

EINE STARKE BASIS FÜR ERFOLGREICHES E-BUSINESS



AUFBAU EINES SAP R/3-FÄHIGEN NETZWERKES

White Paper



Einführung

Moderne ERP-Systeme (ERP - Enterprise Resource Planning) unterstützen die geschäftlichen und strategischen Ziele eines Unternehmens, indem sie zentrale Unternehmensprozesse, wie z. B. Fertigung, Personalwirtschaft oder Rechnungswesen, straffen und integrieren. Häufig stellt die Einführung eines ERP-Systems eine strategische Entscheidung dar, denn die Implementierung und spätere Verwaltung sind meist mit Investitionen in Millionenhöhe verbunden. Heutige ERP-Systeme bündeln die unterschiedlichen Informationsströme eines modernen Unternehmens und nutzen sie als treibende Kraft für Wachstum und geschäftlichen Erfolg. Voraussetzung für den erfolgreichen Einsatz dieser Applikationen ist ein leistungsfähiges und sicheres Netzwerk, denn ERP-Systeme sind nicht nur unternehmenskritisch, sondern stellen auch enorme Anforderungen an das gewählte Netzwerk. Nur wenn die gewählte Technologie die hohen Anforderungen erfüllt, lassen sich alle strategischen Vorteile eines ERP-Systems von Anfang an effizient nutzen. Daher sind hohe Verfügbarkeit, Skalierbarkeit sowie die Fähigkeit, ERP-Anwendungen vor weniger zeitkritischem Verkehr wie Web-Browsing, E-Mail und Dateitransfer zu schützen, von entscheidender Bedeutung. Um diese Anforderungen sicher umzusetzen, ist

jedoch ein Verständnis der Applikation, ihrer Architektur und ihrer Netzwerkanforderungen erforderlich. Diese Informationsbroschüre bietet einen Überblick über die SAP R/3-Umgebung und enthält umfangreiche Empfehlungen für den Aufbau eines geeigneten Netzwerkes zur Unterstützung des R/3-Systems.

SAP gilt unbestritten als weltweit führender Anbieter von betriebswirtschaftlichen Softwareanwendungen. Die betriebswirtschaftliche Standardsoftware SAP R/3 wird auf der ganzen Welt von mehr als 12.000 Unternehmen eingesetzt und ist damit das ERP-System mit dem größten Marktanteil weltweit. SAP beabsichtigt, seine Führungsrolle auch auf die schnell wachsenden Unternehmens- und E-Commerce-Märkte auszuweiten.

Cisco bietet mit seiner führenden Technologie, seiner Erfahrung und seinen zahlreichen Partnerschaften umfangreiche Netzwerklösungen als sichere und skalierbare Plattform für geschäftskritische SAP R/3-Umgebungen. Die technologische Partnerschaft von Cisco und SAP ermöglicht es gemeinsamen Kunden, alle Herausforderungen und Chancen des weltweiten E-Business auf einer sicheren und flexiblen Grundlage zu nut-

2. Überblick über SAP R/3

Das ERP-System SAP R/3 ist ein modulares und skalierbares System, das den Anforderungen der meisten Branchen gerecht wird. Die im Basissystem integrierten Kernapplikationen können in die Module Rechnungswesen, Logistik und Personalwirtschaft unterteilt werden. Jedes dieser Module besteht wiederum aus mehreren Komponenten. So setzt sich das Modul Logistik unter anderem aus den Komponenten Allgemeine Logistik, Materialwirtschaft, Instandhaltung und Produktions-

Die Initiative mySAP.com steht für einen neuen SAP-Kurs und den damit verbundenen Aktivitäten. Ziel dieser Initiative ist es, das herkömmliche ERP-System zu erweitern, um mittels Supply Chain Management und Business-to-Business-E-Commerce eine internetbasierte Kooperation zwischen Unternehmen zu ermöglichen. Dabei soll die Zusammenarbeit der E-Community über Internet-Portale sichergestellt werden.

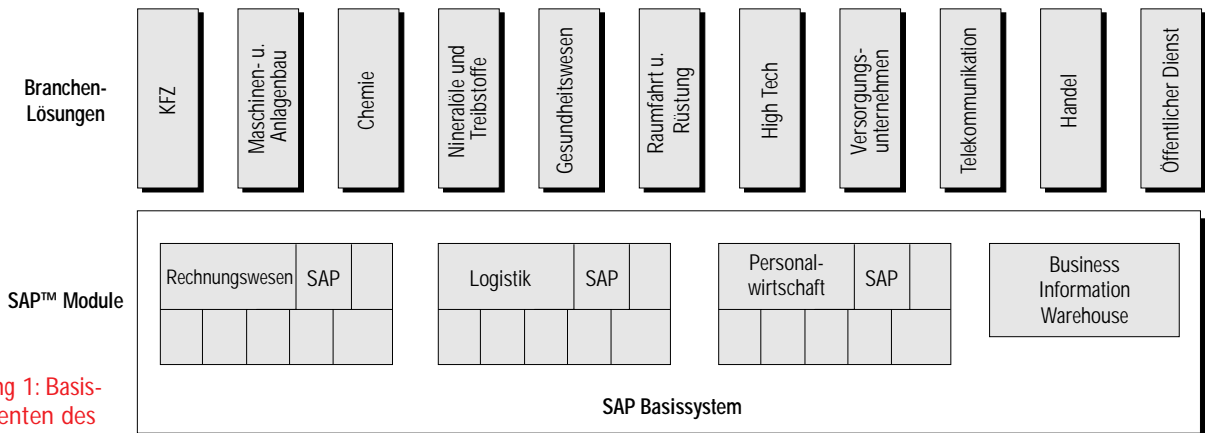


Abbildung 1: Basis-Komponenten des SAP R/3-Systems

Quelle: SAP AG

planung zusammen. Zudem gibt es anwendungsübergreifende Komponenten, die auf in mehreren Applikationen gespeicherte Daten zugreifen und diese nutzen. Zu diesen Applikationen gehören Business Workflow, Business Information Warehouse, Office-Tools wie E-Mail und Textverarbeitung sowie Archivierungsprogramme.

Die SAP-Applikationen sind im Basissystem integriert, das grundlegende Ressourcen zur Verfügung stellt. SAP bietet darüber hinaus branchenspezifische Lösungspakete, beispielsweise für Banken, Einzelhandel, Versorgungsunternehmen oder für das Gesundheitswesen.

2.1 Die SAP R/3-Architektur

Das R/3-System basiert auf einer dreistufigen Client-Server-Architektur mit den Schichten Präsentation/Client, Applikation und Datenbank. Diese Schichten können sich jeweils auf separaten Computern und Servern befinden. Dies ermöglicht eine höhere Skalierbarkeit, verbesserte Abläufe und die Unterstützung mehrerer Plattformen. Die dreistufige Architektur bietet eine erhöhte Performance bei verringertem Netzwerkverkehr, da sämtliche Datenbankabfragen lokal an die Datencenter geleitet werden und lediglich der Verkehr der Präsentationsschicht über das unternehmensweite Netz geführt wird. Jede Schicht erfüllt dabei eigene Funktionen.

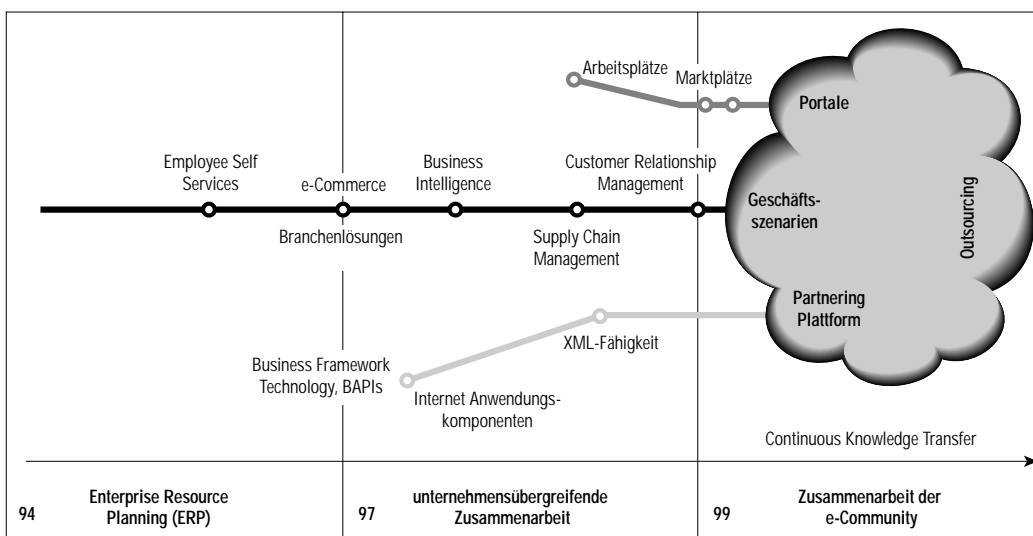


Abbildung 2: Roadmap der mySAP-Initiative von SAP

Quelle: SAP AG

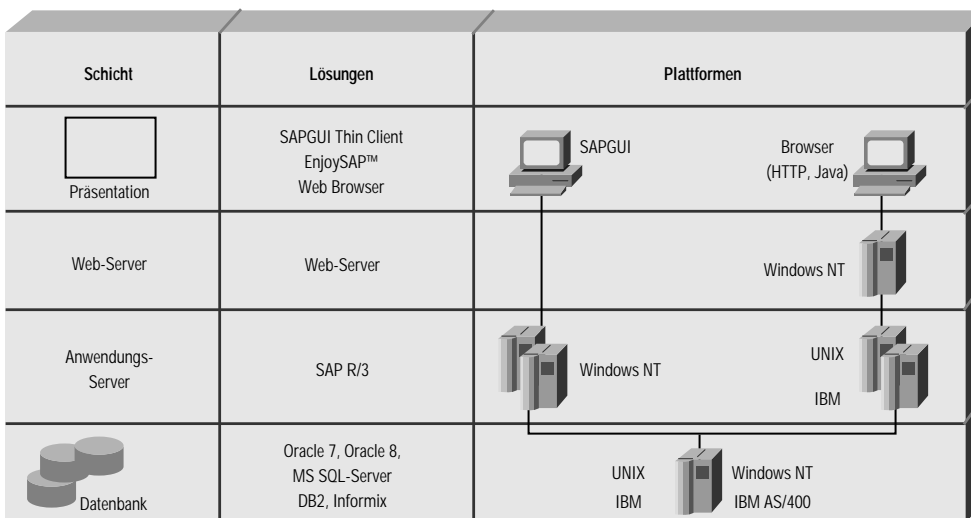
- Die **erste Schicht** besteht aus einem Datenbankmanagementsystem, das die Daten speichert, mit denen die R/3-Anwendungen arbeiten. Die jeweils eingesetzten Datenbanken sind weitgehend vom SAP R/3-System unabhängig, so dass der Kunde und der Systemintegrator frei wählen können, ob sie Oracle, Microsoft, Informix, IBM oder ein anderes Datenbanksystem einsetzen möchten. Sämtliche Daten, die mit einem einzelnen SAP-System oder einer "Instanz" verknüpft sind, befinden sich in diesem zentralen Datenbanksystem.
- Die **zweite Schicht** ist die Applikationsschicht, die das Kernstück des R/3-Systems bildet. Diese Schicht besteht aus der Applikationslogik, die für die Verarbeitung von Client-Transaktionen und Druckaufträgen, die Erstellung von Berichten, die Koordination des Datenbankzugriffs und die Anbindung an andere Anwendungen zuständig ist. Die Anwendungen übersetzen Benutzertransaktionen oder Berichtsanforderungen in entsprechende SQL-Datenbankabfragen und wandeln die Abfrageergebnisse in die vom Client benötigten Informationen um.
- Die **dritte Schicht** besteht derzeit hauptsächlich aus einer Thin-Client-Softwareapplikation namens SAPGUI, die gewöhnlich auf Microsoft Windows-Clients läuft, jedoch auch auf anderen Plattformen eingesetzt werden kann. Über den SAPGUI erhält der Benutzer Standardformulare oder Masken, in denen zur Durchführung bestimmter Geschäftsvorgänge, wie z. B. Auftragerfassung und Buchhaltungs- oder Produktionsplanungsprozesse, Daten eingegeben werden müssen. Diese Masken werden anschließend an einen Applikationsserver gesandt, der die nächste Maske mit den entsprechenden Daten anzeigt. Jeder vom Benutzer ausgelöste Vorgang, wie z. B. die Erfassung eines Auftrages, erfordert in der Regel zahlreiche maskengestützte Interaktionen zwischen Benutzer und Applikationsserver. SAP hat vor kurzem mit der Initiative SAPenjoy einen Schritt unternommen, um die Präsentationsschicht benutzerfreundlicher zu gestalten und noch mehr an spezifische Benutzerprofile und -bedürfnisse anzupassen. Zusätzlich konzentriert sich SAP darauf, die Client-Schnittstelle über einen Web-Browser verfügbar zu

machen, um die wachsende Anzahl gelegentlicher Anwender sowie die Vernetzung über das Internet zu unterstützen. In diesem Fall erfolgt die Kommunikation über einen Web-Server auf einer zusätzlichen Schicht.

