

**IT**

**KOMPE  
NDIUM**

## IT von A-Z

Aus unserem ausführlichen IT-Kompendium haben wir speziell für diesen Magalog die wichtigsten Schlagwörter aktualisiert:

- Rechnerarchitekturen**
- Betriebssysteme**
- Cluster**
- Speichernetzwerke**
- Magnetbandspeicher**

Das komplette Nachschlagewerk finden Sie im Internet. Das Inhalts- und Stichwortverzeichnis ermöglichen einen schnellen Zugriff auf die gewünschten Seiten.

## 1. Rechnerarchitekturen

Die folgenden Abschnitte enthalten einen kurzen Überblick über 64-Bit-Rechnersysteme sowie die wichtigsten, aktuellen CPUs.

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 fertig gestellt. Der Nachfolger Itanium 2 ist seit Ende 2002 verfügbar. AMD liefert den Athlon 64 (Desktop-Version) und den Opteron (Workstation-Server-Version) seit dem 2. Quartal 2003 aus. Intel hat AMDs 64-Bit-Technology lizenziert und sie unter dem Namen Intel® EM64T (Extended Memory 64 Technology) in neue Prozessoren und Chipsätze integriert. Seit dem 3. Quartal 2004 sind die ersten Produkte erhältlich. Erwähnenswert bei der AMD 64-Bit-Architektur und Intel® EM64T ist die vollständige 32-Bit-Kompatibilität. Dadurch laufen auch 32-Bit-Betriebssysteme und -Anwendungen mit sehr guter Performance. Wichtig ist allerdings nicht nur die Verfügbarkeit der Hardware, sondern auch die der passenden Betriebssysteme. Microsofts Windows Server 2003 ist in der Enterprise-Version mit Unterstützung für die IA64-Architektur verfügbar. Eine Version für AMDs 64-Bit-Architektur und Intel® EM64T ist in Vorbereitung. Auch von Windows XP wird es noch eine entsprechende Version geben. Im Linux-Bereich stehen für beide Architekturen Kernel mit entsprechender 64-Bit-Unterstützung bereit. Für den Benutzer werden die Performance-Vorteile der 64-Bit-Architekturen jedoch erst dann richtig zum Tragen kommen, wenn auch die Anwendungen mit 64-Bit-Unterstützung verfügbar sind.

### 1.1 Intel Prozessoren

#### 1.1.1 Intel® Serverprodukte mit 64-Bit

Intel verfügt über zwei sich ergänzende 64-Bit-Architekturen, die einen hervorragenden Wert für alle Bereiche von Unternehmensanwendungen bieten: Die neuen 64-Bit-Plattformen auf der Basis des Intel® Xeon™ Prozessors mit Intel® EM64T bieten die größte Auswahl von Anwendungen für Mainstream-Server- und Workstation-Lösungen. Sie stellen für 32-Bit-Anwendungen eine hervorragende Leistung und für 64-Bit-Anwendungen mehr Reserven bereit und können beide auf eine sehr flexible und kostengünstige Weise eingesetzt werden. Die Plattformen auf der Basis des Intel® Itanium® 2 Prozessors wurden eigens für äußerst anspruchsvolle und unternehmenskritische 64-Bit-Auslastungen entwickelt. Sie bieten die beste Leistung und Skalierbarkeit sowie die beste RAS (Reliability, Availability, Managability – Zuverlässigkeit, Verfügbarkeit, Verwaltbarkeit), aber zu wesentlich geringeren Kosten als proprietäre RISC- und Mainframe-Lösungen.

#### 1.1.2 Intel® Itanium® 2 Prozessor

Mit der Ergänzung der vorhandenen Intel® Itanium® 2 Prozessoren um den Itanium® 2 Prozessor 1,60 GHz mit 9-MB-L3-Cache und die Low-Voltage-Version des Itanium® 2 Prozessors – optimiert für Dualprozessorsysteme – wird die Itanium® Architektur um kostengünstigere und energiesparendere Systeme erweitert.

#### 1.1.3 Intel® Xeon™ Prozessorfamilie

Die Intel® Xeon™ Prozessorfamilie bietet weiterhin die Verarbeitungskapazität und Vielseitigkeit, die für Front-End- und Small-Business-Server sowie für High-Performance-Computing-Systeme in preissensiblen Umgebungen erforderlich sind. Der für Dualprozessor-Server- und -Workstationplattformen konzipierte Intel® Xeon™ Prozessor mit 800-MHz-Systembus ist nun mit Taktfrequenzen zwischen 2,80 GHz und 3,60 GHz erhältlich. Der Prozessor wird mit der neuesten Intel® 90-Nanometer-Prozesstechnologie gefertigt. Er bietet Merkmale wie Hyper-Threading-Technologie, Demand Based Switching (DBS) mit erweiterter Intel® SpeedStep® Technologie, Intel® Extended Memory 64 Technologie und Streaming-SIMD-Extensions 3 (SSE3).

#### 1.1.4 Intel® Pentium® 4 Prozessor Extreme Edition

Der Intel® Pentium® 4 Prozessor mit HT-Technologie bewirkt, dass ein Prozessor Softwareprogrammen gegenüber als zwei Prozessoren erscheint. Im Ergebnis können die Programme effizienter ausgeführt werden. In den Multitasking-Umgebungen von heute wird die Leistung verbessert und eine höhere Reaktionsgeschwindigkeit des Systems erreicht, da der Prozessor Threads, also Programmanweisungen, parallel ausführen kann.

#### 1.1.5 Intel® Pentium® 4 Prozessor

Der für die Hyper-Threading-Technologie geeignete Intel® Pentium® 4 Prozessor mit fortschrittlichem 800-MHz-Systembus ist mit Taktfrequenzen bis 3,80 GHz, 2 MB L2-Cache (Intel® Pentium® 4 670 Prozessor) erhältlich, produziert mit 90-Nanometer-Prozesstechnologie. Er bietet damit verbesserte Übertragungsraten und Antwortzeiten, wie sie für die problemlose Verarbeitung anspruchsvoller Anwendungen wie bei 3-D-Visualisierung oder Betriebssystemen der nächsten Generation erforderlich sind.

#### 1.1.6 Intel® Pentium® M Prozessor

Der Intel® Pentium® M Prozessor ist eine wichtige Komponente der Intel® Centrino™ Mobiltechnologie. Er basiert auf einer speziell für die mobile Computernutzung entwickelten Architektur. Die Vorteile: hervorragende mobile Leistung und Energiespareigenschaften für dünnere, leichtere Notebooks.

#### 1.1.7 Intel® Celeron® D Prozessor

Der Celeron® D Prozessor ist der Nachfolger der Celeron® Prozessorreihe. Celeron® D basiert auf dem Prescott-Kern mit einer maximalen Taktfrequenz von 533 MHz und 256 MB L2-Cache (im Vergleich zu 400 MHz und 128 MB L2-Cache beim Celeron®). Der Intel® Celeron® D Prozessor bietet ein ausgeglichenes Verhältnis von bewährter Technologie und günstigem Preis für Desktop- und Notebook-Computer, die grundlegende Aufgaben erfüllen sollen. Der Intel® Celeron® D Prozessor ist mit Taktfrequenzen bis 3,20 GHz erhältlich. Er ist dafür konzipiert, elementare Computing-Anforderungen zu unterstützen, beispielsweise beim Austauschen von E-Mails mit Freunden und Verwandten und bei der Verwaltung von Finanzen.

#### 1.1.8 Intel® Celeron® M Prozessor

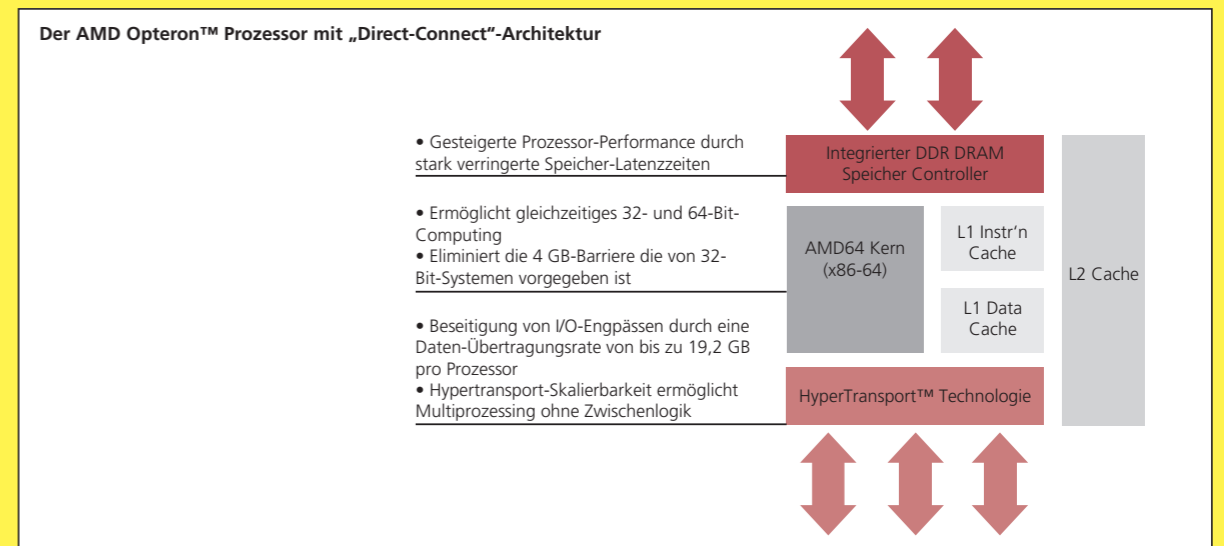
Der Intel® Celeron® M Prozessor basiert auf der speziell für das Mobile Computing entwickelten Mikroarchitektur von Intel®. Er bietet Anwendern ein ausgewogenes Verhältnis von auf Mobilität ausgerichteter Prozessortechnologie, guter mobiler Leistung und außergewöhnlich günstigem Preis in eleganteren, leichteren Notebooks. Die Intel® Celeron® M Prozessorlinie repräsentiert eine neue Generation von Intel® Technologie für das Marktsegment der preisgünstigen mobilen PC.

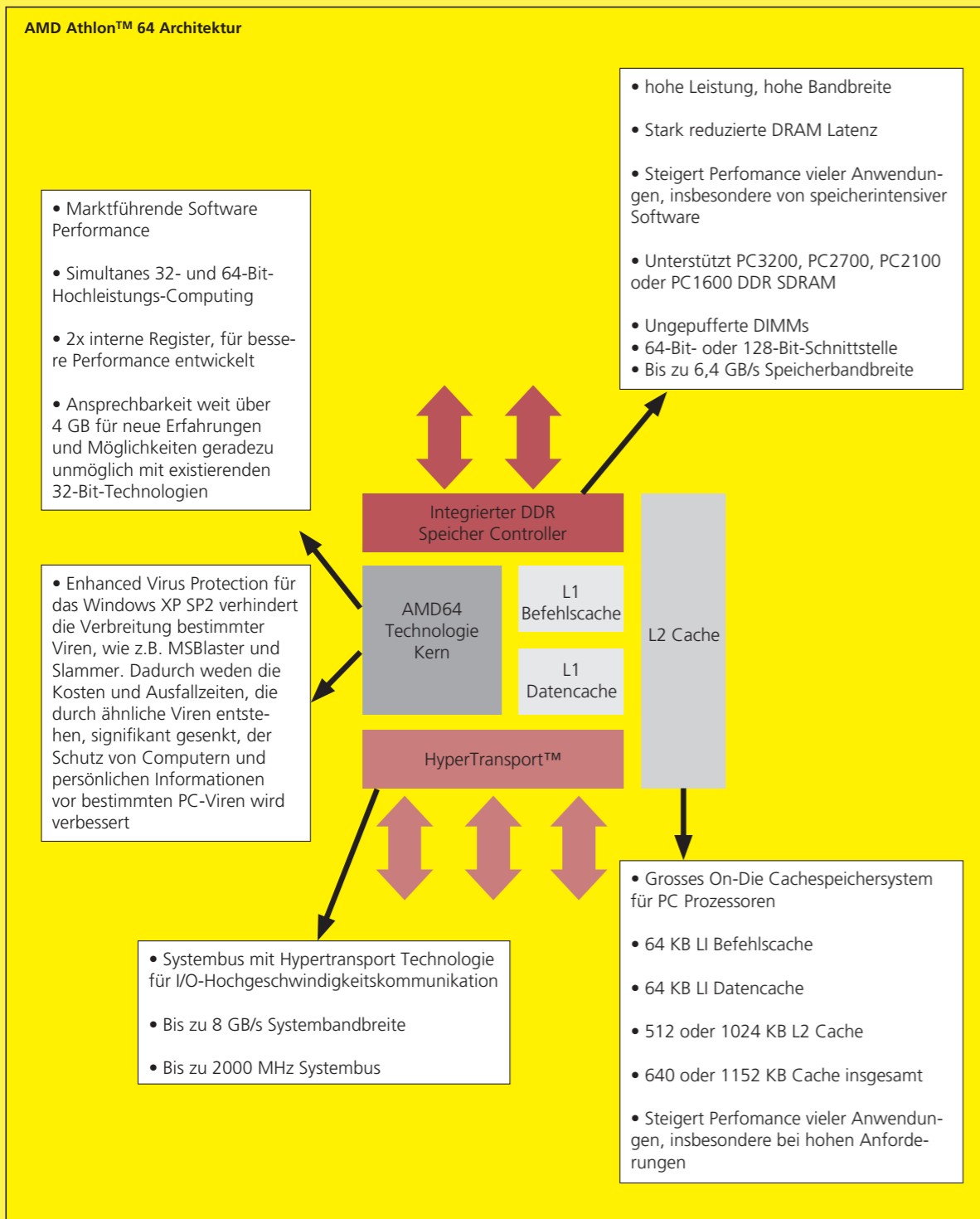
### 1.2. AMD Prozessoren

#### 1.2.1 AMD Opteron™ Prozessor

Der AMD Opteron™ Prozessor mit seinem parallelem 32- und 64-Bit-Computing legt den Grundstein für AMD64-Technologie mit Direct-Connect-Architektur. Der AMD Opteron™ Prozessor wurde dafür entwickelt, bestehende 32-Bit-Applikationen mit herausragender Leistung zu bearbeiten. Gleichzeitig bietet er Kunden einen nahtlosen Migrationspfad zum 64-Bit-Computing. Dieser Prozessor stellt einen Quantensprung hinsichtlich Kompatibilität, Performance, Investitionssicherheit und niedriger Cost of Ownership (TCO) dar. Der AMD Opteron™ Prozessor wird in drei Produktreihen angeboten: die 100er Reihe (1-Weg), die 200er Reihe (bis zu 2-Wege) sowie die 800er Reihe (bis zu 8-Wege).

Der AMD Opteron™ Prozessor besteht aus folgenden Systemkomponenten:





### 1.2.2 AMD Athlon™ 64 Prozessor

Die AMD64 Technologie ermöglicht führende Software-Performance und eröffnet nie da gewesene Computing-Erlebnisse und -Möglichkeiten. Spezifische Eigenschaften der AMD64 Technologie:

- Höchstes Performance-Niveau bei vielen bestehenden 32-Bit-Anwendungen, ohne Änderungen.
- Simultanes 32-Bit- und 64-Bit-Hochleistungs-Computing.
- Verdoppelt die Anzahl der internen Register zur Performance-Steigerung.
- Erweitert den Speicheradressraum über 4 GB hinaus und ermöglicht realistische Darstellungen bei grafikintensiven Anwendungen wie 3-D-Spielen sowie Echtzeitergebnisse bei speicherintensiven Anwendungen wie Digital Media.

>> siehe Schemazeichnung S. 102:

#### AMD Athlon™ 64 Architektur

### Die wichtigsten Vorteile der AMD64 Architektur sind:

#### HyperTransport™ Technologie für I/O-Hochgeschwindigkeitskommunikation

- Ein 16-Bit Link bis zu 2000 MHz
- Bis zu 8 GB/s HyperTransport™ I/O-Bandbreite
- Bis zu 14,4 GB/s Prozessor-to-System-Gesamtbandbreite

Die HyperTransport Technologie™ trägt zur Steigerung der System-Performance bei, da diese bisherige I/O-Engpässe beseitigt, indem es die I/O-Bandbreite steigert und die I/O-Latenzzeiten senkt. Dies bedeutet eine insgesamt bessere Leistung, schnelleres Laden von Anwendungen und überragende Multimedia-Leistungen.

#### Integrierter DDR Speicher-Controller

Der integrierte Double Data Rate (DDR) Speicher-Controller reduziert wirksam eine der gravierendsten und häufigsten System-Engpässe bisheriger Plattformdesigns: die Speicherlatenz. Der integrierte DDR Speicher-Controller des AMD Athlon™ 64 Prozessors bietet folgende Vorteile:

- Performance-Zuwachs durch die direkte Verbindung des Prozessors mit dem Arbeitsspeicher: Die Speicherlatenz wird erheblich gesenkt. Dadurch wird die Performance bei vielen Anwendungen signifikant gesteigert, insbesondere bei speicherintensiven Applikationen wie Digital Media und 3-D-Spielen.
- Unterstützt DDR-Speichertechnologie für Hochleistungssysteme mit niedrigem Total Cost of Ownership und geringem Entwicklungsaufwand.
- Verwendet ECC-Absicherung für eine höhere Systemstabilität und trägt dazu bei, dass Systeme zuverlässig arbeiten.

### Merkmale und Vorteile der AMD64 Architektur

Merkmale	Vorteile
Simultane 32- und 64-Bit Computing-Fähigkeit	Anwender können je nach Wunsch 32-Bit- und/oder 64-Bit-Anwendungen und -Betriebssysteme betreiben – ohne Performance-Kompromisse
Direct-Connect-Architektur bewältigt die wahren Herausforderungen und reduziert die Engpässe von Systemarchitekturen	Erhöht die Speicherlatenz-Performance, bietet ausgewogenere Datendurchsatz und I/O, und ermöglicht erweitertes „linear symmetrical multiprocessing“
Unterstützung von bis zu drei kohärenten HyperTransport™-Links, dadurch werden Spitzenbandbreiten von bis zu 19,2 GB/s pro Prozessor möglich	Stellt beträchtliche I/O-Bandbreite für aktuelle und zukünftige Anwendungsanforderungen bereit
256 Terabyte Speicheradressraum	Schafft signifikante Performance-Vorteile für Anwendungen, bei denen große (oder zahlreiche) Datensätze im Speicher gehalten werden müssen
Skalierbar von 1 bis 8 Prozessoren über gesamte Data- oder Rechenzentren, bei identischer Hard- und Software-Infrastruktur	Ermöglicht maximale Flexibilität der IT-Infrastruktur und trägt grundlegend zum Erfolg bei
Integrierter Speicher-Controller verringert Latenzzeiten beim Speicherzugriff in SMP Serversystemen	Ermöglicht schnelle Datenverarbeitung bei verbesserter Performance und gesteigerter Produktivität
Low-Power-Prozessoren in HE (55 Watt) und EE (30 Watt) bieten kompromisslose Performance	Erhöhte Rechendichte, geringere Betriebskosten für Datacenter mit eingeschränktem Energieverbrauchsbudget

### 1.2.3 AMD Sempron™ Prozessor

Der AMD Sempron™ Prozessor wurde entwickelt, um die täglichen Bedürfnisse von Home- und Business-PC-Anwendern zu erfüllen. Dieser voll ausgestattete Prozessor bietet preisbewussten Käufern von Desktop-PC beste Performance.

