Dr. Suppan International Institute

Der Netzwerk Insider

April 2000

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Ein Jahr danach: Anspruch und Realität von Policy Konzepten

von Dipl.-Inform. Petra Borowka

Verstärkte Service Level Bedarfe führen zu ständig steigenden Anforderungen an Konfiguration und Betrieb von LAN-WAN-Verbundnetzwerken. Dabei sind es nicht vorrangig neue Applikationen mit Video, Sprache und multimedialen Anteilen sondern insbesondere etablierte Produktiv-Anwendungen, die mit erhöhter Dienstgüte betrieben werden sollen.

Im April 1999 haben wir im Netzwerk Insider Möglichkeiten für Quality of Service mit Frame-Techniken im Schwerpunktthema "Quality of Service im LAN: Leistung contra Komplexität" beschrieben. (Auf Wunsch stellen wir diesen Artikel zur Verfügung, wenn er bei Ihnen nicht vorliegt: bitte Anfrage an insider@comconsult.de)

gereiftes Zusammenspiel?

Inzwischen sind Geräte mit Quality of Service-Funktionen für Frame-Technologien soweit gereift, dass sie für einen produktiven Einsatz infragekommen.

Die Konsequenzen liegen auf der Hand: Steigende Komplexität bei Konfiguration, Betrieb und Störfall-Diagnose der Netzwerk- und Server-Infrastruktur.

Daher versuchen Hersteller und Standardisierer mit Policy-Konzepten einen Überbau zu schaffen, um Netzdesign und Netzbetrieb "trotz" Quality of Service mit vertretbarem Aufwand in den Griff zu bekommen.

weiter auf Seite 12

Unser Geleitwort zur persönlichen Bewertung der Marktsituation durch Dr. Jürgen Suppan

Wer ersetzt 3Com, wer gewinnt, wer verliert? 3Com-Produkte noch kaufen oder konsequent aussteigen?

Unser Markt ist in einem merkwürdigen Zustand. Da hinterlässt ein Hersteller 3Com riesige Investitions-Ruinen bei Kunden, die sich sowieso schon seit geraumer Zeit mit Core-Builder-Systemen mehr schlecht als recht abplagen. Und was passiert? Einige Zeitschriften loben auch noch die nun neue Ausrichtung auf den Mittelstand. Kein Wort der Kritik oder des Tadels.

Um es klar auszusprechen: 3Com hat in den letzten 2 Jahren durch sein Marketing und seine Werbung den Kunden auch eine Botschaft vermittelt, ein Versprechen über Produktleistung und Produktverfügbarkeit. Die Nichteinhaltung dieses Versprechens ist an der Grenze zum Betrug. Die Zusage einer 5-jährigen Pflege ist angesichts der Nichtauslieferung wichtiger Merkmale (zum Beispiel Policy Networking) und eines extrem dynamischen Marktes, der eine sehr schnelle Weiterentwicklung neuer Features erfordert (zum Beispiel: Stromversorgung Telefone, Directory Enabled Networking, fehlersichere Architekturen) eine offene Verhöhnung der Kunden. Was lernen wir daraus? Auf jeden Fall besteht der Bedarf nach juristisch perfekt abgefassten Verträgen, die die Erwartungen des Kunden im Rahmen der Nutzungsdauer des Geräts präzise beschreiben und absichern. Speziell die Versorgung mit Ersatzteilen, neuen Software-Releases und bereits erkennbaren zukünftigen Technologien sollte ein wesentlicher Teil eines Vertrags sein. Dummerweise wird damit das Risiko in der Regel nicht zum Hersteller sondern zum Händler verschoben. Damit ist der Händler aufgefordert, sich die Hersteller, die er vertreibt, sehr genau anzusehen und vor allem deren Service- und Pflegeverpflichtungen genau zu hinterfragen.

Was wird nun aus 3Com, wird die Konzentration auf den Mittelstand erfolgreich sein, sollten die weiter von 3Com angebotenen Produkte wie die SuperStack-Serie weiter gekauft werden?

weiter Seite 2

Wer ersetzt 3Com, wer gewinnt, wer verliert? 3Com-Produkte noch kaufen oder konsequent aussteigen?

Die Historie hat meines Erachtens gezeigt, dass in der Folge einer derartigen Entscheidung der Image-Verlust bei den Kunden so groß ist, dass sich viele Kunden abwenden werden.

Hinzu kommt, dass gerade im Kernbereich der zukünftig angebotenen Produkte ernsthafte Alternativen mit einem wesentlich höheren Grad an Investitions-Sicherheit bestehen.

Beispielsweise sind sowohl HP mit den ProCurve-Systemen 4000 (über 380% Wachstum in 1999, siehe gute Übersicht unter http://www.hp.com/rnd/products/3com_main.htm) als auch Nortel Networks mit den BayStack-Produkten 350, 400, 450 sowohl in Preis als auch in Leistung durchaus mit den 3Com Super-

Stack-Systemen vergleichbar, wenn nicht in der Gesamtleistung sogar besser.