Die Applikation und die Datenbank können auf demselben Server installiert werden. Bei den meisten mittleren und größeren Systemen werden die Datenbank- und die Applikationsschicht auf separaten Servern betrieben, wodurch eine höhere Skalierbarkeit erreicht wird. Die Applikationsschicht kann zur Erhöhung der Skalierbarkeit und zur Unterstützung steigender Anwenderzahlen auf mehreren Servern ausgeführt werden.

Viele Organisationen setzen zur unternehmensweiten Abwicklung ihrer Geschäftsprozesse ein einzelnes, zentrales SAP R/3-System (Instanz) ein. Auf diese Weise schaffen sie ein hochintegriertes und konsolidiertes Netzwerk, das alle Geschäftsprozesse, Geschäftsbereiche, Abteilungen und geographischen Standorte abdeckt und auf einer einzelnen zentralisierten Datenbank basiert. Andere Unternehmen entscheiden sich dagegen für mehrere separate R/3-Instanzen, da ihre Abteilungen oder Standorte unterschiedliche Geschäftsprozesse nutzen oder ihre Informationen vollständig separat verwalten wollen. Wenn diese unterschiedlichen Systeme zusammengeführt werden sollen, muss die Kommunikation über die im SAP-System verfügbaren Standardschnittstellen erfolgen.

Wenngleich die R/3-Applikationsschicht auf vielen Servern eingesetzt werden kann, sind einige R/3-Dienste einmalig und können daher nur einmal im gesamten System ausgeführt werden. Diese zentralisierten Dienste bezeichnet man als zentrale SAP-Instanz. Zu ihnen gehört der Message-Service, der die Clients mit den Applikationsservern verbindet und für einen Lastenausgleich über mehrere Applikationsserver hinweg sorgt. Ein weiterer wichtiger Dienst ist der Enqueue-Service, der den Zugriff auf die Datenbank koordiniert. Jeder Dialog, der einen Datenbankzugriff erfordert, muss vom Enqueue-Service auf der Zentralinstanz abgestimmt werden.



Die zentrale SAP-Instanz kann auf demselben Server installiert werden wie die Datenbank. Dies erfolgt häufig, um die für den Datenbankserver bereitgestellte Clustering-Funktion und Redundanz zu nutzen, denn sowohl die Datenbank als auch die Zentralinstanz stellen für sich genommen kritische

Abbildung 3: Dreistufige SAP-Architektur

Quelle: SAP AG

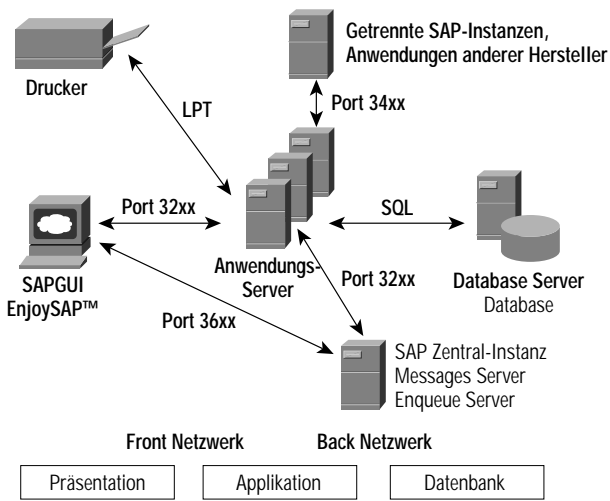


Abbildung 4: Verkehrsströme innerhalb des SAP R/3-Systems

Ausfallpunkte dar. Die Zentralinstanz kann alternativ auf einem separaten Server oder auf einer Gruppe von Servern eingerichtet werden.

2.2 Verkehrsmuster im SAP-Netzwerk

Es gibt zwei verschiedene Hauptverkehrsmuster, die beim Aufbau eines SAP R/3-fähigen Netzes berücksichtigt werden müssen. Das erste Muster ist der Client-zu-Applikationsserver-Verkehr, auch Front-Netzwerkverkehr genannt. Dieser Verkehr muss in der Regel über das unternehmensweite Netzwerk geführt werden, das auch von zahlreichen anderen Anwendungen genutzt wird. Das zweite Muster ist der Applikationsserver-zu-Datenbankserver-Verkehr, oder Back-Netzwerkverkehr, der normalerweise isoliert im Datacenter abgewickelt wird. Die gesamte SAP R/3-Kommunikation beruht auf TCP/IP und bekannten TCP-Portnummern.

2.2.1 Client-zu-Applikationsserver-(Front-Netzwerk)-Kommunikation

SAPGUI Thin Clients:

Der durchschnittliche Bandbreitenbedarf für die Kommunikation zwischen Client und Applikationsserver ist pro Dialogmaske in der Regel relativ klein (ca. 2 KB). Neuere R/3-Versionen (ab 4.5 und höher), die SAPGUIs mit höherem Informationsgehalt verwenden, können eine geringfügig höhere Bandbreite benötigen. Meldet sich der Client über SAPLogon an, gelangt er zunächst zum Message-Server. Dieser leitet den Client an den Applikationsserver mit der höchsten Verfügbarkeit bzw. an den Server weiter, der für seine Client-Anmeldegruppe zuständig ist. Viele R/3-Anwendungen sind OLTP-Anwendungen (OLTP – Online Transaction Processing), bei denen ein Benutzer mehrfach mit dem System interagiert, bevor eine Transaktion, wie z. B. eine Auftrags erfassung, abgeschlossen werden kann. Der Benutzer erwartet üblicherweise bei jeder neuen Dialogmaske eine direkte Reaktion vom System. Aus diesem Grund ist die Reaktionszeit des Systems von entscheidender Bedeutung. Für das SAP-System gilt hinsichtlich der Benutzerzufriedenheit und der Produktivität

im allgemeinen eine Reaktionszeit von 1–2 Sekunden als akzeptabel. Um diese Reaktionszeiten zu garantieren, müssen alle wichtigen Komponenten, einschließlich des Netzwerkes, die entsprechende Serviceklasse bieten.

Web-Browser:

Die Benutzeroberfläche für den Web-Browser wurde als Ergänzung zur SAPGUI eingeführt und entspricht hinsichtlich Bedienung und Design der neuen SAPEnjoy-Oberfläche. Diese Schnittstelle interagiert mit dem vermittelnden Web-Server, der wiederum für jede Client-Sitzung eine SAPGUI-Sitzung mit dem Applikationsserver eröffnet. Der Web-Server kann an jeder Stelle im Netz aufgestellt werden. Es empfiehlt sich jedoch, einen gemeinsamen Standort für Web-Server und Clients zu wählen, da die Datenlast zwischen Web-Browser und Applikationsserver in der Regel wesentlich höher liegt als der SAPGUI-Verkehr.

2.2.2 Applikationsserver-zu-Datenbankserver-(Back-Netzwerk)-Verkehr

Applikationsserver und Datenbankserver befinden sich gewöhnlich im selben Datacenter. Der Verkehr zwischen Datenbankserver und Applikationsserver ist äußerst intensiv. Pro Transaktion sind oft mehrere Datenbankzugriffe zu bewältigen, und die erforderlichen Bandbreiten reichen von wenigen KB bis hin zu mehreren GB – im Durchschnitt ein zehnfach höherer Wert als beim Netzwerkverkehr zwischen Client und Applikationsserver. Daher ist Skalierbarkeit im Back-Netzwerkbereich entscheidend für die SAP R/3-Umgebung. Nur durch hohe Leistungsfähigkeit und geringe Verzögerungen ist die Performance der Applikation selbst gewährleistet.

2.2.3 Weitere Verkehrsmuster

Es gibt weitere R/3-Verkehrsmuster, die eine Rolle spielen, wenngleich sie nicht Teil der zentralen R/3-Anwendung sind. Hierzu gehört der Druckverkehr, der vom Druckspooler des Applikationsservers ausgeht und das Netz mit Daten im mehrfachen MB-Bereich beanspruchen kann. Häufig müssen diese Daten das Netzwerk passieren, um zum nächstgelegenen Drucker für den Benutzer zu gelangen. Zudem verwenden manche Applikationen, wie z. B. die Produktionsplanung, graphische Tabellen mit einer entsprechend hohen MB-Menge an Daten. Ebenfalls berücksichtigt werden muss der Verkehr zwischen Anwendungen, wie zum Beispiel die Aktualisierung des zentralen Data Warehouse aus der R/3-Datenbank oder Disaster-Recovery-Backups im Netzwerk. Eine weitere interessante Applikation von SAP ist das Advanced Planning and Optimization (APO). Sie ermöglicht anspruchsvolle Verfügbarkeitsprognosen, wie z. B. Availability To Promise, und läuft auf einer Datenbank, die regelmäßig nicht nur aktuelle unternehmensinterne Informationen, sondern auch Zuliefererinformationen ansammelt. So können anhand zeitnaher Detailinformationen über alle Glieder der logistischen Kette Liefervorhersagen getroffen werden. Diese Applikation erzeugt regelmäßig hohe Datenmengen, die zwischen den Unternehmen übertragen werden müssen.

3 Überlegungen zur Netzwerkarchitektur

Die gewählte Netzarchitektur stellt einen wesentlichen Erfolgsfaktor für die Umsetzung von R/3-Anwendungen dar. Eine ungeeignete Infrastruktur kann zu verspäteten Systemlieferungen, unbefriedigenden Systemleistungen oder inakzeptablen Ausfallzeiten zu Zeitpunkten führen, zu denen Benutzer und Management naturgemäß die höchsten Erwartungen haben. Ohne den richtigen Aufbau kann die Netzarchitektur nur schwer skaliert und an wachsende Anforderungen angepasst werden, die sich häufig unmittelbar nach dem ersten R/3-Einsatz einstellen. Beim Entwurf eines unternehmensweiten Kommunikationsnetzwerkes, das Zuverlässigkeit und hohe Skalierbarkeit bieten soll, lassen sich bereits in der Planungsphase die Grundsteine sowohl für eine erfolgreiche Erstimplementierung als auch für spätere Aktualisierungen und Erweiterungen legen.

Um die hohen Investitionen für ein R/3-System optimal auszunutzen, sind Unternehmen daran interessiert, das System nicht nur innerhalb des Unternehmens, sondern auch Anwendern auf Campus-Ebene, Außenstellen auf der ganzen Welt, mobilen Usern und Telearbeitern, Zulieferern und sogar Kunden zur Verfügung zu stellen. Mit der dreistufigen R/3-Architektur und den klar definierten Schnittstellen ist dies problemlos umzusetzen. Da die meisten Unternehmen heute ihr R/3-System als integriertes und zentralisiertes System einsetzen, müssen alle Clients über eine geeignete Netzwerkverbindung verfügen, um auf dieses System zugreifen zu können. Darüber hinaus muss das R/3-System als zentrales Backend-System für andere geschäftskritische Customer-Facing-Systeme, wie E-Commerce, Kundendienst und Supply-Chain-Management, bereitstehen. Die wesentliche Anforderung an das Netzwerk besteht in der Bereitstellung einer **skalierbaren, reaktionsschnellen und hochverfügbaren Plattform**, auf der die R/3-Applikation erfolgreich eingesetzt werden kann.

