Datenspiegelung über große Entfernungen (Wide Area)

Ein Leitfaden zu Begriffen und Technologien

BITKOM

Impressum

Herausgeber:
BITKOM
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Albrechtstraße 10

10117 Berlin-Mitte
Tel.: 030/27 576 – 0
Fax: 030/27 576 – 400
bitkom@bitkom.org
www.bitkom.org

Redaktion:	Dr. Ralph Hintemann, BITKOM
Redaktionsassistenz:	Christine Faßnacht
Verantwortliches BITKOM-Gremium:	Arbeitskreis Speichertechnologien
Stand:	November 2007, Version 1.0
Mitarbeit:	Ulrich Hamm, Cisco
	Mika Kotro, EMC²
	Dr. Dietrich Schaupp, IBM
	Horst Wilhelm Stahl, Bull
	Martin Stengel, ADVA

Ansprechpartner:
Dr. Ralph Hintemann, BITKOM e.V.
Tel: +49 (0)30 / 27576 – 250
E-Mail: r.hintemann@bitkom.org

Inhaltsverzeichnis

1 Einleitung

Die Abhängigkeit der meisten Unternehmen von der Datenverarbeitung nimmt permanent zu. Nicht verfügbare EDV-Systeme führen nicht selten zu hohen Umsatzeinbußen und einem Prestigeverlust. Gleichzeitig werden aus Kosten- und Effizienzgründen die EDV Systeme zunehmend zentralisiert. Damit der Ausfall der IT an einer Lokation für das betroffene Unternehmen nicht zu einem Desaster führt, müssen entsprechende Schutzmaßnahmen implementiert werden. Dabei gilt es, mögliche Bedrohungen und ihre Auswirkungen zu bewerten, die notwendigen Vorsorgeaufwendungen zu analysieren und zu dokumentieren.

Viele Rechenzentren entscheiden sich, eine zweite Lokation an einem entfernten Ort für einen Wiederanlauf zu nutzen. Dabei kann es sich um ein eigenes Rechenzentrum oder auch um ein Gebäude eines externen Service-Providers handeln. Alle wichtigen Daten des Unternehmens werden zeitnah in die zweite Lokation übertragen. Dies ersetzt den früher üblichen täglichen Transport von Magnetbändern von dem einen in das andere Rechenzentrum, der die heutigen Anforderungen der meisten Unternehmen nicht mehr erfüllt. Der maximal tolerierbare Datenverlust (RPO = Recovery Point Objective) liegt meistens in der Größenordnung von wenigen Minuten oder sogar Sekunden. Diese Größe ist – gemeinsam mit der Zeit, nach der die EDV-Systeme wieder zur Verfügung stehen müssen (RTO = Recovery Time Objective) – der wesentliche Parameter für die Auswahl der individuellen Lösung.

Diese gestiegenen Anforderungen für eine schnelle Wiederherstellung des EDV-Betriebs nach einem Katastrophenfall und die im gleichen Zug gesunkenen Preise für Speichersysteme und Telekommunikationsleitungen, sind ein Grund dafür, dass heute immer mehr Spiegelungslösungen auch über große Entfernungen zum Einsatz kommen. Gleichzeitig dient die Wide-Area-Technologie auch Unternehmen mit mehreren Standorten der Zusammenführung von Anwendungen, insbesondere der Datensicherung an einem zentralen Ort.

Das vorliegende Papier beschreibt die Technologien, die heute im Einsatz sind, eventuelle Restriktionen, die Vor- und Nachteile und daraus resultierend die möglichen Einsatzgebiete der Wide-Area-Technologien.

2 Motive für den Einsatz von Wide-Area-Lösungen

Für die Koppelung von Rechenzentren über größere Entfernung können unterschiedliche Gründe sprechen. In vielen Fällen ist es der Schutz vor Katastrophen, d.h. die Möglichkeit, das Unternehmensgeschäft auch nach einem Totalausfall eines Rechenzentrums weiter betreiben zu können. Neben dem Katastrophenschutz sprechen aber auch die Möglichkeit einer zentralen Datensicherung (Backup) bei dezentralen Standorten sowie Kostenvorteile durch eine zentrale Administration mehrerer Rechenzentren für Wide-Area-Lösungen.

Ausfall eines Rechenzentrums	Zentrale Backups	Kostenvorteile
■ Mögliche Gründe für den Ausfall: ■ Höhere Gewalt ■ Menschliche Fehlhandlung ■ Vorsätzliche Handlung ■ Organisatorische Mängel ■ Technisches Versagen	■ Backup-Infrastruktur nur an einem Ort vorzuhalten ■ Durch zweiten Standort keine Auslagerung der Backup-Dateien an anderen Ort notwendig ■ Einsatz optimaler Backup-Lösungen auch für kleinere Standorte	■ Zentrale Verwaltung der Infrastruktur möglich ■ Effizienter Personaleinsatz ■ Geringere Aufwendungen für Schulungen

Abbildung 1: Gründe für Wide-Area-Lösungen

Schutz vor Katastrophen

Die Spiegelung der Daten an einen zweiten Standort bietet Sicherheit für den Betrieb der Datenverarbeitung nach Katastrophen, die an einem Standort aufgetreten sind. Auch wenn die Wahrscheinlichkeit für den Totalausfall eines Rechenzentrums eher gering ist, so ist der mögliche Schaden so immens, dass der Aufwand in vielen Fällen gerechtfertigt ist. Je nach Entfernung, den Anforderungen an die Datenkonsistenz und den maximal tolerierbaren Datenverlust kann synchron oder asynchron gespiegelt werden. Damit kann im Katastrophenfall der Betrieb mit einer kurzen Unterbrechung weitergehen. Die Gründe für Ausfälle können vielfältig sein und reichen vom Stromausfall über Feuer, Überschwemmung durch Hochwasser, technische Defekte bis hin zu Sabotage und zu Terroranschlägen.

