives und/oder induktives Überkoppeln in benachbarte Leitungspaare geschieht und dort dem Empfangssignal das eigene, geschwächte Sendesignal mehr oder weniger stark überlagert. Dies führt zu Störungen, so wie man seinen Gesprächspartner unzureichend versteht, wenn das Umgebungsgeräusch zu groß wird. Abgeleitet wird hieraus die Nahnebensprechdämpfung, die je nach Norm einen bestimmten Wert nicht unterschreiten darf.

Norm EIA/TIA-568 TSB-67 für Kabeltester

Um den hohen Anforderungen an Kabelinstallationen für High-Speed-Netze gerecht zu werden, wurde eine Arbeitsgruppe ins Leben gerufen, um die Ergänzung TSB-67 zur Norm EIA/TIA-568 festzulegen. Diese definiert die Anforderungen an Messgeräte zur Überprüfung und Zertifizierung von Kabelinstallationen, die auch für High-Speed-Netze bis 100 Mbit/s geeignet sein sollen. In dieser Arbeitsgruppe sind renommierte Hersteller von Kabeln und Kabeltestern vertreten.

Die Ergänzung TSB-67 bezieht sich nicht auf einzelne Kabelsegmente, sondern auf die gesamte Übertragungsstrecke zwischen zwei aktiven Netzwerkkomponenten, im Allgemeinen also zwischen Station und Hub. Dabei sind zwei Arten von Strecken definiert. Der Basic Link umfasst die fest installierte Strecke von Wanddose, Installationskabel und Patchfeld sowie zusätzlich auf jeder Seite bis zu zwei Meter lange Anschlusskabel des Testgeräts. Der Channel Link definiert die gesamte Übertragungsstrecke bis zu den Anschlüssen der Endgeräte. Dies bedeutet, dass zusätzlich zur fest installierten Strecke des Basic Link auch noch die User-Patchkabel in die Messung mit einbezogen werden.

Die TSB-67 bezieht sich nur auf TwistedPair-Verkabelungen und definiert, welche Parameter der Strecke für das Übertragungsverhalten relevant sind und daher bestimmten Sollwerten unterliegen müssen. Dies sind zum einen Linklänge und Laufzeit der Signale auf dem Link. Zum anderen sind hier Dämpfung und NEXT über dem gesamten definierten Frequenzbereich relevant. Analog zur Einteilung nach TSB-36 wird ein Link in Kategorie 3, 4 oder 5 eingestuft, abhängig davon, welche Sollwerte er einhält.

Für die Messgeräte ist festgelegt, welche Messungen durchgeführt werden müssen, damit der Link als der entsprechenden Kategorie genügend zertifiziert werden kann. Dabei ist ganz genau festgelegt, ab wann ein Link den Test für eine bestimmte Kategorie besteht (Test pass) und wann nicht (Test fail). Die wichtigste und zugleich härteste Anforderung an die Messgeräte besteht in der von ihnen geforderten Genauigkeit. Dabei gibt es zwei Klassen (Accuracy Level 1 und 2) der Messgenauigkeit des Kabeltesters in Bezug auf Dämpfung und NEXT, wobei die Genauigkeit nach Level 2 die höheren Anforderungen an das Messgerät stellt. Bei der Auswahl eines Kabeltesters für Installationen mit Komponenten der Kategorie 5 sollte auf jeden Fall darauf geachtet werden, dass das Gerät die Genauigkeit nach Level 2 sowohl für den Basic Link als auch für den Channel Link erreicht. Nachdem der Standardisierungsprozess der TSB-67 abgeschlossen ist, entsprechen Hand-Held-Kabeltester nun der endgültigen Norm. Da die bisherigen Versionen der Kabeltester bereits den entsprechenden vorläufigen TSB-67 Entwürfen entsprechen, können sie in den meisten Fällen durch ein einfaches Softwareupgrade auch nachträglich der endgültigen Norm angepasst werden.

Troubleshooting in Netzwerken

Neben Verkabelungsproblemen gibt es noch eine Reihe von weiteren Fehlerquellen in Netzwerken. Um diese erkennen und lokalisieren zu können, sind Netzwerkmonitore oder -analyzer besonders geeignet. Der generelle Unterschied zwischen Monitoren und Analyzern liegt in der Vielfalt der Decodierungs- und Eingriffsmöglichkeiten. Ein Netzwerkmonitor agiert typischerweise auf Schicht 3 des ISO/OSI Schichtenmodells, d. h. er liest Pakete vom Netz ein und ordnet diese den entsprechenden Protokollen zu.

Möchte man nun detailliertere Informationen wie zum Beispiel den genauen Inhalt eines Pakets oder gar Frame-Inhalte bis auf Bitebene einsehen, so reicht die Leistungsfähigkeit von Monitoren nicht mehr aus. Dies gilt auch, wenn man Protokolle höherer Schichten





wie SNMP oder Routingprotokolle bis hin zu Anwendungen auf Schicht 7 analysieren möchte.

Für diese Einsatzbereiche muss auf die komplexeren Netzwerkanalysatoren zurückgegriffen werden.

Für Monitoring und Analyse müssen Messungen bei laufendem Netzbetrieb gemacht werden. Generell lässt sich die Empfehlung aussprechen, von seinem Netzwerk „Aufnahmen“ im funktionierenden Zustand zu machen, um bei auftretenden Problemen Vergleichswerte zu haben und so die problembelasteten Parameter schnell ermitteln zu können. Die eigentliche Fehlerquelle kann so einfacher eingegrenzt werden. Ein weiterer praxisbezogener Tip ist, sich bei auftretenden Problemen als erstes die Stellen im Netzwerk genauer anzusehen, an denen sich irgendetwas geändert hat oder haben könnte: z. B. neu hinzugekommene Knoten, geänderte Softwareversionen, Verkabelungsänderungen, Umzüge von Usern oder ganzen Abteilungen.

Im Folgenden werden auftretende Netzwerkfehler und Problemindikatoren kurz diskutiert und mögliche Störquellen genannt.

Local Collisions

Lokale Kollisionen im Netzwerk sind das Ergebnis von zwei oder mehreren gleichzeitig sendenden Stationen. Übermäßig hohe Kollisionsraten im Netz lassen in den meisten Fällen auf Verkabelungsfehler im Netzwerk schließen.

Late Collisions

Late Collisions sind Kollisionen, die außerhalb des Kollisionsfensters von 512 Bit passieren (normale Kollisionen treten innerhalb der ersten 64 Byte auf).

Dies kann generell zwei Ursachen haben: Eine Station ist defekt (Karte, Transceiver etc.) und hält sich nicht an die CSMA/CD-Konvention, sendet also, ohne die Leitung abzuhören. Oder aber die Konfigurationsregeln bezüglich der Kabellänge sind nicht eingehalten worden. Dann wird die maximale Signallaufzeit von 57,6 Mikrosekunden (bei 10 Mbit/s Ethernet) überschritten und die Kollision wird zu spät erkannt.

Short Frame

Dies sind Frames, die kleiner als die minimal zugelassenen 64 Byte sind. Hauptgrund für Short Frames sind fehlerhafte Netzwerkkarten oder Treiber.

Jabber

Frames, die grösser sind als die maximal zugelassenen 1518 Byte, werden als Jabber bezeichnet. Hauptursache sind auch hier defekte Netzwerkkarten und Treiber.

Negative Frame Check Sequence (FCS)

Als FCS bezeichnet man einen Rahmen, dessen Prüfbytes am Ende nicht mit der errechneten Prüfsumme übereinstimmen. Dies deutet auf einen Übertragungsfehler hin. Mögliche Ursachen sind defekte Netzwerkkarten, die Verkabelung oder Einstrahlungen.

Ghosts

Ghost-Frames sind in ihrer Erscheinung ähnlich einem Datenframe, sie haben jedoch keinen richtigen Anfang (Starting Delimiter 10 10 10 11).

Hintergründe der Ghost-Erscheinungen: Potentialausgleichsströme und andere Verkabelungsprobleme können Repeater glauben lassen, dass ein Datenpaket empfangen wurde. Repeater sprechen auch auf Wechsellspannungssignale an, so auch auf störende AC-Anteile, die sich auf Leitungen befinden. Diese Störsignale werden dann aufbereitet und als Datensalat auf das Netzwerk geschickt.

Fehlermeldungen der Netzwerkprotokolle

In den Netzwerkprotokollen selbst sind bereits eine Reihe von Sicherheitsmechanismen implementiert (besonders hervorzuheben ist hier das extrem auf Sicherheit ausgelegte FDDI), die auf Fehlerzustände reagieren und diese protokolliert an die darüberliegende Schicht weiterreichen.

Im TCP/IP Protokoll Suite sind es die ICMP Pakete, die Probleme identifizieren, wie überlastete Knoten, unkorrektes Routing oder nicht erreichbare Knoten. Diese Meldungen können ausgewertet und in die Analyse miteinbezogen werden.



13.3 Remote Monitoring (RMON)

Einsatz von RMON

Schneller Informationsfluss wird zu einem immer wichtigeren Faktor in modernen Unternehmen. Dies bedeutet aber auch eine größere Abhängigkeit von der Dateninfrastruktur, Engpässe und Ausfälle führen so zu immer größeren Kosten.

Der Bedarf, Probleme noch vor dem Auftreten erkennen zu können, führte zu der Standardisierung von Netzwerkmanagement-Funktionen im SNMP-Protokoll. Heute verwendete Protokollanalysatoren werden typischerweise an ein einzelnes Segment angehängt, um ein bereits existierendes Problem zu isolieren. Dahingegen ist RMON ein proaktives Element, das zur Identifikation möglicher Probleme bereits vor ihrem erstmaligen Auftreten dient. Remote Network Monitoring ist als Teil von SNMP unter der Bezeichnung RMON standardisiert. Ein RMON-Netzwerkmonitor, auch Probe genannt, analysiert die Aktivitäten des Ethernet-Segmentes, in dem er installiert ist. Diese Daten meldet er einem zentralen Netzwerkmanagement-System (NMS) über SNMP, auf dem sie grafisch darstellbar sind. RMON Probes werden entweder als separate Hardware-Boxen angeboten oder sind bereits in Netzwerkgeräten wie z. B. Switches integriert. Die Monitore können die Daten über das Netzwerk oder über ein seriell angeschlossenes Modem an das zentrale System weiterleiten. Aufgrund der Standardisierung von RMON kann ein NMS Daten von Probes verschiedener Hersteller auswerten.

In normalen SNMP-Systemen mit Manager (zentrale Software) und Agenten (Knoten im Netz) werden die Daten der Agenten ständig über das Netz abgefragt. Dies hat oft eine Große Netzbelastung zur Folge. Eine richtig konfigurierte RMON-Lösung reduziert die Netzbelastung, da die Monitore statistische Daten zwischenspeichern und in Intervallen oder auf Abruf weiterleiten können. Dabei übernehmen die Monitore im Netz eine Doppelrolle.

Gegenüber dem Managementsystem tritt ein Monitor als SNMP-Agent auf, der Daten liefert, gegenüber den Knoten als SNMP-Manager, der Daten speichert. Auf diese Weise können Netzwerke, besonders über durchsatzkritische WAN-Verbindungen, ohne Große Einschränkungen gemanagt werden.

Eine wichtige Aufgabe von RMON-Produkten besteht in der vorbeugenden Diagnose. Durch die Möglichkeit, Schwellen zu setzen, bei deren Überschreitung frühzeitig Alarm gegeben wird, können drohende Performance-Engpässe im Netz erkannt und Gegenmaßnahmen wie Umstrukturierung oder Erweiterung rechtzeitig eingeleitet werden.

Für eine vernünftige Kosten-Nutzen-Relation ist es meist nicht sinnvoll, jedes Segment mit einem Probe zu bestücken, sondern nur solche mit einer hohen Zahl angebundener Endgeräte oder hohen Verfügbarkeitsanforderungen. In LAN-WAN-Verbundnetzen ist der Einsatz eines RMON Probe pro Standort sinnvoll, um die WAN-Verbindungen zu entlasten. Man braucht aber pro Collision Domain (per Bridge oder Router getrenntes Teilnetz) mindestens einen RMON Probe. Um die Kosten in Grenzen zu halten, sind Switches mit eingebauten RMON Probe eine ideale Lösung, da mehrere Segment mit einem Probe abgedeckt werden können.





13.4 Netzwerk-Security

Die Entwicklung der Computertechnologie von Großrechnern über verteilte Rechner zu Client-Server-Konfigurationen und unternehmensweiten Netzen hat den Bedarf an Sicherungsmaßnahmen drastisch erhöht. Das schnelle Wachstum der Internet-Zugänge setzt die Informationsquellen vieler Unternehmen dem Risiko des unbefugten Zugriffs aus. Und das zu jeder Tageszeit und von jedem Ort der Erde aus. Bedenkt man die Abhängigkeit vieler Unternehmen von diesen Informationssystemen, dann wird klar, dass Manipulationen an diesen Systemen oder der Diebstahl von darauf befindlichen Informationen schwerwiegende finanzielle Folgen haben können. Die Entwicklung offener Systeme macht die Einrichtung hoch entwickelter Sicherheitseinrichtungen, die vor unberechtigten Eingriffen schützen, zwingend notwendig. Das Problem des Missbrauchs von Computer- und Netzwerkeinrichtungen hat fast epidemische Ausmaße angenommen und ist bei weitem nicht mehr auf dafür besonders anfällige Branchen, wie den Kommunikations-, Banken- und den Luft- und Raumfahrtbereich, beschränkt. Dieses Risiko besteht für jedes Netz und jeden Rechner.

Die Situation wird durch die Tatsache verschärft, dass gestohlene oder manipulierte Informationen nicht einfach verschwinden, sondern weiter im Umlauf bleiben. Der Missbrauch von Daten ist nicht sofort offensichtlich. Unbefugte können sich Zugang zu Computern verschaffen und Daten kopieren, ohne eine Spur zu hinterlassen. Welche finanziellen Folgen hat das? Der durch Datenmissbrauch entstandene Schaden geht in die Milliarden -Tendenz steigend.

Der Grund dafür liegt in der Tatsache, dass in vernetzten Umgebungen, wie sie heute überall angetroffen werden, jede angeschlossene Workstation, jeder Laptop-Rechner, jeder Zugangspunkt zum Netz, jeder dezentrale Computer oder jedes verteilte System eine Zugangsmöglichkeit für Unbefugte darstellt. Wenn man sich dann noch das explosionsartige Wachstum des Internets und die im Entstehen begriffene Infoautobahn vor Augen hält, dann steigen die Risiken eines unbefugten Zugriffs auf Dateneinrichtungen exponentiell. Unberechtigtes Eindringen in ein EDV-System kann verheerende Folgen haben. In manchen Branchen kann ein derartiger Vorgang auch das unternehmerische Ende bedeuten. Das Ergreifen von geeigneten Maßnahmen, um Daten vor Diebstahl, Manipulation oder Löschung zu schützen, ist nicht nur eine Notwendigkeit, sondern gehört auch zu den treuhänderischen Pflichten eines Unternehmens.

Für einen erfahrenen Hacker oder einen entschlossenen Insider ist es kein großes Problem, in den Besitz eines Passwortes zu kommen und sich darüber Zugang zu wertvollen Informationen zu verschaffen. Hält sich ein Unbefugter erst einmal in einem mutmaßlich sicheren System unter der „Maske“ eines autorisierten Benutzers auf, verlieren alle Zugangsrechte und Einrichtungen zur Pfadverfolgung ihre Bedeutung. Sicherheitseinrichtungen, die nur einen einzigen Schutzmechanismus vorsehen, z. B. ein statisches Passwort, sind höchst unsicher.

Die Identifizierung autorisierter Benutzer und der Ausschluss aller anderen ist die Grundvoraussetzung für ein Sicherungssystem, das diesen Namen auch verdient.

13.4.1 Benutzeridentifikation

Es gibt drei Methoden zur Benutzeridentifizierung:

1. Ein dem Benutzer bekanntes Geheimnis (Passwort, PIN).
2. Ein Gegenstand im Besitz des Benutzers (Schlüssel, Karte, Ausweis).
3. Ein individuelles Merkmal des Benutzers (Fingerabdruck, Stimme, Muster der Retina), biometrische Daten.

Zur verlässlichen Autorisierung ist der Einsatz von mindestens zwei dieser Methoden notwendig. Diese Methoden, die heute im EDV-Bereich gebräuchlich sind, sind die Basis für eine ganze Reihe von Möglichkeiten zur Benutzeridentifizierung und Autorisierung. Nachfolgend sind die verschiedenen Verfahren sowie ihre jeweiligen Vor- und Nachteile dargestellt.

Verfahren

Die gebräuchlichsten Verfahren zur Benutzeridentifikation sind heute:

Unabhängige Passwörter

- Rückrufsysteme (Dial-Back),
- Autorisierung durch Frage-Antwort-Systeme,
- Software-Token,
- zeitabhängige Token.

Wiederverwendbare Passwörter

Verwendet man das heute am weitesten verbreitete Schutzverfahren, den Einsatz von Passwörtern, so nimmt man folgende Nachteile in Kauf:

- **Passwörter können manipuliert werden;**
- **sie werden in der Praxis nicht in regelmäßigen Abständen geändert; - sie**



können im Besitz von mehr als einem Benutzer sein;

- sie sind abhängig von verschiedenen sozialen Komponenten; - sie können von speziellen Programmen entschlüsselt werden.