Die Netzarchitektur kann durch fünf Konnektivitätsbereiche dargestellt werden (siehe Abbildung 5):

1. **Das Datacenter** – hier befinden sich die zentrale R/3-Datenbank und der Applikationsserver.
2. **Das Campus-Netz** – stellt die Verbindung zu sämtlichen Endanwendern innerhalb des Campus her.
3. Wide Area Network (WAN) - Verbindung von Clients und Systemen in Außenstellen mit dem zentralen Datacenter. Es wird auch eine Verbindung zum SAP Support Center OSS bereitgestellt.
4. **Remote-Access** – Verbindung zu Telearbeitern und mobilen Anwendern über geschaltete PSTN- oder ISDN-Netze bzw. alternativ über Fest- oder xDSL-Netze;
5. **Internet-Anbindung** – Bereitstellung eines ausbaufähigen Zugangs für Mitarbeiter, Kunden und Partner sowie Anbindung an Portale wie mySAP.com.

In dem vorhergehenden Diagramm sind die unterschiedlichen Komponenten und Netzwerke einer typischen SAP R/3-Umgebung vereinfacht dargestellt:

Im Folgenden soll näher auf die Netzwerkanforderungen und empfohlenen Lösungen von Cisco im Hinblick auf Datacenter, Campus-LAN und Wide Area Network eingegangen werden, da es sich hierbei um allgemeine Anforderungen für alle SAP R/3-Umgebungen handelt.

3.1 Aufbau des Datacenters

SAP R/3-Systeme zentralisieren geschäftskritische Unternehmensprozesse. Das Datacenter ist das Herzstück dieses Systems. Ein unzureichender Zugang zu Applikations- und Datenbankservern bedeutet den unvermeidlichen Verlust von Gewinnen und Produktivität und, was häufig noch schwerer wiegt, den Verlust von Kunden. Laut einer kürzlich von Strategic Research durchgeführten Studie müssen ERP-Benutzer ungeplante Ausfallzeiten von durchschnittlich 2,8 Stunden pro Woche hinnehmen. Nach Berechnungen der Standish Group kostet jede Minute eines ERP-Systemausfalls die Fortune 1.000-Unternehmen durchschnittlich \$13.000 (siehe Abbildung 6).

Die Trennung von Datenbank- und Applikationsservern führt zu unnötigem Netzverkehr und verursacht zusätzliche Verzögerungen bei der Ausführung von OLTP-Transaktionen. Eine gemeinsame Aufstellung von Datenbank- und Applikationsserver am gleichen

Die Trennung von Datenbank- und Applikationsservern führt zu unnötigem Netzverkehr und verursacht zusätzliche Verzögerungen bei der Ausführung von OLTP-Transaktionen. Eine gemeinsame Aufstellung von Datenbank- und Applikationsserver am gleichen

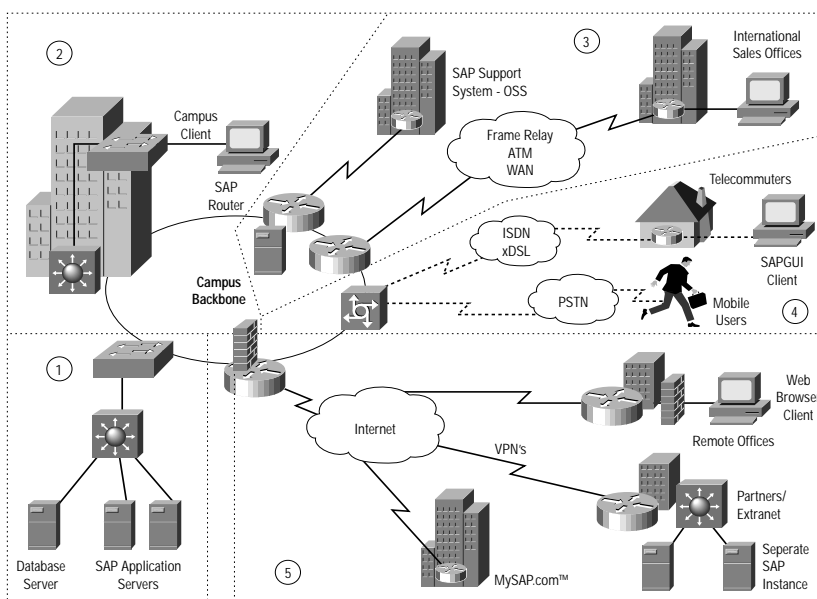


Abbildung 5: Komponenten eines durchgängigen Netzwerks für SAP R/3

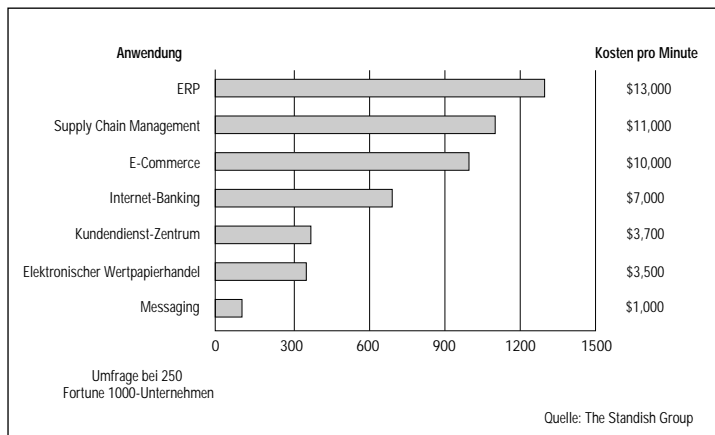


Abbildung 6: Kosten durch ERP-Ausfallzeiten

Standort bietet bessere Möglichkeiten für Schutz und Überwachung. Darüber hinaus unterstützt eine in sich geschlossene Umgebung die systematische Verwaltung des Netzwerks hinsichtlich Performance, Verfügbarkeit und Sicherheit (siehe Abbildung 7).

3.1.1 Datacenter-Skalierbarkeit

Um selbst bei höchstem Datenaufkommen Engpässe im Netzwerk zu vermeiden, müssen Kapazität und Größe der Datacenter-Infrastruktur im Vorfeld geplant werden. Dies kann gleichzeitig mit der Dimensionierung der Server-Hardware erfolgen. Da die Datacenter-Netzarchitektur generell mit erheblich geringeren Kosten verbunden ist als die Server-Hardware, empfiehlt es sich, eher ein überdimensioniertes Netzwerk aufzubauen als Engpässe aufgrund unzureichender Netzwerkressourcen zu riskieren.

In der Vergangenheit war Shared-FDDI die führende Technologie im Bereich der Hochgeschwindigkeits-LAN-Technologien und wurde bevorzugt zur Verbindung von Datenbank- und

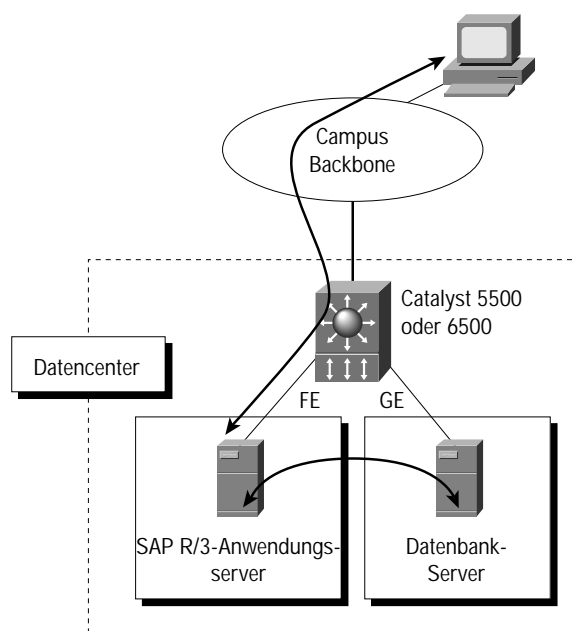


Abbildung 7: Typische Datacenter-Lösung

Applikationsserver eingesetzt. Aufgrund der relativ hohen Kosten und der geringen Weiterentwicklung dieser Technologie verliert FDDI jedoch zusehends an Attraktivität.

Aufgrund der hohen Verfügbarkeit und der weiten Verbreitung werden die Fast-Ethernet und Gigabit-Ethernet-Switching-Technologien immer mehr im Datacenter eingesetzt. Angesichts von leistungsfähigeren Servern mit höheren I/O-Möglichkeiten, eines ständig wachsenden Datenaufkommens und der steigenden Anzahl von Anwendern besteht eine zunehmende Notwendigkeit des Einsatzes solcher Hochgeschwindigkeits-Switching-Technologien. Auf Ethernet-Technologie basierende Netzwerke bieten bei sorgfältiger Ausführung eine außergewöhnlich hohe Performance, Fehlertoleranz und Skalierbarkeit.

Asynchronous Transfer Mode ist eine weitere Hochleistungstechnologie, die in Betracht gezogen werden kann, obwohl sie eher für Campus- und WAN-Backbones mit der typischen Integration von Daten-, Sprach- und Videoverkehr geeignet erscheint und im Datacenter keine erkennbaren Vorteile bietet.

Es ist ebenfalls wichtig, Layer 3- und Layer 4-Leistungsmerkmale durch den Einsatz von Routern oder Multilayer-Switches umzusetzen. Diese ermöglichen die Isolierung des Datacenters von den hohen Datenmengen, die infolge von irrelevantem Broadcast-Verkehr am Campus-Backbone auftreten. Sie bieten darüber hinaus mehr Sicherheit für das geschäftskritische Datacenter und verhindern den unbefugten Zugriff auf sensible Ressourcen. Der Einsatz der Layer 3- und Layer 4-Leistungsmerkmale ermöglicht zudem die Klassifizierung und Prioritätszuordnung des Verkehrs gemäß Unternehmensstrategien, die unterschiedlichen Anwendungen zugeordnet werden können. In zunehmendem Maße werden Switches mit Hochleistungs-Switching und einer Übertragungsrate von einigen Millionen Paketen pro Sekunde sowohl in Layer 2 als auch in Layer 3 eingesetzt. Zwischen Applikations- und Datenbankserver wird Layer 2-Konnektivität empfohlen, wobei für den Client-Server-Verkehr zwischen Applikationsserver und Campus-Backbone in jedem Fall eine Layer 3-Konnektivität erforderlich ist.

Um eine höhere Skalierbarkeit und bessere Steuerungsmöglichkeiten zu erreichen, ist sogar die Isolierung des Applikationsserver-zu-Datenbankserver-Verkehrs vom Client-zu-Applikationsserver-Verkehr zu empfehlen. Dies wird durch die Implementierung eines separaten logischen Subnetzes für die jeweiligen Verkehrstypen realisiert. Dabei werden VLANs und Layer 3-Switching in die Datacenter-Switches eingebunden. Dies erfordert ebenfalls die Installation separater Applikationsserver-NICs (NIC – Network Interface Card), von denen jede separate IP-Adressen aufweist.

Die Multilayer-Switches der 5000- und 6000-Serien von Cisco erfüllen sämtliche angeführten Kriterien. Mit verschiedenen Modellen können die Anforderungen an die Portdichte des einzurichtenden Datacenters erfüllt werden. Es wird häufig empfohlen, Ersatzports für spätere Erweiterungen und zusätzliche Server vorzusehen, die im ursprünglichen Entwurf nicht geplant waren. Beispielsweise benötigt die "Produktions"-Umgebung lediglich einen einzigen Datenbankserver, aber dennoch werden die SAP Entwicklungs- oder Test- und Integrationsumgebungen der IT-Abteilungen häufig in demselben Datacenter untergebracht. Zudem werden auch andere Server, wie z. B. die SAP EDI-Server, im Datacenter aufgestellt.