Zentrale Datensicherung von entfernten Standorten

Über ein Wide Area Network (WAN) ist es auch möglich, eine Datensicherung von Daten, die auf mehrere Standorte verteilt sind, zentral an einem Standort durchzuführen. Das hat den Vorteil,

dass man die Infrastruktur für die Datensicherung nicht an jedem Ort vorhalten muss. Werden lokale Backup-Daten an den zentralen Standort repliziert, werden auf diese Weise die Backup-Daten automatisch an einem zweiten Standort aufbewahrt und es entfällt die sonst häufig extra durchzuführende Auslagerung der Datensicherungs-Medien. Werden die Sicherungsdaten an den zentralen Backupserver gesendet, dann kann durch Replikation der zentralen Datensicherung die komplette Datensicherung des Unternehmens redundant und katastrophensicher durchgeführt werden. Durch eine zentrale Datensicherung lassen sich auch die Daten solcher (kleineren) Standorte optimal sichern, in denen bisher eine Datensicherung aufgrund des hohen Aufwandes nur in geringerem Umfang durchgeführt wurde.

Kostenvorteile durch zentrale Verwaltung

Über eine Wide-Area-Lösung lässt sich die Infrastruktur an entfernten Standorten zu einem großen Teil zentral verwalten. Durch diese Zentralisierung können die IT-Mitarbeiter effizienter eingesetzt und damit Kosten gespart werden. Außerdem sinken die Aufwendungen für Schulungen dieser Mitarbeiter.

Jedes Unternehmen muss individuell für sich selbst bestimmen, ob und in welcher Form sich eine Wide-Area-Lösung zur Abdeckung der eigenen Anforderungen anbietet. Dazu müssen die für das Unternehmen relevanten Gefährdungen und ihre Vermeidung erarbeitet und bewertet werden. Diese sind gemeinsam mit der Verbesserung der Effektivität und Effizienz durch die zentrale Datensicherung und die zentrale Verwaltung den Kosten der Lösung gegenüberzustellen.

3 Fragen, die vor der Entscheidung für eine Wide-Area-Lösung gestellt werden sollten

Vor der Entscheidung für die Auswahl einer Wide-Area-Lösung, müssen zunächst die individuellen Anforderungen und Rahmenbedingungen analysiert werden. Dazu sind insbesondere die folgenden Fragen zu klären:

- Welche und wie viel Daten müssen in welchen Zeitraum vom primären Standort zum sekundären bzw. zum Datensicherungsstandort gespiegelt werden?
- Welche Spiegelungsanwendungen sollen zum Einsatz kommen – Rechner-basierend, Speichersubsystem-basierend, SAN/Appliance-basierend oder Schreiben der Datensicherung vom primären Standort zum sekundären Standort?
- Wie groß ist die Entfernung zwischen den Standorten und wie groß ist die verfügbare Bandbreite zwischen den Standorten?
  Metro-Optische Systeme (DWDM) können in aller Regel bis zu einer Entfernung von ca. 300 km zum Einsatz kommen, CWDM Systeme bis zu ca. 90 km. Größere Entfernungen müssen in aller Regel über eine TCP/IP-Verbindung realisiert werden. Das hat zum einen Auswirkung auf die Übertragungsverzögerung, zum anderen auch – abhängig von der verfügbaren Bandbreite – auf den möglichen Durchsatz.
- Wie groß kann oder wie klein muss die Umschaltzeit zwischen dem primären und sekundären Standort sein? Oder anders ausgedrückt: Welche Wiederanlaufzeit muss garantiert werden (RTO = Recovery Time Objective)?
- Wie groß darf das Delta der Daten zwischen dem primären und sekundären Standort sein? Müssen die Daten synchron oder asynchron gespiegelt werden (RPO = Recovery Point Objective)?
- Müssen die zu übertragenden Daten verschlüsselt werden?

Die Beantwortung dieser Fragen liefern die Voraussetzungen, um eine für den individuellen Anwendungsfall geeignete Wide-Area-Lösung zu finden. So können insbesondere die Anforderungen an den Datendurchsatz, an die tolerierbare Latency (Übertragungsverzögerung) und an die Sicherheitsanforderungen definiert werden.

Anforderungen an den Datendurchsatz

Die Anforderungen an den Datendurchsatz bestimmen die dafür notwendige Bandbreite zwischen den Standorten. Wenn eine IP-basierte Verbindung zwischen den Standorten zum Einsatz kommt, ist zu berücksichtigen, dass dann die Flusskontrolle durch TCP und nicht mehr durch Fibre Channel erfolgt. Der wichtige Unterschied dabei ist, dass TCP einen sogenannten Slow-Start verwendet und dadurch eine Verzögerung beim Erreichen des maximal möglichen

Durchsatzes eintreten kann. Es gibt herstellerabhängige Modifizierungen der TCP-Flusskontrolle, die diese Verzögerung ausschaltet.

Latency

Die Latency (Übertragungsverzögerung) auf der Übertragungsstrecke ergibt sich aus der Signallaufzeit auf der Verbindungsstrecke und den dazwischen liegenden Netzwerkelementen. Die reine Signallaufzeit ist auch bei einer optischen Verbindung 5 µs (Mikrosekunden) pro Kilometer und kann sich bei einer IP-Verbindung durch dazwischen liegende Netzwerkelemente (Router, Switches) auch noch entsprechend vergrößern. Die Nutzung von Verschlüsselung und Komprimierung kann – abhängig von der Implementierung - ebenfalls Auswirkungen auf die Latenzzeit haben (Hardware- oder Software-basierende Verfahren). Durch Schreib-Beschleunigungsfunktionen kann die sogenannte „Roundtrip-Time“ zwischen den Standorten reduziert werden. Das führt zu einer Erhöhung des Durchsatzes oder erlaubt den Einsatz dieser Lösung auch bei einer größeren Distanz zwischen den Standorten bei gleich bleibendem Durchsatz.

Sicherheit

Bei Verbindungen über öffentliche Netze, kann für sensible Daten die Anforderung bestehen, dass diese verschlüsselt werden müssen. Dies ist bei der Auswahl der Übertragungstechnik (DWDM, CWDM oder TCP/IP) zu berücksichtigen.