## 2. Betriebssysteme

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

### 2.1 Windows

#### 2.1.1 Windows 2000

Microsoft Windows 2000, früher unter der Bezeichnung Windows NT 5.0 bekannt, wurde gegenüber Windows NT um etliche 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 4 GB Hauptspeicher und zwei Prozessoren. Windows 2000 Server ist der Nachfolger des Windows NT Server und bietet Hardware-Unterstützung für max. 4 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 8 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. auf einem 8-Prozessor-Server zwei virtuelle Server mit jeweils vier Prozessoren.

#### 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 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. Mithilfe 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

Windows 2000 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 Betriebs 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 Kerberos 5 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.

#### 2.1.2 Windows XP

Windows XP fällt sofort durch das deutlich verbesserte und klare Design auf, das auch von weniger geübten Anwendern intuitiv bedient werden kann. Neben dem neuen Design wurden jede Menge weitere Funktionen entwickelt.

Im neu gestalteten Startmenü sind die am häufigsten verwendeten Anwendungen gruppiert, sodass einfach darauf zugegriffen werden kann. Die fünf bevorzugten Programme werden zuerst angezeigt, das Standard-E-Mail-Programm sowie der Standard-Web-Browser sind jederzeit verfügbar. Zusätzlich kann mit der neuen Taskleiste-Gruppierung Ordnung in die Taskleiste gebracht werden. Geöffnete Dateien werden nun nach Anwendungen gruppiert angezeigt. Neben dem Design gibt es in Windows XP eine Reihe von weiteren Neuheiten, die den Bedienkomfort steigern. Windows erwacht viel schneller aus seiner Schlaffunktion, d.h. die Akkus des Laptops müssen nicht mehr umsonst laufen, da alle Anwendungen auf Abruf sofort wieder einsatzbereit sind. Auch mehrere Personen können nun einen PC zusammen bzw. parallel verwenden. Für jeden Benutzer wird ein eigenes Konto angelegt. Die Benutzer können schnell und einfach gewechselt werden, wobei Anwendungen der anderen Person weiterlaufen. Damit muss beispielsweise ein Download einer Datei aus dem Internet auch bei einem Benutzerwechsel nicht abgebrochen werden, denn alle geöffneten Anwendungen laufen im Hintergrund weiter.

Die Hardware-Unterstützung wurde stark verbessert. Geräte wie Digitalkamera, Scanner oder DV-Videokamera werden automatisch erkannt und alle Aufnahme-, Bearbeitungs- und Wiedergabefunktionen, die Windows XP bereitstellt, können durchgängig genutzt werden.

Die Performance wurde ebenfalls deutlich verbessert. Schon beim Einschalten des Computers wird unter Windows XP die erste Leistungssteigerung sichtbar. Nach mehreren Starts mit derselben Soft- und Hardware arrangiert Windows XP die Startdateien auf der Festplatte für einen schnellen Zugriff. Zusammen mit dem so genannten Prefetching und einem optimierten Netzwerk-Login startet das System bis zu 34 Prozent schneller als mit früheren Windows-Versionen. Dieselbe Funktion bewirkt auch ein schnelleres Starten von Programmen.

Die gesteigerte Multitaskingleistung wird u. a. gestützt durch das Nutzen von Stillstandzeiten für Systemaktivitäten, Anpassen der Benutzeroberfläche an die Möglichkeiten des Computers und eine effiziente Verwaltung des Arbeitsspeichers.

Bei Laptops helfen der Stand-by- und der Ruhezustandmodus. Im Stand-by-Modus schaltet das System Monitor, Festplatten und andere Geräte aus, versorgt aber weiterhin den Hauptspeicher, in dem die offenen Dokumente und Programme gespeichert sind. Nach dem Wiedereinschalten kann die Arbeit dort fortgesetzt werden, wo sie beendet wurde – bei neueren Laptops schon in weniger als 2 Sekunden. Versetzt man den Laptop in den Ruhezustand, so werden die Daten aus dem Hauptspeicher in komprimierter Form auf die Festplatte geschrieben und der Computer wird komplett ausgeschaltet. Das Einschalten dauert aus diesem Modus etwas länger, der Arbeitsplatz präsentiert sich dann aber wie vor dem Ruhezustand. Die in Windows 2000 eingeführten Power-Management-Funktionen wurden nochmals verbessert. Ruhezustand und Standby arbeiten nun wesentlich schneller und zuverlässiger, was Notebook-Batterien schont und mobile Laufzeiten erhöht. Windows XP erlaubt mit Remote-Desktop von überall den Zugriff auf den eigenen Computer-Desktop der Firma – mit all seinen Applikationen, Dokumenten und Netzwerkverbindungen. Über eine sichere, verschlüsselte Internet- oder Wahlverbindung kann man sich mit dem Firmen-PC verbinden und dort eine virtuelle Sitzung eröffnen, die den gewohnten Windows-Desktop auf dem entfernten Computer bereitstellt. Da alle Programme auf dem Firmen-PC laufen und lediglich Tastatur- und Mauseingaben sowie Display-Ausgaben übertragen werden, eignet sich Remote-Desktop ideal auch für Modem- oder ISDN-Verbindungen.

Funknetzwerke (etwa 802.11b/g-WLANs) unterstützt Windows XP Professional serienmäßig. Windows XP Professional erkennt und konfiguriert alles automatisch, sobald eine WLAN-Verbindung besteht oder ein Funkzellen-Roaming stattfindet. Für höchste Abhörsicherheit bei Übertragungen (sowohl in verkabelten Ethernet- als auch in Funknetzwerken) sorgen verteilte oder auf Smart-Cards gespeicherte Zertifikate sowie das 802.1X-Authentifizierungsverfahren.

Windows XP Professional erkennt Netzwerke und ihre TCP/IP-Einstellungen, sodass die Netzwerk-Connectivity des PCs automatisch besteht und auch beim Roaming erhalten bleibt. Sieht das Netzwerk keine automatische Konfiguration vor, bietet Windows XP Professional an, mit alternativen TCP/IP-Einstellungen zu arbeiten. Auf diese Weise kann ein Notebook-Benutzer im Firmennetzwerk seine TCP/IP-Konfiguration dynamisch von einem DHCP-Server beziehen und zu Hause mit statischen TCP/IP-Adressen arbeiten.

Windows XP ist eine konsequente Weiterentwicklung der bewährten Windows-2000-Technologie und arbeitet damit noch stabiler als seine Vorgängerversionen. Die neue Windows-Engine basiert auf der bewährt zuverlässigen 32-bit-Architektur von Windows 2000, die sich durch ein vollständig geschütztes Speichermodell auszeichnet. Bereits bei der Installation kann das Set-up-Programm des Betriebssystems auf Wunsch Treiber-, Kompatibilitäts- und Sicherheits-Updates über das Internet mit einbeziehen, auch wenn diese erst nach Erscheinen der Windows-XP-CD-ROM auf den Markt gekommen sind. Windows Update hält das System auf dem aktuellsten Stand. Service Packs, Problembhebungen und Treiber für neue Hardware-Geräte können mühelos, wenn gewünscht auch automatisch, von Microsoft aus dem Internet heruntergeladen werden.

Unter Windows XP läuft eine Vielzahl von Programmen, die unter Windows 2000 nicht gelaufen sind. Wenn ein Programm nur unter Windows 95 oder Windows 98 ausgeführt werden kann, kann es jetzt höchstwahrscheinlich auch unter dem neuen Betriebssystem ausgeführt werden. Sollte eine ältere Applikation von Windows XP trotzdem einmal nicht unterstützt werden, kann diese in einem speziellen Kompatibilitätsmodus ausgeführt werden, der die Charakteristika früherer Windows-Versionen aufweist.

Windows XP misst der Qualität von Gerätetreibern höchste Priorität bei, da sie maßgeblich zur System-Stabilität beiträgt. Bereits bei der Installation einer neuen Komponente wird angezeigt, ob der Treiber von Microsoft getestet und zertifiziert worden ist. Wurde ein nicht zertifizierter Treiber installiert, der nicht richtig funktioniert, kann binnen Sekunden wieder auf den früheren, funktionierenden Treiber zurückgegriffen werden. Durch das Konzept der so genannten Side-by-Side-DLLs können zusätzlich mehrere Versionen einer Komponente parallel genutzt werden, sodass jede Applikation mit der für sie am besten geeigneten arbeitet.

Sollte trotz des stark verbesserten Treiber-Handlings mal etwas schief gehen, kann man mit der Systemwiederherstellung einen früheren Zustand des PCs wieder herstellen und so alle zwischenzeitlichen Konfigurationsänderungen – selbst noch nach Wochen – rückgängig machen.

Sicherheit wird in Windows XP groß geschrieben. Sensible Dateien können verschlüsselt gespeichert werden, ebenso wie Kennwörter und Benutzernamen in speziellen Bereichen vor unberechtigten Zugriffen geschützt sind. Das verschlüsselnde Dateisystem (Encrypting File System – EFS) ermöglicht es, Dateien, die besonders sensible Informationen enthalten, verschlüsselt auf der Festplatte des PCs oder auf Netzwerk-Servern zu speichern. So werden Daten – einschließlich Offline-Ordern – zuverlässig vor Zugriffen Unbefugter geschützt. Die neue Multi-User-Unterstützung des EFS gestattet es dabei mehreren (legitimierten) Anwendern, sensible Dateien zu verschlüsseln und gemeinsam einzusehen.

Mit der in Windows XP integrierten Internet-Firewall (Internet Connection Firewall – ICF) sind Daten automatisch vor unerlaubten Zugriffen aus dem Internet geschützt. Die Funktion muss lediglich für die gewünschte DFÜ- oder LAN-Verbindung aktiviert werden. Bei allen Verschlüsselungs-Operationen verwendet Windows XP Professional 128-Bit-Schlüssel. Darüber hinaus gibt es viele weitere Sicherheitseigenschaften in Windows XP, wie beispielsweise das Kerberos V5-Authentifizierungsprotokoll, Internet Protocol Security (IPSec), zentral definierbare Sicherheitsrichtlinien und vieles mehr.

Eine Reihe von Features in Windows XP erleichtert die Installation und Administration des Betriebssystems und hilft somit, im Unternehmen Kosten für diese Aufgaben zu senken. Im Folgenden eine Auswahl der entsprechenden Features.

Für Firmen, die Windows XP Professional auf mehreren PC installieren möchten, hat Microsoft ausgereifte und erprobte Mechanismen zur automatischen Installation vorgesehen. Damit lassen sich unbeaufsichtigte Windows-XP-Installationen vorkonfigurieren, sodass der eigentliche Set-up-Prozess zuverlässig und ohne Benutzer-Interaktion ablaufen kann. Betriebssystem-Images auch für PC mit unterschiedlicher Hardware-Ausstattung lassen sich bequem erstellen und mithilfe der zu Windows 2000 kompatiblen Remote-Installationsdienste (RIS) über das Netzwerk automatisch installieren.

Für internationale Unternehmen und Bildungseinrichtungen interessant: Windows XP Professional unterstützt das Multilingual User Interface (MUI). Dabei kann ein PC gleichzeitig mit mehreren Oberflächen (englisch, deutsch, spanisch etc.) versehen werden. So erhält jeder Benutzer den Windows-Desktop in seiner bevorzugten Sprache.

Um die Ausführung unerwünschter Applikationen auf Windows-XP-Professional-PC zu verhindern, können Administratoren auf die Software-Einschränkungsrichtlinien zurückgreifen. Auf diese Weise lassen sich Arbeitsplätze auf die für das Unternehmen wichtigen Programme begrenzen.

In Ergänzung zu den bereits bei Windows 2000 vorhandenen Gruppenrichtlinien stehen bei Windows XP Professional zahlreiche neue zur Verfügung – für eine noch umfassendere, richtlinienbasierte Verwaltung über das Active Directory. Mit dem neuen Windows-XP-Professional-Tool Resultant Set of Policy (RSOP) erhalten Administratoren ein leistungsfähiges Werkzeug, um die Wirkung der verschiedenen angewandten Gruppenrichtlinien auf bestimmte Benutzer und Computer umfassend zu planen und zu überwachen. Für Anwender, die mit ihrem Notebook häufig unterwegs sind, erweisen sich die standortbezogenen Gruppenrichtlinien als überaus nützlich: Befindet sich der Anwender im Büro, kommen die Gruppenrichtlinien des Unternehmens zum Tragen. Unterwegs oder zu Hause jedoch kann der Anwender die für Einzel-PC oder in kleinen LANs nützlichen Funktionalitäten von Windows XP Professional nutzen – und zwar ohne dass hierfür eine Neukonfiguration durch einen Administrator oder den Benutzer selbst erforderlich wird.

Das USMT (User State Migration Tool) erlaubt die leichte Übernahme aller Daten und persönlicher Einstellungen eines Anwenders vom ursprünglichen System auf Windows XP. Bevorzugte Desktop-Einstellungen, Ordner-Optionen des Windows Explorers, Internet-Konfiguration und Favoriten, E-Mail-Zugang, Nachrichten, Adressbuch, Netzlaufwerke und -drucker, bestimmte Ordner etc. sind so mühelos zu übertragen.

Windows XP bietet durchgängige Unterstützung und End-to-End-Integration für alle digitalen Medien. Überspielen und Aufnehmen, Anzeigen und Wiedergeben, Archivieren und Versenden: Kontextsensitiv begleitet Windows XP durch jeden Schritt und schlägt komfortabel alle infrage kommenden Aufgaben automatisch vor. Audio, Foto und Video erschließt Windows XP wie niemals zuvor. Über separate Plugins kann der Media Player MP3-Dateien erstellen sowie DVD-Videos über den PC wiedergeben. Wird eine Digitalkamera oder Scanner mit dem PC verbunden, erkennt Windows XP diese automatisch. Windows XP erkennt, welche Dateien sich in einem Ordner befinden und zeigt nicht nur eine Miniaturansicht an, sondern schlägt die wahrscheinlichsten Aktionen für den jeweiligen Medientyp in der neuen Aufgabenleiste vor: Audiodaten, im Ordner „Eigene Musik“ etwa, werden sofort per Mausklick abgespielt.

Mit der im Hilfe- und Support-Center von Windows XP integrierten Remote Assistance können jederzeit Kollegen oder ein firmeninternes Support-Center zu Hilfe gerufen werden. Anstatt das Problem einem Spezialisten über das Telefon mit Worten zu beschreiben, kann der Experte die Lösung ferngesteuert klar und verständlich direkt auf dem eigenen Bildschirm zeigen. Wird an den helfenden Experten über die Online-Kontakte des Windows Messenger oder per E-Mail eine Einladung geschickt, so erhält dieser die Berechtigung, sich den Bildschirm

des Problem-PCs auf seinem PC anzusehen, um bei der Lösung zu helfen oder diese auf Wunsch sogar selbst durchzuführen – wobei der Anwender jeden Schritt nachvollziehen kann und zu jedem Zeitpunkt die volle Kontrolle behält. Automatisch verfällt nach Beenden der Sitzung die Remote-Unterstützungs-Berechtigung des Experten für den PC des Anwenders. In Unternehmen lassen sich durch dieses umfangreiche und zentrale Support-Werkzeug von Windows XP Support-Anfragen an das eigene Support-Center reduzieren und damit die Kosten für den Support bei Problemen mit Hard- und Software senken.

#### Windows Longhorn

Windows Longhorn wird der definitive Nachfolger von Windows XP für den Konsumentenbereich sein, ließ Microsoft verlauten. Es wird von Longhorn keine Server-Variante geben.

Bisher wurden die Betriebssysteme von Microsoft immer in zwei verschiedenen Versionen für den Client und für Server-Administratoren herausgebracht. Mit Windows 2000 startete dieser Brauch, denn schon damals war die Professional-Version für Workstations und die Server für Highend-Netzwerke und Webhosting ausgerichtet. Mit Windows XP ging man ähnliche Wege, wobei die Variante Windows Server 2003 erst nach über 14 Monaten nach der Erstveröffentlichung von XP verfügbar war.

Nun geht Microsoft mit Windows Longhorn komplett andere Wege, denn diese Version wird lediglich für Clients und Workstations optimiert werden.

Auch Schlüsselemente für die Entwickler-Plattform Windows WinFX unter Windows XP und Windows Server 2003 werden zu diesem Zeitpunkt verfügbar sein. Longhorn bietet Nutzern wesentliche Verbesserungen bei Produktivität, Weiterentwicklungen bei Sicherheit und Zuverlässigkeit sowie wichtige neue Möglichkeiten für Software-Entwickler.

Der Nachfolger mit dem Codenamen Blackcomb soll lediglich auf Server- und Highend-Systemen zum Einsatz kommen.

Aktuellen Informationen zufolge bleibt Microsoft bei seinem Longhorn-Termin, welcher das neue Client-Betriebssystem auf Anfang 2006 plant.

#### 2.1.3 Windows Server 2003

Seit April 2003 ist der neue Microsoft Windows Server 2003 verfügbar. Gegenüber dem Windows 2000 Server wurden viele Eigenschaften und Funktionen weiter- bzw. neu entwickelt. Folgende Versionen sind verfügbar:

##### Windows Server 2003, Standard Edition

- Zweifache symmetrische Multiprozessorverarbeitung (Symmetric Multiprocessing, SMP)
- 4 GB Arbeitsspeicher

### Windows Server 2003, Enterprise Edition

- Achtfache symmetrische Multiprozessorverarbeitung (Symmetric Multiprocessing, SMP)
- Clustering mit bis zu acht Knoten
- 32 GB RAM in 32-Bit-Versionen und 64 GB RAM in 64-Bit-Versionen
- Hot Add Memory
- Non-Uniform Memory Access (NUMA)

### Windows Server 2003, Datacenter Edition

- 32fache symmetrische Multiprozessorverarbeitung (Symmetric Multiprocessing, SMP)
- 64 GB Arbeitsspeicher in 32-Bit-Versionen und 128 GB RAM in 64-Bit-Versionen
- Windows Sockets: Direktzugriff für SANs

Diese Version ist nur über das Windows Datacenter-Programm erhältlich, das ein Paket aus Hardware, Software und Dienstleistungen bietet.

### Windows Server 2003, Web Edition

- Zweifache symmetrische Multiprozessorverarbeitung (Symmetric Multiprocessing, SMP)
  - 2 GB Arbeitsspeicher
  - Windows Server 2003, Web Edition ist speziell auf den Einsatz als Web-Server ausgerichtet. Server mit diesem Betriebssystem können Mitglied einer Active Directory-Domäne sein, den Active Directory-Dienst jedoch selbst nicht anbieten.
- Diese Version ist nur über spezielle Partner verfügbar.

## Die wichtigsten Features von Windows Server 2003 in der Übersicht:

### XML-Webdienste

Die XML-Webdienste enthalten wiederverwendbare, auf Industrie-standards basierende Komponenten, die Funktionen von anderen Anwendungen aufrufen – unabhängig von dem Verfahren, mit dem die Anwendungen erstellt wurden, ihrem Betriebssystem oder ihrer Plattform oder den Geräten, mit denen auf sie zugegriffen wird. Die IIS 6.0-Sicherheitseinstellungen sind bei der Installation gesperrt, damit nur die erforderlichen Dienste ausgeführt werden können. Über den Lockdown-Assistenten für die IIS-Sicherheit wird die Serverfunktionalität je nach den Anforderungen des Administrators aktiviert oder deaktiviert.

### Verzeichnisdienste

Active-Directory-Sicherheitseinstellungen für Benutzer und Netzwerk-Ressourcen umfassen das gesamte Netzwerk und tragen zu einem sicheren End-to-End-Netzwerk bei. Dank einer effizienteren Synchronisation und

Replikation sowie der Zwischenspeicherung von Anmelde-Informationen in Zweigstellen-Domänencontrollern ist Active Directory nun selbst bei unzuverlässigen WAN-Verbindungen schneller und stabiler.