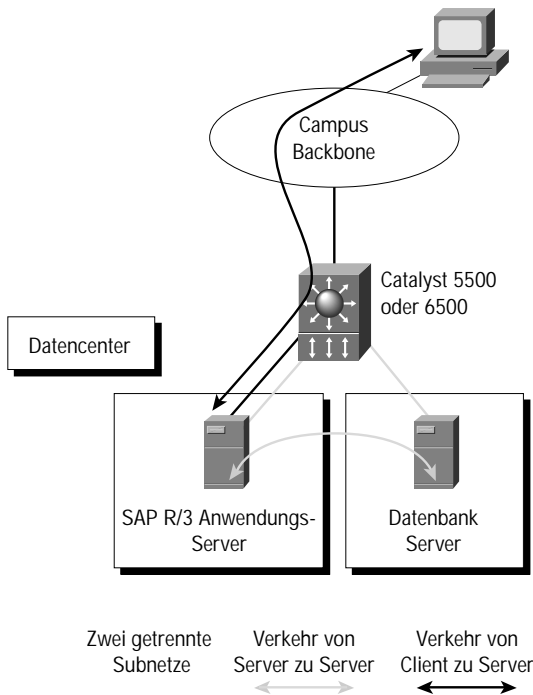


Abbildung 8: Skalierbare Datacenter-Lösung

Eine weitere Möglichkeit besteht darin, die Bandbreite zwischen Server und Netzwerk über die EtherChannel genannte Link-Bundling-Technologie von Cisco zu erhöhen. Zusätzliche Bandbreite kann bei Bedarf einfach durch Multiport-Netzwerkchnittstellenkarten oder mehrere separate NICs, z. B. von HP, Sun, Compaq, Intel und Adaptec, hinzugefügt werden.

Hinsichtlich des Uplink-Datendurchsatzes (Switch zum Campus-Backbone) muss berücksichtigt werden, dass normalerweise der Großteil des über den Datacenter-Switch geleiteten Verkehrs Server-zu-Server-Verkehr ist, der den Campus-Backbone nicht erreichen muss. Es ist dennoch erforderlich, einen Hochgeschwindigkeits-Kanal vorzusehen, um Engpässe beim Client-Server-Verkehr zu vermeiden. Unabhängig davon, ob eine Fast-Ethernet oder Gigabit-Ethernet-Verbindung für diesen Link gewählt wird, besteht die Möglichkeit, den Durchsatz mit der EthernetChannel-Technologie wesentlich zu erhöhen. In manchen Fällen müssen über die Uplink-Verbindung neben dem Client-Server-Verkehr auch andere Verkehrsarten

bedient werden, wie z. B. Druckverkehr, Datenbankkonsolidierungsverkehr und Datenbank-Backup-Verkehr. Wird z. B. ein Außenstellen-Disaster-Recovery-Backup für das R/3-System implementiert, müssen alle Datenbankänderungen regelmäßig und manchmal sogar zeitgleich am anderen Standort erfolgen. Hierdurch kann die Datenlast der Uplink-Verbindung steigen, was eine erhöhte Uplink-Kapazität erforderlich macht.

3.1.2 Hohe Verfügbarkeit des Datacenters

Die Verfügbarkeit der R/3-Datenbank- und Zentralinstanzserver ist für den unterbrechungsfreien Betrieb des Systems und nicht zuletzt auch für den reibungslosen Verlauf der geschäftlichen Vorgänge von grundlegender Bedeutung. Im Zuge der zunehmenden Globalisierung setzt sich immer mehr die Tendenz zu einem ganzjährigen 24 x 7-Betrieb durch. In der Vergangenheit sind hohe Summen in offene Hochverfügbarkeits-Systemlösungen investiert worden. Insbesondere Plattformvertreiber bieten Server-Clustering-Technologien an, die bei Ausfällen eine schnelle Wiederherstellung auf Backup-Servern durchführen. Zudem bieten Vertreiber von Datenbanken und Speichergeräten Backup-Technologien an, mit denen Datenbeschädigung oder -verlust bei einem Hard- oder Softwareausfall verhindert werden. Diese Investitionen machen sich natürlich nicht bezahlt, wenn die Netzarchitektur hinsichtlich der Verfügbarkeit eine geringere Performance bietet. Daher werden R/3-Systeme zunehmend in vollständig redundanten Netzwerken implementiert, die eine automatische Fehlerkorrektur bei allen vorhersehbaren Geräte-, Verbindungs- oder Serverausfällen unterstützen. Im Idealfall vollzieht sich diese Wiederherstellung für den Benutzer transparent, so dass die Applikationssitzung durch den Ausfall nicht beeinträchtigt wird. R/3-Applikationssitzungen werden typischerweise nach 20 Sekunden unterbrochen. Daher sollte eine Netzwerk-Wiederherstellung innerhalb dieses Zeitrahmens erfolgen, um für den Anwender vollständig transparent zu bleiben.

Dieses Ziel geht über die reine Zuverlässigkeit der Netzwerkgeräte hinaus, obgleich es sich hierbei um eine Schlüsselanforderung handelt. Es muss sichergestellt werden, dass das Netzwerk über die nötige Intelligenz verfügt, um einen Geräte- oder Verbindungsausfall in kurzer Zeit zu beheben. Diese Intelligenz muss durch den Einbau bewährter und geprüfter Software in den Netzwerkgeräten integriert werden, die beim Auftreten eines Netzwerk-Problems ein skalierbares und stabiles Rerouting, schnelle Fehlereingrenzung und schnelle Wiederherstellungsmaßnahmen gewährleistet. Zudem muss das Netzwerk so ausgelegt, konfiguriert und betrieben werden, dass eine optimale Nutzung dieser Möglichkeiten gegeben ist.

Diese Netzwerkgeräte sind idealerweise vor ihrem Einsatz auf alle potentiellen Ausfallszenarien in der Serverplattform-Umgebung zu testen. Netzwerkgeräte, Server-Clustering-Technologien, Betriebssystem und Netzwerkschnittstellenkar-

ten müssen reibungslos als Einzelsysteme funktionieren, um nach Server-, Verbindungs- oder Netzwerkfehlern weiterarbeiten zu können. Ein Beispiel für eine Datacenter-Lösung mit hoher Verfügbarkeit wird in Abbildung 9 dargestellt.

Hier wird ein Datenbankserver-Cluster dargestellt, das als Hauptdatenbankserver und Hot-Standby-Backup-Datenbankserver fungiert. Um dasselbe Redundanzniveau für die R/3-Zentralinstanz zu erreichen, kann das Datenbankserver-Cluster entweder auf demselben Server wie die Datenbank, auf einem separaten Server, der zum selben Cluster gehört oder alternativ auf einem vollständig separaten Server installiert werden.

Die anderen SAP-Applikationsserver sind in der Regel nicht geclustert, da sie alle standardmäßig die gleichen Dienste bereitstellen und ein Fehler daher lediglich die auf einem spezifischen Server aktuell laufenden Sitzungen beeinträchtigt. Bei einem Ausfall erhalten die Benutzer sofort wieder Zugang zum System und werden vom Message-Server einfach an einen der anderen verfügbaren Applikationsserver weitergeleitet.

Die in Abbildung 9 dargestellte Netzarchitektur umfasst zwei redundante Catalyst 5500- oder 6500-Switches. Switch A ist der primäre Switch für den Server-zu-Server-Verkehr und Switch B ist der primäre Switch für den Client-zu-Server-Verkehr. Ein an einem der Switches, Line Cards, Verbindungen oder Datenbankservern auftretender Fehler führt automatisch zu einer Fehlereingrenzung. Diese Fehlereingrenzung wird durch die Hochverfügbarkeitslösungen von Cisco ermöglicht. Eine dieser Lösungen, z. B. das Hot Standby Routing Protocol (HSRP), überträgt transparent und sekundenschnell die Layer 3-Funktionalität (z. B. Default-Gateway und Routing-Zuständigkeiten) an den alternativen Switch. Durch die schnelle Fehlereingrenzung ist in allen Fällen (außer bei einem

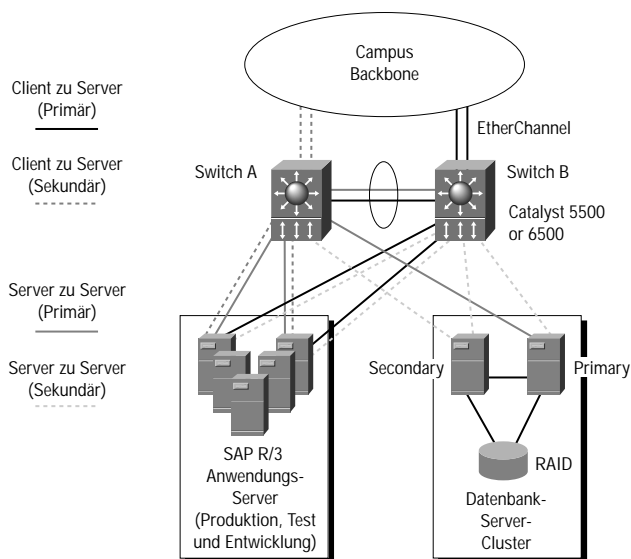


Abbildung 9: Hochverfügbarkeits-Datencenter

Datenbankserver-Ausfall) sichergestellt, dass die Sitzung nicht unterbrochen wird und der Fehler für den Benutzer somit transparent bleibt.

Ein wichtiger Aspekt der Fehlertoleranz im Datacenter besteht im Dual-Homing. Dadurch werden die Netzswitches getrennt und somit die Ausfallsicherheit einer NIC oder eines Switch erhöht.

Beim Dual-Homing werden zwei Netzwerkschnittstellenkarten (NICs) im Server installiert und innerhalb des Server-LAN an zwei verschiedene Netzwerkgeräte angeschlossen. Je nach Hersteller werden verschiedene Hardware-Betriebssysteme und NICs mit unterschiedlichem Dual-Homing angeboten. Daher empfiehlt es sich, das System als Ganzes zu konfigurieren und zu prüfen.

Ein Beispiel für eine gut definierte Konfiguration ist ein HP-UX-Cluster mit der MC ServiceGuard-Clustersoftware und HP-NICs. In diesem Fall teilen sich die Dual-Home-NICs eine virtuelle IP-Adresse und übergeben bei Ausfall der primären Verbindung oder der NIC die MAC-Adresse von der primären NIC an die sekundäre NIC.

Ein weiteres Beispiel ist der Dual-Home-NT-Server, in dem duale NICs von Anbietern wie Intel eingesetzt werden. Hier können beide Schnittstellen gleichzeitig aktiv Daten übertragen, wobei lediglich die primäre Schnittstelle Daten empfängt.

Viele Unternehmen benötigen neben Hochverfügbarkeitslösungen innerhalb eines einzigen Datacenters auch Disaster-Recovery-Lösungen für Szenarien, in denen das Datacenter zerstört wird oder der Zugriff darauf unterbrochen ist. Die unterschiedlichen Stufen des Disaster-Recovery variieren je nach Unternehmen entsprechend den jeweils bevorzugten Sicherheitsstrategien.

Das Spektrum reicht von der Durchführung regelmäßiger Datenbank-Backups auf Band bis hin zur Synchronisierung eines Remote-Datenbankclusters, das im Fall eines Ausfalls des primären Standortes dessen Aufgaben sofort übernehmen kann. Das Disaster-Recovery und das Datenbank-Backup können im unternehmensweiten Netzwerk oder alternativ in einem separaten, zu diesem Zweck eingerichteten Netzwerk durchgeführt werden.

3.2. Aufbau des Campus-LAN

Nach der Erörterung der Datacenter-Anforderungen wird nun auf den zweiten Baustein eingegangen – den Campus. Während das Datacenter in der Regel eine isolierte Umgebung darstellt, die für die R/3-Applikation und den Datenbankserver-Verkehr vorgesehen ist, muss das Campusnetzwerk die unterschiedlichsten Unternehmensapplikationen unterstützen.