4 Technologie-Überblick

4.1 SAN-Kopplung über IP

4.1.1 TCP/IP als Transport-Protokoll

Ein Punkt, der bei Business Continuance und Disaster Recovery Lösungen immer zu Diskussionen führt, ist die Frage der Entfernung des zweiten Standortes. Einigkeit herrscht dahin, dass der zweite Standort soweit entfernt sein sollte, dass eine Katastrophe keine Auswirkungen auf dieses Rechenzentrum haben darf. Die Schwierigkeit dabei ist, dass unterschiedliche Anforderungen unter einen Hut gebracht werden müssen. Größere Entfernungen bedeuten mehr Sicherheit aber natürlich auch eine größere Latenzzeit bei der Übertragung der Daten. Manche Anwendungen sind gegenüber größeren Latenzzeiten sehr empfindlich. Ein gutes Beispiel dafür ist die synchrone Datenspiegelung. Die asynchrone Datenspiegelung ist gegenüber größeren Latenzzeiten wesentlich unempfindlicher. Wenn die Anwendung verlangt, dass im primären und sekundären Standort die gleichen Informationen vorliegen müssen, kommt natürlich nur die synchrone Datenspiegelung in Frage. Das hat zur Folge, dass die maximale Entfernung zwischen primären und sekundären Standorten in der Größenordnung von ca. 100 km liegt. Bei dieser Entfernung kann auf die verschiedensten Übertragungstechniken zurückgegriffen werden, wie z.B. CWDM (Coarse Wavelength Division Multiplexing) oder DWDM (Dense Wavelength Division Multiplexing). DWDM bietet größere Flexibilität, Leistung und Verfügbarkeit, hat dafür aber auch einen höheren Preis als CWDM. Selbstverständlich kann auch IP als Transport-Protokoll in Frage kommen.

Firmen mit Anwendungen, die nur eine asynchrone Datenspiegelung erfordern, haben den Vorteil, dass der zweite Rechenzentrums-Standort sehr weit entfernt sein kann. Dafür müssen aber auch Transporttechniken zum Einsatz kommen, die in der Lage sind solche Entfernungen zu überbrücken – wie z.B. IP. Ein Protokoll, das IP zur Übertragung nutzt, ist FCIP (Fibre Channel over IP). Mit diesem Protokoll können 'Fibre Channel Fabrics' über eine IP-Verbindung transparent gekoppelt werden.

4.1.2 Fibre Channel over IP

FCIP ist ein Protokoll, das innerhalb der Internet Engineering Task Force (IETF) entwickelt und standardisiert wird. Mit FCIP können 'Fibre Channel'-Rahmen transparent über eine IP-Verbindung übertragen werden. FCIP funktioniert ähnlich wie viele andere 'Tunneling'- oder Encapsulation-Protokolle. Bekannte Beispiele sind DLSw (Data Link Switching) oder XoT (X.25 Over TCP). Auch bei FCIP sind an den Außenpunkten Einheiten, die an das 'Fibre Channel SAN' angeschlossen sind und gleichzeitig auch eine Verbindung zum IP-Netz haben. Diese Einheit nimmt die 'Fibre Channel'-Rahmen entgegen, verpackt diese in ein IP-Paket und verwendet TCP auf der Transport-Ebene, um einen zuverlässigen Transport der Pakete zu garantieren. An der Gegenstelle läuft das

ganze Verfahren in umgekehrter Reihenfolge ab. Die FCIP- und TCP/IP-Informationen werden entfernt und es kommt ein 'Fibre Channel'-Rahmen im SAN an.

Wie Vieles, hat auch das FCIP-Protokoll seine Stärken und Schwächen. Durch die transparente Verbindung können die SAN-Administratoren so gut wie alle Management-Prozeduren verwenden, die sie bisher eingesetzt haben. Also ein transparenter Management-Zugriff auf den sekundären Standort. Der Nachteil dabei ist, dass nun aus zwei vorher unabhängigen SANs ein großes SAN gebaut worden ist, es existiert nun also ein geografisch verteiltes SAN. Dabei müssen sich die Anwender hauptsächlich mit zwei Problemen beschäftigen. Das erste Problem ist, dass die Stabilität dieses erweiterten SANs von der Stabilität der Verbindung zwischen den beiden Standorten abhängt. Das zweite Problem ist, dass sich mögliche Schwierigkeiten, die an einem Standort auftreten, nun auch an den anderen Standort verbreiten. Das kann zu Ausfällen führen und ist eigentlich das Gegenteil von dem was erreicht werden soll. Das Ziel ist ja, die Daten und Anwendungen am primären Standort zu schützen und nicht die Wahrscheinlichkeit von Ausfällen zu vergrößern. Es ist daher wichtig, dass Segmentierungsfunktionen zur Verfügung stehen, die eine logische Trennung der einzelnen SANs erlauben und damit die Auswirkung von Ausfällen auf der WAN-Strecke minimiert oder ganz verhindert werden.

Typische Einsatzszenarien für 'Fibre Channel Over IP' (FCIP) können sein:

- Synchrone Daten-Replikation – ermöglicht 'o Recovery Point Objective' (RPO) bei der Nutzung von intelligenten Speichersubsystemen mit Datenreplikations-Software. Die Netzwerk-Latenz ist dabei ein wichtiger Faktor für Disk-I/O-Service-Zeiten und damit auch der Anwendungsleistung. Faktoren, die die Netzwerk-Latenz-Zeit beeinflussen sind:
  - Entfernung
  - 'Store and Forward'-Verzögerung in Router und Switches
  - Last auf der Verbindung durch andere Anwendungen
  - 'Quality of Service' (QoS) Definitionen im Netz
- Optische SAN-Verbindungen werden in diesem Anwendungsbereich bevorzugt eingesetzt, da sie in der Regel die geringere Latenzzeit haben.
- Asynchrone Daten-Replikation – ermöglicht ein niedriges 'Recovery Point Objective' (RPO) bei der Nutzung von intelligenten Speichersubsystemen mit Asynchroner Datenreplikations-Software. Bei dieser Methode hat die Netzwerk-Latenz-Zeit keinen Einfluss auf die Leistung der Anwendung wie bei der synchronen Replikation. Durch Tuning-Maßnahmen bei der Replikations-Software und der FCIP-Verbindung kann der Datendurchsatz verbessert werden.
- Remote Tape Vaulting – ermöglicht Datensicherung auf Magnetplatte (disk) oder Magnetband (tape) in ein entferntes Rechenzentrum für 'Disaster Recovery'. Tape-Anwendungen unterstützen typisch nur einen ausstehenden I/O, was den Durchsatz und die Entfernung limitiert. Es stehen aber auf der SAN/FCIP-Seite Funktionen zur Verfügung wie z.B. 'Write

Acceleration', um den Durchsatz zu optimieren. Optional kann auch Komprimierung verwendet werden.