Rückrufsysteme

Rückrufsysteme in Verbindung mit Passwörtern bieten einen höheren Schutz und haben den Vorteil, dass der Zugriff über die Auflistung der Telefonate festgestellt werden kann. Der zusätzliche Vorteil der Kostenübernahme durch den Anrufer (meistens die Unternehmenszentrale) ist zwar zweckmäßig, jedoch für die Sicherheitsbetrachtungen nicht relevant. Jedoch beinhalten auch Rückrufsysteme noch genügend Nachteile:

- Das Gerät und nicht der Benutzer wird autorisiert;
- Bei mobilen Benutzern ist der Rückruf nur selten zu realisieren;
- Autorisierte Benutzer, die nicht ein bestimmtes Gerät benutzen, könnten ausgeschlossen werden;
- Das System kann durch Anrufweitschaltung manipuliert werden; - Es ist für den Benutzer umständlich und zeitaufwendig.
- Es kann nur für den Zugriff über Wählleitungen eingesetzt werden (daher z. B. kein Schutz für X.25-Zugänge oder Zugang über Internet);
- Es wirkt nicht als Schutz auf der Anwendungsebene oder Protokollebene.

Insgesamt sind Rückrufsysteme nur schwer zu kontrollieren und bieten noch keinen umfassenden Schutz.

Frage-Antwort-Systeme

Frage-Antwort-Systeme bestehen aus zwei Teil-Systemen, wobei das eine System beim Benutzer und das zweite auf dem Host installiert ist. Bei der Durchführung einer Zugangskontrolle schickt das Host-System dem anderen Informationen, die von der Benutzerseite über einen eingebauten Algorithmus verändert und eventuell um Daten ergänzt werden. Diese werden als Resultat an das Host-System zurückgegeben. Ist das Resultat in Ordnung, wird der Zugriff gewährt. Dieser Vorgang kann mehrere Male durchlaufen werden, um eine höhere Sicherheit zu erreichen. Die bei einigen Softwareprodukten üblichen Hardware-Dongle-Systeme gehören auch zu den Frage-Antwort-Systemen.

Diese Systeme bieten eine recht hohe Zugriffssicherheit. Sie besitzen je nach Art des

Systems aber auch Nachteile:

- Der Benutzer muss eventuell mehrere Schritte durchlaufen; - Je nach Art des Systems unhandlich;
- PIN ist in Zeichenfolgen (Token) gespeichert, die ausgetauscht werden, eine zweite PIN wird für den Host benötigt;
- Die Authentisierungssysteme können verliehen oder gestohlen werden; - Der Export ist problematisch.

Software-Token

Wird der Zugangsschutz im Betriebssystem- oder in einer Anwendungssoftware implementiert, wird kein externes Gerät zur Autorisierung benötigt. Dies ist der wesentliche Vorteil der Software-Token.

Die Nachteile dieser Lösung sind:

- Abhängigkeit vom Datenendgerät bzw. dem Betriebssystem; - Der Software-Token kann kopiert oder verändert werden;
- PIN, Schlüssel und Algorithmus sind im Programm gespeichert; - Das Management ist problematisch.

Kontrolle und Pfadverfolgung sind nur sehr mühsam durchzuführen und können zur falschen Person führen. Daher lassen sich der Umlauf und Gebrauch nicht verlässlich kontrollieren.

Zeitabhängige Token

Eine wesentlich höhere Sicherheit bieten zeitabhängige Zeichen- oder Zahlenfolgen, die über aufwendige Algorithmen immer wieder neu berechnet werden. Die Hardware, die dazu benötigt wird, lässt sich auf einer Fläche nicht grösser als eine Kreditkarte unterbringen. Die Vorteile dieses Systems:

- Unabhängig vom Datenendgerät, Kartenlesegerät wird nicht benötigt; - Einloggen erfolgt in einem Schritt, kein Frage-Antwort-Prozess;
- Sicher, beruht auf zwei unabhängigen Faktoren (Benutzereigener PIN und Token);





- Es kann immer nur eine Person zur gleichen Zeit die Tokenkarte besitzen, bei Diebstahl kann die Karte sofort deaktiviert werden. Daher ist der Zugriff selbst dann noch kontrollierbar, wenn PIN und Karte in falsche Hände geraten.

13.4.2 Internet Security

Während die Benutzeridentifikation ein wesentlicher Bestandteil einer Security-Lösung ist, wird darüber hinaus oft vergessen, dass man Schutzmaßnahmen nicht vernachlässigen darf, die innerhalb von Netzwerken den Zugriff zwischen den einzelnen Knoten kontrollieren und regeln. Bestes Beispiel ist hierbei das Internet, das Millionen von Netzwerkknoten miteinander verbindet und prinzipiell den Zugriff auf jeden Knoten gestattet und damit ein potentiell Sicherheitsrisiko für alle Beteiligten darstellt.

In diesem Zusammenhang werden daher immer wieder so genannte Firewall-Systeme erwähnt, die unerwünschte Besucher von dem Zugriff fernhalten und die Herausgabe von sensiblen Daten über das Internet verhindern sollen.

Firewall

Firewalls sind kein Allheilmittel, sie schützen nur gegen ganz bestimmte Einbruchs- und Sabotageversuche. Als Virenschutz sind sie kaum geeignet, genauso wenig verhindern sie Missbrauch durch noch tätige oder ehemalige Mitarbeiter. Die berühmten Hintertürchen, die sich mancher Software-Entwickler oder Systemadministrator einbaut, gehören oft zu den wesentlichen Sicherheitsrisiken. Die Verbindung zum Internet stellt fraglos ein gewisses Risiko dar, aber soll ein Unternehmen deshalb auf die Vorteile der weltweiten Konnektivität verzichten? Immer mehr Firmen sind auf das Internet angewiesen, weil sie von dort Informationen beziehen oder auf dem Internet zur Verfügung stellen. Firewalls sind eine Lösung, um die Vorteile des Internets zu nutzen, ohne die Sicherheitsanforderungen des Unternehmens zu vernachlässigen. Allerdings ist der Schutz nie hundertprozentig und nicht für immer. Man sollte ihn eher mit einer höheren Hürde vergleichen, die ein Eindringling nehmen muss. Als die ersten Viren auftauchten, gab es zunächst keinen Schutz dagegen. Dies führte jedoch nicht dazu, dass die Unternehmen ihre Computer abschalteten und wieder mit Karteikarten arbeiteten, sondern es entwickelte sich ein gesteigertes Bewusstsein gegenüber den Gefahren, die beispielsweise durch Software entsteht, die Mitarbeiter von zu Hause mitbringen. Seit Virenschutzprogramme entwickelt werden, besteht auch die Möglichkeit, Viren aufzuspüren und zu entfernen. Dennoch besteht gegenwärtig kein Grund, Entwarnung zu geben. Vielmehr sieht es so aus, als ob Virenprogrammierer verbesserte Schutzmechanismen als Herausforderung ansehen.

Ähnlich verhält es sich mit Firewalls. Wer ein Unternehmensnetz an das Internet anschließt, ohne zusätzliche Sicherheitsmaßnahmen zu installieren, verhält sich wie ein Computeranwender, der Viren durch Ignoranz zu bekämpfen versucht. Wer jedoch einen Firewall als absolute Sicherheit ansieht, dürfte über kurz oder lang ebenfalls seine

Überraschung erleben. Den Entwicklern des Internet kann jedoch nicht der Vorwurf gemacht werden, sie hätten zu wenig auf Sicherheitsbelange geachtet: 1970 konnte niemand damit rechnen, dass irgendwann mehr als 250 Millionen Menschen über das Internet zu erreichen sein werden. Vereinfacht ausgedrückt besteht das grundlegend-e Problem des Internet darin, dass zunächst jeder fast alles darf. Das heißt vor allem: Jeder beteiligte Rechner kann zu jedem anderen eine Verbindung aufbauen und auf diesem eine Reihe von Diensten (wie Finger, Telnet, FTP oder World Wide Web, WWW) nutzen. Bei der Entwicklung einer Sicherheitsstrategie muss man sich auf eines von zwei Paradigmen festlegen. Das eine besagt, dass alles verboten ist, was nicht ausdrücklich erlaubt ist. Das andere besagt, dass alles erlaubt ist, was nicht ausdrücklich verboten ist.

Im ersten Fall blockiert das Firewall-System zunächst jeglichen Verkehr zwischen dem Internet und dem Unternehmensnetz. Kein Dienst ist zu nutzen, bevor ihn der Systemadministrator nicht explizit freigegeben hat. Das führt im Unternehmen allerdings unter Umständen zu langwierigen und umständlichen Genehmigungsprozeduren. Andererseits schützt diese Vorgehensweise vor potenziellen Risiken, die durch die Nutzung von Diensten entstehen könnten, über die der Administrator zuvor nicht informiert wurde.

Im zweiten Fall blockiert ein Firewall nur die Dienste, die nach Meinung der Verantwortlichen ein besonderes Risiko darstellen, beziehungsweise verhindert den Zugang zu solchen Rechnern, die besonders geschützt werden sollen. Dabei besteht die Gefahr, dass neue, gefahrenträchtige Dienste schon wegen der generellen Freigabe gestattet sind. Zudem können Mitarbeiter Sicherheitslücken unbewusst herbeiführen, ohne dass sie der Administrator erkennt.

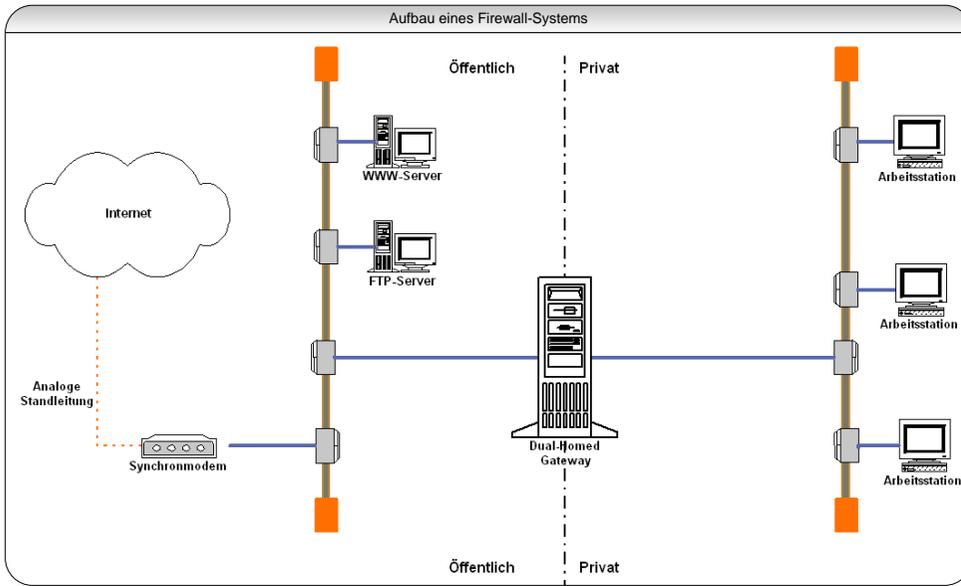
Aufgaben eines Firewalls

Zu den Hauptaufgaben des Firewalls gehört es, einerseits unerwünschten Besuchern aus dem Internet den Zugang zu verwehren und andererseits zu verhindern, dass firmeninterne Daten nach außen gelangen. Beide Aufgaben sind jedoch nicht identisch. Ein Eindringling kann zwar auch an vertrauliche Dokumente gelangen, die größere Gefahr besteht bei ihm jedoch darin, dass er den betroffenen Rechner oder gar das ganze Netz sabotiert.

Über diese beiden Aufgaben hinaus bieten Firewalls die Möglichkeit, den Verkehr zwischen den Netzen zu überwachen beziehungsweise zu protokollieren. So ist es leichter, Einbruchsversuche zu erkennen und vielleicht sogar den Täter zu ermitteln. Zumindest sollte es mit diesem Hilfsmittel möglich sein, genauere Angaben über Herkunft und Vorgehensweise zu erhalten, als dies ohne Schutzmaßnahme möglich wäre.

Firewall-Rechner repräsentieren, da sie als Schnittstelle zwischen Intranet und Internet fungieren, den IT-Sicherheitsstandard des Unternehmens, vor allem, wenn auf ihnen

FTP oder WWW-Server laufen.



Realisierung von Firewalls

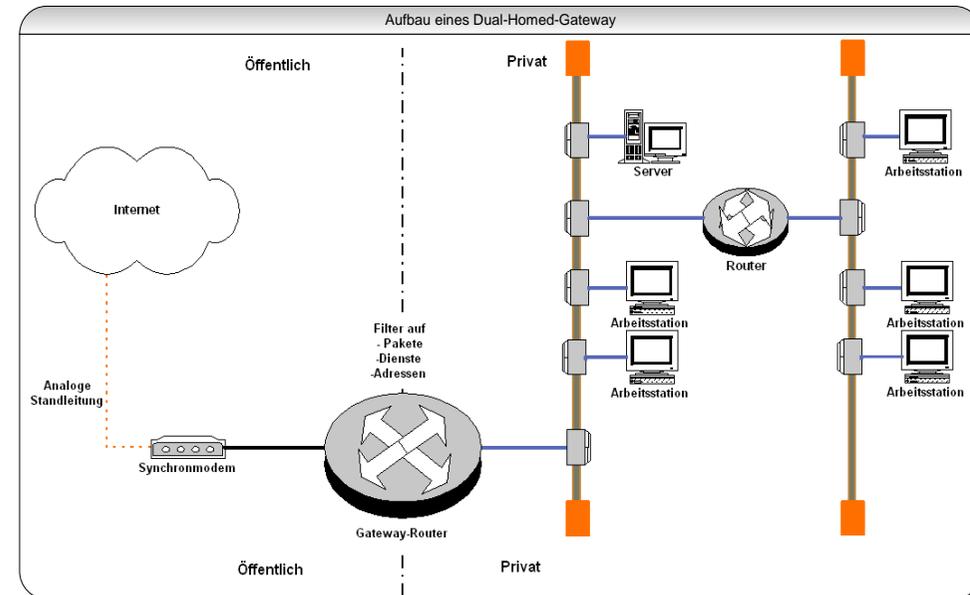
Firewalls lassen sich auf unterschiedliche Weise realisieren. Dabei kann es sich um einen Router handeln, der Pakete nur nach bestimmten Regeln transportiert, oder ein ganzes Subnetz, in dem jeder angeschlossene Computer eine bestimmte Aufgabe wahrnimmt. Bei der Einrichtung zählt sowohl der finanzielle Aufwand durch die Anschaffung zusätzlicher Hardware als auch die Belastung durch zu hohen Wartungsaufwand.

In der Mehrzahl der derzeit existierenden Firewalls sind Paketfilter im Einsatz, da sie relativ einfach zu installieren sind. Oft sind sie sogar die einzige Komponente. Paketfilter können über kommerzielle Router (zum Beispiel Cisco) oder aber auch über eigenständige Rechner realisiert werden. Sie analysieren die Datenpakete und reichen sie nach bestimmten Regeln weiter. Üblicherweise ist jedem Internet Packet (IP) zu entnehmen, an welche Adresse es gelangen soll und welchen Dienst (IP-Port) es nutzt. Der Systemadministrator kann demnach bestimmte Rechner, Subnetze und Dienste sperren. Der Paketfilter hält sich im Allgemeinen an das Paradigma: Alles, was nicht ausdrücklich verboten ist, ist erlaubt. Paketfilter besitzen aber Nachteile: Die Regeln, nach denen sie die Pakete weiterleiten, können in komplexen Installationen schnell sehr kompliziert werden. Zudem sind die meisten Filter nicht in der Lage, genaue Logging-

Informationen aufzuzeichnen. Erfolgt trotz des Paketfilters ein Einbruch in die geschützten Bereiche des privaten Netzes, so ist anschließend kaum etwas über die Arbeitsweise und die Herkunft des Eindringlings zu ermitteln.

Dual-Homed Gateway

Bei einem Dual-Homed Gateway handelt es sich um einen Rechner, der auf der einen Seite über eine Verbindung zum Internet verfügt und auf der anderen Seite mit dem firmeninternen Netz verbunden ist. Er routet kein TCP/IP, so dass niemand aus dem Internet auf Netzwerkebene auf das Firmennetz zugreifen kann. Die Verbindung der beiden Netze erfolgt im Allgemeinen über eigene Applikationen, die Dienste vermitteln. Das Dual-Homed Gateway unterbindet damit alles, was nicht ausdrücklich erlaubt wurde.



Die einfachste Möglichkeit, Mitarbeiter des Unternehmens in einer solchen Umgebung Dienste des Internet nutzen zu lassen, besteht darin, ihnen einen Account auf dem Gateway einzurichten. Dort können sie Applikationen starten, die den TCP/IP-Verkehr im Internet abwickeln. Wenn sie beispielsweise Dateien per FTP transferieren wollen, starten sie über das firmeninterne Netz den FTP-Client auf dem Gateway und kopieren die eintreffenden Daten auf ihren eigenen Rechner. Wenn sie das World Wide Web nutzen wollen, können sie einen X-Window-basierenden WWW-Client auf dem Gateway starten und die Ein- und Ausgaben an ihren Host umleiten. Zu beachten ist, dass ein Firewall nach erfolgreicher Installation selbst das potentielle Ziel von Angriffen von außen





ist. Daher stellt ein allgemeiner Benutzerzugang auf dem Firewall immer ein besonderes Risiko dar. Gelingt es einem Eindringling, sich auf dem Firewall einzuloggen, so ist es für ihn relativ einfach, sich zu weiteren Rechnern vorzuarbeiten. Schon ein zu simples Passwort eines legalen Benutzers des Gateways kann ausreichen, um das gesamte Firewall zu knacken.