### Aktualisierungsverwaltung

Die automatische Aktualisierung bietet die Möglichkeit zum systematischen Herunterladen wichtiger Betriebssystemaktualisierungen, wie etwa Sicherheits-Updates und Patches. Administratoren können wählen, wann diese wichtigen Betriebssystemaktualisierungen stattfinden sollen.

### Internet-Firewall

Die Internet-Firewall des Servers macht die Verbindung zum Internet sicherer.

### Serverhardware-Unterstützung

Spezielle Tools testen neue Gerätetreiber, um den korrekten Betrieb des Servers sicherzustellen.

### Anwendungsprüfung

Anwendungen, die auf Windows Server 2003 ausgeführt werden, lassen sich zuvor testen, beispielsweise auf Beschädigung des Anwendungsspeichers (Heap) und auf Kompatibilität.

### Nachverfolgen von Server-Events

Mithilfe der neuen Protokollierung können Administratoren die Betriebszeit genau aufzeichnen. Sie schreibt die Windows-Ereignisse beim Herunterfahren des Servers in eine Protokolldatei.

### Serverkonfigurationsassistent

Der Serverkonfigurationsassistent führt Administratoren schrittweise durch das Einrichten verschiedener Server-Typen wie zum Beispiel Dateiserver, Druckserver oder Remote-Zugriffsserver. Das stellt sicher, dass die jeweiligen Komponenten von Anfang an richtig installiert und konfiguriert werden.

### Serververwaltungsassistent

Der Serververwaltungsassistent bietet eine Schnittstelle für die fortlaufende Verwaltung des Servers an und erleichtert allgemeine Aufgaben, wie das Hinzufügen neuer Netzwerkteilnehmer und das Entwickeln von Freigaben.

### Remote-Server-Verwaltung

Mit dem Remote-Desktop für Verwaltung (früher bekannt als Terminaldienste im Remote-Verwaltungsmodus) können Administratoren einen Computer über praktisch jeden anderen Rechner im Netzwerk verwalten.

### Schattenkopie

Diese Funktion ermöglicht zeitgesteuerte Netzwerkfreigaben. Administratoren können mit ihrer Hilfe den Inhalt der Netzwerkverzeichnisse sichern und sich auch später noch über den Zustand der Ordner zu diesem Zeitpunkt informieren. Desktop-Nutzer können versehentlich gelöschte Dateien oder Ordner auf Netzwerkfreigaben wiederherstellen, ohne dass der Systemadministrator eingreifen muss.

### Terminalserver

Der Terminalserver gestattet, dass ein Nutzer auf Programme zugreifen kann, die auf dem Server ausgeführt werden. Der Nutzer kann beispielsweise auf einen virtuellen Windows-XP-Professional-Desktop und x86-basierte Windows-Anwendungen zugreifen, auch wenn seine Hardware diese Programme nicht lokal ausführen kann. Der Terminalserver bietet diese Möglichkeit sowohl für Windows- als auch für nicht Windows-basierte Clientgeräte.

### Zusätzliche Funktionen der Enterprise Edition

Clusterdienst: Der Clusterdienst bei Windows Server 2003, Enterprise Edition und bei Datacenter Edition unterstützt Cluster mit bis zu acht Clusterknoten. Dies steigert die Flexibilität beim Hinzufügen und Entfernen von Hardware in einer geografisch verteilten Clusterumgebung. Verbesserte Skalierungsoptionen ergänzen die Clusterverwaltung. Möglich sind verschiedene Clusterkonfigurationen mit zugewiesenem Speicher:

- Mehrclusterkonfigurationen in einem Speichernetzwerk (Storage Area Network, SAN)
- Mehrere Sites überspannende, geografisch verteilte Cluster

### Metadirectory-Dienste

Mithilfe von Microsoft Metadirectory Services (MMS) können Unternehmen persönliche Daten aus mehreren Verzeichnissen, Datenbanken und Dateien in Active Directory integrieren. MMS ermöglicht es, persönliche Daten in einer einheitlichen Ansicht anzubieten, Geschäftsprozesse in MMS zu integrieren und persönliche Daten organisationsübergreifend zu synchronisieren.

### Hot Add Memory

Dieses Merkmal ermöglicht das Erweitern des Arbeitsspeichers des Computers für Betriebssystem und Anwendungen während des laufenden Betriebs. Ein Neustart des Servers ist dabei nicht erforderlich, sodass keine Ausfallzeiten entstehen. Hot Add Memory ist derzeit nur bei Servern möglich, die über die entsprechenden Hardwareunterstützung verfügen.

### Non-Uniform Memory Access (NUMA)

Die Firmware des Systems kann eine Tabelle namens Static Resource

Affinity Table erzeugen, die die so genannte NUMA-Topologie des Systems beschreibt. Mithilfe dieser Tabelle kann Windows Server 2003, Enterprise Edition NUMA auf Anwendungsprozesse anwenden, ebenso wie Standard-Affinitätseinstellungen, Threadplanung und Speicherverwaltungsfeatures. Außerdem werden die Topologie-Informationen Anwendungen zur Verfügung gestellt, die NUMA-APIs nutzen.

### Session-Verzeichnis für Terminal-Dienste

Diese Lastenausgleichsfunktion erlaubt es Nutzern einer unterbrochenen Terminal-Verbindung, die getrennte Session wieder aufzunehmen. Dieses Merkmal ist mit dem Lastenausgleich von Windows Server 2003 kompatibel und wird von entsprechenden Produkten von Drittanbietern unterstützt.

Die zusätzlichen Funktionen der Datacenter-Version umfassen einen erweiterten physikalischen Speicher: Auf Intel-Plattformen mit 32-Bit-Architektur unterstützt Windows Server 2003, Datacenter Edition die physikalische Adresserweiterung (Physical Address Extension, PAE). Sie erhöht die Kapazität des Arbeitsspeichers auf 64 GB. Auf Intel-Plattformen mit 64-Bit-Architektur erhöht sich die Speicherunterstützung auf ein Maximum von 16 Terabyte.

### Windows Sockets: Direktzugriff für SANs

Mithilfe dieses Leistungsmerkmals können Windows Sockets-Anwendungen auf TCP/IP-Basis die Leistungsvorteile von Speichernetzen (System Area Networks, SANs) ohne eine spezielle Änderung nutzen. Der Grundbaustein dieser Technologie ist ein mehrschichtiger Windows Socket-Dienst, der TCP/IP über systemeigene SAN-Dienste emuliert.

### 2.1.4 Windows Small Business Server 2003

Der Windows Small Business Server 2003 ist eine Serverlösung, die kleinen und mittelständischen Unternehmen Features wie z. B. E-Mail, sichere Internet-Konnektivität, geschäftliche Intranets, Remote-Zugriff, Unterstützung für mobile Geräte, sowie eine Anwendungsplattform zur Zusammenarbeit bietet. Windows Small Business Server 2003 ist so benutzerfreundlich, dass er die Netzwerkkonfiguration und die Serverinstallation praktisch von selbst durchführt. Windows Small Business Server 2003, eine Entwicklung der vierten Generation, verbindet das Betriebssystem Microsoft Windows Server™ 2003 als Kernsystem mit Microsoft Exchange Server 2003 und Microsoft Windows® Share-Point™ Services. Mit dieser Kombination von Technologien und durch die Verbindung innovativer Verwaltungstools sind kleine und mittelständische Unternehmen in der Lage, eine schnellere und effizientere Geschäftsumgebung aufzubauen. Der Windows Small Business Server 2003 wird in zwei Versionen angeboten.

### Die Standard Edition enthält:

- Windows Server 2003
- Exchange Server 2003
- Outlook 2003
- Windows SharePoint Services

### In der Premium Edition sind zusätzlich enthalten:

- FrontPage 2003
- SQL Server 2000 SP3
- ISA Server

Die wesentliche Eigenschaften des Windows Small Business Servers 2003 werden im Folgenden kurz vorgestellt.

### E-Mail, Networking und Internet-Konnektivität

Mit Windows Small Business Server 2003 verfügt ein Unternehmen über alles, was zur effektiven Nutzung des Internets benötigt wird. Er bietet eine einfach zu verwaltende Lösung für einen gemeinsamen Internet-zugriff, eine Firewall um das lokale Netzwerk zu schützen, Internet-E-Mail basierend auf dem Exchange Server und Produktivitätstools, wie z. B. Microsoft Outlook® Web Access und Remote Web Workplace.

## 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.

## Linux

Linux ist ein frei verfügbares Multitasking- und Multiuser-Betriebssystem. Es 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 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.

Linux kann auf zwei verschiedene Arten bezogen werden: Alle benötigten Teile lassen sich kostenlos aus dem Internet laden. 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 beigefügten 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.

Neben ihren Distributionen für PC und Workstations bieten sowohl SUSE als auch Red Hat für den Serverbetrieb spezielle Pakete an. Bei SUSE sind dies der SUSE Linux Enterprise Server und der SUSE Linux Standard Server. Neben der Zusammenstellung der Pakete speziell für den Serverbetrieb unterscheiden sie sich noch durch die folgenden Punkte von der normalen Distribution: Zum einen führt SUSE umfangreiche Tests durch, um die Kompatibilität der einzelnen Pakete untereinander und mit wichtigen Businessanwendungen zu gewährleisten. Außerdem garantiert SUSE den Support für das Paket auch nach der Abkün-

digung der jeweiligen Version, und zwar bis zu zwei Jahre. Für das Businessumfeld ebenso wichtig ist die Bereitstellung wichtiger Patches und Updates.

### SUSE LINUX Enterprise Server

Der SUSE LINUX Enterprise Server ist eines der führenden Server-Betriebssysteme für den professionellen Einsatz in heterogenen IT-Umgebungen aller Größen und Ausrichtungen. Er ist für alle relevanten Hardwareplattformen verfügbar: für die 32- und 64-Bit-Prozessoren von AMD und Intel, wie auch für die gesamte eServer-Reihe von IBM, inklusive Mainframes.

Der SUSE LINUX Enterprise Server kann für alle unternehmensrelevanten Server- und Netzwerkdienste eingesetzt werden: von Datei-, Druck-, Web- und Security-, bis hin zu Applikations- und Middleware-Lösungen insbesondere für Server mit hoher Verfügbarkeit, unternehmenswichtigen Daten und Netzwerkdiensten. Ein einziges Server-Betriebssystem mit einer einheitlichen Linux-Codebasis!

### Vorteile

- Massive Kostenersparnis
- Erhöhte Investitionssicherheit durch System-Pflege und offenen Sourcecode
- Mehr Skalierbarkeit und Stabilität
- High Performance Cluster
- High Availability Cluster

### SUSE LINUX Standard Server

Der vollständig grafisch administrierbare SUSE LINUX Standard Server richtet sich an kleine Organisationen und Abteilungen, die künftig ihren Internet-Zugang wie auch E-Mail-, Druck- und Dateidienste verlässlich und sicher realisieren möchten. Der Standard Server ist verfügbar für AMD- und Intel-32-Bit Prozessoren (x86) und unterstützt bis zu zwei CPUs. Mit im Paket enthalten sind Support sowie Wartung durch das SUSE Maintenance Programm.

Für die Einrichtung und Verwaltung des SUSE LINUX Standard Server ist nunmehr nur noch die Kenntnis von Netzwerkadresse, der Informationen des Internetproviders und des Firmen- bzw. Benutzernamens notwendig. Der grafisch konfigurierbare Internet-Zugang bietet auch die Möglichkeit des Zwischenspeicherns und Filterns von Web-Inhalten, was die Sicherheit erhöht und Provider-Kosten spart.

Komplett bearbeitet und erheblich verbessert wurde die Vergabe und Verwaltung von Datei- und Benutzerrechten. Benutzerdaten werden beim SUSE LINUX Standard Server in einem zentralen Verzeichnisdienst (LDAP) verwaltet. Die Sicherheit von Daten wurde durch eine detailliertere Rechteverwaltung mittels so genannter Access Control Lists (ACL) erhöht. Mit dem SUSE LINUX Standard Server können diese auch von

entfernten Rechnern aus über eine Web-Oberfläche einfach und schnell eingerichtet und verändert werden.

Über grafische Konfigurationshelfer (Wizards) sind die Serverdienste anwenderfreundlich konfigurierbar: So zum Beispiel der Einsatz als Windows-Domänen-Controller, als File- und Printserver in Windows-Umgebungen oder als Internet-Zugangsserver und Namens-Server (DNS). Zudem ist beim SUSE LINUX Standard Server auch ein vollständiger E-Mail-Server für kleine Organisationen integriert. Client-Rechner lassen sich einfach und schnell an den SUSE LINUX Standard Server anbinden. Die automatische Vergabe von Netzwerk IP-Adressen (DHCP) kann vollständig grafisch konfiguriert werden. Windows-Domänen-Accounts werden automatisch angelegt. Außendienstmitarbeiter können so über einen sicheren Zugang via VPN auf Firmendaten zugreifen.

Der SUSE LINUX Standard Server enthält neben den zahlreichen Serverdiensten für die sichere und effiziente Nutzung des Internets, den Diensten für Datei- und Druckdienste unter Windows und Unix auch die Möglichkeit für den Einsatz als Applikations-Server. Damit erhalten kleinere Organisationen und Abteilungen ein universelles Server-Betriebssystem für den Aufbau leistungsfähiger Intranets und eine zuverlässige Basis für den Betrieb von Client-Server-Applikationen.

Des Weiteren bietet SUSE fertige Pakete für spezielle Einsatzzwecke, wie z. B. E-Mail-Server oder Firewall an.

Die Entwicklung dieser Pakete spiegelt den allgemeinen Trend wider: Linux kommt immer mehr auch in kommerziellen Systemen zum Einsatz und bietet hier für viele Einsatzzwecke eine kostengünstige und zuverlässige Basis.

## 2.3 Computerviren / Virenarten

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

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

### Dateiviren

Dateiviren hängen 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 Programm-

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

transtec empfiehlt, Systeme mittels geeigneter Virensoftware ständig zu überprüfen. So können massive Schäden im Vorfeld vermieden werden.

## 3. Cluster

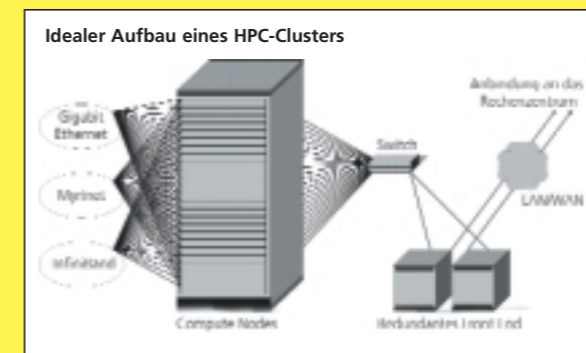
### 3.1 High Performance Computing Cluster

Klassischerweise sind im Bereich der Großrechner (High Performance Computing, HPC) verschiedene Mainframe-Lösungen anzutreffen. Aufgrund ihres sehr viel besseren Preis-Leistungs-Verhältnisses haben sich aber in den letzten Jahren HPC-Cluster auf IA32/IA64-Basis einen nennenswerten Marktanteil erarbeiten können.

#### Der Einsatz eines Großrechners wird üblicherweise aus drei Gründen erwogen:

- Das Problem ist auf Einzelsystemen aufgrund seiner Komplexität prinzipiell nicht lösbar.
- Der Nutzer möchte das Ergebnis mit einer höheren Genauigkeit berechnen.
- Der Anwender möchte Zeit sparen und schneller zum Ergebnis kommen.

Neben dem Preisvorteil spricht auch die gute Skalierbarkeit und die einfache Verwaltung für einen HPC-Cluster als Alternative.



Aus der Sicht des Anwenders besteht ein Cluster aus einer Software-schnittstelle, die seine Applikation auf die Ressourcen verteilt. Diese auch Middleware genannten Programme setzen auf dem Betriebssystem auf. Über ein dediziertes Netzwerk werden die Rechenjobs dann auf die Prozessoren verteilt.

Der Verwaltungsrechner (Front-End) administriert die über ein privates Netzwerk zu erreichenden Rechenknoten (Compute Node). Diese leisten die eigentliche Arbeit und liefern ihre Teilergebnisse wieder an das Front-End. In der Regel kommt preiswerte COTS-Hardware (Common Off The Shelf) zum Einsatz. Die Anzahl der Knoten liegt in der Praxis bei 8 bis 256, sie kann durchaus aber auch in die Tausende gehen. Die Aufgabe des Front End ist es, die Aufträge der Nutzer in einer Warteschlange zu verwalten, die Knoten mit Jobs zu versorgen, die

Ergebnisse nach Eingang zu archivieren und den Betriebszustand der Knoten zu überwachen. Die Managementsoftware ermöglicht es dem Administrator darüber hinaus, defekte Knoten schnell zu ersetzen oder bei Bedarf den Cluster zu erweitern.

Der Ausfall des Front-End führt zu einem Totalausfall der Clusters. Daher sollte es über ein redundantes Netzteil verfügen, über eine USV angeschlossen sein, die Bootfestplatte sollte gespiegelt im RAID 1 vorhanden sein und der Datenbestand ist auf mehrere Festplatten im RAID 5 zu verteilen.

Die Anzahl und Ausführung der Knoten sowie der Netzwerktyp bestimmen die Leistung des Clusters. Zur Optimierung für eine bestimmte Applikation werden verschiedene Architekturen überprüft. Bei den Prozessorvarianten sollte speziell die Intel Xeon EM64T mit der AMD Opteron CPU verglichen werden. Der Hauptspeicher ist so groß zu wählen, dass ein Swappen unterbleibt. Die Geschwindigkeitsanforderungen an die örtlich in den Knoten verbaute Festplatte werden häufig schon von SATA Festplatten erfüllt.

Ein Cluster kann sowohl im Batch- als auch im Parallelbetrieb eingesetzt werden. Im ersten Fall läuft auf allen Knoten das gleiche Programm, beispielsweise ein Raytracer. Vom Front-End werden unterschiedliche Aufgaben oder Startwerte an die Knoten geliefert. Nach der Bearbeitung durch die Rechenknoten gehen die Ergebnisse zurück zum Front-End, welches diese nach einer kurzen Plausibilitätsprüfung aktiviert. Sofort nach dem Ergebniseingang wird die nächste Aufgabe verschickt. Bei der Berechnung eines Spielfilms arbeitet ein Cluster beispielsweise in der Regel im Batchbetrieb. Jeder Knoten berechnet ein anderes Teilbild. Ein Datenaustausch mit anderen Bildern des Films ist nicht nötig. Je mehr Knoten an dem Rechenjob beteiligt sind, umso eher ist der Film fertig.

Im Parallelbetrieb rechnen die Compute-Nodes gleichzeitig an einem gemeinsamen Endergebnis. In diesem Fall muss eine Ergebnisabstimmung untereinander vorgenommen werden, die Daten müssen synchronisiert werden. Im Gegensatz zu einem Mainframe, der als SMP-System (Symmetric Multi Processor) ein zentrales Shared-Memory aufweist, verfügt ein HPC-Cluster über örtlich in den Rechenknoten verteilten Speicher. Um bei einem Betrieb im Parallelmodus trotzdem einen schnellen Zugriff auf die Daten in einem benachbarten Speicherbereich zu erreichen, ist ein leistungsfähiges Netzwerk notwendig.

Das Angebot der Netzwerkkarten hierfür ist breit gefächert. Gigabit-Ethernet ist inzwischen in der Regel standardmäßig bei den Knoten enthalten, lediglich die Kosten eines GigE Switch sind noch deutlich höher als die im 100-MBit/s-Bereich. Für einen Parallelbetrieb im Höchstleistungssegment ist aber die Latenz dieser Technik, die Koordinierungszeit bis zum Beginn der Datenübertragung, oft zu groß. Bis zum Faktor 10



schneller sind hier InfiniBand sowie Myrinet, SCI Dolphin oder Quadrics Netzwerke. Dies wird neben einer optimierten Hardware durch den Einsatz eines proprietären Protokolls erreicht. Welcher der Techniken der Vorzug zu geben ist, muss im Einzelfall geklärt werden. Hilfreich ist ein Vergleich von experimentellen Resultaten im Rahmen einer Testumgebung. InfiniBand weist üblicherweise das beste Preis-Leistungs-Verhältnis auf.