Es ist allgemein bekannt, dass sich die früher gültige 80/20-Regel, die besagte, dass 80 Prozent des Netzwerkverkehrs innerhalb der Workgroup bleiben, umgekehrt hat. Dies ist vor allem eine Folge der unternehmensweiten webbasierten Intranetze, Messaging-Anwendungen und zentralisierten betriebswirtschaftlichen Applikationen wie R/3. Heutzutage ist der Großteil des Campusverkehrs nicht mehr auf die Workgroup beschränkt, sondern wird über das Backbone geleitet, um den Zugriff auf die zentralisierten Unternehmensressourcen zu ermöglichen. Darüber hinaus muss das Campusnetz skalierbar und flexibel sein, um die wachsende Anwenderzahl zu bewältigen und bei Bedarf den Einsatz aktueller Multimedia- und Sprach-Applikationen zu unterstützen.

Obgleich die Bandbreite des dreistufigen Client-zu-Applikationsserver-Verkehrs mit ca. 2 KB pro Dialogschritt relativ gering sein kann, ergibt sich dennoch bei Hunderten oder Tausenden von Anwendern eine enorme Erhöhung des bestehenden Netzwerkverkehrs. Neben dem normalen Client-Server-Verkehr kann auch die Implementierung von R/3 zu einem weiteren Anstieg des Netzwerkverkehrs führen, z. B. durch Serverkommunikation zwischen einem E-Commerce-System und dem SAP-System und nicht zuletzt durch den mit CBT-Aktivitäten verbundenen Multimedieverkehr.

Es empfiehlt sich daher, beim Aufbau von Unternehmensnetzwerken nach Möglichkeit eine modulare Architektur zu wählen.

Dies verringert die Komplexität und erhöht die Verfügbarkeit, was schließlich zu einer höheren Skalierbarkeit des Netzwerks führt. Ein Beispiel für eine modulare Multilayer-Lösung ist in Abbildung 10 dargestellt. Das vorstehend erörterte Datacenter-Modul ist dort mit drei neuen Modulen abgebildet - dem Kern- oder Backbone-Modul, dem Distribution-Modul und dem Access- oder Wiringcenter-Modul.

Der permanente Zugriff auf die R/3-Ressourcen im Datacenter lässt sich für die Campus-Clients und -Systeme nur gewährleisten, wenn ein extrem zuverlässiges und flexibles Netzwerk gewählt und verwaltet wird. Die Unterbrechung des Client-zu-Server-Verkehrs beträgt standardmäßig ca. 20 Sekunden, weswegen die Netzwerke so ausgelegt sein sollten, dass sie nach einem Ausfall innerhalb dieses Zeitraums in jedem Fall eine Wiederherstellung durchführen können. Das Ziel sollte ein Netzwerk ohne einen einzigen Single Point of Failure sein, das mit den entsprechenden intelligenten Strategien ausgerüstet ist, um jeden erdenklichen Ausfall schnell zu erkennen und zu korrigieren. In einem solchen Netzwerk gibt es für jede Verbindung und jedes Netzwerkgerät im Pfad zwischen Client und Server ein Backup. Diese Netzwerksicherheitslösung bietet eine Reihe potentieller Vorteile:

- Die redundanten Netzwerkelemente müssen nicht mit den

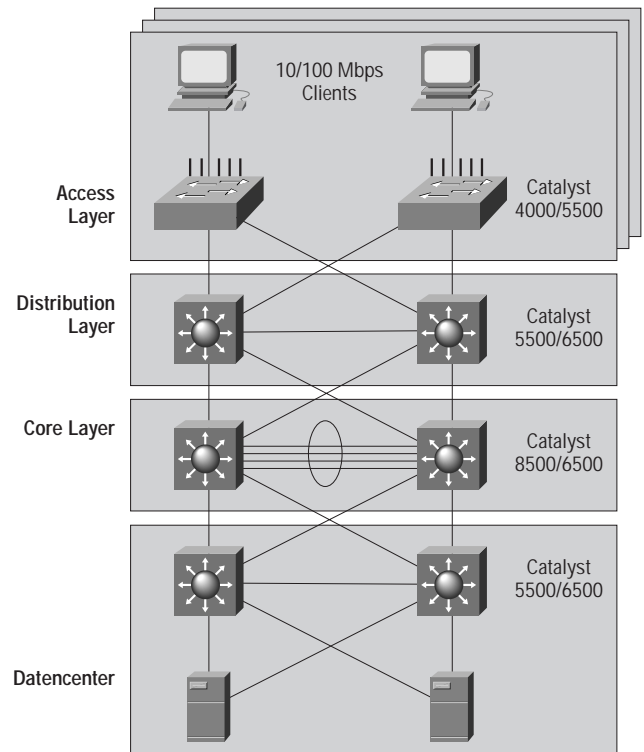


Abbildung 10: Modulares Multilayer-Campusnetzwerk

primären Netzwerkelementen zusammen am gleichen Standort aufgestellt werden. Hierdurch wird die Wahrscheinlichkeit verringert, dass Probleme in der physischen Umgebung den Dienst beeinträchtigen.

- Probleme mit Software-Bugs-/Updates oder Konfigurationsfehlern/-änderungen können häufig separat ohne Unterbrechung des Dienstes in den primären und sekundären Weiterleitungspfaden bearbeitet werden. Daher kann Redundanz auf Netzwerkebene ebenfalls die Auswirkungen von Fehlermechanismen verringern, die nicht mit der Hardware zusammenhängen.
- Die Verkehrslast zwischen den entsprechenden Layern der Netzarchitektur (z. B. Access-Layer zu Distribution-Layer) kann über entsprechende Flexibilitäts-Features und durch sorgfältige Konfiguration zwischen den primären und sekundären Weiterleitungspfaden aufgeteilt werden. Die Redundanz auf Netzwerkebene kann somit ebenfalls mit einer erhöhten Gesamt-Performance und -Kapazität verbunden sein, was wiederum die Zusatzkosten eines redundanten Netzwerkes senken kann.
- Redundante Netzwerke können so konfiguriert werden, dass ein automatisches Umschalten von den primären zu den sekundären Einrichtungen ohne Eingreifen des Operators erfolgt. Die Länge der Dienstunterbrechung entspricht der Zeit, die für das Umschalten benötigt wird. Es sind Umschalt-Zeiten von wenigen Sekunden möglich.

Der **Access-Layer** besteht normalerweise aus hochintelligenten Layer 2-Ethernet/Fast Ethernet-Switches, die zum Anschluss der Benutzerendstationen in Verteilerschränken unter-

gebracht sind. Da bei Clients der Dual-Home-Anschluss an separate Switches sehr unwahrscheinlich ist, können diese Switches zum Single Point of Failure für alle angeschlossenen Clients werden. Aus dieser Sicht kann es empfehlenswert sein, sie auf maximale Ausfalltoleranz zu konfigurieren. Die zugewiesenen 10 bzw. 100 Mbps verhindern, dass Clients mit bandbreitenintensiven Applikationen die Leistung benachbarter Clients mit geschäftskritischen R/3-Applikationen beeinträchtigen. Mehrere Hochgeschwindigkeits-Uplinks zum Distribution-Layer bieten redundante Pfade für Verkehrsübertragungen.

Auch hier zeigt sich: hohe Verfügbarkeit und schnelle Fehlerbegrenzung sind bei Ausfällen von extrem hoher Bedeutung. Cisco hat daher die Layer-Recovery-Technologie, wie z. B. UplinkFast, weiterentwickelt, so dass bei Uplink-Fehlern die totale Transparenz für den Anwender sichergestellt ist.

Cisco bietet verschiedene Switches an, die in Abhängigkeit von der erforderlichen Dichte ideal für den Access-Layer geeignet sind. Die Catalyst 5000-Serie unterstützt hochdichtes Switching für große Verteilerschränke (bis zu 528 Clients). Die Catalyst 4000-Serie sowie die stapelbare 3500-Serie bieten eine geeignete Lösung für mittlere Verteilerschränke, während die Catalyst 2900-Serie eine preisgünstige Switching-Lösung für kleine Außenstellen darstellt.

Der **Distribution-Layer** verfügt über einen Layer 3-Aggregationspunkt für die Access-Layer-Switches. Der Distribution-Layer ist normalerweise für große Campus-Netzwerke mit mehreren tausend Anwendern bzw. bei einem geografisch verzweigten Campus erforderlich. In anderen Fällen können der Distribution- und der Core-Layer zusammengefasst werden. Der Distribution-Layer unterstützt redundantes Layer 3-Switching (Routing) und bietet Hochleistungs-Internetworking sowie eine robuste Fehlertoleranz zwischen den vielfach verbundenen Access-Layer-Subnets und dem Core. Von Cisco bereitgestellte Features wie das Hot Standby Routing Protocol (HSRP) sind von großer Bedeutung, um bei Ausfällen vollständige Transparenz für den R/3-Anwender zu gewährleisten. Die umfassend erprobten Layer 3-Routingprotokolle wie Open Shortest Path First (OSPF) und Ciscos Interior Gateway Routing Protocol (IGRP) bieten Layer 3-Mechanismen für Lastverteilung, höhere Fehlertoleranz und schnelles Rerouting, um von Fehlern betroffene Netzwerkregionen zu umgehen. Sowohl der Catalyst 6500 als auch der Catalyst 5500 stellen hochleistungsfähige, skalierbare und robuste Layer 3-Switching-Plattformen dar, die auf der langjährigen Erfahrung und dem Fachwissen von Cisco im IP-Routing-Bereich basieren. Beide sind für den Distribution-Layer geeignet.

Der **Core-Layer** stellt das Backbone des Netzwerkes dar. Der größte Teil des Netzverkehrs wird über diesen Core ab-

gewickelt. Daher sind hohe Leistung und Verfügbarkeit von extrem hoher Bedeutung. Da der Backbone in der Regel als Drehscheibe für den gesamten Verkehr fungiert, sollte er über eine hoch skalierbare Non-blocking-Architektur verfügen, basierend auf Fast Ethernet, Gigabit Ethernet oder ATM. Der Core-Layer sollte vorzugsweise die hochleistungsfähige Layer 3-Switching-Technologie nutzen, um hohe Skalierbarkeit und stabiles Routing bei einem möglichen Ausfall zu gewährleisten. Auch hier stellt die führende Rolle von Cisco auf dem Gebiet der Layer 2- und Layer 3-Switching-, IP-Routing- und ATM-Technologie sicher, dass der Netzkern diesen strengen Anforderungen gerecht werden kann.

Während für Ethernet-basierte Backbones sowohl die Catalyst 8500-Serie als auch die Catalyst 6500-Serie die ideale Wahl darstellen, ist für ATM-Backbones speziell der Catalyst 8500 geeignet. Im Hinblick auf die im Campus erforderlichen Zusatzdienste, wie z. B. Multicast-, Sicherheits- und Sprachdienste, hängt die Wahl von der spezifischen Umgebung und den konkreten Applikationen ab, die in den LAN- und WAN-Umgebungen des Campus genutzt werden sollen. Wird z. B. eine Applikation wie TIBCO für die SAP-Applikationsintegration genutzt, muss IP-Multicast im gesamten Netzwerk unterstützt werden. Als Faustregel gilt hier: selbst wenn diese Dienste nicht sofort erforderlich sind, ist es sehr wahrscheinlich, dass sich der Bedarf aufgrund von neuen Applikationen einstellen wird. Dieses Thema wird unter besonderer Berücksichtigung der Quality of Service (QoS), die in einer R/3-Umgebung benötigt wird, an späterer Stelle erörtert.