Läuft der gesamte Datenaustausch mit dem Internet über das Gateway, so fällt es dem Systemadministrator leichter, die Aktivitäten eines Eindringlings zu verfolgen, als wenn nur ein Paketfilter installiert ist. Wenn jedoch überhaupt kein allgemeiner Benutzerzugang zur Verfügung steht, so ist schon das Einloggen eines Users auf dem Gateway ein sicheres Zeichen für einen Einbruch. Dieser wird schnell erkannt und kann einfach unterbunden werden. Lässt der Gateway keinen TCP/IP-Austausch zwischen dem Internet und dem firmeninternen Netz zu, und erlaubt es auch keinen Benutzerzugang, so können sogenannte Proxy-Applikationen einzelne Dienste vermitteln. Dabei handelt es sich um dienstspezifische Programme, die Anfragen aus dem Firmennetz entgegennehmen und in das Internet weiterleiten.

Für jeden Dienst muss auf dem Gateway ein eigener Proxy installiert werden, der mit erweiterten Zugangsüberprüfungen und Logging-Fähigkeiten ausgestattet sein kann.

Es sind mehrere hard- oder softwarebasierende Firewall-Systeme am Markt, die vom Systemadministrator auf die individuellen Anforderungen hin konfiguriert werden können.

Einsatz von Zwischennetzen

Anstatt das Internet direkt an das Dual-Homed Gateway zu führen, kann zwischen dem Internet und dem privaten Netz ein Zwischennetz geschaltet sein. Auf dieses halböffentliche Netz können sowohl Mitarbeiter als auch Internet-Teilnehmer zugreifen. Ein Passieren des Netzes ist jedoch aus keiner der beiden Richtungen möglich. Im abgeschirmten Zwischennetz können Rechner untergebracht sein, die vom Internet aus erreichbar sein sollen, wie zum Beispiel FTP- und WWW-Server. Richtet man die Dienste jeweils auf einem separaten Host ein, bleibt die Installation insgesamt besser überschaubar.



13.5 Netzwerkstrategien

Ursprünglich wurden Ethernet-Netze mit 10BASE5-Kabel aufgebaut, danach kam 10BASE2, das in Europa bis heute sehr verbreitet ist. Lichtleiter werden vor allem dann eingesetzt, wenn größere Entfernungen zwischen einzelnen Segmenten überbrückt werden müssen. In den USA hat sich inzwischen 10BASE-T -Verkabelung durchgesetzt. Bei der Neuverkabelung ist besonders der Einsatz eines TwistedPair-Kabels der Kategorie 5 zu empfehlen. Die Verwendung eines solchen Kabels hat den Vorteil, dass im Rahmen von neuen, schnelleren Technologien wie z. B. Fast Ethernet das gleiche Kabel verwendet werden kann.

Einzelne ThickWire- und ThinWire-Segmente werden am besten mit Repeatern verbunden. Repeater sollten nicht nur eingesetzt werden, wenn die maximal erlaubte Kabellänge oder die maximale Anzahl von Knoten erreicht ist, sondern auch zur Segmentierung des Netzes. Die Segmentierung verhindert die Ausbreitung von Fehlern auf andere Segmente, und die Lokalisierung des Fehlers wird erleichtert.

Da es sich bei TwistedPair um Punkt-zu-Punkt-Verbindungen handelt, und daher jede Station direkt an einen Multiport Repeater/Switch angeschlossen wird, ist hier die Fehlerlokalisierung besonders einfach. Die Fehlerausbreitung ist in der Regel auf eine Station begrenzt, sofern nicht ein kompletter Hub ausfällt. Die meisten Repeater verfügen über eine AUI-Buchse, über die sich ein Anschluss an andere Netzwerkmedien einfach realisieren lässt.

Bei größeren Netzen mit vielen Segmenten sind sogenannte Multi-Media-Konzentratoren zu empfehlen. Diese modular aufgebauten Konzentratoren können, je nach Modell, Ethernet-Komponenten wie Repeater, Terminalserver, Bridges, Router und Management-Module aufnehmen. Es gibt auch Konzentratoren, die außer der Ethernet-Topologie auch TokenRing und FDDI unterstützen. Durch den Einsatz von solchen Konzentratoren vereinfacht sich das Netzwerkmanagement erheblich, da sie über Netzwerkmanagementsoftware verwaltet werden können.

Steigen die Antwortzeiten in einem Ethernet-Netzwerk aufgrund der hohen Auslastung auf ein nicht akzeptables Maß, kann man Rechnergruppen, die regelmäßig miteinander kommunizieren, durch Bridges trennen. Mit Multiport Bridges oder auch speziellen Switches kann die Performance weiter verbessert werden.

Will man mehrere Switches oder Multiport Bridges miteinander verbinden, reicht die Geschwindigkeit von Ethernet nicht aus, wenn man ein größeres Netz hat. Als schnelles Backbone kommen Fast Ethernet, Gigabit Ethernet oder auch FDDI in Frage. FDDI ist standardisiert und verfügbar, aber teuer. Durch die hohe Verbreitung ist Fast Ethernet die kostengünstigste Technologie. Für Gigabit Ethernet sind LWL-basierte (Server)Netzwerkadapter, Switches und Buffered Repeater erhältlich. Die Übertragung von Gigabit Ethernet über TwistedPair-Kabel der Kategorie 5 ist derzeit noch in der

Entwicklung. Des Weiteren gibt es herstellerspezifische Lösungen für ein schnelles Backbone.

Mehrere Subnetze, die räumlich weit auseinander liegen, werden in der Regel mit Remote Bridge/Routern verbunden, die über entsprechende WAN-Module verfügen.

Ethernet ist ein busorientiertes Verbindungsmedium. So kann jedes System jedes Paket, das auf seinem Netzwerkstrang übertragen wird, erkennen.

Da die Information in diesen Paketen in der Regel völlig unverschlüsselt übertragen wird, stellt es selbst für einen unerfahrenen Programmierer kein allzu großes Problem dar, auf einem PC oder einer Workstation mit einem kleinen Programm gezielt Informationen zu lesen, die nicht für seinen Rechner bestimmt sind. So lassen sich beispielsweise die Username/Passwort-Kombinationen lesen, die zwischen einem Terminalserver und einem anderen System übertragen werden.

Abhilfe schaffen hier zwei Möglichkeiten: Man trennt kritische Bereiche durch Bridges vom Restnetz ab und stellt sicher, dass auf allen Rechnern der kritischen Bereiche kein spionierendes Programm laufen kann. Zweite Möglichkeit ist die Verschlüsselung von Daten durch entsprechende Software in den Rechnern oder durch zwischengeschaltete Verschlüsselungsboxen. Je größer ein Netz wird, desto wahrscheinlicher treten Fehlersituationen auf. Hilfreich sind hier Geräte mit Statusanzeigen, Netzwerktester, Kabeltester und generell eine übersichtliche Installation, die es ermöglicht, Fehler (z. B. durch Abtrennen von einzelnen Segmenten) schnell zu lokalisieren.





14. Eingabegeräte

14.1 Tastaturen

Für den normalen Einsatz im Büro wird von einer Tastatur lange Lebensdauer, hohe Funktionssicherheit und eine ergonomische sowie sichere Bedienung gefordert.

In jeder Tastatur befindet sich ein Mikrocontroller, der feststellt, welche Taste gedrückt wird und den Tastatur-Code dieser Taste seriell zum Rechner überträgt. Im Tastaturtreiber des Betriebssystems erfolgt dann die Umsetzung des Tastaturcodes in das eigentliche ASCII-Zeichen.

Entscheidend für die dauerhafte Funktionsfähigkeit einer Tastatur ist die mechanische Standfestigkeit der Tasten. In der Regel besitzen die Tastaturen goldene Metallzungenkontakte, was eine hohe Lebensdauer bei ständigem Gebrauch gewährleistet. Einfachere Tastaturen haben dagegen nur eine dünne Kontaktfolie, die empfindlich ist und nur eine kurze Lebensdauer hat.

Ergonomische Keyboards - z. B. das Microsoft Natural Keyboard - stellen eine gesunde Position der Hände und Handgelenke sicher und vermindern dadurch die Gefahr von Verletzungen (u.a. Carpal-tunnelsyndrom CTS oder Sehnenscheidenentzündung). Beschwerdefreies und effektives Arbeiten sind die angenehmen Folgen. Es ist generell wichtig sicherzustellen, dass sich Sitzfläche, Arbeitsfläche und Tastatur in richtiger Anordnung zueinander befinden.

Tastaturen mit eingebauten Zusatzfunktionen haben alle den Vorteil, dass nur eine Schnittstelle am Computer belegt wird, obwohl mehrere Funktionen über das Keyboard zur Verfügung stehen. Es gibt Chipkartenlese-, Barcodelese-, Magnetkartenlese-Tastaturen und Multifunktionale Kartenlese-Tastaturen, die gleich mehrere Funktionen in einer Tastatur vereinen. Eine weitere Variante sind frei programmierbare Tastaturen zum Lesen von Kreditkarten, EC-Karten und Barcodes. Für die Zugangskontrolle können Chipkartenlese Tastaturen mit integriertem Fingerprint-Sensor eingesetzt werden.

14.2 Mäuse und Trackballs

Im Wesentlichen besteht eine Maus aus einer Rollkugel und einer Sensor-Mechanik/Elektronik, die die Drehbewegungen der Kugel erfasst, in einen Datenstrom umwandelt und zum Rechner überträgt. Neueste Modelle arbeiten ohne Kugel, bei ihnen wird die Bewegung der Maus über eine optische Einheit erfasst. Vorteile: keine mechanischen Teile, keine Verschmutzung der Kugel, und die Maus kann unabhängig von der Oberfläche eingesetzt werden. Zusätzlich hat eine Maus auf der Oberseite noch ein bis vier Tasten, die entweder von der eingesetzten Applikation als Funktionstasten genutzt oder vom Benutzer selbst mit Funktionen belegt werden können. Die klassische Maus

erfordert von ihrem Benutzer einiges an Geschicklichkeit, Fingerbeweglichkeit und vor allem einen Schreibtisch mit genügend freier Fläche.

Die neuen Mäusegenerationen - z. B. von Genius, Logitech oder Microsoft - verfügen zusätzlich zu den Funktionstasten über ein kleines Rädchen bzw. eine Tastenwippe. Damit kann der Anwender in diversen Anwendungen zoomen und scrollen, ohne die Maus zu bewegen. Der Bildlauf durch die Informationsfenster wird komfortabler und die Navigation durch das Internet - z. B. mit dem Microsoft Explorer oder auch dem Netscape Navigator - schneller als bisher.

Mäuse ohne lästige Kabelverbindung bieten uneingeschränkte Bewegungsfreiheit auf der Arbeitsfläche. Die Funktechnologie hat inzwischen die Infrarottechnik bei den kabellosen Mäusen abgelöst. Vorteil der Funklösung ist, dass keine direkte Sichtverbindung zum Empfänger vorhanden sein muss, die Funkmaus funktioniert im Umkreis von ca. 2 m. Neu ist die IntelliMouse Explorer: Sie überzeugt durch ihr modernes Design mit silberfarbenem Gehäuse sowie rot schimmernder Unter- und Rückseite. Die neuartige IntelliEye-Technologie sorgt für eine noch nie dagewesene Präzision, da statt der beweglichen Teile (zum Abtasten der Bewegungsänderungen an der Unterseite der Maus) ein optischer Sensor die Bewegungen der Maus erfasst. Das Herzstück der Microsoft IntelliEye-Technologie ist ein kleiner Chip, der einen optischen Sensor und einen digitalen Signalprozessor (DSP) enthält. Der Sensor fertigt rund 1.500 Bilder pro Sekunde von der Arbeitsoberfläche an.

Da auf bewegliche Teile, die Staub, Schmutz und Fett aufnehmen können, verzichtet wurde, muss die IntelliMouse Explorer nicht mehr gereinigt werden. Darüber hinaus arbeitet die IntelliMouse Explorer auf nahezu jeder Arbeitsoberfläche, so dass kein Mauspad mehr erforderlich ist. Die IntelliMouse Explorer ermöglicht mit ihrem Rad und den zwei neuen zusätzlichen Maustasten an der Seite effizientes und komfortables Arbeiten am PC.

Sollte kein Platz auf dem Tisch vorhanden sein, schafft hier ein Trackball Abhilfe, bei dem die Eingabe durch Drehen der obenliegenden Kugel und Bedienen der Tasten erfolgt. Im Grunde ist ein Trackball eine umgedrehte Maus, der auch die gleichen Funktionen erfüllt, aber weniger Platz benötigt.

Für 3D-Anwendungen eignen sich die Standard-Eingabegeräte wie Maus oder Trackball nicht unbedingt, da mit ihnen nur die gleichzeitige Kontrolle von zwei Freiheitsgraden möglich ist. Bei vielen 3D-Anwendungen, wie z. B. Virtual-Reality und 3D-Modellierung, ist aber die Kontrolle von sechs Freiheitsgraden notwendig. Für diese Anwendungen gibt es spezielle 3D-Mäuse, die diesen Anforderungen gerecht werden. Sie vereinen die Funktion einer gewöhnlichen Maus mit der Funktion eines Gerätes zur Bewegungssteuerung von 3D-Grafik-Objekten.



14.3 Scanner

Scanner sind zu einem wichtigen Hilfsmittel zur Übernahme von Daten geworden. Dies können gedruckte Texte, handschriftliche Vorlagen, Fotos oder Zeichnungen sein. Ein Scanner arbeitet nach folgendem Funktionsprinzip: Ein lichtempfindliches CCD-Element (Charge Coupled Device) fährt, angetrieben von einem Schrittmotor, die von einer Lampe beleuchtete Vorlage ab. Das CCD-Element erkennt für die jeweiligen Farben die Helligkeitsunterschiede und wandelt diese in Spannungswerte um. Die analogen Spannungen werden dann von einem Analog/Digital-Konverter in digitale Informationen umgesetzt und an den Rechner übermittelt.

Je nach angewandter Scan-Methode wird der CCD-Lesekopf entweder einmal (one-pass) oder aber für jede der Grundfarben Rot, Grün und Blau (RGB) separat (three-pass) an der Vorlage entlangbewegt. Das one-pass Scannen kann dabei auf zweierlei Weise realisiert werden. Zum einen, indem ein weißer Lichtstrahl auf eine CCD gelenkt wird, die direkt eine RGB-Farbunterscheidung durch Filter vornimmt. Zum anderen kann der Lichtstrahl durch ein Prisma geführt werden, wo er in drei Farben (RGB) gebrochen und auf drei CCDs gelenkt wird. Erstgenannte Methode hat sich beim Scannen durchgesetzt.

Bei der Auswahl eines Scanners sind eine Reihe von Kriterien zu beachten. Die Auflösung eines Scanners wird in dpi (lots per inch) gemessen. Als Faustregel gilt dabei: Je höher die Auflösung, desto besser die Wiedergabe der Vorlage beim erneuten Ausdruck. Die dpi Angabe bezeichnet die Anzahl der Pixel pro Zoll (1 „ = 2,54 cm), die von den Sensoren erfasst werden. Wird ein Bild z. B. mit 100 dpi erfasst, bedeutet dies, dass jedes Zoll in 100 Pixel zerlegt wird. Auf die Fläche gesehen liefert der Scanner also $100 \times 100 = 10.000$ Pixel pro Quadrat Zoll, bei 200 dpi sind es bereits 40.000 Pixel. Dabei wird deutlich, dass eine höhere Auflösung mehr Details einer Vorlage wiedergeben kann.

Zu bedenken ist jedoch, dass eine Verdopplung der Auflösung zu einer Vervierfachung der Datenmenge führt. Bei der eben beschriebenen Auflösung handelt es sich um die physikalische Auflösung eines Scanners. Sie bestimmt die tatsächliche Abtastung der Bildpunkte. Daneben wird immer auch eine mathematisch berechnete, so genannte interpolierte Auflösung eines Scanners angegeben. Mittels Software besteht die Möglichkeit, zwischen zwei erkannten Punkten weitere Zwischenwerte durch Interpolation zu berechnen. Dadurch stehen dem Rechner zusätzliche Informationen über Bildpunkte zur Verfügung, die zu einer Verbesserung des Ausdrucks führen.

Ein weiteres Beurteilungskriterium für einen Scanner ist die Farb- bzw. Bittiefe. Sie legt die Anzahl der beim Scandurchgang erfassten Graustufen bzw. Farben fest. So kann ein 1-bit-Scanner nur schwarz und weiß unterscheiden. Ein Scanner mit 8-bit-Farbtiefe kann dagegen bereits 256 Graustufen bzw. Farben (2 hoch 8) erkennen. Bei 24-bit-Scannern erhöht sich diese Zahl auf 16,7 Millionen Farbmöglichkeiten. Die derzeitige Grenze liegt bei einer Farbtiefe von 36-bit.

Eine Frage, die bei Neuanschaffungen beachtet werden sollte, ist, ob der Scanner Twainkompatibel ist. Hinter Twain (Toolkit without an important name) verbirgt sich eine Vereinbarung führender Peripheriehersteller, einen Software-Schnittstellenstandard zu schaffen, der es ermöglichen soll, aus einer Applikation heraus Scanner verschiedener Hersteller zu nutzen. Wenn also ein Scanner einen Twain-Treiber besitzt, kann jedes Programm, das ebenfalls Twain unterstützt, auf diesen Scanner zugreifen. Twain beinhaltet eine API-Schnittstelle (Applikation Programming Interface = Schnittstelle für die Programmierung von Anwendungsprogrammen) und ein spezielles Protokoll, das die Verbindung mit dem Twain-Treiber des Scanners herstellt und den Scanablauf steuert.