Ein extremer Knotenausbau zur Leistungssteigerung im Parallelbetrieb ist in aller Regel sinnlos. Der Speed-up, also der Zugewinn an Leistung, ist abhängig vom Grad der Parallelisierung der Applikation. Erreicht der Cluster beispielsweise bei 10 Knoten die neunfache Geschwindigkeit eines einzelnen Knotens, hat der Speed-up den Faktor 9. Die gleiche Applikation würde beim Einsatz von 100 Knoten nur die 48fache Einzelknotengeschwindigkeit erreichen.

Bei der Einrichtung und Konfiguration des Betriebssystems auf dem Cluster können verschiedene Wege gewählt werden. Typischerweise werden Cluster mit Linux betrieben. Der Einsatz von Windows ist unüblich und erfordert spezielle Kenntnisse. Eine Windows-Version speziell für HPC-Cluster hat Microsoft für das 2. Quartal 2005 angekündigt. Die Wahl der Linux-Distribution hängt von den Präferenzen des Administrators ab. Die klassische Version ist die lokale Installation des Betriebssystems sowohl auf dem Front-End als auch auf den Knoten. Nachteilig kann bei dieser Lösung der erhöhte Verwaltungsaufwand sein. Soll beispielsweise das Betriebssystem gepflegt werden, so ist das Kernel-Update einzeln auf allen Knoten durchzuführen.

Die Alternative ist eine Installation nach dem Boot-from-LAN-Konzept. Hierbei werden die jeweiligen Images auf dem Front-End abgelegt, welche beim Booten über die Netzwerkkarte in den Hauptspeicher geladen werden. Die örtliche Festplatte dient in der Folge nur noch zum Auslagern von Zwischenergebnissen.

Empfehlenswert ist der Aufbau eines HPC-Clusters in 19-Zoll-Technik. Die Packungsdichte steigt von 0,5 CPU/HE bei Standardgehäusen auf bis zu 2 CPU/HE. Darüber hinaus kann die Kühlung der Knoten verbessert werden und eine Wartung wird erleichtert. Bladesysteme steigern die Packungsdichte auf 4 CPU/HE. Die Abwärme eines Clusters ist nicht zu unterschätzen. Bei 40 Dual-CPU-Knoten mit jeweils 250 Watt werden beispielsweise 10 kW pro 19-Zoll-Rack erreicht. Ein zuverlässiger Betrieb ist oft nur zusammen mit einer Klimaanlage möglich. Wirtschaftlich interessant ist der Einsatz von vollständig wassergekühlten Serverracks.

Der Ausfall eines Rechenknotens ist in der Regel unkritisch. Er vermindert die Clusterleistung im Verhältnis zur Gesamtknotenanzahl. Meist kann daher auf einen Vor-Ort-Service verzichtet werden, was die Anschaffungskosten verringert. Der Tausch defekter Knoten ist leicht vom

Administrator selbst vorzunehmen. Analog dazu ist auch ein späterer Ausbau ohne Probleme zu bewerkstelligen. Zusätzliche Knoten müssen nicht einmal zwingend die gleiche Performance aufweisen. Bei einem im Batchbetrieb genutzten System wird die native Mehrleistung verlustlos integriert. Im Parallelbetrieb wird ein schnellerer Knoten in der Praxis nicht mit der vollen Leistung, sondern lediglich mit der Effektivgeschwindigkeit arbeiten, die der langsamste Knoten der Anlage aufweist. In der Praxis wird der Administrator in diesem Fall daher eher Subcluster definieren, die in sich einheitlich in der Leistung sind.

HPC-Cluster werden inzwischen vielfältig eingesetzt. Typische Beispiele sind die Crashtest-Simulation, die Strömungsberechnung, die Arzneimittelforschung, Datamining im Bank- und Versicherungsgewerbe, Meteorologie, 3-D-Animation, astronomische Berechnungen, wissenschaftliche Analysen, Simulation von Personen- oder Kfz-Verkehr oder die Erstellung von Filmsequenzen. Aufgrund der Stabilität der Lösung und der ausgereiften Technik werden HPC-Cluster in der Zukunft sicher verstärkt zum Einsatz kommen.

**Weiterführende Informationen finden Sie im HPC Whitepaper der transtec AG.**

### 3.2 High-Availability-Cluster

Ein High-Availability-Cluster (HA) 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 aller Regel alle Server in einem Cluster dieselbe Architektur besitzen und unter der gleichen Version des gleichen Betriebssystems laufen.

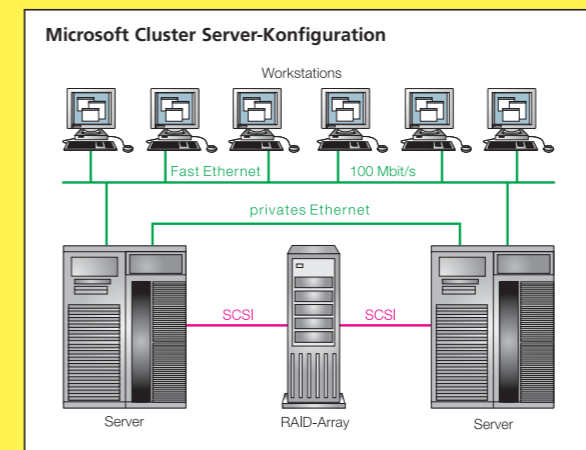
Obwohl es verschiedene Möglichkeiten gibt, wie Cluster aufgebaut sein können, bieten alle die folgenden drei Vorteile:

- 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. Web-Server, 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 Redundanz bei 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 einen einfachen HA-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 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 einen Cluster zu erstellen um 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 sichern 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, einen einzelnen Cluster anstatt der entsprechenden Anzahl unverbundener Server-Systeme zu verwalten.

Die Lastverteilung zwischen den einzelnen Cluster-Servern ist betriebssystemabhängig. Sowohl Unix- als auch Open-VMS-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 Datacenter 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.

#### Hochverfügbarkeits-Cluster mit Linux Failsafe

Die Linux-Failsafe-Clustersoftware ist ein universelles, frei konfigurierbares und fehlertolerantes Hochverfügbarkeitssystem, mit dem einzelne Dienste (Services) redundant aufgebaut werden können. Mithilfe dieser Software kann ein Dienst im Fehlerfall automatisch oder manuell auf einen anderen Node (Server) migriert werden. Ein Fehler muss nicht unbedingt in defekter Hardware liegen: Applikationsfehler, desolante Prozesse und kritische Systemzustände werden ebenfalls als solche erkannt und entsprechend behandelt. Die einzelnen Nodes des Clusters müssen in den meisten Fällen 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 eine Verfügbarkeit von 99,999 Prozent und mehr realisierbar.

## 4. Speicherbusse

## 5. Festplatten und RAID

## 6. Speichernetzwerke

### 6.1 Storage Area Networks

Seit Einführung des ersten IBM-PCs am 12. August 1981 wurden Mainframe-Lösungen zunehmend durch günstigere dezentrale Server und Arbeitsplatzrechner ersetzt. Diese verwalten zumeist nur eine Applikation, die über das SCSI-Protokoll auf lokalen Speicher zurückgreift und über Ethernet mehrere Clients versorgt.

Seit Ende der 90er Jahre machte sich jedoch ein gegenteiliger Trend bemerkbar. Durch die Vielzahl an Serversystemen wurde die immer aufwändigere Verwaltung und zunehmende Komplexität zunehmend zum Engpass für die IT-Abteilungen. Auch ist die dem aktuellen Unternehmensbedarf angepasste, dynamische Nutzung von CPU- und Speicherressourcen nur sehr eingeschränkt möglich.

Die Entwicklung zentraler Speichersysteme und eines effektiveren Protokolls als SCSI gehen zurück auf das Jahr 1988, als Fibre Channel (FC) vom ANSI (American National Standards Institute) erstmals als Norm definiert wurden. Doch es sollte noch ein Jahrzehnt dauern, bis Speichernetzwerke auf FC-Basis eine breite Marktdurchdringung erreichten und als Mainstream-Technologie angesehen werden konnten. Im Wesentlichen haben zwei internationale Organisationen die Standardisierung und Verbreitung von SANs vorangetrieben:

- Storage Networking Industry Association (SNIA)  
www.snia.org  
www.snia-europe.org
- Fibre Channel Industry Association (FCIA)  
www.fibrechannel.org

Grundlage der Speicherzentralisierung wurden die Storage Area Networks (SAN) – ein sekundäres Hochgeschwindigkeits-Netzwerk über das Server und zentrale Speichersysteme kommunizieren und welches parallel zu einem LAN für den Client-Server-Datentransfer existiert.

Der Übergang von serverzentrierter zu speicherzentrierter Infrastruktur erfordert grundlegend neue Ansätze für Hochverfügbarkeit und Datensicherheit in den Unternehmen. Denn ein Ausfall betrifft nicht länger einen einzelnen Server und dessen Anwendungen, sondern mehrere Server und deren Applikationen gleichzeitig. In der Folge werden klassische Mainframe-Features wie redundant ausgelegte Speichersysteme und Datenpfade, zeitpunktgesteuerte Datenkopien (Snapshots) sowie synchrone/asynchrone Replikation in die Open-Systems-Welt übernommen.

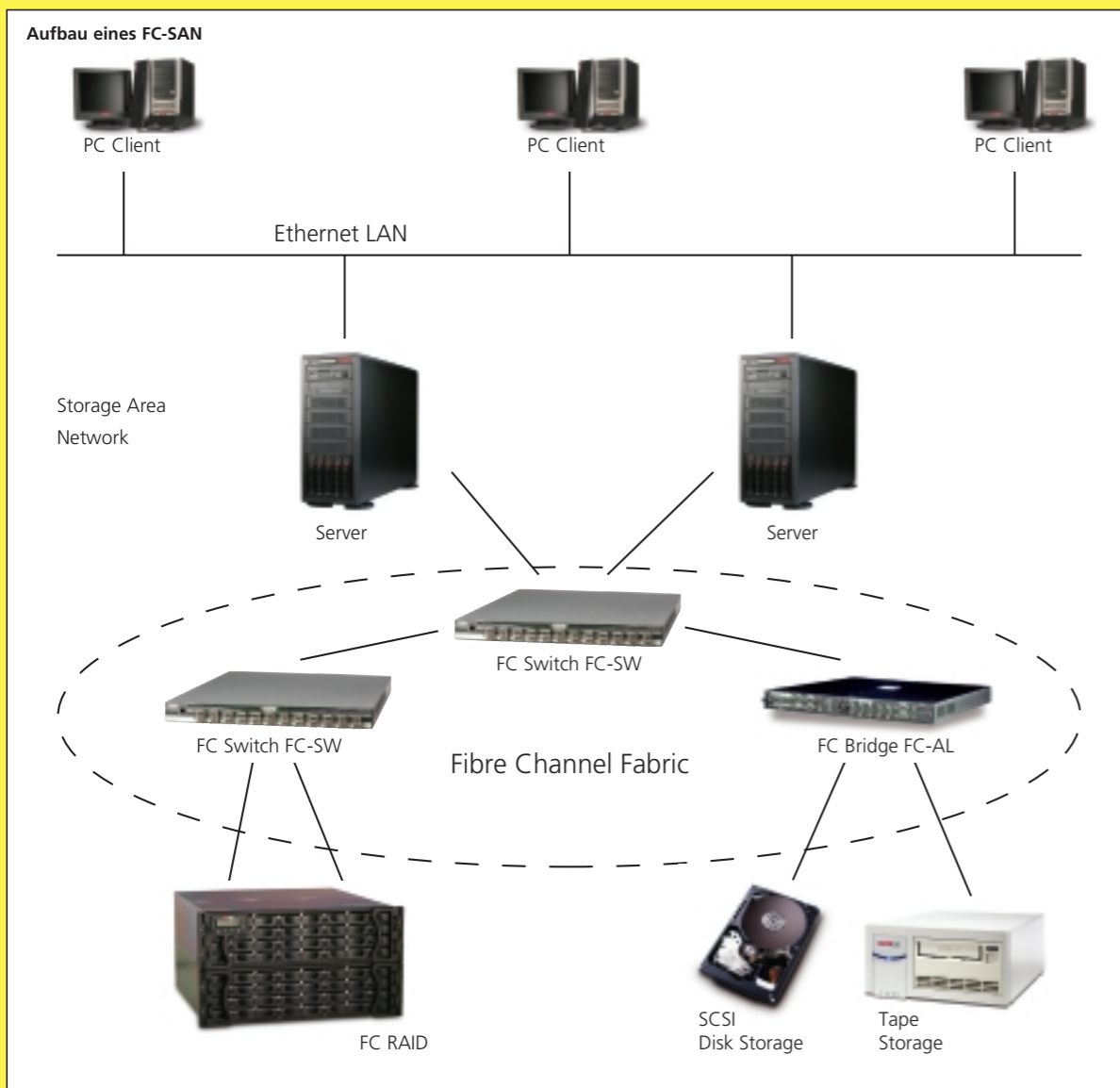
Doch die Einführung der SANs geht nicht ohne Probleme vonstatten. Dem Anwender werden nicht nur eine sehr hohe Performance in Aussicht gestellt, sondern auch gemeinsame Nutzung und flexible Zuweisung der Speicherressourcen unter den Serversystemen, sowie eine weniger aufwändige Verwaltung. Einige dieser Versprechen sind inzwischen Realität. Die höhere Bandbreite und I/O-Leistung von FC-Speichersystemen sind unumstritten. Studien von Marktforschern wie IDC und Gartner belegen regelmäßig, dass IT-Administratoren nach Einführung eines SANs bis zu siebenmal mehr Speicher verwalten können. Außerdem ist die Beschleunigung der Datensicherung und die Entlastung des LANs durch FC-Netzwerke ein höchst willkommener Nebeneffekt.

Desillusionierend war jedoch die Realität in Hinsicht auf Flexibilität und Verwaltung. Die automatisierte, dynamische Zuweisung von Speicherressourcen wurde erst mit zunehmender Marktreife der Virtualisierungslösungen in den vergangenen zwei Jahren möglich. Die gemeinsame Nutzung eines logischen SAN-Volumens durch mehrere nicht gedockte Server bleibt auch heute noch eine Herausforderung. Mangelnde Kompatibilität von Standardprodukten, zahlreiche proprietäre Lösungen sowie fehlende Standards für die Verwaltung waren gang und gäbe für FC-SANs.

Doch die mangelnde Interoperabilität ist auch durch Anwenderdruck heute weitestgehend überwunden. Proprietäre Lösungen beschränken sich nur noch auf die hochpreisigen Enterprise-Speichersysteme von Anbietern wie EMC, IBM oder Hitachi. Zudem wurde im April 2003 die SMI-S 1.0 Spezifikation (früher als BlueFin bekannt) von der SNIA verabschiedet und von der IT-Industrie akzeptiert, sodass nun auch ein Standard für die Verwaltung der Speichersysteme vorliegt. Des Weiteren wurde mit iSCSI ein Standard für günstigere, ethernetbasierende Speichernetzwerke definiert. Die Geschichte der SANs wird sich weiter entwickeln, und man darf auf die Fortschritte der nächsten Jahre gespannt sein.

>> siehe Schemazeichnung S. 118:

#### Aufbau eines FC-SAN



## 6.2 Fibre Channel

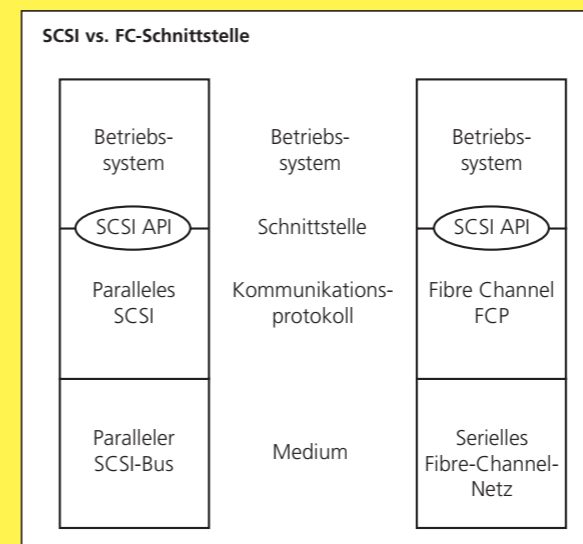
### 6.2.1 Fibre-Channel-Grundlagen

Fibre Channel (FC) ist die allgemeine Bezeichnung für eine Normenreihe, die vom ANSI 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:

- Hochgeschwindigkeitsübertragung großer Datenmengen
- Abspaltung des logischen Protokolls von der physischen Schnittstelle
- Neudefinition und Implementierung von Schnittstellen
- Implementierung unterschiedlicher Protokolle und nach Möglichkeit deren gleichzeitige Übertragung auf demselben Unterbau
- Vereinheitlichung der Schnittstellen und Reduktion der Anzahl der Schnittstellenformate

Für bitparallele Signalübertragung macht sich bei hohen Taktraten nachfolgend beschriebene Herausforderung zunehmend bemerkbar. Signale, die am Sender gleichzeitig auslaufen, müssen auch beim Empfänger nahezu gleichzeitig ankommen, was bei steigenden Übertragungsraten zunehmend problematisch wird. Serieller Datentransport hat keine solche Beschränkung der Phasenverschiebung. Daher war es für eine Hochgeschwindigkeitsübertragung von Daten nahe liegend, die SCSI-Befehlsätze auf ein serielles Interface aufzusetzen um u. a. das Problem der Phasenverschiebung zu lösen.

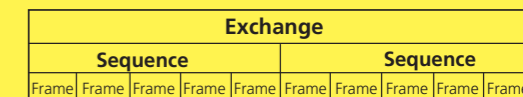


FC stellt daher nur eine Protokollschnittstelle auf serieller Hardware zur Verfügung, um andere Protokolle – primär SCSI, aber auch IPI-3, IP, etc. – auch simultan zu transportieren. Dies ist möglich, indem FC als Träger für diese Befehlsätze dient, und zwar so, dass der Empfänger zwischen beiden unterscheiden kann. Diese Trennung der I/O-Operation von der physikalischen Schnittstelle ist ein wichtiges Leistungsmerkmal. Hierdurch „sehen“ alle auf einem Server laufenden Anwendungen über FC angeschlossene Geräte als normale SCSI-Devices und senden/erhalten SCSI-I/O-Requests. Es mussten keine oder nur geringfügige Software- bzw. Treiber-Änderungen vorgenommen werden.

Zusätzlich wurde zur Steigerung der Übertragungsraten der Protokoll-overhead im Vergleich zu Parallel-SCSI und -TCP/IP deutlich reduziert. Bei gegebener Taktrate kann ein FC-SAN eine Nutzdatenauslastung von über 90 Prozent für sich verbuchen, während herkömmliche Netzwerke im realen Betrieb lediglich 20 bis 60 Prozent der maximal möglichen Übertragungsrate erreichen.