Weitere Informationen zum Aufbau des Campus-Netzwerkes erhalten Sie unter:

http://www.cisco.com/warp/public/779/largeent/desing/large_campus.html

3.3 WAN-Aufbau

Da sich schätzungsweise 50% aller R/3-Clients außerhalb des Campus-Netzwerkes befinden, ist die Bereitstellung skalierbarer und zuverlässiger Remote-Konnektivität von wesentlicher Bedeutung. Das Ziel der meisten Unternehmen besteht in der Sicherstellung geeigneter Performance und Verfügbarkeit bei gleichzeitiger Senkung der hohen Kosten für die WAN-Infrastruktur, die 40-60% der Netzwerk-Gesamtkosten (Cost of Ownership) ausmachen können. SAP R/3 wurde zwar auch für den Anschluss von Clients über relativ langsame WAN-Verbindungen entwickelt, dennoch muss darauf geachtet werden, dass das Netz so aufgebaut und konfiguriert wird, dass schnelle Performance mit hoher Verfügbarkeit gewährleistet ist.

Für den Anschluss mobiler R/3-Clients an einen zentralen Standort stehen unterschiedliche Dienstoptionen zur Verfügung. Hierzu gehören Frame Relay, ATM, Leased Line, X.25 und ISDN, wobei häufig eine Kombination dieser Applikatio-

nen innerhalb eines Unternehmens vorzufinden ist. Die unterschiedlichen Routing-Plattformen von Cisco unterstützen ein breites Dienstespektrum und gewährleisten Interoperabilität und Funktionalität auf höchster Ebene. Die Spitzenprodukte von Cisco aus der 7200-Serie und der 7500-Serie können typischerweise am Standort des SAP-Datencenters eingesetzt werden, um die erforderliche Konnektivität zu einer Vielzahl von Access-Routern in den jeweiligen Außenstellen herzustellen.

Frame Relay ist derzeit wahrscheinlich der meistgenutzte Dienst für den Anschluss von Außenstellen. Die am häufigsten eingesetzten Frame Relay-Netzwerke verwenden eine "Stern"- oder "Hub-and-Spoke"-Topologie, die den SAP R/3-Systemanforderungen für den Anschluss aller Clients an ein zentrales Datacenter entspricht.

IP-VPN-Netze gewinnen bei der Vernetzung von Außenstellen, Partnern, Kunden und mobilen Anwendern zunehmend an Bedeutung. Das Hauptziel ist hier eine umfassende, kostengünstige Vernetzung aller Beteiligten, die eine Schnittstelle zum R/3-System benötigen.

3.3.1 Anforderungen an die WAN-Bandbreite

Bei der Planung der erforderlichen WAN-Bandbreitenkapazität für R/3-Verkehr und den restlichen über das WAN geleiteten Applikationsverkehr ist es wichtig, den bestehenden Verkehr und die grundlegenden Verzögerungsmerkmale zu analysieren. Beispielsweise benötigt der primäre R/3-Verkehr eine bestimmte Bandbreite, es muss aber auch weiterer potentieller Verkehr, wie Dateitransfer, Drucken, E-Mail und Internetzugang, berücksichtigt werden. Bei den Überlegungen zu der zusätzlichen durch die neuen R/3-Applikationen benötigten Bandbreite kann folgende Schätzung zugrunde gelegt werden:

Bei einem Dialogschritt (oder einer Maskenänderung) werden ungefähr 2,0 KB Daten zwischen Applikationsserver und Client übertragen. Die folgende SAP-Formel kann als grobe Richtlinie für die Berechnung der zusätzlichen WAN-Leitungskapazität verwendet werden, die für die Unterstützung des Netzwerkverkehrs zwischen Applikationsserver und Client erforderlich ist:

$$\text{SAP R/3-Bandbreitenanforderung} = 16.000 \times \text{Anzahl der aktiven R/3-Anwender} \\ / (\text{Dialog Think Time} + \text{Response Time}) \text{ Bits/sek.}$$

SAP empfiehlt, auf keinen Fall eine Leitungskapazität $\leq 9,6$ KB zu verwenden.

Diese Berechnung ist eine hilfreiche Richtlinie, gilt jedoch nur für den Standardzugriff auf SAPGUI. Sie umfasst keine weiteren Anforderungen an den Netzwerkverkehr, wie Sprach-, E-

Mail-, FTP- oder Druckverkehr. Daher ist es sehr wichtig, in der Phase vor dem Einsatz von SAP R/3 eine Baseline für den Netzwerkverkehr vorzusehen, so dass sämtliche Netzwerk-anforderungen im Rahmen der gewählten Architektur berücksichtigt werden können. Zusätzlich zu dem SAPGUI-Verkehr ist weiterer SAP-Verkehr innerhalb des WAN, wie z. B. Druckverkehr, Datenbank-Backup etc. zu berücksichtigen.

Neben der Sicherstellung von ausreichender Bandbreite zur Unterstützung der unterschiedlichen WAN-basierten Applikationen wird dringend empfohlen, Quality of Service (QoS)-Mechanismen einzusetzen, um vorhersehbare R/3-Reaktionszeiten, auch zu verkehrsstarken Zeiten, zu gewährleisten. Dies wird an späterer Stelle noch erörtert.

3.3.2 WAN-Flexibilität

Hohe Verfügbarkeit über das gesamte WAN hinweg ist für die meisten Unternehmen mit abgesetzten R/3-Applikationen ein wichtiges Thema. Die Routing-Lösungen von Cisco bieten umfangreiche Funktionen, um diesen Anforderungen gerecht zu werden.

Um Redundanz auch in den Außenstellen zu garantieren, sollten alle großen Netzwerkhubs über zwei Zugangspunkte zum WAN-Dienst und zwei Router für Lastenausgleich und Backup verfügen. Bei kleineren Standorten basiert das Backup-Medium häufig auf ISDN oder einem zweiten Frame Relay-PVC (PVC – permanent virtual circuit). Bei Standorten, an denen verschieden geroutete lokale Loops nicht zur Verfügung stehen, bedienen sich die Unternehmen häufig alternativer Strategien wie Satellitenverbindungen.

Wo ein 24 x 7-Dienst erforderlich ist, können Unternehmen sich nicht einfach auf die Dienstbereitungsverträge von Diensteanbietern verlassen. Aus diesem Grund stellen viele Unternehmen die vollständige Redundanz eigenverantwortlich sicher, wobei die Redundanz sogar über verschiedene WAN-Diensteanbieter gewährleistet wird.

Die erweiterten IOS-Softwarefunktionen von Cisco für erhöhte Fehler toleranz im WAN umfassen:

- Einstellbares Routing-Protokoll für schnelle Fehlereingrenzung
- Hot Standby Routing Protocol (HSRP)
- Lastverteilung über Layer 3-Links
- Backup-Links mit ISDN- oder WAN-Medien
- fortschrittliche eingebettete Tools zur Problembehebung
- eine große Zahl von Netzwerkmanagement-Tools zur Überwachung und Lokalisierung von Fehlern

4. Optimierung von R/3-Applikationen innerhalb eines Netzwerks

Die Einhaltung akzeptabler Reaktionszeiten stellt eine Hauptanforderung für SAP R/3-OLTP-Umgebungen dar. Dazu müssen sämtliche Infrastrukturkomponenten, einschließlich Plattform, Datenbank, Clients und natürlich auch das Netzwerk selbst, über die Ressourcen und die Intelligenz zur Vermeidung von Verzögerungen oder Engpässen verfügen.

R/3-Applikationen werden in der Regel nicht als erste Anwendung in einem Netzwerk eingesetzt, sondern eher im Rahmen einer Migration innerhalb einer bestehenden Infrastruktur. Aus diesem Grund müssen sich neue R/3-Applikationen die knappen Ressourcen mit einer Vielzahl anderer Netzanwendungen teilen.

Gemäß der Gartner-Gruppe:

- werden bis 2003 vor allem Anwendungspakete wie R/3 die LAN-Bandbreite des Backbones um das Zehn- bis Zwanzigfache und die WAN-Bandbreite um mindestens 300 Prozent erhöhen;
- werden im Jahr 2000 bis zu 20 Prozent der wichtigsten Netzwerk-Applikationen schwerwiegende Performance-Probleme haben;
- werden sowohl die QoS-Anforderungen für vernetzte Applikationen als auch die Dienstbereitungsverträge für Netzwerk-Performance den traditionellen Ansatz einer Überdimensionierung der Bandbreitenkapazität unbrauchbar machen.

Die Notwendigkeit von QoS gilt sowohl für neue als auch für bereits existierende R/3-Systeme. QoS bezieht sich auf die Fähigkeit, bessere Dienste für ausgewählte vernetzte Applikationen zu bieten. Hat ein Unternehmen aufgrund einer Überlastung des Netzwerks Performance-Probleme mit dem R/3-System, ist der Bedarf offensichtlich. Auch wenn die Erhöhung der Bandbreite eine mögliche Antwort darstellt, handelt es sich dabei häufig nur um eine vorübergehende Lösung, da der anderweitige konkurrierende Verkehr weiter ansteigt. Darüber hinaus kann die Erhöhung der Bandbreite, insbesondere bei WANs, auch die teuerste Lösung sein.

Eine andere Strategie, die das Problem nur verschleiert, besteht darin, den Einsatz zusätzlicher geschäftskritischer Applikationen, wie Sprache und Multimedia, aufzuschieben, um den bestehenden geschäftskritischen R/3-Verkehr zu schützen. Hierdurch erreicht das Unternehmen weder die für den Unternehmenserfolg erforderlichen Produktivitätsgewinne und Wettbewerbsvorteile, noch nutzt es seine Netzarchitektur in vollem Umfang. Andere Unternehmen verzögern das Zusammenwachsen ihrer unterschiedlichen Netzwerke oder WAN-Verbindungen und verzichten so auf enorme Vorteile.

Der Einsatz applikationsbasierter QoS kann diese Probleme lösen und bietet folgende Vorteile:

- Verbesserung der Endnutzerzufriedenheit durch konstante Bereitstellung des Bedarfs an Reaktionszeiten für R/3-Applikationen
- Schnellerer und effizienterer Einsatz von R/3-Systemen durch Vermeidung von Netzwerkproblemen
- Geringere Gesamtkosten (TCO), einschließlich des geringeren Bedarfs an Netzinfrastruktur

Der Einsatz applikationsbasierter QoS kann gleichzeitig die Performance erhöhen und Gesamtkosten senken.

Die Unternehmensleitung wünscht in der Regel Reaktionszeiten für Transaktionen im Bereich von einigen Sekunden, wobei aggressivere Unternehmen bereits versuchen, Reaktionszeiten zwischen einer und zwei Sekunden zu erzielen. Wenn die derzeitige Grundverzögerung einer transatlantischen Frame Relay-Verbindung beispielsweise 400 msec betragen kann, bleibt nicht mehr viel Spielraum für zusätzliche Verzögerungen aufgrund überlasteter Netzwerke oder langsamer Verarbeitung auf den Servern.

4.1. Implementierung von QoS in R/3

QoS sollte eingesetzt werden, um vor allem den Datenfluss bei R/3-Applikationen gegenüber weniger kritischem Verkehr wie Web-Browsing, E-Mail und Dateitransfer bevorzugt abzuwickeln.

Die Netzwerkgeräte von Cisco sind in der Lage, alle Verkehrsströme sowohl auf der Grundlage von Layer 3- und Layer 4-Parametern als auch über die entsprechende physische Geräteschnittstelle zu klassifizieren und ermöglichen somit den selektiven Einsatz von QoS gemäß Applikationstyp. Darüber hinaus wird derzeit an einer Verbesserung der Verkehrsklassifizierung gearbeitet, um über alle Layer hinweg bis hin zum Layer 7 eine genauere Unterteilung und höhere Flexibilität zu erreichen. An dieser Stelle wird lediglich auf die Verwendung von Layer 3- und Layer 4-Parametern eingegangen, die den meisten derzeitigen R/3-Anforderungen entsprechen:

- IP-Quell- und Zieladressen
- Protokoll
- TCP- oder UDP-Quell- und Ziel-Portnummern

Bei den meisten großen R/3-Installationen werden mehrere Applikationsserver eingesetzt. In einigen Fällen replizieren mehrere physikalische Server die gleiche Applikation, können jedoch verschiedenen Logon-Gruppen oder Funktionen zugeordnet sein, (z. B. Transaktion versus Report-Verarbeitung). In vielen Fällen werden verschiedene Funktionsmodule für se-

parate physikalische Server konfiguriert. QoS kann in beiden Fällen über die Quell- und Ziel-IP-Adresse der Server angewendet werden.