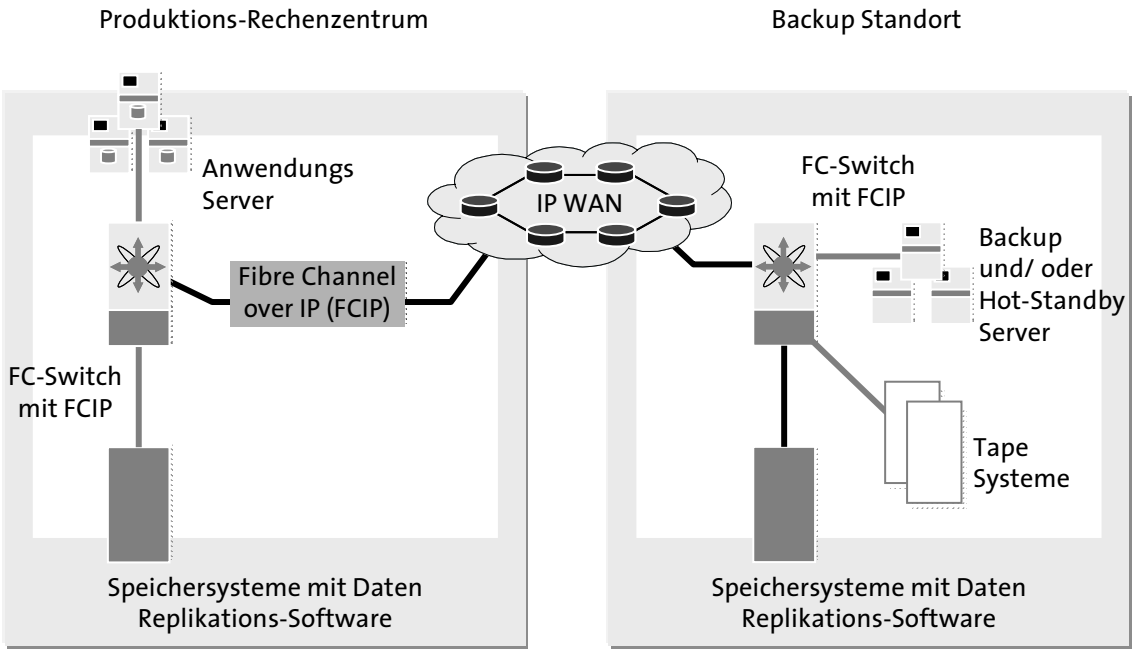

Abbildung2: FCIP-Topologie

4.1.3 Latenz-Zeiten durch die FCIP-Verbindung

Die Latenz-Zeiten einer FCIP-Verbindung hängen von mehreren Faktoren ab. Nachfolgend sind die wichtigsten aufgezählt :

- Grundsätzlich natürlich die Entfernung
- Die Netzwerktopologie zwischen den Standorten (Anzahl 'Hops' Router, Switches)
- Müssen die Daten verschlüsselt werden?
- Wird Komprimierung verwendet?
- TCP-Flusskontrolle und Window-Sizes
- Frame-Größen -> Fibre Channel – Ethernet
- Protokollumsetzung

Das Umsetzen von Fibre Channel auf 'Fibre Channel over IP' (FCIP) erzeugt ebenfalls eine zusätzliche Latenz. Diese ist abhängig von der Implementierung (HW oder SW) und kann ca. 70 µs bis 75 µs pro Ende betragen. Die maximale 'Fibre Channel Frame Size' ist größer als die Standard-Ethernet-MTU (Maximum Transfer Unit). Dies ist ein wichtiger Punkt, da in der Regel die Umsetzung auf Ethernet erfolgt. Wenn die Standard-Ethernet-MTU von 1500 Bytes verwendet wird, kann das bedeuten, dass die 'Fibre Channel Frames' in mehrere Ethernet-Frames segmentiert werden müssen. Dies bedeutet zusätzlichen Verwaltungsaufwand (overhead). Das kann beim

Einsatz von Ethernet „Jumbo-Frames“ vermieden werden. Dabei können bis zu 8 KB große Ethernet-Frames zum Einsatz kommen. Das reduziert den Overhead und die Latenz und führt dadurch zu einem besseren Durchsatz.

Die Verschlüsselung benötigt ebenfalls Zeit. Eine HW-basierende Lösung ist dabei in jedem Fall einer SW-basierenden Lösung vorzuziehen, da diese erheblich weniger Zeit benötigt.

Inwieweit die Verwendung von Komprimierung sinnvoll ist, hängt von der Bandbreite ab. Je größer die Bandbreite desto kleiner der Komprimierungsfaktor, um keine Nachteile durch die Komprimierung entstehen zu lassen.

Die Flusskontrolle bei TCP unterscheidet sich von der Fibre-Channel-Flusskontrolle. Ein wichtiger Unterschied ist der Slow-Start, der bei TCP verwendet wird. (Siehe auch „Anforderungen an den Datendurchsatz“ in Kapitel 3)

4.1.4 Ende-zu-Ende-Latenz bei unterschiedlicher Last auf den FCIP-Verbindungen

Die Ende-zu-Ende-Latenz bei FCIP-Verbindungen hängt im Wesentlichen auch von der Netzwerktopologie ab, d.h. bei einer Punkt-zu-Punkt-Verbindung, die exklusiv für FCIP verwendet wird, ohne weitere Netzwerkelemente, ist diese kleiner und auch einfacher zu betreiben. In diesem Fall sind keine zusätzlichen Maßnahmen zu implementieren, die die FCIP-Daten priorisieren (QoS) solange die Bandbreite insgesamt immer für FCIP zur Verfügung steht. Wird die Verbindung gemeinsam mit anderen Anwendungen genutzt, müssen Verfahren zum Einsatz kommen, die die FCIP-Daten priorisieren bzw. die Minimum- und Maximum Bandbreite, die für FCIP benötigt wird, garantiert.