### Datentransport und Frame-Struktur

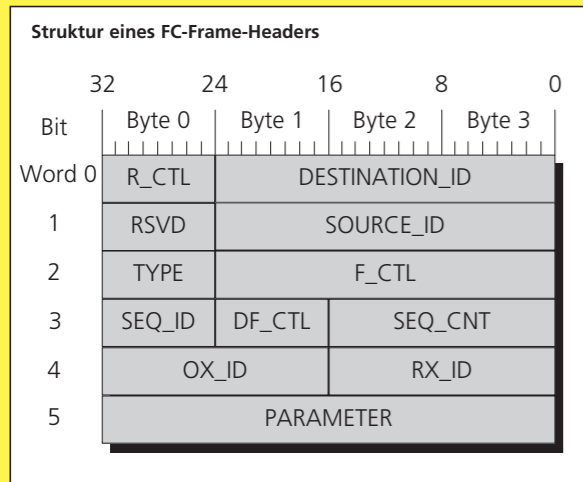
Der gesamte Verbindungsablauf zweier FC-Geräte wird **Exchange** genannt. Ein Exchange besteht aus Sequences, die in Frames unterteilt, übertragen und an der Gegenstelle in umgekehrter Reihenfolge wieder zusammengesetzt werden.



Ein FC-Frame besteht aus so genannten Transmission Words (TW), die eine Länge von 4 Bytes aufweisen. Die Framesize ist variabel und beträgt maximal 2148 Byte. Im Frame enthalten sind die Nutzdaten, ein Frameheader, optionale Header, CRC-Information, ein SOF (Start of Frame) und ein EOF (End of Frame). Nach Abzug aller Zusatzinformation bleiben maximal 2048 Byte als reine Nutzdaten pro Frame übrig. Der kürzeste FC-Frame (also ein Frame ohne Nutzdaten) ist damit 36 Bytes lang. Dies entspricht einem maximalen Nutzdatenanteil von 95,3 Prozent.

SOF	Frame Header	Otionale Header	CRW	EOF
1 TW	6 TW	(64 Bytes)+Daten 0-528 TW	1 TW	1 TW

Der 6 TW große (24 Byte) Frame-Header ist in Felder unterteilt, die Kontrollinformationen enthalten. Unter anderem findet man hier auch die Ursprungsadresse und die Zieladresse des FC-Frames.



Zielsetzung bei der Entwicklung von Fibre Channel war außerdem die Zusammenfassung der beiden etablierten Arten der Datenübertragung (Channel-Technologie, Netzwerk) unter Verwendung der jeweiligen Vorteile dieser Technologien. Fibre Channel sollte die besten Aspekte dieser beiden konträren Kommunikationsverfahren in einer neuen I/O-Schnittstelle kombinieren, die blockbasierten Datenzugriff mit netzwerktypischen Eigenschaften versieht

### **i** Klassische I/O-Kanäle

- **Blockbasierter Datenzugriff**
- **Arbeitet in abgeschlossener strukturierter Umgebung, deren Konfiguration vorab definiert ist**
- **Peripherie-Geräte sind direkt mit Hostsystem verbunden**
- **Jede Änderung zieht Veränderung der Konfiguration nach sich**
- **Das Host-System ist der Träger der Konfigurationsinformation**
- **Transfer großer Datenmengen zwischen Rechner und Gerät**
- **Verarbeitungs-Overhead ist auf ein Minimum reduziert und erfolgt mit wenig bis gar keiner Softwareunterstützung**
- **Wichtigste Anforderung für die Übertragung von Daten ist die fehlerfreie Übermittlung, wobei die Übertragungverzögerung zweitrangig ist**

### **i** Netzwerke

- **Filebasierter Datenzugriff**
- **Arbeitet typischerweise in einer offenen unstrukturierten Umgebung, die sich aus Serversicht unvorhersehbar ändern kann**
- **Jeder Host kann mit jedem Gerät zu jedem Zeitpunkt kommunizieren (Peer-to-Peer)**
- **Erhöhte Softwareunterstützung erforderlich zur Steuerung der Zugriffsberechtigung, Auf- und Abbau von Sitzungen, Verpacken der Daten in Pakete, Routing, etc.**
- **Im Allgemeinen großer Protokoll-Overhead, d. h. schlechtes Verhältnis zwischen Gesamt- und Nutzdaten**
- **Es gibt hier auch Anwendungen, die nicht auf fehlerfreie Übertragung der Daten angewiesen sind. Beispielsweise ist bei Video/Audio-Streaming die möglichst verzögerungsfreie Übertragung der Daten zumeist wichtiger als ihre fehlerfreie Übermittlung**

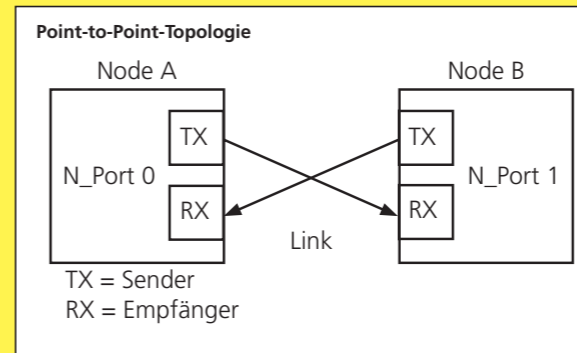
#### 6.2.2 Topologien für Fibre-Channel-Netzwerke

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. Jeder Fibre-Channel-Port verfügt über einen Sende- und einen Empfangskanal. Die Verbindung von Sende- und Empfangskanälen zweier Ports erfolgt über elektrische Leiter oder über die heute üblichen Lichtwellenleiter und wird Verbindung (engl. Link) genannt.

Die Art und Weise, wie zwei oder mehr Ports miteinander verbunden sind, wird unter der Bezeichnung Topologie zusammengefasst. Die Fibre-Channel-Norm definiert drei Topologien: Point-to-Point, Arbitrated Loop und Fabric.

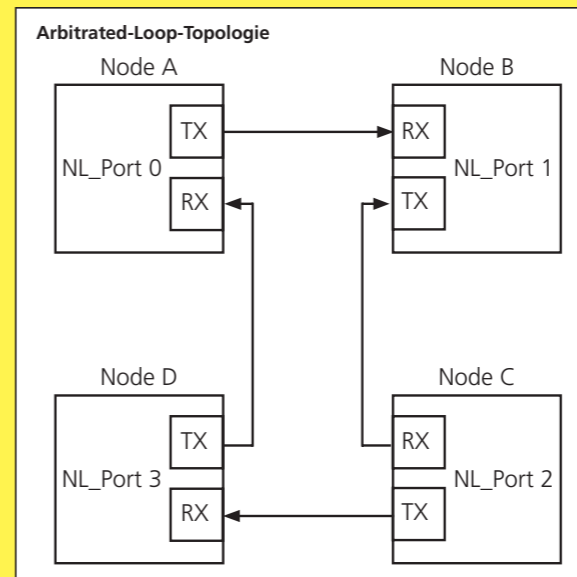
##### Point-to-Point

Dies ist die einfachste Möglichkeit, zwei FC-Ports miteinander zu verbinden. Durch einen Crosslink werden die beiden Ports miteinander verbunden, sodass die gesamte Bandbreite den beiden Geräten zur Verfügung steht. Die Ports werden hier als N\_PORTS bezeichnet.



##### Arbitrated Loop

Im Arbitrated Loop (AL) sind die Ports zu einem Ring zusammengeschaltet. Es können bis zu 126 Ports miteinander verbunden werden. Die Datenpakete werden von Port zu Port weitergegeben. Sie werden nur von den Ports, für die sie bestimmt sind, angenommen. Nicht für einen Port bestimmte Pakete werden von diesem einfach weitergegeben. Alle Ports teilen sich die Bandbreite. Es sind jeweils zwei Ports gleichzeitig aktiv. Arbitrated Loop wird auch von einem Loop Switch realisiert. Hier allerdings ohne die Einschränkung der verminderten Bandbreite durch mehrere Geräte.



Um RAID-Speichersysteme besser handhaben zu können, unterstützt der FC-AL neben der normalen Kabelverbindung auch die Backplane-Architektur. Die Festplatten werden über einen 40-poligen SCA-Stecker (Single Connector Attachment), der sowohl Datenleitungen als auch

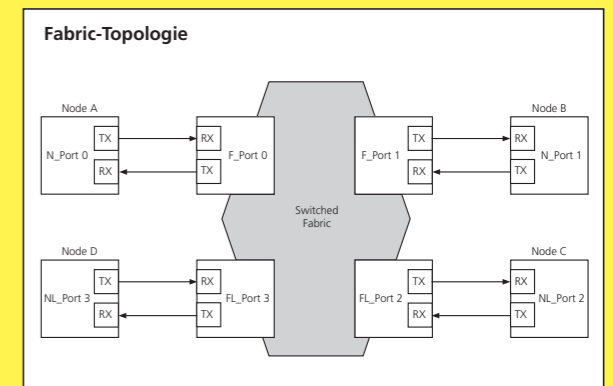
Stromversorgung beinhaltet, an die Backplane angeschlossen. Steckt in einem Port kein Laufwerk, überbrückt die Backplane-Logik den leeren Steckplatz, und der Kreis bleibt geschlossen. Eine weitere Aufgabe der Backplane ist die automatische Konfiguration des Laufwerks sowie die Sicherstellung der Hot-Plug-Funktion, also der Wechsel eines Laufwerks während des Betriebs.

Das gleiche Prinzip wird auch von Fibre-Channel-Hubs verwendet. Da bei einem Fibre-Channel-Loop der Ausfall eines Geräts 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. Der Datenfluss zu den anderen Devices wird so nicht unterbrochen und der Bus arbeitet normal weiter. FC-AL-Produkte werden seit 1996 angeboten, sind aber heutzutage nur noch in einigen Low-Cost-Produkten anzutreffen. Fast alle Produkte unterstützen heute neben FC-AL auch Fibre-Channel-Fabrics.

##### Fabric

Ein Fabric erlaubt dynamische Kopplungen zwischen Knoten über die an dieses Netzwerk 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 über eine Verbindung angeschlossen. Jeder Port in einem Fabric wird F\_Port genannt. Jeder Knoten kann mit jedem anderen an F\_Ports desselben Fabrics angeschlossenen Ports mithilfe der Fabric-Netzwerkdienste kommunizieren (Peer-to-Peer-Prinzip). Bei dieser Art von Topologie wird das Routing und die Bestimmung des Transportweges für die einzelnen zu übertragenden FC-Frames vom Fabric anstelle der Ports durchgeführt. Ein weiteres Verbindungselement in Fabrics sind E\_Ports (Extension Ports), über die mehrere Knoten (in der Regel FC-Switches) direkt miteinander verbunden werden können, um verfügbare Bandbreiten zu optimieren oder eine höhere Verfügbarkeit im Netzwerk zu realisieren.



Die Fabric- und Arbitrated-Loop-Topologien können miteinander gemischt werden, um den Knoten eine Vielzahl von Dienst- und Leistungsgraden zu verleihen. Zudem können in einem Fabric andere Netzwerke wie etwa SONET, ATM oder IP (auch FCIP bzw. FC-over-IP genannt) zwischen einzelnen Fabric-Elementen benutzt werden, um räumliche Entfernungen zwischen Knoten zu überbrücken, die zu groß sind, als dass sie von der FC-Lichtleiter-Verbindung zwischen N\_Ports bewältigt werden könnten. Diese speziellen Verbindungen können zwischen Fabric-Elementen bestehen, die über ein größeres geographisches Gebiet verteilt und nicht direkt an Knoten angeschlossen sind.

#### World Wide Name und FC Address

Die Funktion des Fabric ist der eines Fernsprechsystems vergleichbar: Wir wählen irgendeine Rufnummer und das Fernsprechsysteem findet den Pfad zum gewünschten Zielanschluss. Wenn eine Vermittlungsstelle oder Verbindung abstürzt, leitet das Fernsprechsysteem die Anrufe über andere Pfade um, was der Anrufer selten bemerkt. Die meisten von uns wissen nichts von den Zwischenverbindungen, die das Fernsprechsysteem schaltet, um unseren einfachen Anruf erfolgreich werden zu lassen. Dieselbe Systematik nutzt auch TCP/IP, woran man wiederum die früher erwähnte Doppelfunktion des Fibre Channel als I/O- wie auch als Netzwerk-Standard erkennen kann.

Ebenso wie wir beim Fernsprechsysteem den Anrufer über eine Rufnummer mit einzelnen Bestandteilen wie Ländervorwahl, Ortsvorwahl und Teilnehmernummer identifizieren, benötigt auch Fibre Channel eine Teilnehmerkennung.

FC-Nodes und Ports werden weltweit eindeutig mit ihrem World Wide Name (WWN bzw. WWP) identifiziert. Der WWN/WWP wird üblicherweise in hexadezimaler Schreibweise angegeben und hat eine Länge von 64 Bit. WWN/WWP sind Geräteadressen – vergleichbar mit MAC-Adressen – und dienen zur Identifizierung der Nodes/Ports selbst.

Zur Adressierung der Datenpakete in einer FC-Umgebung hingegen wird eine 24 Bit lange Fibre Channel Address oder PORT\_ID benutzt, was zu einer Gesamtanzahl von über 16 Millionen verbindbarer Ports führt. Dieser Adressraum steht nur in wirklichen Fabric-Topologien mit entsprechenden Protokollen zur Verfügung:

**Bit 23-16**    **Bit 15-8**    **Bit 7-0**  
Domain Address    Area Address    Loop Address

In der FC-Arbitrated-Loop-Topologie wird vom FC-AL-Protokoll jedoch zur Adressierung nur das unterste Byte benutzt. Es stehen nur 126 Adressen, die Loop IDs, zur Verfügung. Diese Loop Address wird AL\_PA

(Arbitrated Loop Physical Address) genannt. Möchte man noch nach Herkunft und Ziel unterscheiden, so spricht man von der AL\_PD (Destination) und AL\_PS (Source).

Für die meisten Geräte kann individuell festgelegt werden, ob die AL\_PA dynamisch oder statisch vergeben wird. Dynamische Vergabe der AL\_PA ist für Betriebssysteme und Anwendungen, die nach Devicepfaden auf Speichergeräte zugreifen, nicht zu empfehlen. Denn wird durch einen erneuten Verhandlungsprozess eine andere AL\_PA zugewiesen. So verändern sich die Devicepfade, und das Gerät kann nicht mehr angesprochen werden. Im schlimmsten Fall wird sogar ein falsches Gerät benutzt.

#### 6.2.3 Verkabelung von Fibre-Channel-Netzwerken

Die zwei grundsätzlichen Möglichkeiten sind elektrische Datenübertragung über Kupferkabel und optische Übertragung über Glasfaserkabel, wobei heute fast nur noch die optische Verkabelung in FC-Geräten wie Switches und Hostbusadaptern anzutreffen ist.

##### Kupferkabel

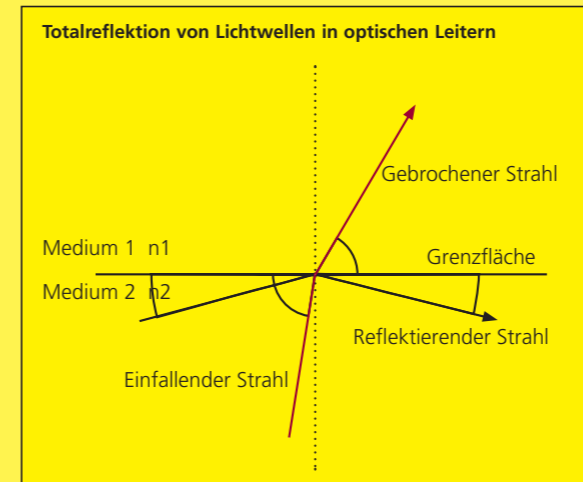
Grundsätzlich gibt es Ausführungen für 1 GBit und 2 GBit mit den Steckerformaten DB9, HSSDC und HSSDC-2. Die maximal mögliche Kabellänge liegt bei ca. 20 Metern. Es gibt jedoch auch spezielle „equalized“ Kabel für 1 GBit/s mit bis zu 40 Metern Länge.

##### Lichtwellenleiter/Glasfaserkabel

Lichtwellenleiter (LWL) bzw. Glasfaserkabel nutzen als physikalisches Grundprinzip der Datenübertragung die Totalreflexion von Lichtwellen beim Übergang vom optisch dichteren zu optisch dünnerem Medium. Die Signalübertragung erfolgt durch Lichtimpulse eines Lasers oder einer LED, die innerhalb der Glasfaser übertragen werden.

Der LWL mit dem einfachsten Aufbau besteht aus einem konzentrischen optischen Kern mit einer hohen Brechzahl, der mit einem optischen Mantel kleinerer Brechzahl versehen ist. Licht, das in einem gewissen Winkelbereich in den LWL eintritt, wird durch fortlaufende Totalreflexion an der Grenze von Kern und Mantel weiterbefördert.

Vorteile der LWL sind große Übertragungsraten bis in hohe Gbit/s-Bereiche, die Möglichkeit der Überbrückung weiter Entfernungen sowie die Unempfindlichkeit gegenüber elektromagnetischen Störungen.

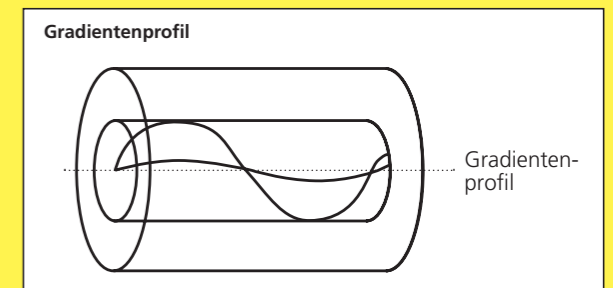
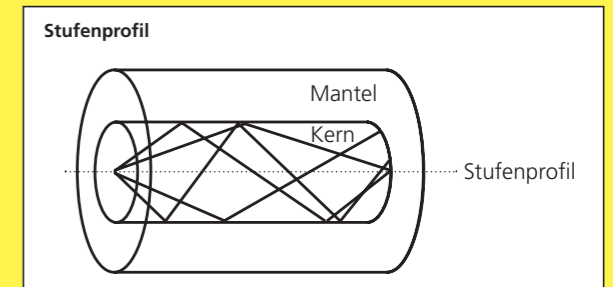


Die Signalqualität und damit die maximal mögliche Übertragungsdistanz wird prinzipiell durch die Verformung der Signale während ihrer Ausbreitung bestimmt. Nachfolgend beschriebene Faktoren führen zu einer Verschlechterung des Ausgangssignals.

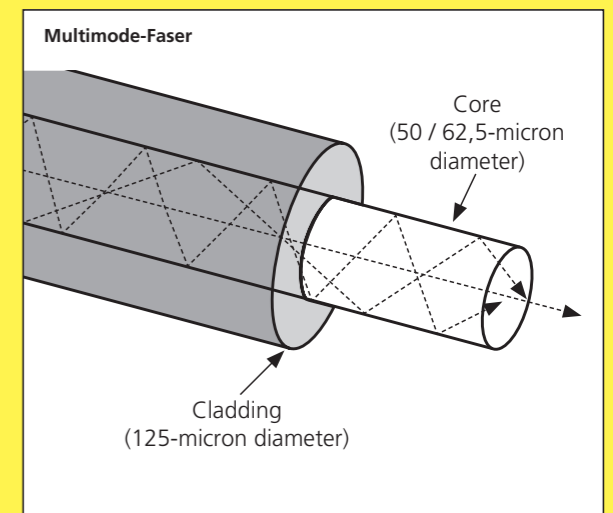
- **Dämpfung:** Durch Wechselwirkung des Lichts mit dem Medium wird der Signalpegel bei immer größerer Strecke immer geringer. Nach einer gewissen Strecke kann nicht mehr zuverlässig zwischen 0- und 1-Pegel unterschieden werden.
- **Dispersion:** Mit diesem Begriff bezeichnet man die Verformung des Signals in Ausbreitungsrichtung. Als Folge starker Dispersionseffekte kann nicht mehr zwischen benachbarten Signalpeaks unterschieden werden. Üblicherweise wird nach spektraler Dispersion und modaler Dispersion unterschieden.
  - **Spektrale Dispersion:** Laufzeitunterschiede aufgrund der Wellenlänge. Die Ausbreitungsgeschwindigkeit des Lichts hängt von der Wellenlänge ab. Da die verwendeten Lichtquellen nie 100 Prozent monochromatisch sind, wird es bei großen Übertragungsstrecken durch Laufzeitunterschiede aufgrund der unterschiedlichen Wellenlänge immer zu einer Verformung des Signals kommen.
  - **Modale Dispersion:** Verschiebungen aufgrund der unterschiedlichen Lichtwege in der Faser.