Eine weitere Klassifizierung von R/3-Datenströmen ist über die Layer 4-Portnummern möglich, die zum Aufbau von TCP-/UDP-Verbindungen über IP genutzt werden.

Zur Verwaltung mehrerer Instanzen einer Applikationsinstallation können die Standard-Portnummern verwendet oder neue Portnummern konfiguriert werden. Eindeutige, bekannte Portnummern, die die Anwendungserkennung erleichtern, werden von verschiedenen Systemkomponenten verwendet, wie Client-Server, Message-Server, Gateway-Server und Druck. Diese Portnummern sind in Abbildung 4 dargestellt.

4.1.1 Welche QoS-Funktionen können genutzt werden?

Es gibt zwei Möglichkeiten, QoS einzusetzen. Differenzierter Service weist den Datenströmen je nach Applikation, Benutzer oder Inhalt die Priorität zu. Dieser Dienstyp ist für den Großteil des geschäftskritischen Verkehrs, der minimale Verzögerungen und fehlerfreie Übertragung erfordert, am besten geeignet. Garantierter Service reserviert eine bestimmte Bandbreitenkapazität für eine ausgewählte Sitzung und eignet sich ideal für spezifischen und konstanten Bandbreitenbedarf wie Video-Datenverkehr.

R/3-Systeme weisen die folgenden Merkmale auf, die für differenzierten Service sprechen:

- Verzögerungs- und Fehlerempfindlichkeit, jedoch keine Bandbreitenempfindlichkeit

- Toleranz gegenüber Laufzeitschwankungen
- Viele Sitzungen mit jeweils geringem Bandbreitenbedarf
- Nach Transaktionstyp variierende Bandbreitenverwendung

Da sowohl die R/3-Applikationen als auch die jeweils eingesetzte Netzwerkarchitektur sehr unterschiedlich sein können, sollte eine möglichst breite Palette an QoS-Mechanismen eingesetzt werden, so dass der Applikationsbedarf unabhängig von den verwendeten Medien oder Netzwerkgeräten komplett abgedeckt wird. Zudem ist die Verwendung eines Signalisierungs-Mechanismus wichtig, der die unterschiedliche Bevorzugung von verschiedenen Applikationen lückenlos signalisieren kann.

Im nachfolgenden Abschnitt "Grundlegende QoS-Architektur" werden die drei Komponenten beschrieben, die für den Einsatz von QoS im Netz erforderlich sind, einschließlich heterogener Technologien (IP, ATM, LAN-Switches etc.).

Grundlegende QoS-Architektur

In der grundlegenden Architektur sind die drei Hauptelemente für die QoS-Implementierung enthalten (siehe Abbildung 11):

- QoS-Mechanismus innerhalb eines einzigen Netzwerkelements (zum Beispiel Queuing-, Scheduling- und Verkehrsgestaltungs-Tools)
- QoS-Signalisierungs-Techniken zur netzweiten QoS-Koordination zwischen den Netzwerkelementen
- QoS-Richtlinien-, Management- und Abrechnungsfunktionen zur Kontrolle und Verwaltung des End-to-End-Verkehrs in einem Netzwerk.

4.1.2 Das Cisco QoS-Toolkit

Die Cisco IOS-Software bietet verschiedene QoS-Tools, um die QoS-Klassen für die R/3-Applikation zu gewährleisten. Diese Tools werden normalerweise in einem einzigen Netzwerkelement eingesetzt, entsprechend der in Abbildung 11 dargestellten grundlegenden Architektur. Diese Tools werden in der Regel an einer Schnittstelle aktiviert, um die geeigneten QoS-Merkmale für eine bestimmte Netzwerk-Applikation zur Verfügung zu stellen. Die Cisco IOS-QoS-Tools verfügen über drei Hauptfunktionen – Überlastmanagement (Queuing und Scheduling), Überlastvermeidung und Verkehrsgestaltung. Darüber hinaus bieten die Cisco IOS-Tools einen Link-Efficiency-Mechanismus, der in die anderen drei Funktionen integriert ist und zusätzliche QoS-Funktionalität bereitstellt.

Überlastmanagement-Tools

Eine Möglichkeit für den Umgang mit eingehender Verkehrsüberlastung in einem Netzwerk ist die Verwendung von Queuing-Algorithmen, die den Verkehr sortieren. Anschließend wird eine Methode definiert,

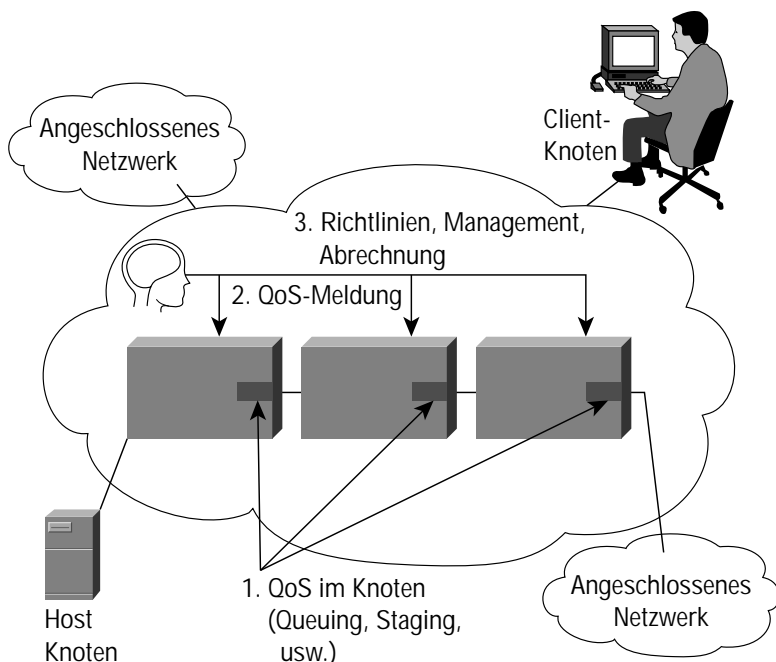


Abbildung 11: Grundlegende QoS-Architektur

um den Verkehr auf einem Output-Link nach Priorität zu behandeln. Die IOS-Software von Cisco enthält folgende Queuing-Tools:

- Priority Queuing (PQ)
- Custom Queuing (CQ)
- Weighted Fair Queuing (WFQ)
- Class-Based Weighted Fair Queuing (CB-WFQ)

Die jeweiligen Queuing-Algorithmen wurden zur Lösung eines bestimmten Verkehrsproblems im Netzwerk entwickelt und haben eine jeweils eigene Auswirkung auf die Netzwerk-Performance. Im Rahmen durchgeführter Prüfungen mit ERP-Applikationen hat sich CB-WFQ in einigen Applikationssituationen als sehr effektiv erwiesen, während CQ in anderen Situationen am wirksamsten war.

Überlastvermeidungs-Tools

Überlastvermeidungs-Tools überwachen die Verkehrslast im Netzwerk, um Überlastungen an den üblichen Engpässen im Netz zuvorkommen und diese zu vermeiden, im Gegensatz zu Überlastmanagement-Verfahren, die eingesetzt werden, wenn eine Überlastung bereits eingetreten ist. Das primäre IOS-Überlastvermeidungs-Tool von Cisco Weighted Random Early Detection (WRED). WRED ist in der Lage, Verkehr mit niedrigerer Priorität selektiv zu verwerfen, wenn an der Schnittstelle eine Überlastung eintritt, und differenzierte Performance-Merkmale verschiedener Service-Klassen bereitstellen.

Verkehrsgestaltungs- und Überwachungs-Tools

Die QoS-Software-Lösungen von Cisco bieten zwei Verkehrsgestaltungs-Tools zur Verwaltung von Verkehr und Überlastung im Netz: Generic Traffic Shaping (GTS) und Frame Relay Traffic Shaping (FRTS).

GTS verfügt über einen Mechanismus, um den Verkehrsfluss an einer definierten Schnittstelle zu überwachen. Somit kann Verkehr mit einem bestimmten Profil so gestaltet werden, dass er entsprechende Downstream-Anforderungen erfüllt, wodurch Engpässe vermieden werden. In Topologien mit Unstimmigkeiten im Datenprofil kann GTS Zugangslisten einsetzen, um den zu gestaltenden Verkehr auszuwählen. GTS arbeitet hier mit verschiedenen Layer 2-Technologien, einschließlich Frame Relay, ATM und Ethernet.

Frame Relay TS kann Engpässe in Frame Relay-Netzwerken mit Hochgeschwindigkeits-Verbindungen in der Zentrale und Niedriggeschwindigkeits-Verbindungen in den Niederlassungen beseitigen.

4.1.3 QoS-Signalisierung

Die QoS-Signalisierung stellt eine Form der Kommunikation innerhalb des Netzes dar. Sie ermöglicht es einer End-Station oder einem Netzwerkelement, bestimmte Anforderungen an ein benachbartes Gerät zu richten. Ein IP-Netzwerk kann bei-

spielsweise einen Teil des IP-Packet-Header verwenden, um eine spezielle Behandlung von prioritärem oder zeitkritischem Verkehr anzufordern. Die QoS-Signalisierung ist für die Koordination der oben erwähnten Methoden zur Verkehrsbehandlung von Nutzen und spielt eine Schlüsselrolle bei der erfolgreichen Konfiguration eines netzwerkweiten QoS-Dienstes.

Echtes netzwerkweites QoS erfordert, dass alle Elemente im Netzwerkpfad – Switch, Router, Firewall, Host, Client etc. – ihren Teil zu QoS beitragen, und dies alles muss über QoS-Signalisierung koordiniert werden. Die Herausforderung besteht jedoch darin, eine robuste QoS-Signalisierungs-Lösung zu finden, die heterogene Netzarchitekturen vollständig abdeckt. Es gibt zwar zahlreiche realisierbare QoS-Signalisierungs-Lösungen, die zwar QoS lokal unterstützen, aber oft keine ausreichende netzwerkweite Funktionalität bieten.

Die IOS-Software von Cisco nutzt die netzwerkweite Ausprägung des IP, um dieser Herausforderung durch Überlagerung der für die Layer 2-Technologie charakteristischen QoS-Signalisierungs-Lösungen mit Layer 3 IP-QoS-Signalisierungs-Methoden zu begegnen. Diese Methoden umfassen Resource Reservation Protocol (RSVP) für garantierte Dienste – eher geeignet für Applikationen, die konstante Bandbreiten erfordern – und IP-Precedence, das die Signalisierung bei differenzierten Diensten durchführt, die für R/3 geeignet sind.

IP-Precedence verwendet zur Spezifizierung der Service-Klasse eines jeden Pakets die drei Precedence-Bits im Type of Service (ToS)-Feld des Ipv4-Headers. Der Verkehr kann mit IP-Precedence in bis zu sechs Service-Klassen unterteilt werden (zwei weitere sind für die interne Nutzung durch das Netz reserviert). Die Queuing-Technologien im Netzwerk können dieses Signal nutzen, um die geeignete prioritäre Behandlung bereitzustellen. Mit IP-Precedence können diese Service-Klassen über den bestehenden Queuing-Mechanismus im gesamten Netzwerk (zum Beispiel WFQ und WRED) eingerichtet werden, ohne dass Änderungen an den vorhandenen Applikationen vorgenommen oder komplizierte Anforderungen an das Netzwerk gestellt werden müssen.

IP-Precedence wird derzeit um zusätzliche Granularität und Flexibilität erweitert, so dass eine bessere Unterstützung aktueller Sprach- und Video-Applikationen über den neueren DiffServ IETF-Draft-Standard möglich sein wird. Die derzeitigen sechs Klassifizierungsebenen werden dadurch auf 64 Klassifizierungsebenen erweitert.