Mit Twain wird deutlich, dass zum Scannen auch eine leistungsfähige Software benötigt wird. Denn der Scanner liefert dem Rechner lediglich in digitalen Daten, was er sieht.

Was der Rechner dann daraus macht und wie die Daten weiterverarbeitet werden, ist eine Frage der Software. Ein spezielles Problem stellt dabei die Zeichen- bzw. Texterkennung dar. Eingescannte Texte müssen zuerst mit einem speziellen Texterkennungs- bzw. OCR-Programm (Optical Character Recognition) bearbeitet werden, um als Textdatei weiterverarbeitet werden zu können.

In der Regel ist im Lieferumfang der Scanner ein Standardsoftwarepaket enthalten. Dabei ist jedoch zu beachten, dass sich diese Scan-Software-Pakete zum Teil erheblich in ihrem Leistungsumfang voneinander unterscheiden. Oftmals wird auch nur eine LE-Version (Limited Edition) der Software mitgeliefert.

14.4 Strichcodeleser

Wichtig bei Scannern ist zudem, ob eine Durchlichtoption zum Einscannen transparenter Medien (z. B. Dias, Filme) vorhanden ist. In der Regel wird dazu ein Durchlichtaufsatz mit Fluoreszenzlampen auf dem Scanner angebracht.

Strich- oder Barcodes sind heute in der gesamten Warenwirtschaft zu finden. Mit ihrer Hilfe können geringe Datenmengen sehr einfach, schnell und vor allem sicher für die Weiterverarbeitung in einen Computer eingelesen werden.

Es gibt eine Vielzahl von Codes für unterschiedliche Einsatzgebiete. Dargestellt werden die Codes mit einer Sequenz schmaler und breiter Striche bzw. Lücken. Beim optischen Abtasten werden die unterschiedlichen Reflexionen der dunklen Striche und der hellen Lücken im Empfänger in entsprechende elektronische Impulse umgewandelt. Diese Impulse werden von einem Mikroprozessor in rechnerverständliche Zeichen gewandelt und dann übertragen.





Weit verbreitet sind Strichcodeleser, die über das Tastaturkabel zwischen Tastatur und Rechner bzw. Bildschirmterminal angeschlossen werden. Diese Strichcodeleser benötigen weder eine zusätzliche Schnittstelle im Rechner noch eine eigene Stromversorgung. Eine besondere Programmierung oder Änderung der Hard- oder Software ist nicht erforderlich, da die Daten des Strichcodelesers vom Rechner genauso behandelt werden wie Tastatureingaben. Der Rechner unterscheidet nicht, ob die Daten vom Strichcodeleser oder von der Tastatur kommen. Das Umschalten zwischen der Dateneingabe über Decoder oder Tastatur erfolgt automatisch.

Inzwischen sind Funklösungen die Alternative, denn durch ihren Einsatz kann vor allem der

Aufwand beim Wareneingang von unhandlicher Ware (z. B. Monitorpaletten) wesentlich reduziert werden. Die Funk-Basisstation wird zwischen Tastatur und Rechner eingeschleift, das Einlesen der Strichcodes erfolgt analog zu den herkömmlichen Leseinheiten. Hauptvorteil ist die Mobilität, denn Funkscanner haben eine max. Reichweite von rund 30 m. Unterschiede zwischen den Strichcodelesern bestehen in der Anzahl der lesbaren Codes, in der Funktion der Code-Erkennung (automatisch/einstellbar), im Ableseabstand und der Leseart. Hierbei kommen Lesestift, CCD und Laserpistole zum Einsatz. Stiftleser sind ideal bei geringen Datenmengen. Als Lichtquelle wird eine rote LED verwendet. Um den Code korrekt erkennen zu können, muss der Stiftleser direkten Kontakt mit dem abzulesenden Code haben.

Bei CCD-Barcodelesern handelt es sich um Nahkontaktleser. Der Leseabstand liegt zwischen direktem Kontakt und wenigen Zentimetern. Laser-Barcodeleser können Codes noch bei großen Entfernungen (70 cm) und wechselnden sowie gekrümmten Oberflächen reproduzieren. Als Lichtquelle ist eine Laserdiode im Einsatz.



15. Terminals

PCs oder Workstations sind inzwischen ein fester Bestandteil von fast jedem Arbeitsplatz. Konventionelle Bildschirmterminals, die über die serielle Schnittstelle entweder direkt oder über einen Terminalserver mit dem Rechner verbunden sind, werden immer seltener eingesetzt. Nur noch bei Anwendungen, die ohne Grafik auskommen, wenig rechenintensiv sind und bei denen es auf die Kosten pro Arbeitsplatz ankommt, kommen sie noch zum Einsatz. Vor allem im Unix-Bereich bekommen diese Terminals immer mehr Konkurrenz von leistungsfähigen Arbeitsplatzrechnern wie Workstations oder PCs: Diese können die Daten lokal verarbeiten, sind aber erheblich teurer und wartungsintensiver als die Bildschirmterminals. Von ihrer Funktionalität und vom Anschluss her stehen die X-Window-Terminals zwischen Bildschirmterminals und Workstations.

Network Computer (NC) sind inzwischen zwar am Markt erhältlich, aber durchgesetzt haben sie sich bislang noch nicht, zumal mit den so genannten Windows Based Terminals (WBTs) eine Alternative vorhanden ist.

Für beide Bereiche scheint es im ersten Ansatz wieder ein Schritt zurück zu sein, da ähnlich wie bei X-Terminals die Daten zentral gehalten und Anwendungen über eine einheitliche Oberfläche dargestellt werden. Bei genauerer Betrachtung werden aber die damit verbundenen Vorteile gegenüber dezentralem Programmablauf ersichtlich.

Die Entscheidung, welcher Gerätetyp und welches System eingesetzt werden soll, ist wegen der hohen Anschaffungskosten und Folgekosten für Betreuung, Wartung, Energieverbrauch usw. besonders wichtig.

15.1 Alphaterminals

Alphaterminals sind dort sinnvoll einsetzbar, wo keine Grafikfähigkeit notwendig ist, d.h. zum Beispiel dann, wenn das Terminal ausschließlich zur Datenbankabfrage eingesetzt wird. Zur Kommunikation mit dem angeschlossenen Rechner müssen lediglich die benötigten Protokolle von dem jeweiligen Terminal unterstützt werden. Historisch bedingt haben die verschiedenen Hersteller für ihre Systemumgebungen spezifische Protokolle und damit Terminals zur Kommunikation mit dem Computer entwickelt. Alphaterminals sind in Single- und Multi-Session-Versionen erhältlich.

15.2 X-Window-Terminals

X-Window-Terminals wurden entwickelt, um eine einheitliche Benutzeroberfläche für unterschiedliche Rechner-Plattformen zu erhalten. Der Bedarf für ein solches Window-System, das hersteller- und hardwareunabhängig Informationen über das Netzwerk verteilt, entstand bereits in den frühen achtziger Jahren am MIT (Massachusetts Institute

of Technology) in Boston. Basierend auf diesen Anforderungen wurde das X-Window-System entwickelt, das 1986 mit der Version 10 (X10) kostenlos an Dritte weitergegeben wurde. Viele Hersteller nutzten diese Möglichkeit und unterstützen die aktuelle Version X11 R6 als Grafik- und Window-Protokoll für ihre Produkte. Inzwischen werden die klassischen X-Windows-Terminals immer mehr durch Thin Client Lösungen abgelöst. Bei dieser Lösung werden PCs oder auch Net-PCs mit entsprechender Software (Exceed von Hummingbird) um die X-Windows-Terminal-Funktionen erweitert. Die Xware Applikationen können unter Windows 3.1/95/98 und Windows NT/2000 installiert werden.

Das X-Window-System wird eingesetzt, um Systemen und Anwendungen, die unter den unterschiedlichsten Architekturen und Betriebssystemen laufen, eine problemlose Kommunikation zu ermöglichen. Über die grafische Benutzeroberfläche können an jedem X-Window-Terminal oder Thin Client mit Xware Software mehrere Applikationen aufgerufen werden, ohne laufende Anwendungen zu verlassen. Informationen können so aus einer Anwendung in eine andere übernommen werden (Copy and Paste Funktion), was vor allem bei Büroarbeitsplätzen mit wechselnden Anwendungen von großem Vorteil ist. Durch das X-Window-System erscheint dem Benutzer das Netzwerk als ein einzelnes, großes Computer-System.

Das X-Window-Terminalkonzept setzt auf dem Client-Server-Modell auf. Der Server ist als darstellender Teil zuständig für die Darstellung und die Verarbeitung der Ein- und Ausgabe über Bildschirm, Tastatur und Maus. Auf dem funktionellen Teil, dem Client, läuft hingegen die eigentliche Applikation. Client und Server können auf getrennten Systemen laufen, solange diese über ein Netzwerk miteinander verbunden sind. Wichtig ist nur, dass Server und Client das gleiche Netzwerkprotokoll, in der Regel TCP/IP, zur Verständigung nutzen. Verglichen mit Workstations stellen X-Window-Terminals eine preisgünstige Alternative dar, zumal hier die Systemverwaltung ausschließlich zentral erfolgen kann, was den Aufwand für das Systemmanagement erheblich verringert. Die beim Einsatz von X-Window-Terminals möglichen Netzwerkengpässe sollten jedoch, z.B. durch den Einsatz von schnellen Backbones, vermieden werden. Die Leistungsfähigkeit von X-Window-Terminals wird durch einen standardisierten Benchmark ermittelt und in sogenannten XStones angegeben. Die benötigte Speichergröße differiert je nach Anzahl der geöffneten Fenster und Grafikapplikationen, so dass hier keine generellen Angaben gemacht werden können.

Es gibt Entwicklungen, die darauf abzielen, die Leistungsfähigkeit und Einsatzgebiete von X-Window-Terminals deutlich zu erweitern. Bedingt durch die enorme Anzahl kaufmännischer und technischer Software für Microsoft Betriebssysteme ist man bestrebt, auch diese Applikationen auf X-Terminals zu integrieren. Das X-Terminal ist dann in der Lage, gleichzeitig neben den X-Anwendungen eines Unix-Servers auch Windows-Anwendungen eines Windows-Servers verarbeiten und darstellen zu können. Es ist sogar möglich, mit Copy and Paste Informationen zwischen X- und Windows-Applikation auszutauschen. Hierzu gibt es auf dem Markt diverse Softwarelösungen, die in Funktionalität und Systemvoraussetzung stark variieren. Mit der oben bereits kurz erwähnten Xware Software wird ein gegensätzlicher Weg beschritten, indem PCs um die





X-Windows-Funktionen erweitert werden.

15.3 PCs und Workstations

Alternativ zu Bildschirmterminals werden heute oft PCs mit Terminalemulationen eingesetzt, falls der Benutzer auf Anwendungen eines Host-Rechners zugreifen will. Vorteil ist, dass der zentrale Rechner mit kleineren Aufgaben, wie beispielsweise Textverarbeitung, nicht belastet wird und die PCs auch für andere Aufgaben eingesetzt werden können. Nachteil einer solchen Lösung ist allerdings, dass der Systemaufwand für die Administration erheblich ansteigt, da ein Teil der Daten nur lokal vorhanden ist und außerdem Updates an jedem Rechner separat eingespielt werden müssen. Mit der Anzahl an PCs, die mit einem Netzwerk verbunden sind, steigt daher der Aufwand für die Systempflege erheblich an. Ein weiterer Nachteil von PCs ist der größere Aufwand für den Anwender, der nicht nur die Bedienung des zentralen Rechners, sondern auch die des PCs erlernen muss. Dieser Nachteil kann durch den Einsatz von Workstations mit gleicher CPU-Architektur oder zumindest gleichartigem Betriebssystem wie dem des Hostrechners (Beispiel dafür sind SPARCserver und SPARCstations mit Solaris) behoben werden. Solche Workstations sind in der Lage, durch die Möglichkeit der lokalen Verarbeitung den Hostrechner zu entlasten.

Im Vergleich zu den X-Window-Terminals kann bei Workstations lokaler Plattenplatz bereitgestellt werden. Gegenüber PCs ergibt sich der Vorteil der einheitlichen Benutzung sowie der einfacheren Systemadministration. Andererseits muss man mit dem Nachteil leben, dass die üblichen Personal Productivity Anwendungen wie z.B. Office-Pakete nur mit Mühe verwendbar sind.

15.4 Network Computer (NCs) & Co.

Nach wie vor sind Network Computer (NCs) ein Thema auf dem IT-Markt. Neben dem klassischen NC sind zwei weitere Produktgruppen in der Diskussion, die dem Anwender ähnliche Vorteile - allerdings auf einer anderen Technologie basierend - bieten. Es sind dies die so genannten Windows Based Terminals sowie NetPCs.

Ganz generell kann für die drei Produktbereiche folgende Aussage gemacht werden: Ziel ist es, preisgünstige Desktops („Thin Clients“) bereitzustellen, die von mächtigen Servern abhängig sind. Es soll also das Prinzip der zentralen Datenverwaltung und Administration verwirklicht werden: so, wie es aus der „guten alten X-Terminal-Zeit“ in Erinnerung ist. Während das Windows Based Terminal für alle Applikationen ausschließlich und zu 100% auf einen Windows NT Server zurückgreift, können beim NC durchaus einige Prozesse lokal laufen. Neben Java-Applikationen und Internet-Browsern ist das auch für diverse Terminalemulationen der Fall. Auf dem Server hingegen laufen lediglich die

Windows-, Unix- und Mainframe-Applikationen. Der Net-PC bietet sowohl die Möglichkeit, Applikationen lokal auszuführen (z.B. Windows-Programme), als auch den Weg über den Server zu gehen.

15.4.1 Network Computer (NCs)

Network Computer sind mittlerweile zur Marktreife gelangt. Die Nachfrage wächst weiter und die Zahl der Hersteller und Geräte zeigt, dass mit Netzwerk-Computing in bestimmten Bereichen stark zu rechnen ist.

Als Client ist in dieser Architektur kein hochgerüsteter PC mehr erforderlich, sondern eben nur noch der NC. Dieser zeichnet sich hauptsächlich durch folgende Eigenschaften aus:

- NCs benötigen keine Festplatte,
- NCs sind für den Einsatz im Intranet vorbereitet, - leistungsfähige CISC- oder RISC-Prozessoren, - umfassende Grafik- und Audiofähigkeit.

Im Vergleich zu einem PC weist der NC signifikante Vorteile auf, die dem Anwender bereits vor der Kaufentscheidung bewusst sein sollten. Das bedeutet unter anderem: - Administrationskosten um ein Vielfaches geringer;

- Sicherheit und Integrität des netzwerkorientierten Systems deutlich höher (Stichwort: Zentrale Datensicherung);
- Wartung des Clients bzw. der Client-Software entfällt; wesentlich geringere HelpdeskFunktionen erforderlich;
- zentrale Verwaltung der Anwendungen, dadurch jederzeit gleicher Versionsstand im Unternehmen;
- neueste Software-Versionen können ohne aufwendige Installations- und Wartungsarbeiten bereitgestellt werden, da die entsprechenden Module nur auf den Server geladen werden müssen;
- Web-Browser als Client-Software stehen preisgünstig zur Verfügung - geringer Schulungsaufwand.

Zusammenfassend kann dies auf einen Nenner gebracht werden: Wesentliche Reduzierung der Total Cost of Ownership (TCO) als genereller Vorteil der Thin Clients. Von den Firmen Apple, IBM, Netscape, Oracle und Sun wurde ursprünglich in einem



sogenannten „Network Computer Reference Profile“ genau definiert, welche Mindestanforderungen ein NC erfüllen muss. Mittlerweile wurde das Profil von The Open Group (TOG) übernommen. Diese internationale Organisation ist auch dafür verantwortlich, dass das Profil stets auf den aktuellen Stand gebracht wird. Mehr über TOG und ihre Mitglieder. unter <http://www.opengroup.org>.

NCs von Herstellern wie NCD (NCD NC), Tektronix (Netstation), IBM (Network Station), Neoware (Workstation) oder Sun (JavaStation) erfüllen diese Vorgaben vollständig, wobei sie sich aber in Ausstattung und Zusatzfeatures teilweise unterscheiden.

15.4.2 Windows Based Terminals (WBTs)

Ein Windows Based Terminal (WBT) ist eine Thin Client Hardware mit Windows CE als Betriebssystem, die mit einem Windows Terminal Server (für Windows NT 4.0 bzw. Windows 2000) oder MetaFrame Server verbunden wird. Ein WBT benutzt entweder das von Microsoft entwickelte sogenannte Remote Desktop Protokoll (RDP, früher auch als TSHARE bekannt) oder das ICA Protokoll von Citrix, um mit dem Server zu kommunizieren. Die aktuelle Entwicklung zielt klar auf die Unterstützung von Windows NT 4.0 und Windows 2000. Hier kommt Microsofts Windows NT 4.0 Server Terminal Server Edition ins Spiel. Es handelt sich dabei um eine multiuser-fähige Version des NT 4.0 Servers, die aus drei Komponenten besteht. Zum einen beinhaltet sie die Client Software, die dem Anwender Zugriff auf 32-bit Windows-Applikationen bietet (Software Clients für NT Workstation 4.0, Windows 95, Windows for Workgroups 3.11 und Windows CE). Zum zweiten ist der Server Kernel enthalten, der es ermöglicht, mehrere Clients zu verwalten. Die letzte Komponente bildet das bereits angesprochene RDP, das die Verbindung zwischen Server und Client herstellt. Bei Windows 2000 übernehmen die Terminal Services, die in allen Windows 2000 Server Versionen enthalten sind, diese Funktionen.