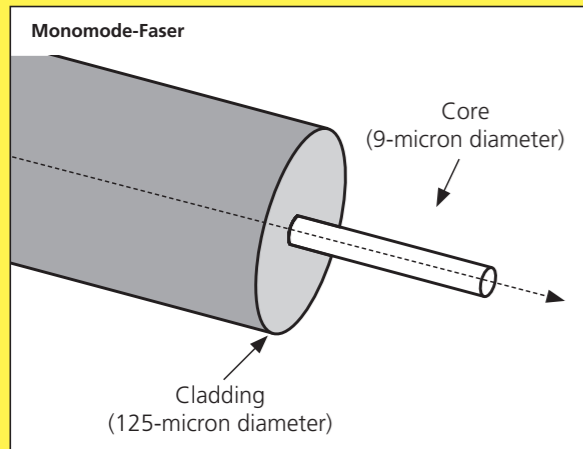
Das Lichtsignal kann in unterschiedlichen Winkeln in die Glasfaser eintreten. In geometrisch-optischer Näherung nennt man Licht mit großem Winkel zur optischen Achse Licht hohen Modes. Licht nahe der optischen Achse heißt entsprechend Licht niederen Modes. Licht hohen Modes muss einen längeren Weg zurücklegen als ein Signal niederen Modes. Das führt zu Laufzeitunterschieden und damit zu Dispersionseffekten im Ausgangssignal. Diesem Effekt kann man durch spezielle Glasfasern entgegenwirken:

■ **Gradientenprofilfasern:** Hier nimmt der Brechungsindex von innen nach außen stetig ab, wodurch dem Auseinanderlaufen des Signals entgegen gewirkt wird. Man spricht in diesem Zusammenhang von einem Gradientenprofil.



■ **Monomode-Fasern:** Im Gegensatz zu den Multimode-Fasern leiten sie nur Licht einer bestimmten Wellenlänge. Ihr Kerndurchmesser ist so klein gewählt, dass sich das Licht fast nur noch entlang der Längsachse ausbreiten kann.

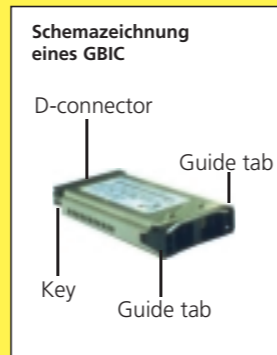




Zusammengefasst kann man also sagen, dass die maximale Kabellänge bei LWL abhängig ist von Faserdurchmesser, Übertragungsrate, Wellenlänge des verwendeten Lichts sowie der spektralen Güte der Lichtquelle. Laser werden hauptsächlich in zwei verschiedenen Wellenlängenbereichen eingesetzt: 770–860 nm (Short Wave) sowie 1270–1355 nm (Long Wave). Multimode/Single Mode bezeichnet dabei die Art und Weise, wie die Laserimpulse im Glasfaserkern übertragen werden. Multimode bedeutet: auf verschiedenen Wegen. Dies ist bedingt durch den größeren Durchmesser des Kabelkerns. Single Mode bedeutet: Übertragung auf einem Weg. Wegen des kleinen Durchmessers des Glasfaserkerns gibt es nur einen möglichen Lichtweg. Multimode wird benutzt für Short-Wave-Laser, Single-Mode für Long-Wave-Laser.

#### Signalumwandlung im Fibre Channel

Bei der Übersetzung elektrischer Signale in den Server- und Speichersystemen in optische oder elektrische Signale für Fibre Channel nutzen heute praktisch alle Devices so genannte GBIC (Gigabit Interface Connector) oder SFP (Small Form-factor Pluggable). Diese stellen eine Kombination aus Transmitter und Receiver, einen so genannten Transceiver, dar. Ursprünglich verbreitet waren die GBICs mit den Anschlussarten DB9, HSSDC, SC-Longwave und SC-Shortwave. Im Zuge einer Miniaturisierung der Schnittstellen, um eine höhere Packungsdichte auf den Geräten zu erzielen, und des Übergangs zu einer Übertragungsrate von 2 Gbit/s wurden die GBICs von den SFPs, die heute der allgemeine Standard sind, abgelöst. Erhältlich sind zumeist Ausführungen mit elektrischen Schnittstellen im HSSDC-2-Format, sowie optischen Schnittstellen mit LC-Longwave- oder LC-Shortwave-Anschluss. SFPs sind Transceiver, die in entsprechende Slots der Geräte eingesteckt werden. Geräte mit SFP-Slots sind also sehr flexibel in Bezug auf das Schnittstellenformat. GBICs und SFPs sind hot-swap-fähig, können also im laufenden Betrieb aus- und eingebaut werden.



### 6.3 SMI-S – der neue Standard für SAN-Management

Für die Verwaltung auf den unteren Schichten im SAN gibt es ANSI-, IETF- und ISO/IEC-Normen. Vom Vorteil ist, dass Fibre Channel und SCSI in ihrer Weiterentwicklung zueinander kompatibel geblieben sind. Daher müssen bei der Migration vom parallelen SCSI-Bus zum seriellen FC-Link die betroffenen Anwendungen nicht umprogrammiert werden. Dienste wie die Gehäuseüberwachung (SAF-TE, SES) und Fehlerbehandlung sind ebenfalls für beide Techniken standardisiert. Was bislang jedoch fehlte, war die darüberliegende Schicht von API-Standards für die Zusammenarbeit der Speichersysteme, Server und Software in einem heterogenen Netzwerk – unabhängig davon, ob das SAN auf Fibre Channel oder Ethernet und iSCSI-TCP/IP basiert.

Heute existieren herstellerspezifische, proprietäre Management-Softwarepakete für jedes einzelne SAN-Device (HBAs, Switches, Speichersysteme, Bandsysteme). Herstellerübergreifende Verwaltung im SAN, wie zum Beispiel von McDATA's SANavigator-Software offeriert, erfordert die sehr aufwändige Programmierung der Schnittstellen zu jeder einzelnen zu unterstützenden herstellerspezifischen API.

SMI-S definiert hingegen eine allgemeine, modulare Schnittstelle zur Verwaltung von Speichernetzwerken. Als objektorientierte Spezifikation stellt sie einheitliche Kriterien zur Verfügung, um Objekte in einem SAN zu identifizieren, klassifizieren sowie reale und virtuelle Ressourcen zu überwachen und Informationen unter Nutzung eines gemeinsamen Transportmechanismus zu übertragen. Ein Objekt kann dabei ein komplettes RAID oder auch nur ein defekter Sektor auf einer Festplatte sein. Ziel von SMI-S ist die Ermöglichung einer web-basierenden Management-Oberfläche für alle Devices in einem SAN – unabhängig vom Hersteller.

Die Storage-Management-Interface-Specification (SMI-S) wurde als neuer Standard erstmals im April 2003 von der SNIA Distributed Management Task Force (DMTF) verabschiedet und ist aus der IBM-Initiative BlueFin hervorgegangen. Basierend auf dem Common Information Model (CIM) handelt es sich um eine wesentliche Erweiterung der WBEM-Technik (Web-Based Enterprise Management), die auf drei offenen Standards basiert:

- DMTF's CIM
- XmlCIM – eine speziell für CIM definierte XML Code-Spezifikation
- HTTP – als Informations-Transportmechanismus zwischen Applikationen und CIM-konformen Systemen

Die WBEM-Architektur wurde unter Berücksichtigung der besonderen Anforderungen des Speicherbetriebes angepasst. In der ersten Generation unterstützt und standardisiert SMI-S die folgenden SAN-Management-Funktionen:

- Entdeckung – automatische Identifikation und Registrierung von Devices (HBAs, Switches, RAIDs, Bandsysteme) in einem SAN
- Überwachung – kontinuierliche Überprüfung des SAN-Fabric-Zustandes und des Betriebes jedes Devices im SAN (so genanntes Health Monitoring)
- Device Management – aktive Kontrolle, Konfiguration und Rekonfiguration von Devices im SAN

SMI-S ist dabei deutlich effektiver als SNMP (Simple Network Management Protocol), das heute bereits einige Speichersysteme über eine Reihe von MIBs (Management Information Bases) unterstützen, um mit Framework-Applikationen (IBM TSM, HP OpenView, CA UniCenter, etc.) über Ethernet zu kommunizieren. Unter SNMP werden alle Parameter einzeln von allen Komponenten im Netzwerk unter Kenntnis von genauer IP-Adresse und Passwort aktiv abgefragt.

Mit einem einheitlichen SMI-S Formular werden die benötigten Parameter automatisch von den vorhandenen und neu hinzugefügten Komponenten (Client genannt) abgefragt und der Speicherverwaltungs-Software (Provider genannt) zur Verfügung gestellt. Außerdem ist nicht nur die Überwachung, sondern auch die Konfiguration/Rekonfiguration der Clients möglich. Über so genannte Lock-Manager unterstützt SMI-S zudem die gleichzeitige Kommunikation eines Providers mit mehreren Clients.

Noch ist die Umstellung der Produkte auf SMI-S durch die Hersteller in den Anfängen. Bis Ende 2005 sollen aber über 80 Prozent aller SAN-Devices entweder mit einer Übersetzungsschnittstelle der nativen API auf den SMI-S Standard (Proxy Modell) oder bereits mit einer SMI-S kompatiblen API (Natives Modell) ausgestattet sein. SMI-S wird dann ohne Zweifel die Verwaltung von Produkten innerhalb eines SANs

erheblich vereinfachen, den Schulungsaufwand senken und SNMP als Managementstandard ablösen.

### 6.4 iSCSI – das IP-basierte Speichernetzwerk

Das Internet SCSI Protokoll (iSCSI) definiert einen Standard, um SCSI-Befehle auf Basis einer TCP/IP-Kommunikation zu übertragen und stellt somit beim Aufbau von Speichernetzwerken eine Alternative zu Fibre Channel dar. Ebenso wie Fibre Channel ermöglicht iSCSI eine blockbasierte Kommunikation in einem Netzwerk.

Bei den SCSI- und FC-Standards handelt es sich um US-Normen der ANSI-Komitees T10 (SCSI) und T11 (Fibre Channel). Während alle Richtlinien in Verbindung mit der IP-Protokollfamilie und somit auch für iSCSI von der IETF (Internet Engineering Task Force) erarbeitet werden, welcher einen losen Zusammenschluss von Experten darstellt. Neben iSCSI sind dies unter anderem FCIP, iFCP, mFCP oder auch iSNS.

Weitergehende Informationen finden Sie unter:

- [www.ietf.org](http://www.ietf.org)
- [www.snia.org](http://www.snia.org)

Die Design-Richtlinien der IETF für iSCSI sind wie folgt:

- SCSI-Devices müssen mittels IP-Verbindung untereinander kommunizieren können
- TCP soll als Transportprotokoll dienen
- TCP-Verbindungen sollen sparsam genutzt werden
- Ethernet- und IP-Standards dürfen für iSCSI nicht modifiziert werden
- Die Serversysteme müssen im IP-Netzwerk gleichzeitig auf mehrere Speichersysteme zugreifen können
- Leistungssteigerungen der SCSI-Geräte im IP-Netzwerk müssen von der iSCSI-Spezifikation zugelassen werden

Die Vorteile von iSCSI liegen in der Nutzung von TCP/IP-fähigen Infrastruktur-Komponenten zum Aufbau eines Storage Area Networks (SAN). Administratoren können ihre bestehenden Erfahrungen hinsichtlich der Verwaltung von IP-LANs und -WANs für den Aufbau eines SANs nutzen und müssen sich nicht in andere Technologien wie FC einarbeiten. Außerdem können iSCSI-SANs mittels Breitband-Verbindungen Standortübergreifend miteinander verbunden werden, wodurch beispielsweise asynchron replizierte Speichersysteme realisiert werden können. Der Nachteil liegt in dem zusätzlichen Protokoll-Overhead in IP-Netzwerken – im Vergleich zu FC- Speichernetzen. TCP/IP sendet kleine Datenpakete und geht dabei grundsätzlich von einem unzuverlässigen Transportweg aus. Es existiert kein vorgegebener, fester Übermittlungsweg, wie bei SCSI oder Fibre Channel. Übermittelte Pakete können auf unterschiedlichen

Wegen, zeitversetzt, mit Übermittlungsfehlern oder überhaupt nicht ankommen. Dem Empfänger obliegt die Aufgabe der Zusammensetzung der Pakete in die richtige Reihenfolge und erneute Anforderung fehlender Informationen. Ein FC-SAN hingegen übermittelt Daten blockweise auf dem kürzesten Weg und unter Einhaltung der korrekten Reihenfolge zwischen Server- und Speichersystemen. Diese systemimmanenten Unterschiede machen deutlich, dass iSCSI-Speichernetzwerke auf absehbare Zeit hinsichtlich der erzielbaren Bandbreite und Latenz nicht mit FC-SANs vergleichbar sein werden. Als günstiges, zentrales Speichernetz mittlerer Leistungsfähigkeit, mit der Option zur einfachen Anbindung anderer Standorte, findet iSCSI jedoch zunehmend Anwender.

**iSCSI – SCSI over IP**

Die SCSI-Protokoll-Familie kennt im Wesentlichen zwei SCSI-Geräte-Zustände: Initiators und Targets. Diese Zustände sind unabhängig von der zugrunde liegenden Hardware zu betrachten. Jedes SCSI-Gerät könnte Initiator oder Target der SCSI-Kommunikation sein. Der Initiator setzt im Wesentlichen Kommandos ab, die vom Target durchgeführt und quittiert werden. Der SCSI-Controller (auch Hostbusadapter) übernimmt in der Regel die Rolle des Initiators, während SCSI-Endgeräte (Festplatten, Storage-Systeme, Band-Libraries, usw.) primär als Target agieren.

Analog zu Fibre Channel, bei dem SCSI-Befehle mit einem Fibre-Channel-Header versehen in FC-Frames eingeschlossen und seriell via Kupfer- oder Glasfaserleitungen übertragen werden, stellt iSCSI eine ebensolche Basis zur Kommunikation über eine TCP/IP-Infrastruktur zur Verfügung. iSCSI ist serverseitig somit als ein Interface zwischen der TCP/IP-Schnittstelle einer Netzwerkkarte und dem SCSI-Subsystems des Betriebssystems zu verstehen.

>> siehe Schemazeichnung S. 127 oben:

**Speichernetzwerk-Technologien im Vergleich**

Ein iSCSI-SAN könnte analog zum klassischen FC-SAN aus mehreren iSCSI-Initiatoren (i. d. R. Servern) und einigen iSCSI-Targets, wie RAID-Systeme oder Band-Libraries, bestehen. Jedes am iSCSI-SAN partizipierende Endgerät muss über mindestens einen Ethernet-Anschluss mit iSCSI-Protokollunterstützung verfügen, um mit einer Infrastruktur-Komponente (Switch, Router, usw.) verbunden werden zu können. Optimalerweise sollte zur iSCSI-Anbindung ein Gbit-Ethernet-Anschluss zur Verfügung stehen, der exklusiv der iSCSI-Kommunikation zugeordnet ist. Falls bestehende SCSI- oder FC-Geräte mit in das iSCSI-SAN integriert werden sollen, können diese über iSCSI-Gateways integriert werden.

Damit ein Initiator ein Speichersystem finden kann, benötigt er eine Liste der IP-Adressen von iSCSI-Geräten, die ein so genanntes Target-Portal

zur Verfügung stellen. Diese Adressen können manuell gepflegt, über ein Broadcasts ermittelt oder über das Internet Storage Name Service Protokoll (iSNS) erfragt werden, welches das Auffinden von Geräten für iSCSI-Initiatoren erleichtert.

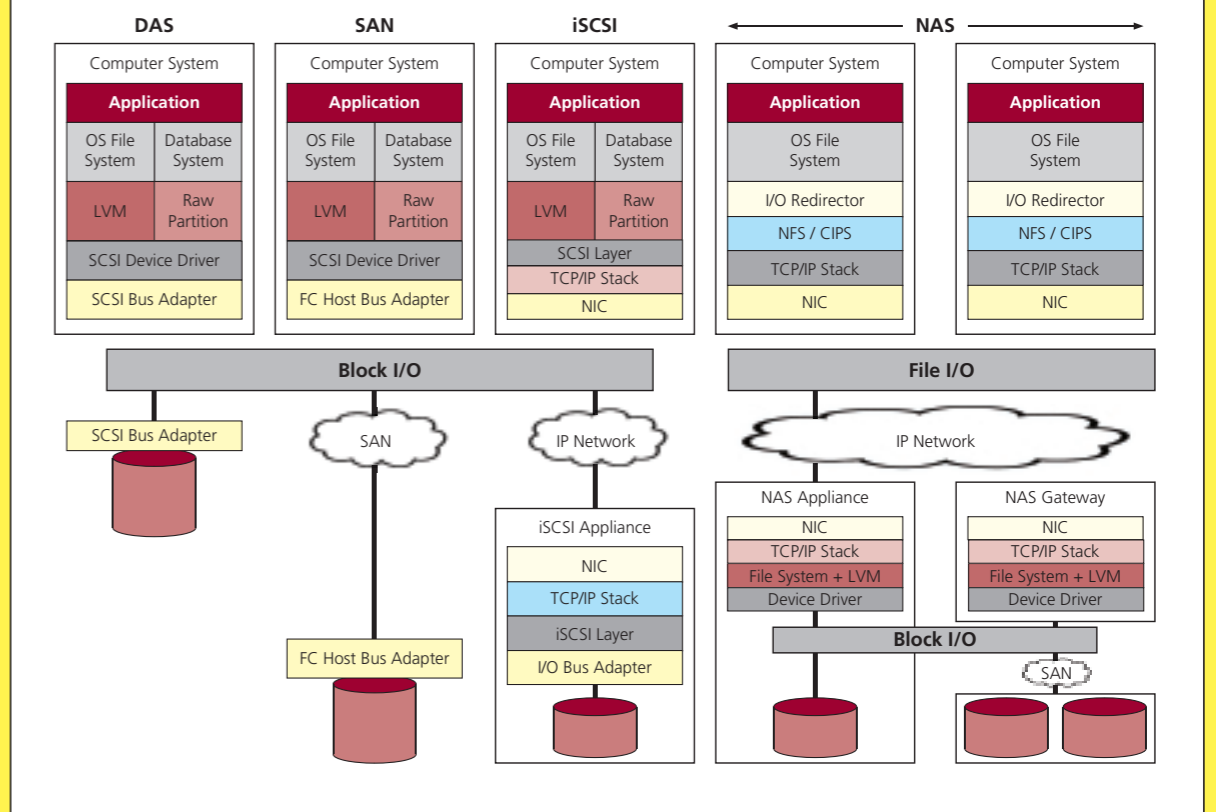
**Adressierung und Namensgebung im iSCSI-Protokoll**

iSCSI nutzt TCP/IP für eine zuverlässige Datenübermittlung über ein potenziell unzuverlässiges Netzwerk. Der iSCSI-Layer übernimmt dabei über Betriebssystemschnittstellen SCSI-Befehle und verpackt diese für den Transport in TCP/IP konforme Pakete bzw. Frames. Das iSCSI-Protokoll überwacht dabei die Integrität und Verifikation der jeweils angeforderten Lese-/Schreib-Operation. In der Praxis sind dabei sowohl auf Initiator- als auch auf Target-Seite multiple Zugriffe zu verarbeiten.