Weitere Informationen zu den Cisco QoS-Netzwerk-Lösungen erhalten Sie unter:

http://www.cisco.com/warp/public/cc/cisco/mkt/ios/tech/tch/qosio_wp.htm

4.2 Policy Networking

Die intelligenten Netzwerklösungen von Cisco bieten dem Anwender eine breite Auswahl an QoS-Mechanismen, die sämtliche R/3-Applikationen unterstützen. Der Einsatz dieser Features kann jedoch für Netzwerkmanager, die große Netzwerke verwalten, eine komplexe Aufgabe darstellen. Es besteht eindeutig ein Bedarf an Technologien zur konsistenten dynamischen Steuerung und Konfiguration dieser QoS-Funktionen über das gesamte intelligente Netzwerk hinweg. Netzwerkgeräte müssen regelmäßig angepasst werden, um die steigende Anzahl an Benutzern, neue Implementierungen, die Benutzermobilität sowie die ständig zunehmenden neuen Applikationen zu unterstützen.

Diese Kundenanforderungen werden über das Policy-Networking bedient. Der Bedarf an Policy-Networking wird durch Geschäftsanforderungen, die Markt- und Wettbewerbskräften unterworfen sind, verstärkt. Der Netzwerkmanager muss in der Lage sein, diese Geschäftsanforderungen bestimmten Richtlinien zuzuordnen und damit in ein konkretes Netzwerkverhalten umzusetzen. Betreibt ein Unternehmen zum Beispiel eine R/3-Applikation, um strategische Wettbewerbsvorteile zu erreichen, dann können Richtlinien definiert werden, die den R/3-Verkehr prioritär behandeln. Auf diese Weise werden strategische Unternehmensziele automatisch in ein entsprechendes Netzwerkverhalten übertragen.

4.2.1 CiscoAssure Policy Networking

Die CiscoAssure Policy Networking-Initiative richtet sich an Kunden mit Policy Networking-Bedarf. Mit CiscoAssure Policy Networking können Unternehmen und Applikationen die in Cisco-Netzwerke integrierte Intelligenz nutzen. Die CiscoAssure Policy-Netzarchitektur basiert auf vier Bausteinen:

- Intelligente Netzwerkgeräte – Router, Switches und Access-Server, die die Cisco IOS-Software ausführen, ermöglichen und unterstützen Policy-Dienste im Netzwerk (siehe nachstehende Abbildung 12).
- Policy-Dienste – setzen die strategischen Unternehmensziele in Netzwerkkonfigurationen um und aktivieren Richtlinien für QoS, Sicherheit und weitere Netzwerkdienste.
- Policy-Verwaltung – ermöglicht die zentrale Konfiguration von regelbasierten Richtlinien zur Steuerung der Dienste innerhalb der Netzarchitektur.
- Registrierungs- und Verzeichnisdienste – stellen eine dynamische Verbindung zwischen Adressen, Applikationsprofilen, Benutzernamen und weiteren Informations-Datenspeichern her.

4.2.2 Zentralisierte QoS-Policy-Verwaltung

Der Cisco QoS Policy Manager (QPM) ist ein mit umfangreichen Funktionen ausgestattetes QoS-Policy-System, das die Konfiguration und den Einsatz von QoS-Policy-Funktionen in Unternehmensnetzwerken vereinfacht. QPM zeichnet sich durch eine Vielzahl entscheidender Vorteile aus: es ermöglicht verbesserte differenzierte Dienste, automatisiert die QoS-Policy-Verwaltung und verbessert die Kosteneffizienz von WAN-Verbindungen. QPM stützt sich auf IP-Precedence für die netzwerkweite QoS-Policy-Implementierung und ermöglicht Netzwerkmanagern die schnelle Anwendung kombinierter QoS-Policy-Maßnahmen, um die Performance von geschäftskritischen Applikationen wie R/3 sicherzustellen.

QPM weist u. a. folgende Vorteile auf:

- Zentrale Steuerung der Policy-Maßnahmen über eine komfortable grafische Benutzeroberfläche. Der Policy-orientierte Ansatz ermöglicht das systemübergreifende Konfigurieren, Ändern und Einrichten von QoS und macht die Konfiguration auf Geräteebene überflüssig.
 - Komfortable Tools für die Cisco-spezifische Konfiguration von Verkehrsklassen und Einrichtung von QoS-Policy-Maßnahmen zur Differenzierung von QoS-Service-Klassen.
- QoS-Domänenkonfiguration – eine intelligente Gruppierung von Schnittstellen, um QoS-Mechanismen selektiv für die jeweilige Policy-Domäne zu aktivieren.
- Zuverlässige Policy-Implementierung – Überprüfung der Policy-Validierung, Vorschau auf Konfigurationsänderungen, teilweise Aktualisierung von Zugangssteuerungslisten (ACL-Access Control List) und Funktionen zur Job-Überwachung, um einen sicheren Einsatz von QoS-Policy-Maßnahmen auf Geräten von Cisco zu gewährleisten.

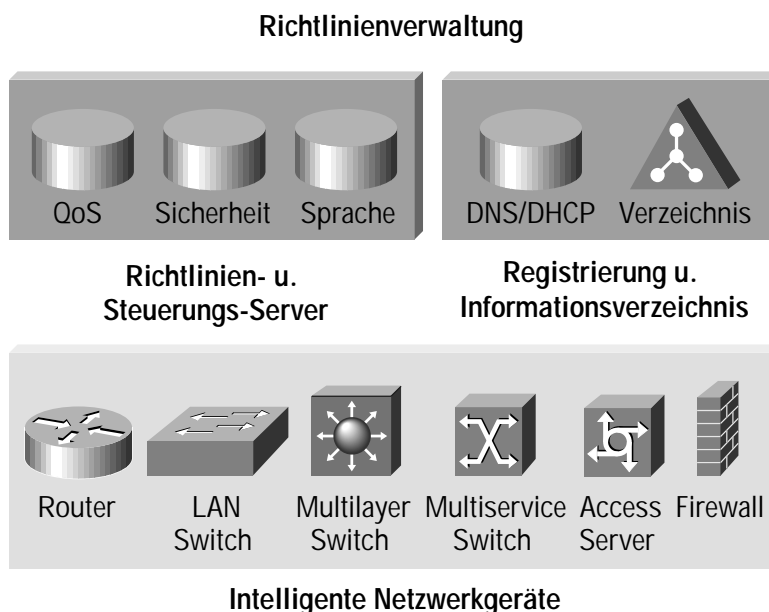


Abbildung 12: CiscoAssure-Architektur

- Web-basiertes Reporting – Web-basierte Reports, die eine rasche Anzeige und Analyse der eingesetzten QoS-Policy-Maßnahmen ermöglichen.

Mit dem Cisco Policy Manager lassen sich die Performance-Anforderungen von R/3-Applikationen automatisch in QoS-Policy-Maßnahmen umsetzen.

Weitere Informationen zum QoS Policy Manager von Cisco erhalten Sie unter:

http://www.cisco.com/warp/public/cc/cisco/mkt/enm/cap/qospm/prodlit/qospm_ds.htm

4.2.3 Überwachung der R/3-Performance

Die meisten Unternehmen stellen zumindest grundlegende SLA-Anforderungen an die Performance der SAP R/3-Transaktionen. Die Einhaltung dieser Anforderungen kann mit den Management- und Überwachungs-Tools des CCMS von SAP überwacht werden. Neuere CCMS-Versionen sind sogar in der Lage, die R/3-Client-Server-Verkehrsverzögerung netzwerkweit zu erkennen und liefern sowohl Angaben zu einzelnen Transaktionen als auch Durchschnittswerte. Auf diese Weise wird der Netzwerkmanager gewarnt, wenn es irgendwo im Netz zu Überlastungen und zu nachfolgenden Verzögerungen bei R/3-Transaktionen kommt.

Die Tools von Cisco zur Überwachung von Performance und Verfügbarkeit sind in der Lage, überlastete Netzregionen präzise zu lokalisieren. Durch diese Information kann der Netzwerkmanager die richtige Vorgehensweise wählen und beispielsweise neue QoS-Policy-Maßnahmen definieren und einleiten oder zusätzliche Bandbreiten im überlasteten Netzsegment bereitstellen. Diese Tools arbeiten mit Cisco Internetwork Performance Monitor IPM, das mittels eingebetteter Cisco IOS-Agenten permanent die Verzögerung zwischen zwei Netzwerkgeräten überwacht.

Weitere verfügbare Überwachungs-Tools beinhalten WAN Switch Probes und Traffic Director Application zur Überwachung von WAN-SLAs.

4.2.4 Einsatz von CiscoAssure QPM und Cisco IOS-QoS-Funktionen für SAP R/3

Der SAP R/3-Verkehr wurde mit einer Vielzahl von Cisco IOS-QoS-Mechanismen unter Überlastbedingungen geprüft. Diese QoS-Mechanismen erwiesen sich alle als wirksam (siehe Abbildung 13). Diese Tests zeigen eindrucksvoll, dass Netzwerke von Cisco selbst unter extremen Überlastbedingungen eine extrem sichere und konstant leistungsfähige Plattform für R/3-Anwendungen bilden.

Der nachstehende Test wurde in Zusammenarbeit mit SAP in Walldorf durchgeführt. Die Ergebnisse können als Richtwert für die Verwendung von grundlegenden Cisco IOS-Mechanismen auf einer 64-kbps-Verbindung mit hohem FTP-Verkehr und gleichzeitiger Versorgung von 10 SAP R/3-Anwendern herangezogen werden.

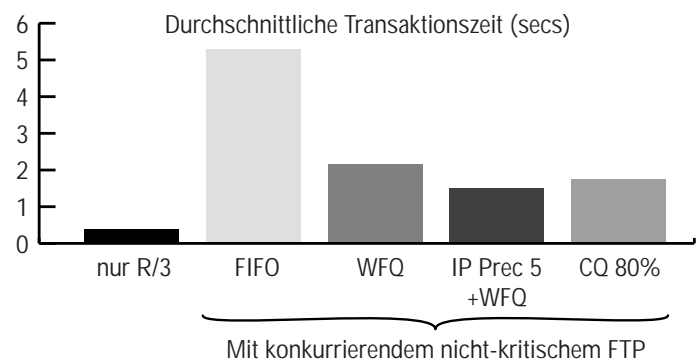


Abbildung 13: Beispiel für die Verbesserung der Reaktionszeit durch den Einsatz von QoS

5. Schlußfolgerung

Zusammenfassend lässt sich feststellen, dass das R/3-System enorme Anforderungen an die IT-Netzinfrastruktur eines Unternehmens stellt. Um den erfolgreichen Einsatz dieser geschäftskritischen Applikationen zu gewährleisten, muss das Netzwerk-Team frühzeitig in die Planung einer skalierbaren, flexiblen und intelligenten Architektur einbezogen werden. Auf diese Weise lässt sich sicherstellen, dass das R/3-System die hohen Erwartungen sowohl der Unternehmensleitung als auch der Anwender erfüllt.

Cisco stellt komplette Netzwerk-Lösungen für den erfolgreichen Einsatz von ERP-Systemen bereit, deren Erfolg auf der führenden Cisco-Technologie, auf langjähriger Erfahrung, erstklassigem Support und zahlreichen Partnerschaften mit Software- und Hardwareherstellern sowie auf dem Einsatz von Systemintegratoren beruht.

Insbesondere besteht eine technologische Partnerschaft zwischen Cisco und SAP. Die beiden Unternehmen arbeiten eng zusammen, um den erfolgreichen Einsatz von R/3-Applikationen sicherzustellen. Die Partnerschaft von Cisco und SAP bietet so allen gemeinsamen Kunden eine leistungsstarke und sichere Plattform für erfolgreiches E-Business.





Cisco Systems E-Mail: info-center@cisco.com

Web-Seite: <http://www.cisco.de>

Telefon: 018 03/67 10 01, Fax: 0811/5543-10