Wichtig ist in diesem Zusammenhang die Lizenzierung. Jeder Client benötigt zuerst eine Server ClientAccess Lizenz (CAL). Zusätzlich ist auf dem Client eine Terminal Services CAL nötig. Systeme mit Windows 2000 Professional enthalten automatisch eine solche Lizenz, sie müssen nicht zusätzlich lizenziert werden. Um auch nicht-windows-basierte Hardware ansprechen zu können, bietet Citrix das Produkt MetaFrame an. Das Nachfolgeprodukt von WinFrame erweitert den Windows Terminal Server sowohl server- als auch clientseitig. Unter Nutzung des ICA Protokolls wird es so u.a. möglich, auch Java-basierende Rechner, MACS, Unix Rechner oder ICA WBTs zu unterstützen.

MetaFrame dient als Grundlage für Application Publishing, einem neuen Weg für moderne Client/Server-Architekturen. Der Client bekommt vom Server nur die Fensterdarstellung über das Netz zugespielt. Kernstück dafür ist das ICA-Protokoll (Independent Computing Architecture). ICA trennt die Applikationslogik vom Darstellungsinterface ab und überträgt nur den Bildschirminhalt vom Server zum WBT - analog zu Microsofts RDP. Die neueste MetaFrame Version (1.8 Feature Release 1) bietet einige neue interessante Features. Es sind nun bis zu 16 Millionen (true-color)

Farben möglich (RDP unterstützt maximal 256 Farben). Darüber hinaus wird eine web-basierte Client Installation ermöglicht und es gibt erweiterte Sicherheitsfunktionen.

Die Hardware in Form von Thin Clients wird von verschiedenen Herstellern angeboten, z.8. die ThinSTARs von NCD, das Capio von Boundless, Neowares Neostation oder auch die Winterm 3000 Serie von Wyse.

Herstellerlinks zu NCs und WBTs:

<http://www.ncd.com>

<http://www.boundless.com>

<http://www.neoware.com>

<http://www.wyse.com>

15.4.3 NetPCs

Im Gegensatz zu den NCs, die hauptsächlich mit Intel i960- und PowerPC-Prozessoren (NCD, IBM, Neoware) bzw. MicroSparc-II-Prozessor (Sun) ausgestattet sind, werden die NetPCs (z.B. von Microsoft) auf der Grundlage von Intel Pentium CPUs ausgestattet sein. Hauptunterschiede gegenüber NCs oder WBTs: Das Betriebssystem der NetPCs bleibt ebenso wie die typische Hardwareausstattung (z.B. lokale Laufwerke und Festplatten) sehr umfangreich. Teurere Anschaffungskosten für den Client sowie erhöhte Cost of Ownership sind die Folge. Das Konzept der zentralen Datenverwaltung und Administration ist damit in diesem Produktbereich nicht voll verwirklicht. Vielmehr bilden NetPCs zwischen PCs und Thin Clients eine weitere Kategorie an Arbeitsplatzrechnern.

Welche Hersteller und welche Produkte sich am Markt letztlich durchsetzen werden, ist momentan noch nicht klar abzusehen. Fest steht jedenfalls, dass sowohl PCs als auch NCs und WBTs ihren Einsatzbereich haben werden und immer mehr Anwendungen durch das Internet beeinflusst werden. Bei der Entwicklung der Internet Appliances steht als Zielsetzung, aus Geräten des normalen Gebrauchs autonome und kommunizierende Geräte zu entwickeln. Die Internet Appliances sind untereinander vernetzt und können Daten austauschen. Mittlerweile gibt es interessante Zwischenergebnisse dieser Entwicklung, so z.B. die Vernetzung von Haushaltsgeräten mit dem Ziel, jedes Gerät unabhängig vom Standort des Besitzers zu steuern und zu kontrollieren. So kann von nahezu jedem Internet-Terminal die gesamte Haus- und Heimelektronik gesteuert werden. Dabei tritt die zugrunde liegende Technologie in den Hintergrund, die Anwender- und Bedienungsfreundlichkeit werden den Bedürfnissen des Nutzers angepasst.





16. Ausgabegeräte

16.1 Bildschirmausgabe

16.1.1 Monitor-Grafikkarten-Kombination

Für den Bildaufbau wird im Monitor (Kathodenstrahlbildschirm) ein Elektronenstrahl erzeugt, der mit einer festgelegten Frequenz horizontal und vertikal über die Bildfläche abgelenkt wird. Für die Synchronisation der beiden Frequenzen sendet die Grafikkarte entsprechende Impulse an den Monitor. Da die meisten Grafikkarten jedoch nur bestimmte Vertikal- und Horizontalfrequenzen unterstützen, kann nicht jede Grafikkarte mit jedem Monitor kombiniert werden. Die heute angebotenen Monitore sind so genannte Multifrequenz-Monitore, bei denen die Zeilenfrequenz nicht fest vorgegeben ist, sondern sich in gewissen Grenzen nach dem jeweiligen Eingangssignal richtet. Daher ist man beim Einsatz eines solchen Monitors in der Auswahl der Grafikkarte weniger eingeschränkt als es früher bei Festfrequenzmonitoren der Fall war. Die Entscheidung für eine bestimmte Grafikkarte sollte immer im Zusammenhang mit der für einen Monitor getroffen werden. Hierbei sind Kriterien wie Auflösung, Bildwiederhol- und Zeilenfrequenz sowie Anschlussart zu beachten.

Die Auflösung eines Monitors steht für die Anzahl der Bildpunkte, die auf dem Monitor dargestellt werden. Ein Bildpunkt, auch Pixel genannt, entspricht der kleinsten adressierbaren Einheit.

Die Bildwiederholfrequenz gibt an, wie oft das gesamte Bild pro Sekunde aufgebaut wird. Je höher sie ist, desto ruhiger erscheint das Bild. Optimal sind Werte ab etwa 73 Hz, bei denen das Auge kein Flimmern mehr erkennen kann: Damit ist bei längerem Aufenthalt am Bildschirm ein ermüdungsfreies Arbeiten möglich. Der empfohlene Richtwert liegt heute bei 85 Hz.

Die Zeilenfrequenz steht für die Zeit, die für den Aufbau einer Bildschirmzeile benötigt wird. Sie errechnet sich aus der Bildwiederholfrequenz und der Zeilenzahl des dargestellten Videomodus und wird in kHz angegeben. Sie ist also abhängig von der Auflösung und der Bildwiederholfrequenz des Monitors.

Für höchste Bildqualität empfiehlt transtec den Einsatz eines BNC-Kabels. Dies sind Hochfrequenzkabel mit separaten, abgeschirmten Leitungen für die Grundfarben Rot, Grün und Blau (RGB). Da hierbei Signalüberlagerungen verhindert werden, ist eine bessere Bildqualität möglich. Im Lieferumfang ist in der Regel ein VGA-Kabel enthalten. Welches Kabel bei transtec Monitoren mitgeliefert wird, kann dem Monitorkapitel entnommen werden. BNC Kabel müssen separat bestellt werden und sind im Zubehörcapitel des Katalogs zu finden. Daneben sind aber auch ergonomische Anforderungen zu berücksichtigen. So sollte ein Monitor dreh- und neigbar sein, damit er der Haltung des Benutzers optimal angepasst werden kann und nicht durch eine falsche

Körperhaltung langfristig gesundheitliche Schäden entstehen. Es wird empfohlen, den Bildschirm so aufzustellen, dass er leicht aufwärts geneigt ist und sich die Augenhöhe des Benutzers in etwa mit der oberen Bildschirmkante deckt. Um ein entspanntes Arbeiten zu ermöglichen, sollte zudem auf eine ausreichend große Bildschirmdiagonale geachtet werden. Wichtig für die benötigte Bildschirmdiagonale ist die Art der Anwendungen, für die ein Monitor eingesetzt werden soll. Die heutigen Applikationen mit ihren zahlreichen Menü- und Buttonleisten erfordern eine grafische Auflösung von mindestens 800 x 600 Bildpunkten bei einer Bildschirmdiagonale von 38,1 cm (15"). Sollen jedoch mehrere Applikationen bzw. Fenster gleichzeitig geöffnet werden, stößt der Anwender bei einem 15"-Monitor schnell an die Grenzen. In diesen Fällen eignet sich eine Auflösung von 1024 x 768 Bildpunkten, die ab einem 43,1 cm (17")-Monitor sinnvoll einsetzbar ist. Für CAD-, Grafikdesign- und DTP-Anwendungen sind 48 cm bzw. 50 cm (19"), 50,8 cm (20") oder 53 cm bzw. 55 cm (21") Monitore mit einer Auflösung von 1280 x 1024 Bildpunkten geeignet. Für komplexere Anwendungen in diesem Bereich sollten 1600 x 1200 Bildpunkte gegeben sein.

Ein weiterer wichtiger Punkt bei der Auswahl von Monitoren ist die Stärke der vom Monitor ausgehenden Strahlung. Hier sind von verschiedenen Instituten Richtwerte definiert worden. Ein wichtiger Standard ist MPR-II, eine Strahlungsempfehlung für elektromagnetische Wechselfelder, elektrische Wechselfelder und elektrostatische Aufladungen vom Schwedischen Prüfinstitut aus dem Jahre 1990. Monitore, die die Werte dieser Empfehlung unterschreiten, bezeichnet man üblicherweise als strahlungsarm. Immer wichtiger werden jedoch die weltweit strengsten Empfehlungen der Schwedischen Angestelltenvereinigung, TC092. Die jeweils geltenden Grenzwerte sind in der untenstehenden Tabelle dargestellt. Neben diesen Grenzwerten schließt ein Monitor, der nach TCO92 geprüft wurde, auch einen geringeren Stromverbrauch ein. Wird der Monitor eine gewisse Zeit nicht benutzt, schaltet er in einen Energiesparmodus, bei dem der Stromverbrauch bei weniger als 30 Watt liegt.

TCO95 geht noch einen Schritt weiter und umfasst zusätzlich auch Umweltschutzaspekte von Gerät und Verpackung (z. B. Recyclingfähigkeit). Zudem werden die Anforderungen um niedrige Geräuschkentwicklung und Wärmeabstrahlung erweitert.

Eigenschaft	Frequenz	MPR-II	TC092
Magnetisches Wechselfeld	5 Hz bis 2 kHz	bis 250 nT	bis 200 nT
	2 kHz bis 400 kHz	bis 25 nT	bis 25 nT
Elektrisches Wechselfeld	5 Hz bis 2 kHz	bis 25 V/m	bis 10 V/m
	2 kHz bis 400 kHz	bis 2,5 V/m	bis 1,0 V/m
Elektrostatische Aufladung		bis +/- 500 V	bis +/- 500 V

Monitorstrahlung



Seit Januar 1999 besteht die neueste Richtlinie: TC099. Um nach TCO99 zertifiziert zu werden, müssen Monitore neue und verschärfte Anforderungen an Qualität und Ergonomie erfüllen. Erstmals wird eine Mindest-Bildwiederholffrequenz von der Auflösung und Gerätegröße abhängig gemacht (Beispiel: 17"-Monitor mit 1024 x 768, mind. 85 Hz). Weitere Neuerungen: Nur noch 15 Watt Stromverbrauch im Energiesparmodus (vorher 30 Watt), Verbot von brom- und chlorhaltigen Stoffen und Vermeidung von Schwermetallen sowie verbindliche Recyclingvorschriften in den jeweiligen Ländern.

16.1.2 Grafikstandards

Im PC-Bereich haben sich im Laufe der Zeit unterschiedliche Grafikstandards entwickelt, die sicherstellen, dass Grafikkarten, Monitore und Anwendungsprogramme untereinander kompatibel sind. Der Video Graphics Array Standard (VGA-Standard) und der Super-VGA-Standard sind heute am wichtigsten. Die Auflösung beim VGA-Standard beträgt 640 x 480 Punkte, wobei 16 aus einer Palette von 256 Farben gleichzeitig dargestellt werden. In einem zusätzlichen Modus können 256 Farben gezeigt werden, jedoch nur bei 320 x 200 Bildpunkten.

Super-VGA (SVGA) und XGA stehen für höhere Auflösungen von bis zu 1024 x 768 Bildpunkten. Für die Darstellung von 16 aus 256 Farben wird ein Bildschirmspeicher von 512 KB benötigt. Bei 1 MB Speicherausbau können insgesamt 256 Farben aus einer Palette von 16.7 Millionen Farben dargestellt werden.

Für Workstations sind die Grafikstandards aus dem PC-Bereich nur von geringer Bedeutung. So ermöglichen die im Compaq/Digital-, HP-, IBM- und SGI-Umfeld einsetzbaren Grafikkarten Auflösungen von 1024 x 768 und 1280 x 1024 bis zu maximal 1600 x 1280 Pixel bei unterschiedlichen Bildwiederholffrequenzen. Die in SPARC-Stations eingesetzten Grafikkarten unterstützen meist eine Auflösung von 1152 x 900 Bildpunkten bei einer Bildwiederholffrequenz von 66 oder 76 Hz. Daneben stehen aber auch im SPARC-Bereich Grafikkarten zur Verfügung, die den VGA-Standard unterstützen oder Auflösungen von 1024 x 768 bis zu 1600 x 1280 erreichen.

Der Großteil der heute auf dem Markt verfügbaren Grafikkarten besitzt eigene Grafik-Coprozessoren. Diese Grafik-Coprozessoren, die von unterschiedlichen Herstellern angeboten werden, entlasten die Rechner-CPU. Sie erhalten nur wenige Befehle von der Rechner-CPU und sprechen ihrerseits direkt den adressierbaren Bildwiederholfspeicher der Grafikkarte an.

16.1.3 Bildschirmtypen

Kathodenstrahlbildschirme

Bei Kathodenstrahlbildschirmen entsteht das auf dem Monitor angezeigte Bild durch das Auftreffen eines Elektronenstrahls auf dem Leuchtstoff an der Innenseite der Monitorscheibe. Zur Erzeugung der Farben stehen drei Leuchtstoffe für die Grundfarben Rot, Grün und Blau zur Verfügung. Der Farbmischung liegt das sogenannte additive Verfahren zugrunde, d.h. wenn ein Strahl auf einen der Leuchtstoffe trifft, wird Licht in der entsprechenden Farbe ausgestrahlt. Durch die Kombination der drei Grundfarben können dann Farben mit unterschiedlicher Helligkeit erzeugt werden.

Damit die Strahlen auf den jeweils richtigen Leuchtstoff treffen, ist vor dem Leuchtstoff eine Maske angebracht. Bei den klassischen Kathodenstrahlbildschirmen ist dies eine Lochmaske. Dabei handelt es sich um eine Metall- oder Keramikplatte mit einer Vielzahl von Löchern, durch die der Elektronenstrahl bzw. die Elektronenstrahlen geführt werden, so dass er/sie den korrekten Punkt auf dem Bildschirm trifft/treffen. Der kürzeste Abstand zweier gleichfarbiger Bildpunkte auf einem Bildschirm gibt Aufschluss über die Feinheit der Lochmaske und indirekt damit verbunden über die Anzahl der Grafikpunkte, die ein Monitor als einzelne Elemente darstellen kann. Je kleiner die Lochmaske, desto schärfer die Abbildung.

Zu den qualitativ hochwertigen Monitoren gehören Geräte mit einer Black-Trinitron-Bildröhre (Trinitron ist eingetragenes Warenzeichen der Sony Co.). Bei einem Trinitron Monitor wird anstelle einer Lochmaske eine Streifenmaske eingesetzt. Diese besteht aus durchgehenden Spalten (Streifen), durch die der Elektronenstrahl gelenkt wird. Da durch die Streifen ein beträchtlich größerer Strahl geleitet werden kann als durch eine Lochmaske, ergeben sich schärfere Bilder und leuchtendere Farben. Weiterhin besitzt ein Trinitron-Monitor den Vorteil einer flacheren Bildschirmoberfläche. Bei herkömmlichen Lochmaskensystemen ist die Grundform eine Kugel, die sich selbst bei den moderneren FST-Bildschirmen (Fiat Screen Tube) nur schwer abflachen lässt. Ein Trinitron-Monitor ist dagegen wie ein Zylinder geformt. Der Bildschirm liegt wie ein Fenster in diesem Zylinder. Durch einen vergrößerten Radius des Zylinders nähert sich die Bildschirmoberfläche eines Trinitron-Monitors immer mehr der einer ebenen Fläche an. Die flachere Bildschirmoberfläche verhindert Verzerrungen. Gerade Linien sehen gerade aus und erfüllen die Anforderungen für moderne CAD/CAM- und Grafikanwendungen. Darüber hinaus wird durch das schwarzgetönte Glas, das bei Black-Trinitron-Bildschirmen eingesetzt wird, einfallendes Fremdlicht (wie Sonnenstrahlen oder Lampenlicht) weitestgehend absorbiert.





LCD-Bildschirme

Neben den klassischen Kathodenstrahlbildschirmen werden die LCD-Bildschirme (Liquid Crystal Display) immer interessanter. Außer einem niedrigen Stromverbrauch (ca. 8 W) und einem sehr geringen Platzbedarf (Bautiefe im Bereich von 20 cm) besitzen diese Displays diverse weitere Vorteile.

Flachbildschirme schneiden vor allem bei den Emissionen wesentlich besser ab. Röntgenstrahlung, elektrostatische Felder und Magnetfelder treten systembedingt nicht mehr auf. Aus diesem Grund gehören Fehler in Konvergenz, Schärfe und Abbildungsgeometrie der Vergangenheit an. Die Folge ist eine sehr hochwertige Ausgabequalität mit klaren, hellen und gestochen scharfen Bildern. Selbst kleine Schrift ist leicht lesbar.