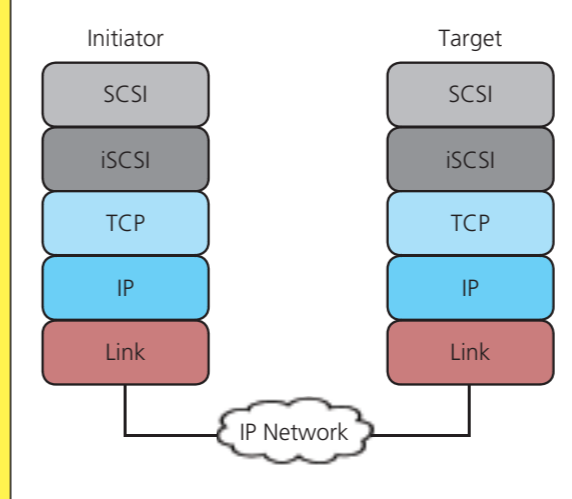
>> siehe Schemazeichnung S. 127 unten:

**iSCSI Protokoll Layer**

**Speichernetzwerk-Technologien im Vergleich**

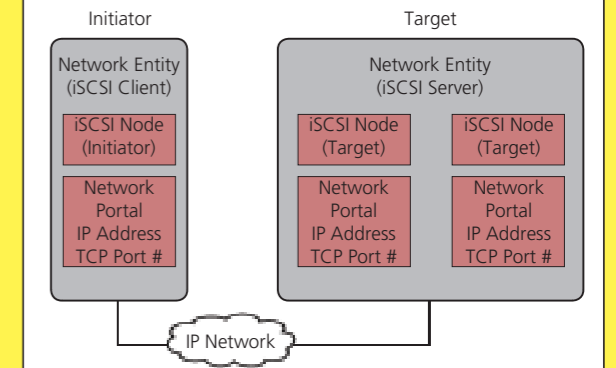


**iSCSI Protokoll Layer**



Als Teilnehmer in einem IP-Netzwerk haben Initiators und Targets eine Netzwerkennung, welche der zugeordneten IP-Adresse entspricht. Wie in der nächsten Abbildung dargestellt kann eine Network-Entity dabei ein oder mehrere iSCSI-Knoten haben.

**Aufbau einer iSCSI Network Entity**



Ein iSCSI-Knoten identifiziert ein über das Netzwerk zugängliches SCSI-Gerät. Bei einem RAID-System sind diese iSCSI-Knoten typischerweise die logischen Laufwerke (LUNs). Jeder iSCSI-Knoten wird durch einen dedizierten iSCSI-Namen identifiziert, der zu 255 Bytes lang sein kann.

Die Kombination aus IP-Adresse und TCP-Port erzeugt eine eindeutige Adresse für ein iSCSI-Gerät innerhalb eines Netzwerks, während der 255 Bytes lange iSCSI-Name eine für Anwender lesbare alphanumerische Kennung ermöglicht. Eine Trennung von iSCSI-Name und iSCSI-Adresse stellt sicher, dass z. B. ein Speichersystem unabhängig von seinem Standort immer dieselbe Kennzeichnung hat. Denn während sich die IP-Adresse bei einem Umzug in ein anderes Netzwerksegment ändert, bleibt der iSCSI-Name bestehen und ermöglicht den Initiatoren eine schnelle Wiederentdeckung des Gerätes. Dieser Umstand hat den Vorteil, dass ein redundantes RAID-System mit multiplen Netzwerkpfaden zum Server über den iSCSI-Namen dennoch als ein einziges Gerät identifiziert werden kann. Ein iSCSI Name besteht dabei aus drei Teilen: einer Typkennung, der namensgebenden Stelle und einer eindeutigen Kennung, vergeben durch die namensgebende Stelle.

Im Fibre Channel dient der 64 Bit lange, hexadezimale World Wide Name (WWN) zur globalen Identifikation eines Devices, während die 24 Bit lange Fibre-Channel-Adresse als Netzwerkennung dient. Zur einfacheren Verwaltung heterogener FC- und IP-Netzwerke kann auch ein WWN als iSCSI-Name verwendet werden. Die Typbezeichnung ist dann „eui“ (IEEE EUI Format) für „Extended Unique Identifier“.

Zusätzlich zum iSCSI-Name unterstützt das iSCSI-Protokoll noch einen ergänzenden Alias. Dieser dient zur Unterstützung der IT-Administratoren und kann genutzt werden, falls der iSCSI Name durch den Hersteller oder eine andere Instanz vorgegeben ist und keine bzw. geringe Relevanz hat. Der Alias kann ebenfalls bis zu 255 Bytes lang sein und z. B. beim Login genutzt werden. Das iSCSI-Protokoll sieht vor, dass Management-Software die Aliase dem Administrator entweder über ein Command Line Interface (CLI) oder eine GUI anzeigt.

**iSCSI Session Management**

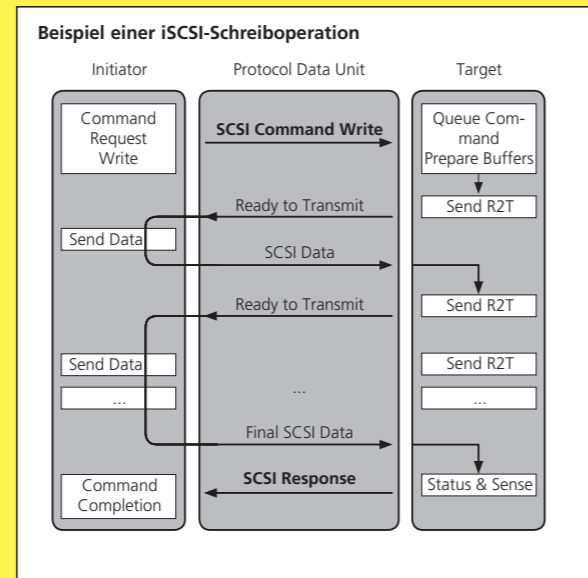
Eine iSCSI-Session zwischen einem Initiator und einem Target muss analog zum Fibre Channel Port Login (PLOGI) durch einen iSCSI-Login authentifiziert werden. Die iSCSI-Spezifikation unterstützt dabei die folgenden Authentifizierungsmethoden:

- KR5 – Kerberos V5
- SPKM1 & SPKM2 – Simple Public-Key Generic Security Service (GSS) API
- SRP – Secure Remote Password
- CHAP – Challenge Handshake Authentication Protocol
- None – Keine Authentifikation

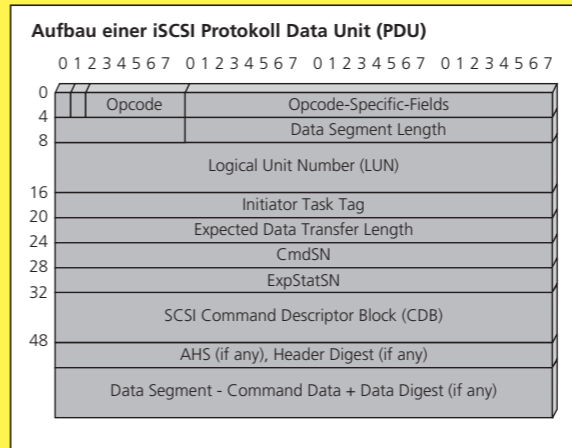
Während des Logins werden zwischen den Geräten iSCSI-Namen, Aliase und variable Parameter, wie die Wahl des zu nutzenden Sicherheitsprotokolls, die Anzahl unterstützter paralleler TCP-Verbindungen, Timeout-Werte oder die maximale unterstützte Größe des Data-Payloads, ausgetauscht. Bei unterschiedlichen Werten wird immer der größte gemeinsame Wert für die iSCSI-Session genutzt. Die Parameter werden dabei als Textfeldeinträge ausgetauscht:

**Originator sends** <key> = <value>  
**Responder replies** <key> = <value> | None | Reject | NotUnderstood | Irrelevant

Sobald der Login-Prozess abgeschlossen ist, können zwischen Initiator und Target SCSI-Befehle übermittelt werden. Falls für eine Sitzung mehrere TCP-Verbindungen aufgebaut wurden, muss jedes Befehl-/Ergebnis-Paar über dieselbe Verbindung übermittelt werden. Dies wird als Connection Allegiance bezeichnet und stellt sicher, dass Lese- und Schreiboperationen ohne zusätzlichen Overhead durch die Überwachung mehrerer TCP-Verbindungen durchgeführt werden können.



Die Abarbeitung eines SCSI-Befehls zwischen iSCSI-Initiator und -Target beinhaltet, wie in obiger Abbildung dargestellt, die Übermittlung mehrerer untergeordneter Befehls-, Status- und Datenpakete. Sie wird iSCSI Protocol Data Units (PDUs) genannt.



Mit der ersten PDU wird in unserem Beispiel vom Initiator an den Target ein SCSI-Befehl zum Schreiben bestimmter Blöcke übermittelt. Da TCP/IP für die Übertragung kontinuierlicher Byte-Ströme entwickelt wurde, gibt es keinen Mechanismus zur Erkennung der Blockgrenzen des SCSI-Befehls im Byte-Strom. iSCSI verwendet stattdessen im PDU-Header ein Feld, in dem die Befehls-Blocklänge steht. Und während im klassischen LAN-Betrieb ein Byte-Strom die Länge unendlich annehmen kann, ist für iSCSI eine maximale Länge von 232-1 definiert. Nach Erhalt des SCSI-Befehls bestätigt der iSCSI-Target seine Bereitschaft zum Datenempfang zusammen mit der Angabe der maximal freien Buffergröße mit einem „Ready to Transmit“ R2T PDU. Die Geschwindigkeit des Datenflusses wird damit im Gegensatz zum normalen TCP/IP-Betrieb aktiv vom iSCSI-Target-Gerät gesteuert.

Falls ein Initiator vom Target keine Antwort auf ausstehende Befehle erhält, kann er den Status des Targets erfragen bzw. überprüfen. Dieser iSCSI-NOP-Out-Befehl mit gesetztem P-Bit (Ping) kann auch Testdaten beinhalten, die vom Target intakt zurückzuliefern sind. Falls der Target nicht antwortet oder die retournierten Testdaten korrupt oder unvollständig sind, kann der Initiator die Verbindung schließen und eine neue Session starten.

Während in einem FC-SAN die Verbindungen zwischen Server und Speichersystemen in der Regel fest definiert sind und nur für Wartungsarbeiten oder beim Booten des Servers unterbrochen werden, können in einem iSCSI-SAN, je nach der durch die Initiators erzeugte Last, mehr oder weniger TCP-Verbindungen benötigt werden. Daher kann ein Initiator eigenständig zusätzliche Verbindungen zu einem Target aufbauen oder einzelne TCP-Verbindungen schließen. Ein kompletter Logout ist in der Regel nur bei Verbindungsfehlern oder Wartungsarbeiten an den Servern bzw. Speichergeräten notwendig.

**SCSI Fehlerbehandlung**

Die traditionelle SCSI-Architektur geht von einem weitgehend störungsfreien Umfeld aus. Direkt angeschlossene SCSI-Geräte nutzen einen dedizierten, parallelen Bus zur Datenübertragung – wohl getrennt von jedweden Netzstörungen. Ein iSCSI-Netzwerk hingegen kann nicht nur über ein stabiles, lokales Gigabit-Ethernet aufgebaut werden, sondern auch über fehleranfällige WAN- und Internetverbindungen. Daher beinhaltet die iSCSI-Spezifikation Adaption- und Fehlerbehandlungsroutinen für eine ganze Reihe denkbarer Störungen. Um eine zuverlässige Fehlerbehandlung zu gewährleisten, müssen daher sowohl Initiator als auch Target einen Puffer aufweisen. In ihm werden Befehlen und Antworten bis zur jeweiligen Bestätigung der Gegenstelle gespeichert.

Eine einzelne PDU kann innerhalb des iSCSI-Frames fehlende oder inkonsistente Daten aufweisen. Dies wird Formatfehler genannt und führt zum Verwerfen der iSCSI-PDU durch den Empfänger. Dieser retourniert ein Reject-PDU an den Sender, das angibt, an welcher Stelle das erste korrupte Byte entdeckt wurde. Eine andere Kategorie von iSCSI-Fehlern sind korrupte Daten im Data-Payload (Data Digest Error) oder Header (Header Digest Error). Auch hier wird das betroffene PDU verworfen und ein Reject-PDU gesendet.

Die Fehlerkorrekturmechanismen in einem iSCSI-Netzwerk beinhalten also zum einen das Aufspüren und den Neuversand korrupter oder fehlender iSCSI-Frames. Zum anderen die Prüfung, Terminierung und den Neustart von inaktiven oder abgebrochenen TCP-Verbindungen. Schließlich sieht das iSCSI-Protokoll die Beendigung einer kompletten Session mit Abbruch aller Tasks und anschließendem erneuten Login vor, falls alle andere Fehlerbehebungsversuche erfolglos sind.

**iSCSI-Performance**

Unserer Erfahrung nach liegen derzeit die effektiv erzielbaren Transferaten in einem 1-Gbit-Ethernet-iSCSI-Netzwerk bei 30 bis 60 MByte pro Sekunde. Jedoch sind mehrere Faktoren hierbei zu berücksichtigen.

Mit iSCSI ist zum einen kein Video-Streaming oder ähnlicher Dauerdatenverkehr realisierbar, da die Qualität der Datenübermittlung nicht im gleichen Maße wie bei einem SCSI-Bus oder FC-Netzwerk garantiert werden kann. Zum anderen ist die direkte Kommunikation zwischen zwei iSCSI-Targets, zum Beispiel einem Festplattensystem und einer Band-Library, für Serverless-Back-up nicht möglich.

Des Weiteren ist einer der wichtigsten und oft erwähnten Faktoren die zu erwartende CPU-Belastung. Das Ver- und Entpacken der SCSI-Befehle in TCP/IP-Pakete beeinträchtigt nicht nur die Leistungsfähigkeit der in ein iSCSI-Netzwerk eingebundenen Server, sondern auch die der



Speichersysteme. Mehrere Anbieter offerieren daher TCP/IP-Offload-Engines (TOE) oder spezielle iSCSI-Hostbusadapter, die, anstelle einer normalen Gigabit-Ethernet-Netzwerkkarte eingesetzt, diese Operationen auf einer eigenen CPU ausführen und dadurch den zentralen Systemprozessor entlasten. Jedoch liegen die Kosten hierfür nahe an den Preisen für Fibre-Channel-Hostadapter und verringern den Kostenvorteil von iSCSI gegenüber FC deutlich. Die Alternative ist die Verwendung von marktüblichen günstigen Ethernet-Netzwerkkarten zusammen mit so genannten iSCSI-Software-Initiatoren (Microsoft, Cisco, u. a.) bzw. spezieller iSCSI-Target-Software für Storage-Systeme.

Fujitsu Siemens hat für die CPU-Last konkrete Zahlen ermittelt: So benötigt ein marktüblicher Server mit Intel-Architektur für einen Durchlauf durch einen SCSI-Treiber etwa 5000 CPU-Zyklen, während für einen TCP/IP-Stack mindestens 50.000 Zyklen erforderlich sind. Dazu kommt noch der iSCSI-Stack-Overhead. LAN-Experten verwenden gern folgende Faustregel: Die Übertragung von 1 Bit beansprucht 1 Hz Taktfrequenz des Prozessors. Eine TCP/IP-Verbindung mit 1 Gbit/s lastet also einen Prozessor mit 1 GHz voll aus. Da viele externe RAID-Systeme noch schwächere CPUs einsetzen, kann es bei softwaregesteuerten iSCSI-Speichersystemen zu Leistungseinbrüchen unter Datenlast kommen. Bei aktuellen Single-Prozessor-Servern entspricht die Belastung durch iSCSI damit ca. 30 %, bei einem Dual-Prozessor System nur noch ca. 15 %. Ob dies für den Anwender tolerabel ist, kann nur im Einzelfall entschieden werden. Jedoch wird die Verfügbarkeit günstiger TOE-Karten bzw. iSCSI-Hostbusadapter mit der zu erwartenden Verbreitung von 10-Gbit-Netzwerken zunehmend relevant werden.

## 7. Magnetbandspeicher

### 7.2.4 SAIT-Laufwerke

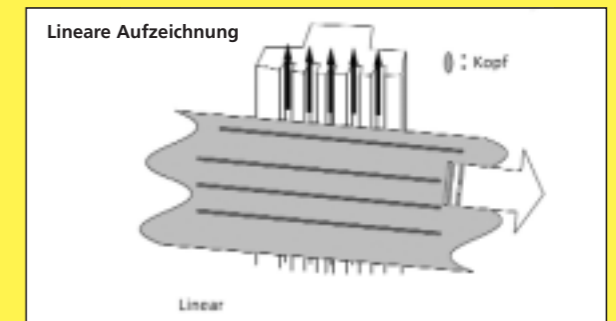
#### Meilensteine in der Entwicklung von Sony

##### (S)AIT-Bandtechnologie und -Bandlaufwerken

- 1996 – Sony stellt die Advanced-Intelligent-Tape-Technik (AIT) vor
- 1996 – Einführung von AIT unter Verwendung der AME-Bänder
- 1996 – Das englische Magazin „Byte“ zeichnet die AIT-1 mit dem Preis für die beste neue Technologie aus
- 1997 – AIT-1 wird durch den Verband der Europäischen Computer Hersteller (ECMA, European Computer Manufacturers) als Standard etabliert
- 1998 – Ankündigung von AIT-2
- 1998 – Die Speicherkapazität von AIT-1 wird von 25 GB auf 35 GB erhöht
- 1999 – Auslieferung der ersten AIT-2-Laufwerke
- 1999 – Gründung des AIT-Forums in Denver
- 1999 – Prototyp eines AIT-Laufwerks mit mehr als 1 MB pro Quadratzoll Aufzeichnungsdichte
- 1999 – die ECMA führt AIT-2 als einen Industriestandard ein
- 2000 – AIT-2 wird mit dem Preis „Bestes Speichermedium und Peripherie“ durch das Magazin „Imaging & Document Solutions“ ausgezeichnet
- 2000 – AIT-3 wird angekündigt
- 2000 – Einführung der AIT-1-Value-Serie und Erhöhung der Transferrate auf 4 MB pro Sekunde
- 2000 – Ein Prototyp eines AIT-Laufwerks erreicht 6,5 Gbit/s pro Quadratzoll Aufzeichnungsdichte
- 2001 – Sony stellt AIT-WORM-Laufwerke (Write Once, Read Many) und -Medien vor
- 2001 – Markteinführung der AIT-3-Laufwerke und Speichermedien durch Sony
- 2001 – Das Konsortium der Speichertechnologie-Hersteller (INSIC) beschließt die R-MIC-Spezifikation (Remote-Memory-In-Cassette)
- 2001 – Sony stellt die SAIT-Technologie vor
- 2002 – Sony bricht den Rekord für Speicherdichte: 11,5 Gbit/s pro Quadratzoll
- 2002 – Erste Modelle der SAIT-1-Laufwerke und -Medien werden den OEMs geliefert
- 2003 – Auslieferung der marktreifen SAIT-1-Laufwerke und -Medien

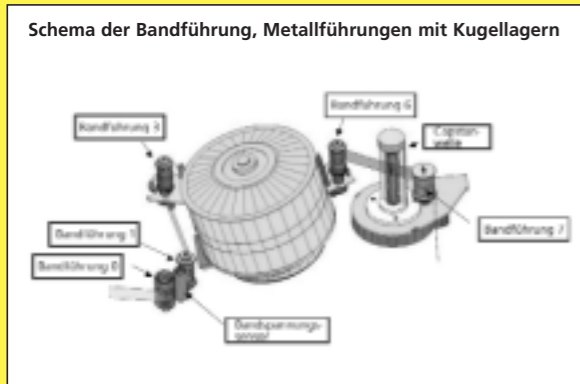
#### Schrägsपुरaufzeichnung

Hinter der hohen Aufzeichnungskapazität von SAIT steckt die Technologie der Schrägsपुरaufzeichnung. Das Band läuft an dem rotierenden, schräg angebrachten Lese-/Schreibkopf vorbei und erreicht so gegenüber einer linearen Aufzeichnung eine bis zu zweifache Aufzeichnungsdichte. Die Vorzüge der Schrägsपुरaufzeichnung gehen jedoch über den Vorteil der größeren Dichte hinaus. Unter anderem sind die geringere Beanspruchung der Laufwerksmechanik und die verlängerte Lebensdauer der Bänder zu nennen.