QoS bzw. die Priorisierung der FCIP-Daten müssen natürlich durchgehend implementiert werden und im laufenden Betrieb überwacht werden. Bei der Nutzung eines Service-Providers ist das ein wichtiger Punkt bei der Definition der Anforderungen. Dabei darf natürlich nicht vergessen werden, dass die Stabilität und Qualität ebenfalls entscheidende Parameter sind. Wiederholte Übertragungen der Datenpakete haben einen großen negativen Einfluss auf Durchsatz und Zuverlässigkeit.

4.2 WDM für den Eigenbetrieb von Rechenzentren

4.2.1 WDM Technik im Vergleich

4.2.1.1 DWDM Dense Wave Division Multiplexing

Die DWDM-Technik zeichnet sich durch eine hohe Dichte der zu übertragenden Wellenlängen über ein Faserpaar aus. Je nach Hersteller können zwischen 16 und 64 Wellenlängen übertragen werden (ITU-T G.694). Die Idee dabei ist, viele unabhängige Datenströme gleichzeitig über

dieselbe Fibre-Faser zu übertragen, indem jeder Datenstrom in „einer anderen Farbe“ übertragen wird. Neben der Kapazität ist die Reichweite ein wesentlicher Unterschied zu einem CWDM-System. Es können Entfernungen ohne Verstärker bis ca. 100 km erreicht werden. Mit dem Einsatz von Verstärkertechniken sind je nach Ausbaustufe des Systems bis zu 250 km erreichbar. Dabei kann mit einem DWDM-System über ein Glasfaserpaar bis zu 640 Gbit/s übertragen werden.

4.2.1.2 CWDM Coarse Wave Division Multiplexing

Die CWDM-Technik unterstützt bis zu acht von der ITU–T G.694 spezifizierte Wellenlängen. Der Wellenlängenabstand beträgt 20 nm pro Wellenlänge. Bei der DWDM-Technik beträgt dieser üblicherweise 1,6 nm oder 0,8 nm. Dadurch ergeben sich auch die wesentlichen Unterschiede zwischen den beiden Techniken. CWDM kann weniger Bandbreite übertragen, ist in der Entfernung limitierter (ca. 60 km – 80 km) aber dafür im Preis deutlich günstiger.

4.2.2 Topologien

Bei beiden Verfahren werden folgende Topologien unterstützt:

- Point-to-Point
- Linear add/drop
- Ring

Die Point-to-Point (P-t-P)-Topologie ist die meistverbreitete und klassische Verbindung zur Koppelung von zwei Standorten. Bei der P-t-P-Verbindung werden die Daten von einem Standort A zu einem entfernten Standort B in einer 'eins-zu-eins-Verbindung' übertragen.

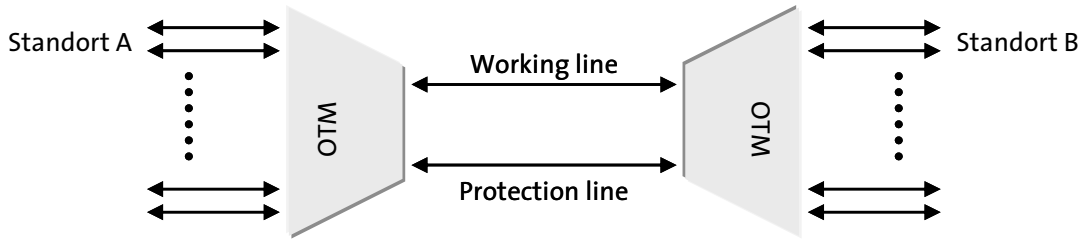

Abbildung 3: Point-to-point-Topologie

Bei der 'Linear add/drop'-Topologie werden üblicherweise mehr als zwei Standorte miteinander vernetzt. Dabei werden Daten von einem Standort A sowohl zu einem Standort B als auch zu einem Standort C übertragen. Wellenlängen werden in jedem Standort herausgenommen oder eingespeist (add&drop).

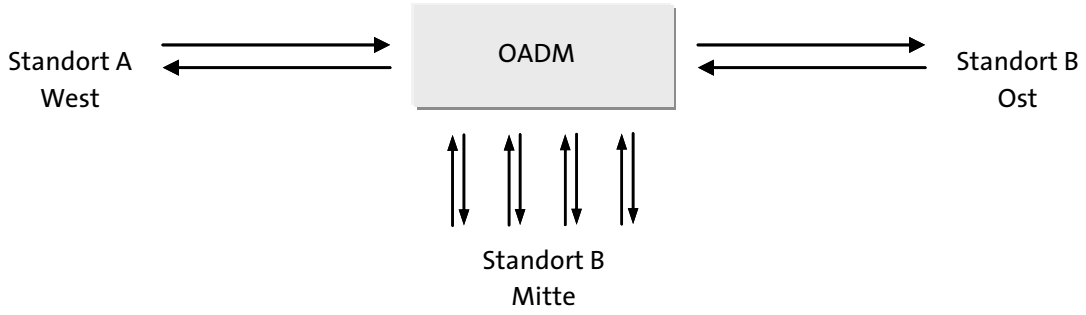

Abbildung 4: 'Linear add/drop'-Technik

Bei der Ring-Topologie werden mehrere Standorte in einem Ring verbunden. Dadurch kann jeder Standort mit jedem anderen Standort Verkehrsbeziehungen betreiben. Diese Topologie wird sehr häufig für sogenannte Carrier-Netze eingesetzt. Im Rechenzentrumsbetrieb kommt diese Technik seltener zum Einsatz, da diese sehr komplex und teuer ist. Durch die Arbeitsweise kann sie unterschiedliche Laufzeiten verursachen. Diese verschiedenen Laufzeiten können bei bestimmten Anwendungen zu großen Problemen führen.