Bei den angegebenen Bild diagonalen handelt es sich um die tatsächlich sichtbare Bildfläche. Ein 14"-Flachbildschirm entspricht zum Beispiel einem 15"-CRT-Monitor, ein 18-Zöller in etwa einem 20-Zöller.

Alle LC-Displays nutzen zur Bilderstellung eine Anordnung aus vertikalen und horizontalen Leitungen (Matrix). Um Bildschirmpunkte gezielt ein- und auszuschalten, wird auf die einzelnen Leitungen Spannung angelegt, so dass am Kreuzungspunkt ein elektrisches Feld entsteht. Durch diesen punktweisen Bildaufbau verschwindet der von CRT-Monitoren bekannte Flimmereffekt, die Vertikalfrequenz (Bildwiederholrate) entfällt vollständig.

Bei der Passiv-Matrix-Technologie entsteht nicht nur genau am Kreuzungspunkt, sondern auch entlang der Leitungen ein elektrisches Feld. Dieses ist zwar schwächer, bei zu hoher Feldstärke entstehen jedoch graue Punkte in der Umgebung des eigentlich adressierten Punktes. Daher darf die Feldstärke nicht zu hoch gewählt werden, was einen geringeren Kontrast zur Folge hat. Das Kontrastverhältnis bei Passiv-Matrix-Displays liegt deshalb kaum über 20:1.

Wesentlich brillantere Farben und ein weitaus besseres Kontrastverhältnis von bis zu 300:1 erreichen sogenannte Aktiv-Matrix-Displays. Hier sind an den Kreuzungspunkten der Leitungen zusätzlich winzige Transistoren angebracht. Die Ansteuerung kann deshalb über ein relativ schwaches Feld erfolgen, das vom Transistor um ein Vielfaches verstärkt wird. Andere Zellen bleiben unbeeinflusst, es kommt nicht zu unerwünschten Farbeeinflüssen. Generell gilt, dass Passiv-Matrix-Displays (DSTN) für die Darstellung von Grafiken und Programmen ohne bewegte Bilder geeignet sind. Für die Wiedergabe von Videosignalen und Multimedia-Präsentationen werden jedoch Aktiv-Matrix-Displays (TFT-Technologie) benötigt, die eine wesentlich höhere Anzeigegeschwindigkeit und brillantere Farbdarstellung ermöglichen.

Die in diesem Katalog angebotenen Modelle (siehe diverse Kapitel Flachbildschirme von Philips und Eizo (Seite 190)), benötigen keine speziellen Grafikkarten, sondern können 1:1 gegen einen Kathodenstrahlbildschirm ausgetauscht werden. Es gibt jedoch auch Flachbildschirme auf dem Markt (z. B. von SGI), die eine proprietäre Lösung darstellen und die anstatt der herkömmlichen Grafikkarte eine spezielle Karte benötigen.

Um die bestmögliche Ausgabequalität zu erzielen, sollte die Grafikkarte auf die maximal mögliche Auflösung des Displays abgestimmt werden. Außerdem muss in erster Linie auf eine saubere Synchronisation zwischen Karte und Flachbildschirm geachtet werden. Diese Einstellung wird durch die Clock Rate (Grobsteuerung) und die Phase (Feintuning) vorgenommen und optimiert.

16.2 LC-Displays und LCD-Projektoren

Für Präsentationen oder Schulungen bietet es sich an, den Bildschirminhalt der Workstation oder des PCs allen Teilnehmern zugänglich zu machen. Während beim Einsatz von Overhead-Folien eine längere Vorbereitungszeit benötigt wird (für Ausdrucke, Kopien etc.), können die Daten beim Einsatz von LC-Displays oder LCD-Projektoren bis zu Beginn

- und sogar während - des Vortrages geändert werden. Das LCD-Panel wird auf den Overhead-Projektor gelegt und zusätzlich zum Monitor an der Workstation bzw. am PC angeschlossen. Der aktuelle Bildschirminhalt wird auf die Leinwand projiziert, die Daten können während des Vortrages interaktiv beeinflusst werden.

Im Unterschied zu den LC-Displays wird beim Einsatz von LCD-Projektoren kein zusätzlicher Overhead-Projektor benötigt. Durch die Unabhängigkeit vom Tageslichtprojektor fällt bei Präsentationen in fremden Räumen der Unsicherheitsfaktor weg, zumal ein Overheadprojektor mit 250 Watt, wie er häufig eingesetzt wird, für ein LCD-Panel nicht ausreicht. Hinzu kommt, dass diese Projektoren mit der gleichen Leistung ein helleres Licht projizieren können, da die Lichtquelle wesentlich besser ausgenutzt wird. Bei Präsentationspanels wird stets ein Teil der Durchlichtfläche vom Rahmen abgedeckt, wohingegen beim Projektor die Lichtquelle voll auf das integrierte LCD-Panel konzentriert wird.

Die Mehrzahl der auf dem Markt befindlichen LC-Displays und LCD-Projektoren erreicht mit 640 x 480 Pixel VGA-Auflösung. Die derzeit maximal erreichbare Auflösung beträgt 1280 x 1024 Bildpunkte.



16.3 Drucker

Zur Ausgabe von Texten und Grafiken auf Papier, Folie oder Klebeetiketten sind Drucker erforderlich. Zu den wichtigsten Druckertypen zählen heute Nadel-, Tintenstrahl- und Laserdrucker sowie Thermotransfer-, Thermosublimations- und Phase-Change-Drucker. Da im Druckbereich die Farbdarstellung immer mehr an Bedeutung gewinnt und Drucker fast aller Technologien in Farbversionen erhältlich oder optional aufrüstbar sind, werden zunächst einige Grundlagen erläutert, die allen Farbdruckern gemeinsam sind. Die dann folgenden Abschnitte, in denen sowohl auf die Druckverfahren als auch auf die Vor- und Nachteile der einzelnen Technologien eingegangen wird, sollen helfen, aus der Vielzahl der Möglichkeiten das richtige Gerät auszuwählen.

Im Geschäftsumfeld hält Farbe mehr und mehr Einzug und wird bevorzugt für Geschäftsgrafiken, Diagramme, Tabellen oder Präsentationsfolien eingesetzt, da diese Dokumente damit nachhaltig an Aussagekraft gewinnen. Untersuchungen haben ergeben, dass durch die Verwendung von Farbe die Leserschaft einer Publikation um bis zu 40% vergrößert werden kann. Das Verständnis wird sogar um 73% verbessert.

Grundsätzlich sollte bei der Auswahl eines Druckers, ob es sich nun um einen monochromen oder einen Farbdrucker handelt, nicht allein der Anschaffungspreis ausschlaggebend sein. Vielmehr sollten auch die laufenden Kosten für Verbrauchsmaterialien berücksichtigt werden, da diese -je nach Drucktechnologie, Art und Anzahl der erzeugten Drucke in der Lebensspanne eines Druckers vielfach höher sein können als die Kosten des Druckers selbst. Bei der Errechnung der im Folgenden erwähnten Druckkosten pro Seite wurde der Anschaffungspreis für den jeweiligen Farbträger (z. B. Druckkopfpatrone oder Toner cartridge) ins Verhältnis gesetzt zu der vom Hersteller zugesicherten möglichen Anzahl von Ausdrucken. Die Kosten für Papier bzw. Spezialpapier wurden (soweit möglich) von den reinen Druckkosten pro Seite getrennt, um auch einen Vergleich zwischen den verschiedenen Technologien zu ermöglichen. Als Anschaffungspreise für die jeweiligen Farbträger wurden die Katalogpreise verwendet. Da sich Preise für Drucker-Verbrauchsmaterialien jedoch häufig ändern, sind diese Angaben lediglich als Richtwerte zu verstehen.

16.3.1 Farbdrucker

Unabhängig von Drucktechnologie oder Farbträger entstehen Farbausdrucke immer mit Farbträgern in den Mischfarben Cyan, Magenta und Gelb. Schwarz kann entweder als vierte Farbe vorhanden sein oder aber aus den anderen drei Farben zusammengemischt werden. Das aus den drei Mischfarben erzeugte Schwarz erreicht allerdings nicht denselben intensiven Ton wie ein separat vorhandenes Schwarz. Der transtec Katalog wird z. B. im Offsetdruck mit genau diesen vier Farben hergestellt. Farbdrucker, die nicht wie Sublimationsdrucker in der Lage sind, Halbtöne mit fließenden Farbabstufungen und -übergängen zu erzeugen, simulieren Zwischentöne über das Dithering-Verfahren. Durch dieses Verfahren werden Druckpunkte aus den Farben Cyan, Magenta, Gelb und ggf. Schwarz innerhalb einer Zelle (z. B. 6 x 6 Punkte) so verteilt, dass für das menschliche

Auge ein bestimmter Farbton erzeugt wird. Soll z. B. die Farbe Violett gedruckt werden, werden abwechselnd Farbpunkte in Magenta und Cyan gesetzt. Je mehr verschiedenfarbige Punkte in einer Zelle abgedruckt werden müssen, um einen bestimmten Zwischenton darzustellen, desto geringer wird die für das menschliche Auge sichtbare Auflösung.

16.3.2 Tintenstrahldrucker

Bei Tintenstrahldruckern haben sich zwei Drucktechniken durchgesetzt: Das Bubble-Jet-Verfahren und das Drop-on-Demand-Verfahren. Beim Bubble-Jet-Verfahren befindet sich vor jeder Druckdüse der Druckkopfpatrone ein eingebautes Heizelement, das die in der Düse befindliche Tinte innerhalb sehr kurzer Zeit stark erhitzt. Während nun ein Teil der Tinte durch die Erhitzung verdampft, wird der andere Teil in Tropfenform auf das Papier geschossen. Der Nachteil dieses Druckverfahrens besteht im Verschleiß, den der Druckvorgang mit sich bringt: Nach einiger Zeit fallen einzelne Heizelemente aus und die Qualität der Ausdrücke verschlechtert sich entsprechend.

Diesem Nachteil wirkt das Drop-on-Demand-Verfahren entgegen. Hier übernehmen sog. Piezo-Elemente die Rolle der Heizeinheiten. Der piezoelektrische Effekt bewirkt, dass sich bestimmte Kristalle durch das Anlegen einer elektrischen Spannung verformen. Beim Druckvorgang wird also elektrische Spannung an das Piezo-Element der Düse angelegt, das sich dann schlagartig verformt. Hierbei wird die Düse stark zusammengepresst und der in der Düse befindliche Tintentropfen auf das Papier geschleudert. Eine Druckkopfpatrone von Hewlett-Packard für die DeskJet-Serie verfügt z. B. über 48 Düsen, die über die Steuerelektronik des Druckers angesteuert werden.

Die Vorteile von Tintenstrahldruckern liegen hauptsächlich in einem günstigen Anschaffungspreis, hoher Schriftqualität, Grafikfähigkeit und einer niedrigen Geräuschkulisse. Diese Eigenschaften machen sie zu idealen Ausgabegeräten für kleine und mittlere Druckaufkommen. Interessant sind Tintenstrahldrucker auch für Anwender, die Farbausdrucke erstellen möchten, da Farbtintenstrahldrucker im Anschaffungspreis eine preisgünstige Alternative zu Farbdruckern anderer Technologien darstellen.

Der Nachteil dieser Geräte besteht darin, dass das verwendete Druckmedium großen Einfluss auf die Qualität des Ausdrucks hat. Für qualitativ hochwertige Ausdrücke wird daher die Verwendung von meist teurem, speziell beschichtetem Papier und von Spezialfolie empfohlen. Die Ausdrücke sind zudem nicht licht- und wasserfest. Da Tintenstrahldrucker bei hoher Seitenfärbung aufgrund der Kosten für die Verbrauchsmaterialien schnell unrentabel werden, eignen sie sich eher für Bereiche, in denen keine volle Seitendeckung gefordert ist. Legt man einerseits den Anschaffungspreis für eine Druckkopfpatrone und andererseits die vom Hersteller angegebene Anzahl druckbarer Seiten zugrunde, so belaufen sich die reinen Druckkosten pro Seite für einen Schwarz/Weiß Ausdruck auf ungefähr EUR 0,03/ SFr. 0,05 (bei ca. 5% Flächendeckung, was einer vollen Textseite entspricht) zuzüglich der





Kosten für Spezialpapier, wenn ein sehr hochwertiger Ausdruck gefordert ist.

Der anfallende Restmüll in Form von leeren Tintenpatronen kann heute an diverse Recyclingfirmen geschickt werden, die das Leergut, manchmal sogar gegen eine kleine Prämie, zurücknehmen.

16.3.3 Thermotransferdrucker

Das Thermotransfer-Prinzip basiert auf dem Abschmelzen einzelner Druckpunkte von einer mit Wachsfarbstoff beschichteten Polyesterfolie. Dieser Vorgang erfolgt durch eine Vielzahl an Heizelementen, die horizontal in einer Druckzeile angeordnet sind. Als Farbträger können monochrome (Schwarz), dreifarbige (Cyan, Magenta, Gelb) oder vierfarbige (Cyan, Magenta, Gelb und Schwarz) Thermotransferrollen eingesetzt werden. Jede Rolle setzt sich aus seitengroßen Segmenten der einzelnen Farben zusammen. Um eine einzelne Seite zu bedrucken, befördert die Mechanik des Druckers zunächst die erste Mischfarbe (z. B. Cyan) nach vorne. Nun wird jeder einzelne Druckpunkt, dessen Farbe Cyan beinhaltet, gesetzt.

Ist die erste Farbe Cyan komplett abgerollt, wiederholt sich derselbe Vorgang mit den anderen Farben.

Die Vorteile dieser Drucktechnologie liegen in einer brillanten, stark abdeckenden Farbpalette. Die mit diesem Verfahren erzeugten Dokumente sind licht- und wasserecht. Ein Nachteil besteht darin, dass die Thermotransferrollen nicht bedarfsgerecht verbraucht werden: Die Druckmechanik rollt für jede zu bedruckende Seite die Wachsfolie mit allen Farben ab, egal, ob sie alle benötigt werden oder nicht. Die Druckkosten hängen somit nicht vom Füllungsgrad der Seite ab. Für eine DIN-A4-Seite belaufen sie sich auf etwa EUR 0,6/ SFr. 1,10 (3-Farbrolle) zuzüglich der Kosten für Spezialpapier, die bei ca. EUR 0,13/ SFr. 0,25 für eine DIN-A4-Seite liegen. Es empfiehlt sich daher, Farbthermotransferdrucker nur in Bereichen einzusetzen, in denen eine möglichst hohe Seitendeckung gefordert ist. Hier liegen die Kosten der Verbrauchsmaterialien dann unter den entsprechenden Kosten von Farbtintenstrahldruckern. Bedruckt werden können ausschließlich Spezialfolie und Thermotransferpapier sowie hochwertiges Normalpapier, das jedoch vor dem eigentlichen Druck durch das Auftragen einer Trägerschicht die Eigenschaften von Thermotransferpapier erhalten muss. Diese, auf speziellen Dreifarbtansferrollen zusätzlich enthaltene, transparente Zwischenschicht gleicht die raue Oberflächenstruktur von normalem Laserpapier aus und bildet eine glatte Oberfläche und harte Haftfläche für die Wachsfarbe.

16.3.4 Thermosublimationsdrucker

Mit Sublimationsdruckern lassen sich fotorealistische Ausdrücke erzeugen. Ähnlich der Thermotransfertechnologie arbeitet auch das Sublimationsverfahren mit einer Trägerfolie in den vier Farben Cyan, Magenta, Gelb und Schwarz, von der die Farbe mit Hilfe von Heizelementen abgeschmolzen wird. Das Wachs wird so stark erhitzt, dass es gasförmig in Spezialpapier hineindiffundiert. Sublimation bedeutet aus physikalischer Sicht das Überspringen eines Aggregatzustandes, hier wird der flüssige Zustand übersprungen.

Jedes einzelne Heizelement im Druckkopf kann 256 unterschiedliche Temperaturen erzeugen. Die von der Trägerfolie abgeschmolzene Farbe wird umso intensiver übertragen, je höher die Temperatur des Heizelementes ist. Daher kann jede Farbe in bis zu 256 Intensitätsstufen abgedruckt werden. Sublimationsdrucker erreichen eine echte Farbauflösung von 300 x 300 Punkten pro Zoll, da Halbtöne nicht aus einer Zelle mit einzelnen Punkten erzeugt werden müssen, sondern durch Verschmelzen der Farben im Papier erreicht werden.

Der Vorteil dieses Druckverfahrens liegt in der hohen Qualität der erzeugten Farbausdrücke. Als Nachteile sind die hohen Kosten für Spezialpapier und Farbbrollen und die damit verbundenen hohen Kosten pro Seite zu erwähnen. Sie belaufen sich auf etwa EUR 0,6/ SFr. 1,10 für Spezialpapier in DIN-A4-Größe. Da wie beim Thermotransferverfahren der Verbrauch der Farbbrollen nicht bedarfsgerecht erfolgt, sondern für jede zu bedruckende Seite Trägerfolien in allen Grundfarben abgerollt werden, sollte diese Technologie ebenfalls nur für Bereiche mit hoher Seitendeckung eingesetzt werden.