#### Die servogeregelt Capstanwelle

Die Daten sind auf den SAIT-Bändern in spiralförmigen Spuren aufzeichnet und werden entlang dieser Spiralen ausgelesen. Während der Aufnahme muss die Geschwindigkeit des Bandes konstant bleiben, um eine genaue Spurlage zu erreichen. Durch den phasengeregelten Servomotor der Capstanwelle wird die Spur mikrometergenau eingehalten. Fehlersignale kontrollieren die Geschwindigkeit der Capstanwelle, sodass die Spuren präzise auf den Lesekopf treffen. Diese Methodik hat eine hohe Datenintegrität, die gewährleistet, dass die Daten nach der Aufzeichnung auch sicher wieder gelesen werden können. Die Kapazität lässt sich zudem nachträglich erhöhen.



**Reduzierte Bandbelastung**

SAIT verwendet rotierende Führungsrollen aus Metall mit eingebauten Kugellagern, die einen ermüdungsfreien Betrieb für das Band und den Laufwerksmechanismus garantieren.

**Bandspannung**

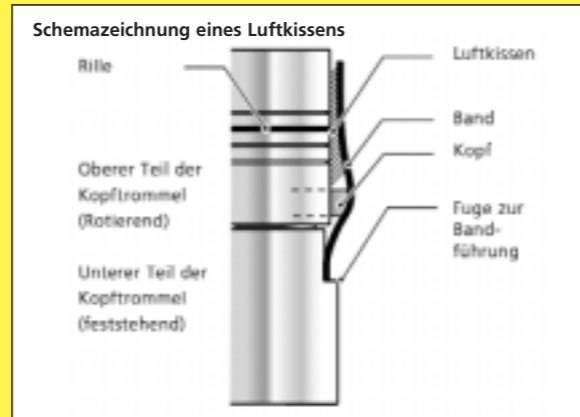
Veränderungen in der Spannung des Bandes können Lese-/Schreibfehler verursachen und zu einer frühzeitigen Alterung des Mediums und der Mechanik führen. Die SAIT-Technik verwendet einen Bandspannungssensor, dessen Messwerte dazu verwendet werden, um eine stabile und gleichmäßige Bandspannung zu gewährleisten. Hierdurch wird die durchschnittliche Zuverlässigkeit nochmals wesentlich erhöht.

**Vergleich der Bandspannung**

	SAIT	LTO2	SDLT600
<b>Gramm</b>	10	100	100

**Optimales Luftkissen**

In die Kopftrommel ist eine dünne Rille eingebracht. Dadurch entsteht ein gleichmäßiges mikrometerfeines Luftkissen. Dies führt dazu, dass das Band, obwohl es unter geringer Spannung steht, einen gleichmäßigen Abstand zur Oberfläche der Kopftrommel hat. Das schützt das Band vor möglichen Beschädigungen und trägt daher ebenso zur Verbesserung der Zuverlässigkeit von SAIT bei.



**Geringe Bandgeschwindigkeit**

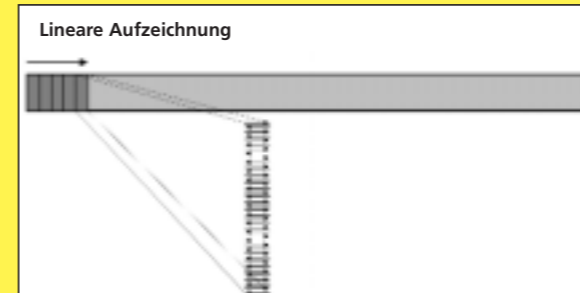
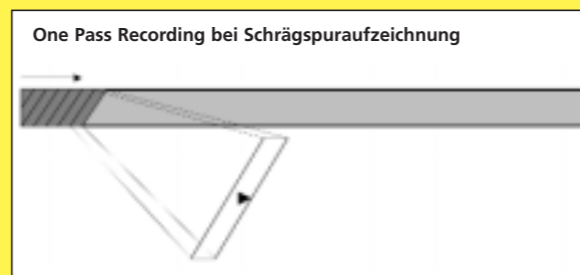
Die durch den Bandlauf erzeugte Reibung erzeugt Hitze, die im Extremfall zur Zerstörung des Bandes führen könnte. Bei SAIT rotiert der obere Teil der Kopftrommel mit gleichmäßig hoher Geschwindigkeit, um eine ausreichende Band-zu-Kopf-Geschwindigkeit zu ermöglichen, wogegen das Band mit geringer Geschwindigkeit und dadurch mit geringer Reibung am Kopf entlanggeführt wird. Zusätzlich zur Minimierung der Reibung wird dadurch auch ein geringer Spurbstand erreicht, was eine hohe Aufzeichnungsdichte ermöglicht.

**Vergleich der Bandgeschwindigkeit (Zoll pro Sekunde)**

	SAIT	LTO2	SDLT600
<b>Lesen/Schreiben</b>	1	217-232	108

**Single-Pass-Aufnahme**

Im Gegensatz zu herkömmlicher linearer Aufnahmemechanik, die bis zu 56 serpentinenförmige Spuren jeweils vom Anfang bis zum Ende des Bandes schreibt, bevor die Bandkapazität erreicht ist, wird bei der Schrägschreibaufzeichnung das SAIT-Band in nur einem Durchlauf aufgezeichnet. Dies führt nicht nur zu einer geringeren Abnutzung der Laufwerksmechanik und des Mediums, sondern verbessert durch Eliminierung des so genannten Shoe-Shine-Effekts auch die Gesamtleistung.



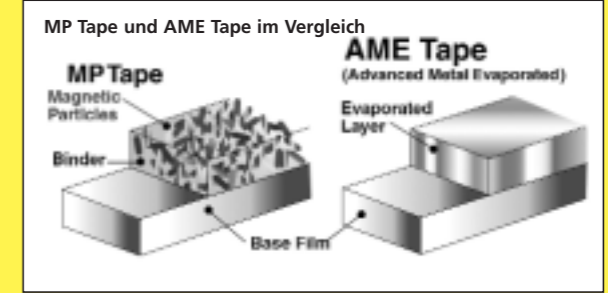
**Benötigte Bandläufe für eine Aufnahme**

	SAIT	LTO2	SDLT600
<b>Durchläufe</b>	1	64	40
<b>Spuren</b>	133 pro Gruppe	512	640
<b>Kanäle</b>	8	8	16

**Advanced-Metal-Evaporated-Medien (AME)**

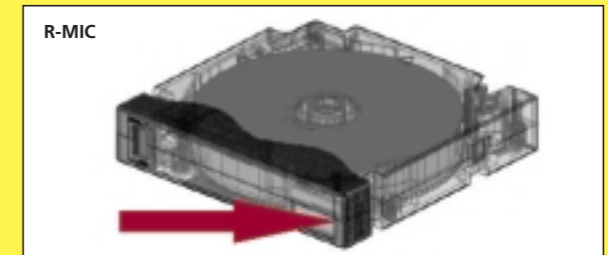
Metal-Partikel-Medien (MP), die von den meisten Laufwerkstechnologien verwendet werden, benutzen einen Polymer-Kunststoff, um das magnetische Material an den Film des Mediums zu binden. Die Verwendung dieser Polymere hat aber Nachteile: Mit der Zeit kann das Polymer verspröden, verursacht meist durch Feuchtigkeit oder Temperaturschwankungen. Die dadurch abfallenden Partikel lagern sich am Kopf an und erfordern häufiges Reinigen. Über einen längeren Zeitraum kann dies zum Zerfall der Oxidschicht führen, einer Reaktion auch bekannt als Sticky-shed-Syndrome, wobei die Oberfläche des Bandes aufweicht und klebriges Material absondert. Dies kann nochmals die Reibung erhöhen und zur Verschmutzung des Kopfes, zu Bandsalat und Schäden an Hardware und Medien führen.

SAIT verwendet die Advanced-Metal-Evaporated-Technik (AME). AME hat sich bereits im Einsatz mit der Exabyte-Mammoth- und Sonys AIT-Technik bewährt. Bei AME wird reines Kobalt als magnetisches Medium verwendet. Dieses wird mit Vakuumtechnik auf den Trägerfilm aufgedampft. Im Ergebnis führt dies zu einer höheren Aufnahmedichte als bei der Verwendung der MP-Medien. Die Ablagerungen am Kopf sind nachweislich wesentlich kleiner im Vergleich zu MP-Bändern, da kein Polymer benutzt wird, um die Magnetpartikel an den Trägerfilm zu binden. Ein Sticky-shed-Syndrome kann daher gar nicht mehr auftreten. Um die Lebensdauer der AME-Medien weiter zu verbessern, wird das Band zusätzlich mit einem diamantharten Kohlenstofffilm (DLC, Diamond-Like Carbon) versiegelt, der dem Band eine extreme Widerstandsfähigkeit gegen Abnutzung verleiht.



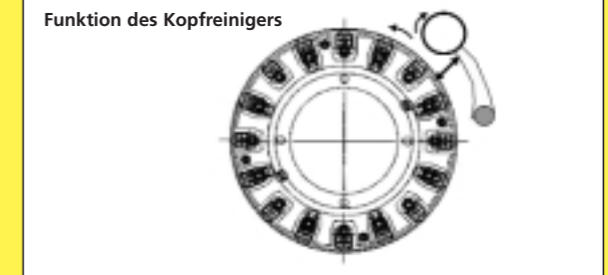
**Remote-sensing-Memory-in-Cassette (R-MIC)**

SAIT beinhaltet ebenso wie AIT-Medien einen nicht im Band befindlichen, 8 kByte großen Festspeicher (R-MIC), der in die Kassette integriert ist. Darin wird ein Ereignis-Log sowie die Bandposition aufgezeichnet, um die Lade- und Umspülzeiten zu verringern und somit die durchschnittliche Geschwindigkeit zu erhöhen. Auch hierdurch wird die Bandabnutzung verringert, da das Band nicht bemüht werden muss, um diese Informationen zu lesen. Dies führt zu einer weiteren Verlängerung der Lebensdauer sowohl der Medien als auch der Hardware.



**Eingebauter Kopfreiniger**

SAIT-Laufwerke haben einen eingebauten Kopfreiniger, um der Verschmutzung des Kopfes vorzubeugen. Kopfverschmutzung führt zu Lese- und Schreibproblemen und verursacht Schäden an Kopf und Band. Die automatische Reinigung der Kopftrommel verringert in entscheidendem Maße deren Verschmutzung und verbessert somit die Datensicherheit sowie die Zuverlässigkeit von Laufwerk und Medien.



**Fehlerkorrektur**

SAIT verfügt über eine besonders zuverlässige Fehlerkorrektur. Der Verlust an Kapazität pro Spur ist geringer als bei bestehenden Techniken zur Neuauzeichnung fehlerhaft geschriebener Daten, da ein erneuter Schreibvorgang auf mehreren verschiedenen Bereichen pro Block möglich ist. Dies ergibt außergewöhnlich genaue Korrekturaufzeichnung. Weiterhin können bis zu 16 Prozent der Einzelfehler einer gesamten Spur durch den eingesetzten Dreifach-Fehlerkorrektur-Code korrigiert werden. Durch diese Dreifach-Fehlerkorrektur wird die Zuverlässigkeit von SAIT signifikant erhöht.

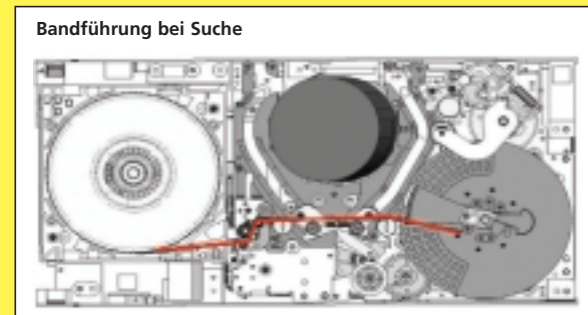
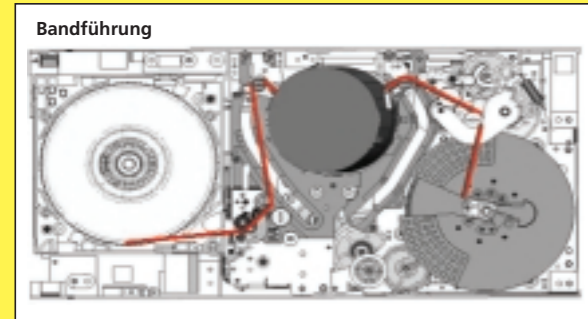
**ECC – Error Correction Code**

	SAIT	LTO-2	SDLT600
ECC Levels	3	2	unbekannt

**Doppelte Bandführung**

Die SAIT-Technik verwendet zwei Bandwege, um reibungslosen Betrieb und minimale Reibung zu gewährleisten. Nur während des Lesens, Schreibens und langsamer Bewegung des Bandes ist das Band um den Kopf gewickelt.

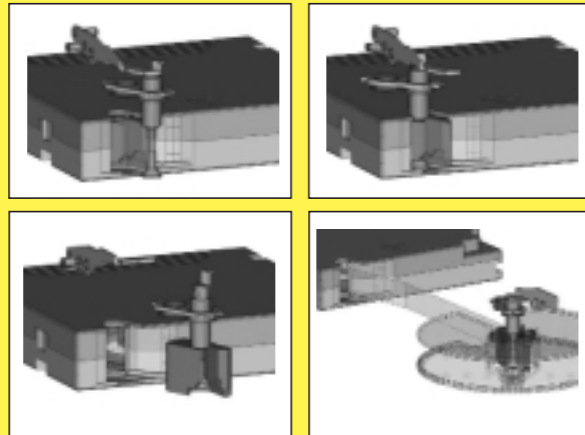
Bei Suchvorgängen, die mit hoher Geschwindigkeit ablaufen, wird ein anderer, einfacherer Weg für das Band gewählt, da das R-MIC für die genaue Positionierung verwendet werden kann.



**Einfacher Lade- und Entlademechanismus**

Der automatische Ladevorgang eines Bandes mit nur einer Spule ist nicht immer zuverlässig. Manchmal kann die Mechanik nicht das Vorspannband greifen, das Vorspannband wird falsch eingezogen oder sogar zerstört.

**Lade- und Entlademechanismus**



Der bei SAIT verwendete Band-Lade- und Entlademechanismus ermöglicht einen zuverlässigen Ladevorgang, bei dem ein Fehlladen des Bands von vornherein ausgeschlossen ist. Drei kontaktfreie optische Sensoren überwachen das Einfädeln des Bandes. Falls dennoch ein Fehler auftritt, wird dies dem Laufwerk durch die Sensoren mitgeteilt und der Vorgang automatisch wiederholt.

**Optische Sensoren**

Kontaktfreie optische Sensoren werden verwendet, um Band und Laufwerk zu überwachen, z. B. beim Einlegen des Bandes. Dies verbessert ebenso die Präzision. Durch Vermeidung des physikalischen Kontaktes mit der Mechanik wird die Abnutzung des Laufwerks und der Sensoren verringert und deren Lebensdauer erhöht.

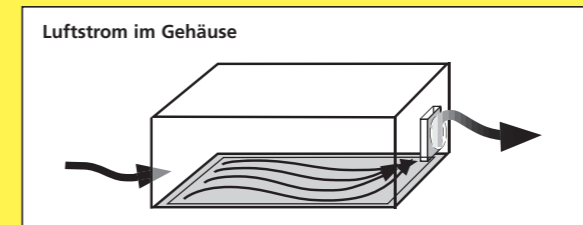
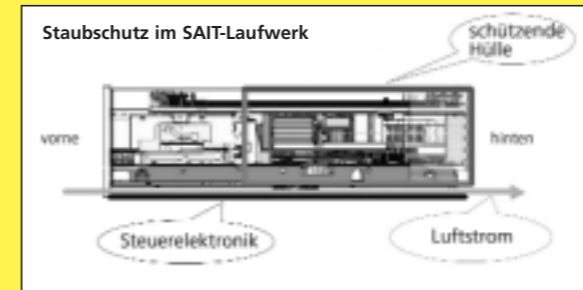
**Staubgeschütztes Design**

Staub und andere Verunreinigungen sind schädlich, sowohl für das Gerät als auch für das Band. Sie verursachen Probleme beim Betrieb einschließlich Lese-/Schreibfehlern und können so zu Datenverlust führen. SAIT ist so konzipiert, dass Staub- und andere Verunreinigungen der Laufwerksmechanik auf ein Minimum reduziert werden.

Frontblenden sollen das Laufwerk vor Verunreinigungen durch Staub schützen. Die Blende fungiert als eine Barriere, die verhindert, dass Staub durch den Medienschlitz in die Laufwerksmechanik eindringt. SAIT-Laufwerke haben zusätzlich eine interne Schutzklappe, um die Mechanik besser vor Verunreinigung zu schützen.

**Versiegelung der Bandlaufwerkseinheit**

Zusätzlich ist das gesamte Gerät mit einer Hülle umgeben, bei der die Wärme verursachenden Teile getrennt von der Mechanik sind. Der Luftstrom unter dem Laufwerk führt zu einer effizienten Kühlung der Laufwerkselektronik. Dadurch wird nicht nur die Langlebigkeit erhöht, sondern ein wirklicher Staubschutz erreicht: Das Gerät ist praktisch staubresistent.



**Schlussbetrachtungen**

Die von Sony entwickelte SAIT-Bandlaufwerkstechnologie ist neben den existierenden Marktstandards LTO Ultrium und SuperDLT eine Bereicherung für den Markt und spiegelt Sonys jahrelange Erfahrung in der Forschung und Entwicklung magnetischer Aufzeichnungstechnik wider. Die technologischen Vorteile von SAIT – das AME-Band, R-MIC, 3-fach-ECC, das Bandladesystem und das staubgeschützte Design – machen alle zusammen ein Bandlaufwerk aus, welches sich sehr gut für den Einsatz in anspruchsvollen Back-up-Lösungen eignet und die notwendige Zuverlässigkeit aufweist.

**Durchschnittliche Zuverlässigkeit**

	SAIT	LTO-2	SDLT600
MTBF	500.000 Std.	250.000 Std.	250.000 Std.
Duty Cycle	100 %	100 %	100 %
durchschnittliche Kopflebensdauer bei 25 °C	50.000 Std.	60.000 Std.	50.000 Std.

- 8. Optische Speicher
- 9. Arbeitsspeicher
- 10. Kommunikation
- 11. Standards und Normen
- 12. Das OSI-Referenzmodell
- 13. Übertragungsverfahren und -techniken
- 14. Personal Area Network PANs
- 15. Local Area Network LANs
- 16. Metropolitan Area Network MANs
- 17. Wide Area Network WANs
- 18. LAN Core-Lösungen
- 19. Eingabegeräte
- 20. Datenkommunikation
- 21. Terminals
- 22. Ausgabegeräte
- 23. Multimedia
- 24. Unterbrechungsfreie Stromversorgung

**>> Die Kapitel 8 bis 24 finden Sie im Internet**