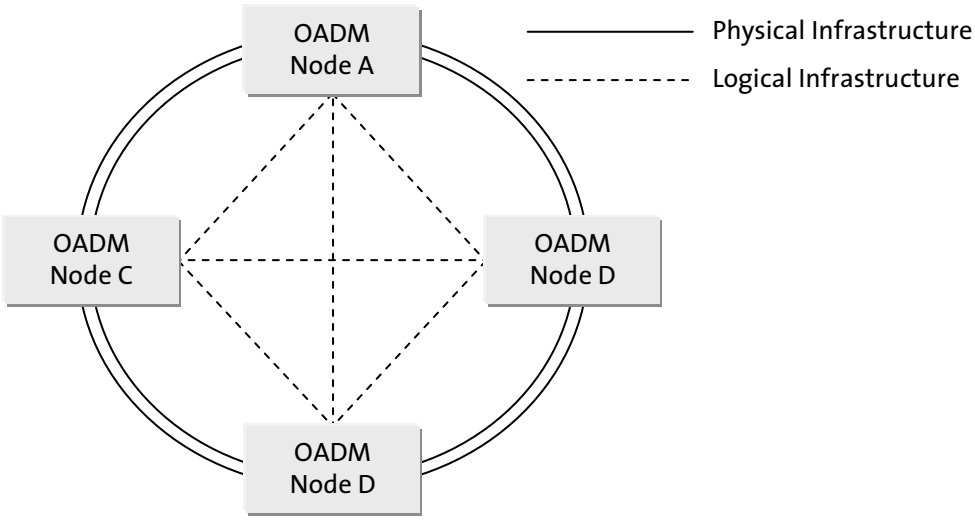

Abbildung 5: Ring-Topologie

4.2.3 TDM-Technik

Die 'Time Division Multiplexing' (TDM)-Technik wird dazu verwendet das WDM-System noch effizienter zu gestalten. Dabei werden mehrere 'lokale Anwendungen' gebündelt und über ein und dieselbe Wellenlänge übertragen. Somit ist das System, wie der Abbildung unten gezeigt, in der Lage mit einem 4:1 TDM-Modul bei 64 DWDM Wellenlängen 256 Anwendungen über ein System mit einem Faserpaar zu betreiben. Die Idee hier ist, mehrere langsame Datenströme, die, jeder für sich, deutlich unter der Nominalübertragungsbreite von 1, 2, 4 oder mehr Gbit/s liegen, zu bündeln. TDM kann gleichzeitig mit WDM genutzt werden, um die vorhandenen Glasfasern wirklich optimal zu nutzen.

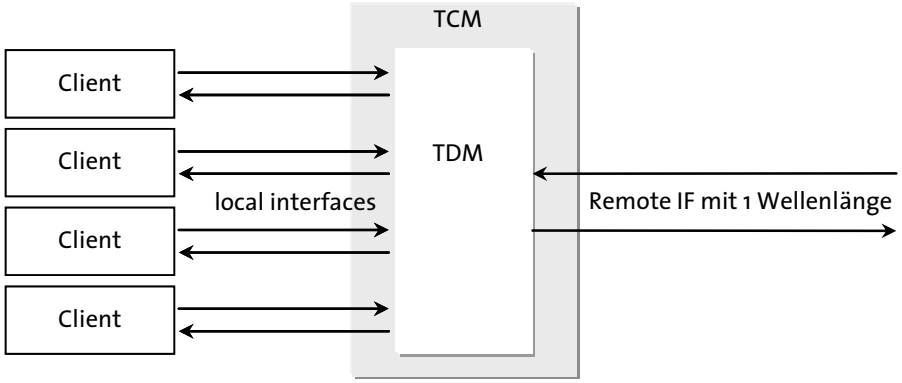

Abbildung 6: TDM im 4:1-Betrieb – 4 Anwendungen über eine Wellenlänge

4.2.4 Ein – und Zweifaserbetrieb

Um mit der Ressource Glasfaser sparsam umzugehen, gibt es DWDM-Hersteller, die sowohl den Betrieb über ein Glasfaserpaar (Zweifaserbetrieb) als auch den Betrieb mit einer Faser (Einfaserbetrieb) ermöglichen.

4.2.5 Protokolle, Leistung und Latenz

Der große Vorteil eines WDM-Systems ist, dass dieses protokoll- und bittransparent arbeitet. Somit ist das System in der Lage sämtliche Protokolle zu übertragen. Die Verzögerungszeit innerhalb des Systems ist sehr gering. Sie bewegt sich zwischen 200 ns bei Single-Channel-Karten und bis zu 10 ms bei TDM-Channel-Karten. Somit kann in den meisten Fällen mit der Lichtgeschwindigkeit die gesamte Verzögerungszeit bestimmt werden.

Bei 10 km beträgt diese 0,1 ms (Hin- und Rückweg). Dies und die hohe Skalierbarkeit sind entscheidende Vorteile gegenüber anderen Lösungen, z.B über IP. Deshalb werden WDM-Systeme sehr häufig verwendet, wenn synchrone, sehr breitbandige und/oder eine große Anzahl von Anwendungen benötigt werden. Aufgrund der Skalierbarkeit, der Umsetzung von Multi- auf Singlemode und der Verstärkung werden WDM-Systeme mittlerweile sehr häufig auch für größere Entfernungen eingesetzt. Die neueren Protokolle wie Fibre Channel, FICON oder Gigabit-Ethernet ermöglichen eine Übertragung über größere Entfernungen, teilweise nahezu ohne Leistungseinbußen. Natürlich schränken Protokolle wie ESCON oder manche Cluster-Lösungen die Entfernungen teilweise noch ein. Hier eine nicht vollständige Aufzählung solcher Protokolle:

- Fast Ethernet, Gigabit Ethernet, 10G Ethernet
- 1Gbit/2Gbit/4Gbit/10Gbit Fibre Channel/FICON
- STM-1, STM-4, STM-16, STM-64
- OC-1, OC-12, OC-64, OC-192

4.2.6 Schutz und Sicherheit

Sehr wichtig für eine Hochverfügbarkeitslösung sind natürlich Schutz- und Sicherheitsaspekte. Durch sogenannte Fibre-Protection-Umschaltmodule kann ein Ausfall einer Glasfaser zu 100 % abgesichert werden. In diesem Fall schaltet das Modul automatisch auf den Zweitweg um. Intelligente Umschaltmodule messen ständig sowohl den aktiven Primary-Weg als auch den inaktiven Datensicherungs-Weg. Durch diese Leitungsüberwachung- und Qualitätsmessung ist immer ein sicherer Betrieb gewährleistet. Oftmals können so Angriffe auf die Glasfaser oder Verschlechterungen der Übertragungsqualität schnell registriert und die Ursachen behoben werden.