16.3.5 Phase-Change-Drucker

Die Bezeichnung dieses Druckverfahrens ist darauf zurückzuführen, dass die Farbträger während des Druckvorganges mehrmals ihren Aggregatzustand ändern. Häufig wird auch synonym die Bezeichnung Solid-Ink-Drucker oder Festtintendrucker verwendet. Als Farbträger dienen bei diesem Druckverfahren vier feste Farbstifte in den Farben Cyan, Magenta, Gelb und Schwarz. Beim Druckvorgang sorgen Heizelemente dafür, dass von diesen Farbstiften jeweils eine kleine Menge Tinte in einen Vorratsbehälter abgeschmolzen und dort bei einer Temperatur von ca. 90 Grad Celsius in flüssigem Zustand gehalten wird. Die in diesem Vorratsbehälter befindliche flüssige Tinte wird nach demselben Verfahren wie bei den Tintenstrahldruckern auf das Druckmedium gesprüht. Beim Auftreffen der Tinte auf Papier oder Folie erkaltet diese sofort und geht wieder in den festen Aggregatzustand über. Ein wesentlicher Vorteil dieser Technologie ist die verbrauchsorientierte Abnutzung der Farbträger. Weiterhin ist für den Druck kein Spezialpapier erforderlich, es können unterschiedliche Papierarten bedruckt werden. Dieses Druckverfahren eignet sich daher insbesondere für Anwender, die verschiedene Papierarten mit unterschiedlicher Seitenfärbung bedrucken möchten. Die Druckkosten



belaufen sich auf ungefähr EUR 0,6/ SFr. 1,10 pro DIN-A4-Seite (90g/qm, 30% Füllungsgrad). Die maximalen Druckkosten für eine DIN-A4Seite (90g/qm, 100% Füllungsgrad) können etwa EUR 1,6/ SFr. 2,80 betragen.

16.3.6 Laserdrucker

Laserdrucker arbeiten nach elektrofotografischem Verfahren: Beim Druckvorgang wird zuerst die im Drucker befindliche Bildtrommel elektrisch geladen. Anschließend überträgt ein über ein Spiegelsystem geleiteter Laserstrahl zeilenweise das Druckbild auf die Trommel. Für jeden Zeilenpunkt, der nicht gesetzt werden soll, schaltet der Drucker den Laserstrahl ab. Am Auftreffpunkt des Laserstrahls wird die elektrische Ladung der Bildtrommel neutralisiert. An diesen neutralisierten Punkten nimmt die Trommel im weiteren Verlauf des Druckvorganges den Toner auf, der dann auf das Papier übertragen und durch Hitze und hohen Andruck fixiert wird.

Dieses Verfahren trifft sowohl für monochrome als auch für Farblaserdrucker zu. Nur wird bei den angebotenen Farblaserdruckern der gesamte Vorgang einmal für jede Mischfarbe wiederholt. Allerdings läuft nicht das zu bedruckende Papier viermal durch das Gerät, sondern ein spezielles Band, auf dem die zu druckende Seite aufgezeichnet wird. Von der Druckertrommel wird dieses Druckbild in einem einzigen Arbeitsgang auf Papier oder Folie übertragen.

Einige Hersteller haben Verfahren entwickelt, die durch steuerbare Punktgrößen oder variable Punktpositionierung das Druckbild deutlich verbessern. HP beispielsweise nennt sein Verfahren Resolution Enhancement Technology (RET). Dieses eingebaute Feature kann softwareunabhängig durch die Optimierung der Punktgröße und deren Positionierung im Verhältnis zu den benachbarten Punkten besser gerundete Kurven, schärfere Linien/Kanten und glattere Übergänge erzeugen.

Der Vorteil von Laserdruckern liegt vor allem in der hohen Druckqualität und Grafikfähigkeit sowie der geringen Geräuschkentwicklung beim Druckvorgang. Da ihr Anschaffungspreis über dem von Tintenstrahldruckern liegt, werden Laserdrucker vor allem für höhere Druckaufkommen empfohlen. Auf dem Markt erhältlich sind Laserdrucker mit Druckgeschwindigkeiten von vier bis 40 Seiten pro Minute. Die Kosten für Verbrauchsmaterialien liegen bei Laserdruckern mit hohem Druckvolumen unter den Vergleichswerten für Tintenstrahldrucker. Beachtet werden sollte, dass bei vielen Geräten mit der leeren Toner cartridge automatisch auch die Bildtrommel ausgetauscht wird. Dies resultiert in einem stets sauberen Schriftbild, erhöht jedoch den Anschaffungspreis der Toner cartridge. Wird einerseits der Anschaffungspreis für die Toner cartridge mit Bildtrommel und andererseits die vom Hersteller angegebene Anzahl möglicher Druckseiten pro Kassette berücksichtigt, so ergeben sich reine Druckkosten von ca. EUR 0,015/ SFr. 0,03 (zuzüglich Papierkosten) pro Seite. Der Wert bezieht sich auf eine Flächendeckung von 5%, was einer voll bedruckten Textseite entspricht. Aus diesen Angaben wird deutlich, dass für größere Druckvolumina auf jeden Fall ein Drucker

mit hohem Durchsatz angeschafft werden sollte.

Nachteile von Laserdruckern sind die hauptsächlich beim Betrieb älterer Geräte entstehenden relativ hohen Ozonwerte und die umweltbelastende Entsorgung der Belichtungseinheiten und Toner kassetten. Neue Laserdruckermodelle emittieren weit weniger Ozon, bei manchen Geräten ist der Ozonausstoß kaum oder gar nicht mehr messbar.

Wie die Tintenpatronen können auch leere Toner kassetten an diverse Recyclingfirmen geschickt werden, die das Leergut, oft sogar gegen eine kleine Prämie, zurücknehmen. Dadurch können die Anwender zum aktiven Umweltschutz beitragen.

16.3.7 Matrixdrucker

Matrix- oder Nadeldrucker drucken durch einen mit Nadeln bestückten, auf einer Schiene befestigten Druckkopf. Dieser Druckkopf wird mit Hilfe der Schiene horizontal über das Farbband bewegt, das zwischen Papier und Druckkopf gespannt ist. Die einzelnen Nadeln hämmern nun auf das Farbband und hinterlassen damit einen Abdruck auf dem Papier. Die Anzahl der Nadeln hat entscheidenden Einfluss auf die Druckqualität: Schriftbild und Grafikfähigkeit bei 24-Nadeldruckern sind deutlich besser als bei 9-Nadeldruckern.

Mit einigen Modellen können auch Farbausdrucke erzeugt werden. Sie arbeiten mit einem Farbband, das über vier Farbstreifen verfügt.

Der Vorteil von Matrixdruckern liegt in einem relativ niedrigen Anschaffungspreis und geringen laufenden Kosten für Verbrauchsmaterialien. Sie können in einem Druckvorgang mehrere Durchschläge verarbeiten und Endlospapier bedrucken. Daher werden diese Geräte heute hauptsächlich für das Bedrucken von Etiketten oder Formularen mit mehreren Durchschlägen sowie den Ausdruck von Listen eingesetzt. Der Nachteil von Matrixdruckern liegt vor allem in der hohen Geräuschkentwicklung und der geringen Druckqualität bei einer niedrigen Anzahl von Nadeln sowie der langsamen Druckgeschwindigkeit im Letter-Quality-Modus (Schönschrift-Modus).

16.3.8 Druckerprotokolle

Synonym zu dem Begriff Druckerprotokoll wird häufig auch das Wort Druckersprache benutzt. Die meisten Laserdrucker beherrschen die Protokolle HP PCL und/oder PostScript. PostScript ist eine druckerunabhängige Seitenbeschreibungssprache, bei der ein Schrifttyp (Font) durch mathematische Kurven (Bezier-Kurven) definiert ist. Wegen ihrer hohen Leistungsfähigkeit und der flexiblen Befehlsstruktur wird in vielen Bereichen mit PostScript gearbeitet.



HP PCL (Printer Communication Language) ist eine von Hewlett-Packard entwickelte Steuersprache für Drucker, die auch von zahlreichen anderen Herstellern genutzt wird. HP PCL 6 ist eine Weiterentwicklung von HP PCL 5 und zu dieser abwärtskompatibel. Neuerungen in PCL 6 sind beschleunigtes Drucken vor allem komplexer Grafiken, verbesserte Druckqualität sowie erhöhter Netzdurchsatz durch Verwendung kleinerer und kompakterer Befehle. Deutliche Leistungssteigerungen sind vor allem unter Microsoft Windows zu erwarten, da die neuen PCL 6 Befehle das Graphical Direct Interface (GDI) unterstützen. Einige Geräte beherrschen auch die Plottersprache HP-GL (Hewlett Packard Graphics Language). Das in HP PCL 5 integrierte Protokoll HP-GL/2 ist eine Weiterentwicklung von HP-GL und zu diesem nicht abwärtskompatibel.

Eine Implementierung der Plottersprache HP-GL oder HP-GU2 auf Laserdruckern hat den Vorteil, dass Plotterkommandos vom Laserdrucker aufbereitet und in eine entsprechende Grafikdarstellung überführt werden können. Der Austausch eines Plotters gegen einen HP-GL- oder HP-GU2-fähigen Laserdrucker kann deshalb völlig problemlos und ohne Treiberanpassungen vorgenommen werden. Die Ausgabe von Grafiken, die auf einem Plotter technisch bedingt lange dauern, kann so mit einem Laserdrucker sekundenschnell realisiert werden. Dabei muss jedoch auf Farbdarstellung verzichtet werden.



17. Multimedia

Multimedia ist inzwischen nicht mehr nur ein weitverbreitetes Schlagwort, sondern in vielen Anwendungen bereits fest implementiert.

Allgemein wird unter Multimedia die Kombination von verschiedenen Medienformen wie Standbilder (z.B. unter Verwendung digitaler Kameras), Audio, Bewegtbilder, Texte und Grafiken bezeichnet. Viele Rechner erledigen weitere Aufgaben. Es können normale Musik-CDs abgehört, E-Mails mit Toninformationen verschickt werden. Der PC dient auch als Telefonanlage, die Anrufe weiterleitet, oder als Anrufbeantworter, der ankommende Telefonate beantwortet.

Videokonferenzsysteme bekommen eine immer größere Bedeutung, da nicht nur ein normales Videobild übermittelt werden kann. Es ist möglich, Konferenzen mit mehreren angeschlossenen Partnern abzuhalten und Dokumente über große Entfernungen schnell und kostengünstig auszutauschen. In Verbindung mit Multimedia werden immer auch CD- und DVD-Laufwerke sowie Jukeboxen genannt. Der Grund hierfür ist, dass die Datenmenge generell sehr hoch ist und deswegen besonders preisgünstige, schnelle Speichermedien mit hoher Kapazität benötigt werden. Diese Technologien sind im Kapitel Massenspeicher aufgeführt. Auf die einzelnen Funktionen wird im Folgenden eingegangen.

17.1 Digitale Kameras

Digitale Kameras nehmen durch die rasant wachsenden Multimedia-Anwendungen einen immer größeren Stellenwert ein. Sollen Bilder mit dem Computer bearbeitet werden, muss bei einer konventionellen Kamera erst der Film entwickelt und dann das Dia oder der Papierabzug gescannt werden. Bei der digitalen Kamera wird das Bild digital auf einem internen Speicher abgelegt und über eine Schnittstelle oder eine Diskette zum Computer übertragen.

Der Anwender kann Bilder vergrößern, verkleinern, in Dokumente integrieren und über Online-Dienste verschicken. Desktop-Publishing, Präsentationen sowie einfachere Marketingbroschüren können ohne Scanner schnell und einfach mit Bildern gefüllt werden. Steht zudem ein geeigneter Farbdrucker - z.B. von HP, Lexmark oder Tektronix - zur Verfügung, kann der Arbeitsablauf „fotografieren - sehen - bearbeiten - ausdrucken“ komplett abgeschlossen werden.

Tintenstrahldrucker von HP,

Tintenstrahlplotter von HP,

Laserdrucker von HP,

All-in-one Geräte von HP,

Postscript-Farbdrucker von Tektronix

Die Auflösung der digitalen Bilder erreicht mittlerweile annähernd die Qualität herkömmlicher Kleinbildabzüge. Kleinere Abstriche müssen lediglich bei der Datenkomprimierung gemacht werden.

17.2 Sprachanwendungen

Sprache ist ebenso wie Musik ein analoges Signal, das durch Digitalisierung in eine rechnerverarbeitbare Form gebracht und dann von einer Soundkarte wieder in analoge Signale gewandelt werden kann. Zur Ein- und Ausgabe sowie zur Bearbeitung von Toninformationen wird eine so genannte Audioschnittstellenkarte, im PC-Bereich auch Soundkarte genannt, benötigt. Soundkarten und Multimediazubehör sind im Kapitel Multimediazubehör (Seite) zu finden.

Das über Mikrofon oder Überspielkabel eingespeiste analoge Audiosignal wird von der Audiokarte mehrere tausend Mal pro Sekunde abgetastet (Sampling). Die Qualität der Abtastung ist abhängig von der Auflösung des Digital-Analog-Umsetzers (z.B. 8, 10 oder 16 Bit) sowie von der Abtastfrequenz (Anzahl der Messungen pro Sekunde). Dieses Verfahren nennt man Puls- Code- Modulation (PCM). Möchte man Sprache über weitere Strecken, z.B. via E-Mail, übertragen, müssen die Datenmengen möglichst klein gehalten werden. Dazu werden die Signale über ADPCM (Adaptive Differential PCM) vor dem Senden komprimiert und beim Empfänger wieder dekomprimiert.

17.3 Videobearbeitung

Videokarten finden heute in den unterschiedlichsten Bereichen Anwendung. Neben dem Einsatz zur Erstellung digitaler Videoclips für Schulungszwecke oder Präsentationen wird auch die Darstellung von Live-Video oder Video-On-Demand ein immer größeres Thema. Live-Video ermöglicht dem Anwender, parallel zu laufenden Applikationen Nachrichtensendungen mitzuverfolgen.

Ein weiteres Anwendungsgebiet ist die Echtzeit-Übertragung komprimierter Videobilder über Netzwerke. Die Videos können auf einem Videoserver, der mit einer solchen Karte ausgerüstet ist, gespeichert werden. Entfernt sitzende Anwender, die über das Netzwerk Zugriff auf diesen Videoserver haben, können dann via Video-On-Demand die gespeicherten Videofilme auf ihrer Workstation anschauen oder dort zur Weiterverarbeitung abspeichern.





Zur Erstellung von Präsentationen können Videos von einem angeschlossenen Videorecorder oder einer Videokamera in die Workstation eingelesen werden und -je nach Wunsch - entweder ganze Videosequenzen manipuliert oder Standbilder abgespeichert und in Demos eingebunden werden.

Voraussetzung für die Erstellung von Videoclips ist der Einsatz einer Videokarte, die die Videosequenzen oder Standbilder von einem angeschlossenen Videorecorder, einer Videokamera oder TV-Geräten auf der Festplatte abspeichert. Videosoftware bietet dann die Möglichkeit zur Manipulation der Videos. Da die Videodaten ohne bemerkbaren Qualitätsverlust vervielfältigt und geschnitten werden können, ist der Videoschnitt letztlich eine Frage von Dateikopier- und -löschbefehlen. Darüber hinaus bietet die Videoverarbeitung per Computer den Vorteil, dass auf jedes einzelne Bildstück des digitalisierten Materials sekundenschnell zugegriffen werden kann. Lästige Umspulzeiten entfallen. Die Übernahme einzelner Videobilder oder ganzer Videosequenzen in den PC oder in die Workstation kann über Videokarten mit unterschiedlichen Leistungsmerkmalen erfolgen, die im Folgenden aufgezeigt werden.

Um Echtzeit-Videos oder Fernsehbilder am Monitor darzustellen, wird eine sogenannte Overlaykarte benötigt, die die aufwendige Digitalisierung der Videodaten umgeht. Diese Overlaykarten besitzen meist keine bzw. nur eine eingeschränkte Grabbing-Funktion und sind damit lediglich als Fernsehempfänger oder für Überwachungskameras einsetzbar. Das Videosignal wird von der Overlay- auf die Grafikkarte übertragen, so dass die Darstellung keine Rechenzeit erfordert. Das Videobild wird in einem separaten Fenster auf dem Monitor angezeigt.

Zusätzlich zur Video- und Overlayfunktion ist bei einigen Videokarten bereits eine Grafikkarte integriert. Damit wird eine separate Grafikkarte überflüssig und für beide Funktionen wird nur ein Steckplatz im PC benötigt. Noch einen Schritt weiter gehen solche Videokarten, die über einen TV-Tuner verfügen. Damit kann neben Live-Videos jede beliebige Live-TV-Sendung in einem Fenster am Bildschirm dargestellt werden.

Um ganze Videosequenzen am Bildschirm darzustellen und zu digitalisieren, werden Echtzeit-Digitizer benötigt, die das Videosignal in digitale Bilderfolgen umwandeln.

Das Hauptproblem beim Abspeichern von Videosequenzen sind jedoch stets die enormen Datenmengen, die bei der Digitalisierung von Bildern und Videos anfallen. Für die Digitalisierung von einem Videobild mit 24-bit Farbtiefe werden ca. 1.2 MB benötigt. Bei einem PAL-Signal von 25 Bildern pro Sekunde entsteht so eine Datenmenge von 30 MB pro Sekunde. Zum Abspeichern von Videosequenzen sollte daher eine Videokarte mit Hardware-Kompression zum Einsatz kommen. Die Datenkompression verringert den Speicherbedarf und erhöht gleichzeitig die Verarbeitungsgeschwindigkeit der Videobilder. Außerdem wird durch die Kompression die benötigte Bandbreite bei Datenübertragungen über das Netzwerk verringert.