4.2.7 Eigenbetrieb und Management

Das Management eines WDM-Systems überwacht jede einzelne Komponente. Es gibt Auskunft über die Verbindungen und deren Leitungsqualität. Die meisten WDM-Chassis sind hochverfügbar ausgestattet (Power&Fan). Das WDM-System kann meistens über ein eigenes GUI überwacht werden als auch problemlos in ein übergreifendes Netzwerkmanagement System eingebunden werden.

Der Zugriff auf das WDM-System ist üblicherweise „SSH und RADIUS“ gesichert. Durch die Modularität, Hochverfügbarkeit und ein einfaches Einbinden und Überwachen in ein Netzwerkmanagement System eignet sich ein WDM-System ideal zu einem Eigenbetrieb. Die meisten WDM-Systeme sind einfach zu konfigurieren und selbstverständlich unterbrechungsfrei zu erweitern. Damit ist ein WDM-System im Vergleich zu anderen Übertragungstechniken wenig komplex und sehr leistungsfähig.

4.2.8 Zusammenfassung

Aufgrund der Verfügbarkeit von CWDM- und DWDM-Systemen ist eine Koppelung von Rechenzentren wesentlich einfacher und effizienter geworden. Hinsichtlich Entfernungen, Anbindung verschiedener Standorte, Übertragung unterschiedlicher Protokolle/Applikationen und zuletzt unterschiedlich benötigter Ausbaustufen eignet sich das WDM-System geradezu exzellent für eine Verbindung.

5 Glossar

5.1 Übertragungstechniken

DWDM

Das DWDM (Dense Wavelength Division Multiplex) ist eine Variante der Wellenlängenmultiplex-verfahren (Abk. WDM für Wavelength Division Multiplex oder WDMA für Wavelength Division Multiple Access).

Beim Wellenlängenmultiplexverfahren werden Lichtsignale, die aus verschiedenen Spektralfarben (Lichtfrequenzen) bestehen, zur Datenübertragung in einem Lichtwellenleiter verwendet. Über Laser oder Licht emittierende Dioden (LED) erzeugte Spektralfarben bilden jeweils einen eigenen Übertragungskanal.

DWDM gilt zurzeit als die leistungsstärkste Variante der WDM-Verfahren. Die zur Übertragung im Glasfaserkabel verwendeten Wellenlängen (Spektralfarben) liegen sehr dicht beieinander; der Abstand der Wellenlängen beträgt nur 0,8 Nanometer (nm) bei 100 GHz bzw. 1,6 nm bei 200 GHz. Dies kann erreicht werden, indem temperatur- und wellenlängenstabilisierte Laser (thermostatierte DFB-Laserdioden) und hochwertige Filter eingesetzt werden. DWDM ermöglicht Datenübertragungsraten von 10 bis 40 Gbit/s pro Kanal bei bis zu 160 Kanälen. Damit rücken Übertragungswerte von insgesamt 1 Tbit/s in den Bereich des Möglichen.

Abhängig von Hersteller, Netzdesign und Glasfasertyp sind optische Verstärker in Abständen von 80 bis 200 km erforderlich. Eine elektrische Datenregeneration muss jeweils nach 600 bis 2000 km erfolgen. Der wesentliche Anwendungsbereich von DWDM liegt in der Übertragung über weite Entfernungen im Wide und Global Area Network.

CWDM

CWDM (Coarse Wavelength Division Multiplex – grobes Wellenlängenmultiplexverfahren) ist eine gegenüber DWDM kostengünstigere Variante eines WDM-Verfahrens. Der Abstand der Wellenlängen liegt zwischen 8 nm und 50 nm im sogenannten dritten optischen Fenster bei 1550 nm und zwischen 5,7 nm und 50 nm im zweiten optischen Fenster (1310 nm). Auf Singlemode-Glasfasern ist ein Kanalraster von 20 nm mit 18 Kanälen (1270 nm ... 1610 nm) standardisiert. Durch diese „grobe“ Aufteilung der Wellenlängen können kostengünstige Laser und Komponenten verwendet werden. Im Wellenlängenmultiplex werden Datenübertragungsraten bis 2,5 Gbit/s und Leitungsreichweiten bis 70 km ohne Signalverstärkung erreicht. Das Haupteinsatzgebiet von CWDM liegt im Stadtbereich (sog. Metropolitan Area Network).

Ein Übergang von der CWDM-Technik zur DWDM-Technik kann mittels Hybrid-CWDM/DWDM erfolgen.

Ethernet

Ethernet stellt eine kabelgebundene Datennetztechnik für lokale Datennetze (LANs) dar. Damit wird der Datenaustausch in Form von Datenrahmen zwischen allen in einem lokalen Netz angeschlossenen Geräten, wie z.B. Computern oder Druckern ermöglicht. In seiner traditionellen Ausprägung erstreckt sich das LAN dabei nur über ein Gebäude. Heute verbindet die Ethernet-Technik auch Geräte über weite Entfernungen.

Ethernet ist seit den 1990er Jahren die meistverbreitete LAN-Technik. Sie umfasst Festlegungen für Kabeltypen und Stecker, beschreibt die Signalisierung für die Bitübertragungsschicht und legt Paketformate und Protokolle fest. Ethernet ist weitestgehend in der IEEE-Norm 802.3 standardisiert. Ethernet kann die Basis für Netzwerkprotokolle, wie z.B. TCP/IP bilden.

5.2 Anwendungen

Synchrone Spiegelung

Um neben der Systemverfügbarkeit auch bei der Datenverfügbarkeit durch Redundanzen gegen Ausfälle gesichert zu sein, können Daten über Spiegelungen/Replikationen synchron oder asynchron auf einem zweiten Speichersystem redundant vorgehalten werden. Bei der synchronen Datenspiegelung verfügen Primär- und Sekundärsystem zu jedem Zeitpunkt über denselben Datenbestand, d.h., die Daten werden auf beide Speichersysteme gleichzeitig geschrieben. Der Vorgang gilt erst dann als abgeschlossen, wenn der Block auf dem Speicher am entfernten Standort abgelegt wurde und die Bestätigung dafür beim Quellsystem eingetroffen ist. Hierdurch kommt es also zu Verzögerungen (ca. 1msec/100km). Synchrone Spiegelungen sind heute bis zu einer maximalen Entfernung von 100 km üblich. Die synchrone Spiegelung hat den Vorteil, dass zu jeder Zeit eine identische Kopie aller Daten verfügbar ist.

Asynchrone Spiegelung

Bei asynchroner Spiegelung/Replikation werden die Daten ebenfalls redundant vorgehalten, es liegt jedoch nicht zum jedem Zeitpunkt der identische Datenbestand zwischen Ursprungs- und Zielsystem vor. Asynchrone Spiegelung wird typischerweise bei Distanzen größer als 100 km eingesetzt. Bei einem Ausfall des Primärsystems kann es also vorkommen, dass Daten, die auf das Primärsystem geschrieben wurden und in der Anwendung bestätigt worden sind, noch nicht auf das Spiegelsystem gespeichert wurden. Dieser mögliche Datenverlust muss in den Wiederanlaufplänen des Unternehmens berücksichtigt werden.

Oft werden daher zwischen Ursprungs- und Zielsystem in festgelegten Intervallen die inzwischen aufgetretenen Änderungen übertragen. Im Katastrophenfall wird dann auf den letzten konsistenten Stand zurückgesetzt, der maximale Datenverlust beträgt also die Dauer eines Intervalls.

5.3 Protokolle

TCP

Das Transmission Control Protocol (TCP) ist ein Protokoll, über das die Art und Weise des Datenaustausches zwischen Computern geregelt ist. TCP wird von allen Betriebssystemen moderner Computer beherrscht. TCP gilt als zuverlässiges, verbindungsorientiertes Transportprotokoll in Computernetzwerken und ist Teil der Internetprotokollfamilie. TCP ist ein sehr weit verbreitetes Protokoll. Dies liegt an einer Reihe von positiven Eigenschaften. So werden z.B. Datenverluste erkannt und automatisch behoben, die Datenübertragung ist in beiden Richtungen möglich und eine Netzwerküberlastung wird verhindert.

Die erste Standardisierung von TCP erfolgte im Jahre 1981 als RFC 793. Es gibt heute viele Erweiterungen, die in jeweils neuen RFCs, einer Reihe von technischen und organisatorischen Dokumenten zum Internet, spezifiziert werden und alle zu TCP gehören.

Zwischen den zwei Endpunkten einer Netzwerkverbindung stellt TCP - im Unterschied zum verbindungslosen UDP (User Datagram Protocol) - einen virtuellen Kanal her. In den meisten Fällen setzt TCP auf das IP (Internet-Protokoll) auf. Aus diesem Grund wird häufig auch vom TCP/IP-Protokoll gesprochen.

IP

Das Internet Protocol (IP) ist ein weit verbreitetes Netzwerkprotokoll. IP bildet die erste vom Übertragungsmedium unabhängige Schicht der Internetprotokollfamilie. Mittels der IP-Adresse und der Subnet Mask können Computer innerhalb eines Netzwerkes in logische Einheiten, sogenannte Subnetze, gruppiert werden. So ist es möglich, Computer in größeren Netzen zu adressieren und Verbindungen zu ihnen aufzubauen. Das Internet Protocol stellt die Grundlage des Internets dar.

Heute ist im Internet fast ausschließlich die Version IPv4 im Einsatz. Allerdings steht die Nachfolgeversion IPv6 bereits zur Verfügung. IPv6 wird von zahlreichen Betriebssystemen sowie einer Reihe von Endanwendungen unterstützt. Der Hauptgrund für einen großflächigen Umstieg auf IPv6 ist der wesentlich größere Adressraum. Allerdings stehen gerade in Europa und Nordamerika aus historischen Gründen ein Großteil des 32 Bit großen Adressraums von IPv4 zur Verfügung, so dass hier der Druck zum Umstieg noch nicht besonders groß ist. Im asiatischen

Raum spielt dagegen der Adressmangel eine größere Rolle. Der Umstieg auf IPv6 ist dort bereits weiter vorangeschritten und findet insbesondere beim Aufbau neuer Backbones Anwendung.

FCIP

Mit 'Fibre Channel over IP' (FCIP) wird die Übertragung des 'Fibre Channel Protocol' (FCP) über IP-Netze ermöglicht. So können Speichersysteme auch über LAN oder WAN verbunden werden. Dabei können die Vorteile der IP-Technik (z.B. preiswerte Ethernettechnik oder Verschlüsselungsmöglichkeiten) genutzt werden.

6 Abkürzungsverzeichnis

ATM	Asynchronous Transfer Mode
CWDM	Coarse Wavelength Division Multiplexing
DLSw	Data Link Switching
DWDM	Dense Wavelength Division Multiplexing
ESCON	Enterprise System Connection
FC	Fibre Channel
FCIP	Fibre Channel over IP
FCP	Fibre Channel Protocol
FDDI	Fibre Distributed Data Interface
FICON	Fiber Optic Connection
GbE	Gigabit Ethernet
HW	Hardware
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
iFCP	Internet Fibre Channel Protocol
I/O	Input/Output
IP	Internet Protocol
IPv4	Internet Protocol (Version 4)
IPv6	Internet Protocol (Version 6)
ITU	International Telecommunications Union
LAN	Local Area Network
MTU	Maximum Transmission Unit
OADM	Optical Add/Drop Multiplexer
OC	Optical Carrier
OSC	Optical Supervisory Channel
OTM	Optical Terminal Multiplexer
P-t-P	Point-to-Point
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RPO	Recovery Point Objective

RTO	Recovery Time Objective
SAN	Storage Area Network
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSH	Secure Shell
STM	Synchronous Transfer Mode
SW	Software
TCM	Time Compression Multiplexing
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
UDP	User Datagram Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WDMA	Wavelength Division Multiple Access
X.25	Eine von der ITU-T standardisierte Protokollfamilie für großräumige Computernetze (WANs) über das Telefonnetz
XoT	X.25 Over TCP

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. vertritt mehr als 1.000 Unternehmen, davon 850 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Gerätehersteller, Anbieter von Software, IT-Services, Telekommunikationsdiensten und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V

Albrechtstraße 10
10117 Berlin

Tel.: 030/27 576-0
Fax: 030/27 576-400

www.bitkom.org
bitkom@bitkom.org