Eine Kompression ohne Verlust an Qualität ist mit vertretbarer Rechenzeit nur bis zu einem Verhältnis von 1:2 möglich. Praktisch alle Lösungen für Videokompression müssen aber weit höhere Kompressionsraten erreichen. Softwarelösungen verwenden Algorithmen, die mit geringen Verlusten an Bildqualität Kompressionsraten bis 1:20 bewirken. Aufgrund dieser eingeschränkten Kompressionsrate setzen viele Video-Digitizer auf den Kompressionsstandard JPEG. Spezielle integrierte Schaltungen auf der Videokarte erlauben es, Videos in Echtzeit, d.h. mit mindestens 25 Bildern pro Sekunde, bis um den Faktor 1:10 zu komprimieren und zu dekomprimieren. Dieser Kompressionsalgorithmus arbeitet jedoch vor allem bei höheren Kompressionsfaktoren nicht verlustfrei, d.h. man kann Original und komprimiertes Bild nicht nur unterscheiden, sondern aus dem komprimierten Bild lässt sich das Original nicht mehr rekonstruieren. Es entstehen sogenannte Würfeffekte, die Bildbestandteile werden extrem grobkörnig. Der Grad der Kompression kann variabel eingestellt werden. In der Praxis muss hier ein Kompromiss gefunden werden, da hohe Qualität geringe Kompression und damit eine hohe Datenmenge bedeutet.

Motion-JPEG arbeitet ebenfalls nur mit Einzelbildern, es entsteht im Prinzip eine Datei aus lauter JPEG-komprimierten Einzelbildern.

MPEG berücksichtigt darüber hinaus auch, dass die Veränderung von einem Bild zum nächsten meistens nur gering ist. Das Verfahren eliminiert die Ähnlichkeiten aufeinander folgender Bilder. Nur nach jeweils zwei Bildern pro Sekunde enthalten die volle, unabhängige Information des Einzelbildes. Alle dazwischenliegenden Bilder enthalten nur noch die Veränderungen zum vorhergehenden Bild. Festzustellen, welcher Teil des Bildes sich im nächsten wiederverwerten lässt, verlangt eine enorme Rechenleistung. Aus diesem Grund sind Video-Digitalisierungskarten mit MPEG-Bewegungskompression sehr teuer.

Um eine angemessene Ausgabequalität der erstellten Videosequenzen zu gewährleisten, empfiehlt es sich, von vornherein nur hochwertiges Ausgangsmaterial zum Digitalisieren zu verwenden. Beim Digitalisieren von VHS-Videos stößt man schnell auf Probleme bei der Bildqualität. S-VHS oder, noch besser, professionelles Betacam eignet sich weitaus besser. Falsch ist, dass wegen der Qualitätsverluste durch Kompression die Eingangsqualität keine große Rolle spielt. Fehler wie Drop-Outs oder Rauschen machen sich nach der Digitalisierung doppelt bemerkbar. Insbesondere auf Rauschen reagieren die Kompressionsverfahren wie MPEG sehr empfindlich, da sich dann von Einzelbild zu Einzelbild sehr viele Informationen ändern.

Sind die Videobilder auf der Festplatte gespeichert, können diese über Videobearbeitungs-Software beliebig geschnitten und manipuliert werden. Mit Hilfe von Überblendungen und anderen Trickeffekten können so eigene Videofilme erstellt werden.

Werden entsprechende Bibliotheken und Programmierschnittstellen mitgeliefert, können für die Bildverarbeitung auf der Workstation oder auf dem PC eigene Programme



geschrieben werden. Für Schulungs- und Präsentationszwecke lassen sich so die gewünschten Bildfolgen zusammenstellen und beispielsweise mit Texteinblendungen kombinieren. Lernprogramme können so gestaltet werden, dass der Benutzer individuell anwählt, welches Kapitel er mit welchem Schwierigkeitsgrad am Bildschirm dargestellt haben möchte. Die Software sucht dann die entsprechenden Bilder.

Vor allem für Produktpräsentationen bietet es sich an, die zuvor digitalisierten Videosequenzen nach der Bearbeitung auf dem Videorecorder oder Fernseher auszugeben. Hierfür muss die Videokarte einen eigenen Video-Ausgang besitzen. Vorteil ist, dass ein Fernseher wesentlich preisgünstiger ist als ein Großbildschirm mit entsprechender Diagonale. Darüber hinaus können die Videos auch einem größeren Publikum über einen Videoprojektor präsentiert werden. Ebenso stellt die Erstellung von Video-Tapes einen interessanten Aspekt dar, zumal die auf dem Tape gespeicherten Daten dann über jeden beliebigen Videorecorder am Fernseher angezeigt werden können.

17.4 Videokonferenzsysteme

Videokonferenzsysteme bekommen eine immer größere Bedeutung in Unternehmen, da sie eine enorme Kostenersparnis bedeuten können. Kommunikation mit Ton und

Bild bedeutet eine leichtere und deutlichere Verständigung zwischen einzelnen und ganzen Gruppen von Kommunikationspartnern. Durch die flächendeckende Verbreitung von ISDN ist es einfach geworden Videokonferenzsysteme aufzubauen. Die meisten heute erhältlichen Systeme beinhalten eine geeignete Grafikkarte, Videokamera, Mikrofon, eine ISDN-Karte sowie die benötigte Software. Durch die ITU-Industriestandards 11.323 (LAN), 11.320 (ISDN) und 1.120 (gemeinsamer Datenzugriff) ist es auch möglich, mit Videokonferenzsystemen anderer Hersteller, die diese Normen beinhalten, zu kommunizieren.





18. Unterbrechungsfreie Stromversorgung

Unterbrechungsfreie Stromversorgungen (USV) versorgen ein Computersystem oder verschiedene Peripheriegeräte oder auch Telefonanlagen weiter mit Batteriestrom, sollte die Netzversorgung einmal ausfallen.

Ein unerwarteter Netzausfall führt zum Verlust aller Daten und Programme im Arbeitsspeicher eines Computers. Der Inhalt einer Platte kann in einen inkonsistenten Zustand geraten, wenn der Stromausfall während eines Schreibvorgangs stattfindet oder Inhalte von WriteCache-Speichern nicht vor dem Stromausfall auf die Platte geschrieben wurden. Deswegen ist es wichtig, bei solchen Störfällen den Rechner geregelt herunterzufahren.

Bei Netzstörungen sollte man aber nicht nur an einen Stromausfall denken, sondern auch an Störungen, die durch lokale Belastungen des Stromnetzes auftreten können. Solche Über- oder Unterspannungen können durch einen ausgeprägten Belastungswechsel verursacht werden, der von einem im Hausnetz angeschlossenen Gerät ausgeht. Sollte eine Unterspannung über längere Zeit andauern, wird das Computernetzteil diese registrieren und den Computer abschalten, was gleichbedeutend ist mit einem Netzausfall. Auch kurzfristige Unterspannungen können Probleme erzeugen. Durch einen kurzen Spannungspuls kann es zu nicht nachvollziehbaren Systemabstürzen oder Programmfehlern kommen. Überspannungen sind verantwortlich für eine Vielzahl an Hardwareausfällen, sie verschleißen Computerbauteile, besonders Netzteile.

18.1 USV-Technologien

Bei USVs unterscheidet man zwischen zwei verschiedenen Technologien. Es gibt sogenannte Online- sowie Offline-Modelle.

Offline-Modelle arbeiten wie ein Notstromaggregat und schalten sich erst dann ein, wenn der Strom ausgefallen ist. Dadurch entstehen entsprechende Schaltzeiten, die im Bereich von wenigen Millisekunden liegen. Bei PCs reicht diese Zeit in der Regel aus, ohne dass eine Störung im Rechner auftritt. Bei anderen Systemen kann schon diese kurze Umschaltzeit zu Datenverlusten führen. Die Line-Interaktive USV ist eine Weiterentwicklung der Offline-Technologie. Durch einen parallel zur Spannungsversorgung der USV geschalteten Regelkreis werden die Schwankungen der Netzspannungen auf einen für den Verbraucher tolerierbaren Wert reguliert und Netzressourcen optimal genutzt, da bei Spannungseinbrüchen nicht gleich auf Batteriebetrieb geschaltet wird. Dies erhöht die Batterielebensdauer. Aber auch diese verbesserte Version der Offline-Technologie reicht nicht aus, wenn die angeschlossenen Geräte auf durch das Umschalten auftretende Phasenverschiebungen empfindlich reagieren. Das ist zum Beispiel bei vielen Anlagen der Telekommunikation der Fall.

Mehr Datensicherheit bieten Online-Modelle, die allerdings aufgrund der aufwendigeren Technologie normalerweise teurer sind als entsprechende Offline- oder Line-Interaktive Modelle. Die eingehende Netzspannung wird galvanisch getrennt und gleichgerichtet. Die gleichgerichtete Spannung wird geglättet, stabilisiert und wieder in eine saubere Wechselspannung gewandelt. Dieses Verfahren gewährleistet für die angeschlossenen Verbraucher weitestgehende Abschirmung von Spannungsschwankungen, Unterbrechungen, Rauschen oder Spikes.

Die Aufladung der Batterie erfolgt während des Normalbetriebs. Fällt das Netz völlig aus, übernimmt die ständig aufgeladene Batterie gleitend und unterbrechungsfrei den Energiefluss zum Wechselrichter. Diese Technologie erzeugt permanent eine völlig neue, netzunabhängige Spannung. Neben den fehlenden Schaltzeiten haben die Online-Geräte also auch den weiteren Vorteil, als Spannungs-Konstanthalter und Netzfilter arbeiten

zu können. Nachteilig bei Online-Modellen sind die höheren Energieverluste durch die kontinuierliche Versorgung über den Wechselrichter. Die hohe Wärmeentwicklung bedingt den Einsatz von Lüftern, was wiederum zu einer höheren Geräusentwicklung führt.

18.2 Dimensionierung

Die richtige Dimensionierung erfolgt nach der auf den Typenschildern angegebenen Leistung in VA (VoltAmpere) oder der Berechnung der Scheinleistung bei nichtlinearen Lasten. Wird auf dem Typenschild die Leistung in VA angegeben, kann die Leistung der einzelnen Geräte einfach addiert werden. Dazu gehören unter anderem auch Bildschirme, Terminals, externe Datenspeicher und Peripheriegeräte. Erfolgt die Angabe in Watt, so muss die Scheinleistung rechnerisch ermittelt werden. Hierzu wird die Angabe in Watt mit einer Konstanten multipliziert. Bei den derzeit üblichen Schaltnetzteilen kann ein Faktor von 1,4 angesetzt werden.

Rechenbeispiel: Typenschildangabe von 150 W Wert in VA ergibt sich zu $150 \cdot 1,4 = 210$

Sind Systemerweiterungen geplant oder abzusehen, sollten diese Komponenten bei der Dimensionierung der USV mit berücksichtigt werden. Übersteigt der Stromverbrauch der angeschlossenen Geräte durch eine nachträgliche Erweiterung die Leistungsfähigkeit der USV, dann kann ein ordentliches Herunterfahren der Systeme nicht mehr gewährleistet werden. Es wird empfohlen, in regelmäßigen Abständen die Funktionsfähigkeit der USV mit allen angeschlossenen Geräten zu testen.

Da eine USV nur eine vorübergehende Sicherung eines Systems ermöglicht, können die angeschlossenen Rechner und Peripheriegeräte nur für kurze Zeit mit Batteriestrom versorgt werden. Diese Überbrückungszeit lässt sich so auswählen, bzw. durch Batterieerweiterungssets anpassen, dass Daten wie auch Programme im Falle eines



Stromausfalls ordnungsgemäß gesichert werden können.

Wichtigster Bestandteil jeder USV sind die Batterien, deren durchschnittliche Lebensdauer bei 3 bis 5 Jahren liegt und stark von der Batterietemperatur beeinflusst wird. Tests von Herstellern haben ergeben, dass bei einer Erhöhung der Umgebungstemperatur um 5 Grad Celsius die Lebensdauer der Batterie um durchschnittlich 10% sinkt.

18.3 Alarmierung/Schnittstellen

Die Alarmierung über kritische Zustände, wie einen Stromausfall oder eine Störung der USV selbst, sollte gleichermaßen über das Netzwerk, E-Mail, Pager, Fax sowie GSM-Telefone möglich sein. Bei einer Meldung der USV sollte gewährleistet sein, dass vordefinierte Befehle oder Scripts (".exe, *.bat, *.com, *.cmd, etc.) automatisch ausgeführt werden. Alle Vorkommnisse werden in einer Logdatei gespeichert. Das Führen einer separaten Batterie-Log-Datei ist dabei aufgrund der Wichtigkeit der Batterie als Energiespeicher der USV-Anlage unbedingt erforderlich, um ihren Status eindeutig beurteilen zu können. USV-Geräte sind in der Regel mit einer RS-232 Schnittstelle ausgestattet, über die der Anschluss an den Rechner erfolgt. Bei allen USVs, die transtec anbietet, ist im Lieferumfang eine Management- und Shutdown-Software für alle gängigen Betriebssysteme (Windows 98/NT/2000, Unix, NetWare und OS/2) enthalten. Updates können kostenlos von der Homepage des jeweiligen Herstellers heruntergeladen werden. Die Installation ist aufgrund der Benutzerführung sehr einfach durchzuführen: Unter Windows 98 werden z. B. die USVS von MGE automatisch erkannt, da die Treiber bereits in Windows 98 enthalten sind.

18.4 Shutdown

Ein durch die USV-Management-Software ausgelöster Shutdown beinhaltet folgende Merkmale:

1. **Speichern des Cache-Inhaltes auf der Festplatte,**
2. **Speichern des aktuellen Zustandes der offenen Dateien (Windows),**
3. **ordnungsgemäßes Beenden sämtlicher Applikationen,**
4. **Ausführen eventuell hinterlegter Befehle (z. B. Backup fahren, Datenbank sichern etc.),**
5. **Durchführen eines ordentlichen Systemabschlusses und**
6. **Abschalten der USV.**

Es ist möglich, einen genau festgelegten Ein- bzw. Ausschaltplan für die USV zu

definieren.

18.5 Netzwerkweite Kommunikation

Das Managen einer USV-Anlage ist von jeder Arbeitsstation im Netz möglich. Sind innerhalb eines Netzwerks mehrere USVs installiert, können diese von jedem berechtigten Arbeitsplatz netzwerkweit administriert werden.

Meldungen, durch die USV-Management-Software ausgelöst, können zeitgesteuert an vordefinierte Netzwerkteilnehmer gesendet werden. Diese Meldungen können editiert werden und Änderungen von jeder Arbeitsstation sind sofort aktiv. Somit entfällt ein erneutes Rebooten der Shutdown-Software oder gar des Rechners. Funktionen wie Verändern von Einstellungen, Rebooten des Netzwerkes o.ä. sind passwortgeschützt.

Sind mehrere Netzwerkteilnehmer (Server, Workstations, Gateways, Hubs, Router etc.) des gleichen Netzwerkbetriebssystems an eine USV angeschlossen, so kann eine Gruppe erstellt werden. Dies bedeutet, dass ein Rechner seriell mit der USV verbunden ist und als Gruppen-Controller arbeitet. Dieser stellt die USV-Informationen im Netzwerk zur Verfügung. Auf allen weiteren Netzwerkkomponenten ist die Shutdown-Software installiert; die Komponenten sind als Gruppenmitglieder definiert. Deren Verhalten kann jedoch unabhängig vom Controller vorgegeben werden. Somit ist z. B. ein sequentieller Shutdown aller dieser Netzwerkkomponenten gewährleistet.

Ebenso sollte auch der Test aller in einem Netzwerk befindlichen USV-Anlagen durch den Anwender von einer Arbeitsstation aus initialisierbar sein.





19. Anhang

Zu dieser Buchreihe gehören:

- **Excel 2010 auf einen Blick - Einführung in Excel 2010** ^[1]
 - Handbuch (excel2010einf.pdf / 192 Seiten)
 - Eine Einführung in Excel 2010 mit detaillierten Anweisungen
 - Preis: 15,00 €

- **Excel 2010 auf einen Blick - Funktionen** ^[1]
 - Handbuch (excel2010funk.pdf / 420 Seiten)
 - Das zweite Buch zu Excel 2010 in dem die einzelnen bereits in Excel integrierten Funktionen und Formeln beschrieben werden
 - Preis: 25,00 €

- **Excel 2010 auf einen Blick - Funktionen in Beispielen**
 - Datei (excel-Funktionen.xlsx / 417 Register)
 - Die in „Excel 2010 auf einen Blick - Funktionen“ beschriebenen Funktionen werden hier als Beispiele in einer Excel-Arbeitsmappe nochmals dargestellt
 - Preis: 15,00 €

^[1] Bei Kauf beider Excel 2010-Bücher erhalten Sie „Excel 2010 auf einen Blick – Funktionen in Beispielen“ kostenlos dazu.

Weitere Bücher, die von mir im Rahmen der VHS-Kurse, erstellt und erweitert wurden:

- **Word 2010 auf einen Blick – Einführung in Word 2010**
 - Handbuch (word2010einf.pdf / 247 Seiten)
 - Eine Einführung mit Beispielen in Word 2010
 - Preis: 20,00 €

- **Outlook 2010 auf einen Blick – Einführung in Outlook 2010**
 - Handbuch (outlook2010einf.pdf / 180 Seiten)
 - Eine Einführung in Outlook 2010
 - Preis: 18,00 €

- **Computer auf einen Blick**
 - Was versteht man unter folgende Begriffe:
WAN, WLAN, LINUX, RAM, Festplatte, usw.
 - Woraus setzt sich ein Computer zusammen, usw.
 - Eine Einführung in Hard- und Software
 - Preis: 10,00 €

^[2] Bei Kauf aller Bücher (... 2010 auf einen Blick) erhalten Sie „Excel 2010 auf einen Blick – Funktionen in Beispielen“ und das Buch „Computer auf einen Blick“ kostenlos dazu.



20. Notizen

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....