Und: diese Hersteller folgen mit ihrer dynamischen Produktentwicklung den neuesten Trends wie ausfallsichere Architekturen und Low-End-Layer-3-Switching (beim letzteren wird es in der zweiten Jahreshälfte einen riesigen Boom an sehr schnellen und sehr preiswerten Layer-3-Switch-Systemen geben. Wir kennen die neuen Geräte schon, dürfen aber noch nicht darüber reden. Eines aber darf gesagt werden: Layer-3-Gigabit-Leistung zum heutigen Layer-2-10/100-Preis steht direkt vor der Tür). Angesichts dieser Konkurrenz-Situation und der sehr schnellen Entwicklung halte ich den Wechsel von 3Com zu HP oder Nortel Networks für naheliegend.

Dementsprechend werden Sie auch bei HP auf der Web-Seite begrüßt:

"Willkommen 3Com-Kunde und Händler!"

Wenn 3Com Gefahr läuft, seine bisherigen Kunden zu verlieren, wie sind die neuen Produkte von 3Com zu beurteilen, speziell die IP-Telephonie und die Funknetze? Hat 3Com durch die Konzentration auf derartige Produkte eine Chance, sich neu auszurichten?

Meine ganz persönliche Meinung: mindestens in Deutschland nicht. Die NBX-Lösung für IP-Telephonie ist durch und durch proprietär, unterstützt zur Zeit weder S0 noch Primärmultiplex, lässt sich nicht im Anlagenverbund mit QSIG-Schnittstelle betreiben. Im direkten Vergleich zu Alcatel, CISCO und Nortel kann 3Com mit IP-Telephonie im deutschen Markt nicht bestehen. Die 3Com-Produkte für Wireless LANs nach 802.11 werden immer noch nicht ausgeliefert. Aber schon jetzt ist klar: hier wird ein erheblicher Wettbewerb herrschen. In diesen Markt geht im Moment jeder Netzwerk-Hersteller. Und zudem sind Anbieter tätig, die sehr auf den europäischen Markt optimierte Produkte anbieten.

Im direkten Vergleich von 3Com und Elsa würde ich mich beispielsweise klar für Elsa entscheiden. Die Elsa-Produkte sind deutlich preiswerter und die Elsa Access Points haben neben der üblichen 10/100-Ethernet-Schnittstelle bereits eine ISDN-Schnittstelle und fungieren für das Home Office oder den Small Business Bereich als Internet Zugangs-Router (haben wir getestet: funktioniert ohne Probleme innerhalb von 10 Minuten mit allen heute üblichen Merkmalen wie CHAP, Kanalbündelung, Filterung etc.).

Aus dieser Darstellung leite ich die Gefahr ab, in der sich 3Com mindestens in Deutschland befindet. 3Com läuft Gefahr, die alten Kunden zu verlieren und in den "neuen" Geschäftsfeldern nicht erfolgreich zu sein.

Wer wird von dieser Situation profitieren? Welche Hersteller bieten eine langfristige Investitionssicherheit und Bestandsgarantie bei einem gleichzeitig guten Preis-Leistungs-Verhältnis?

Das Grundproblem unseres Marktes besteht in den sehr kurzen Produkt-Lebenszyklen von typischerweise maximal 3 bis 4 Jahren (siehe Bild, Quelle Nortel Networks). Wer in diesen sehr kurzen Zyklen mit einem Produkt falsch liegt wie 3Com mit den CoreBuildern (zu hohe Entwicklungskosten, zu geringer Umsatz), der braucht sehr viel Geld im Rücken, um dies abfangen zu können und den Kunden weiterhin eine konsequente Weiterentwicklung bieten zu können. Eine Reihe von Anbietern hat dieses Geld. Dazu zählen u.a. Alcatel, CISCO, HP, Lucent (durch die Ausgliederung mit Abstrichen) und Nortel Networks. Diese Unternehmen haben zum Teil nennenswerte Reserven und sichern ihre Existenz durch ein breiteres Produkt-Portfolio ab. Auch bei diesen Anbietern besteht ein Restrisiko durch das Bekenntnis zum Shareholder-Value, der den kurzfristigen Gewinn höher bewertet als die langfristige Kundenbindung. Sprich: auch diese Anbieter könnten ganze Produktreihen aus dem Angebot nehmen, um ihre Profitabilität zu sichern.

Hier bleibt wieder nur der Verweis auf den entsprechend abgefassten und abgesicherten Kaufvertrag.

Impressum

Verlag:
Dr. Suppan
International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland
Niederlande

Telefon 02408/14907
Telefax 02408/149233

Herausgeber
und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

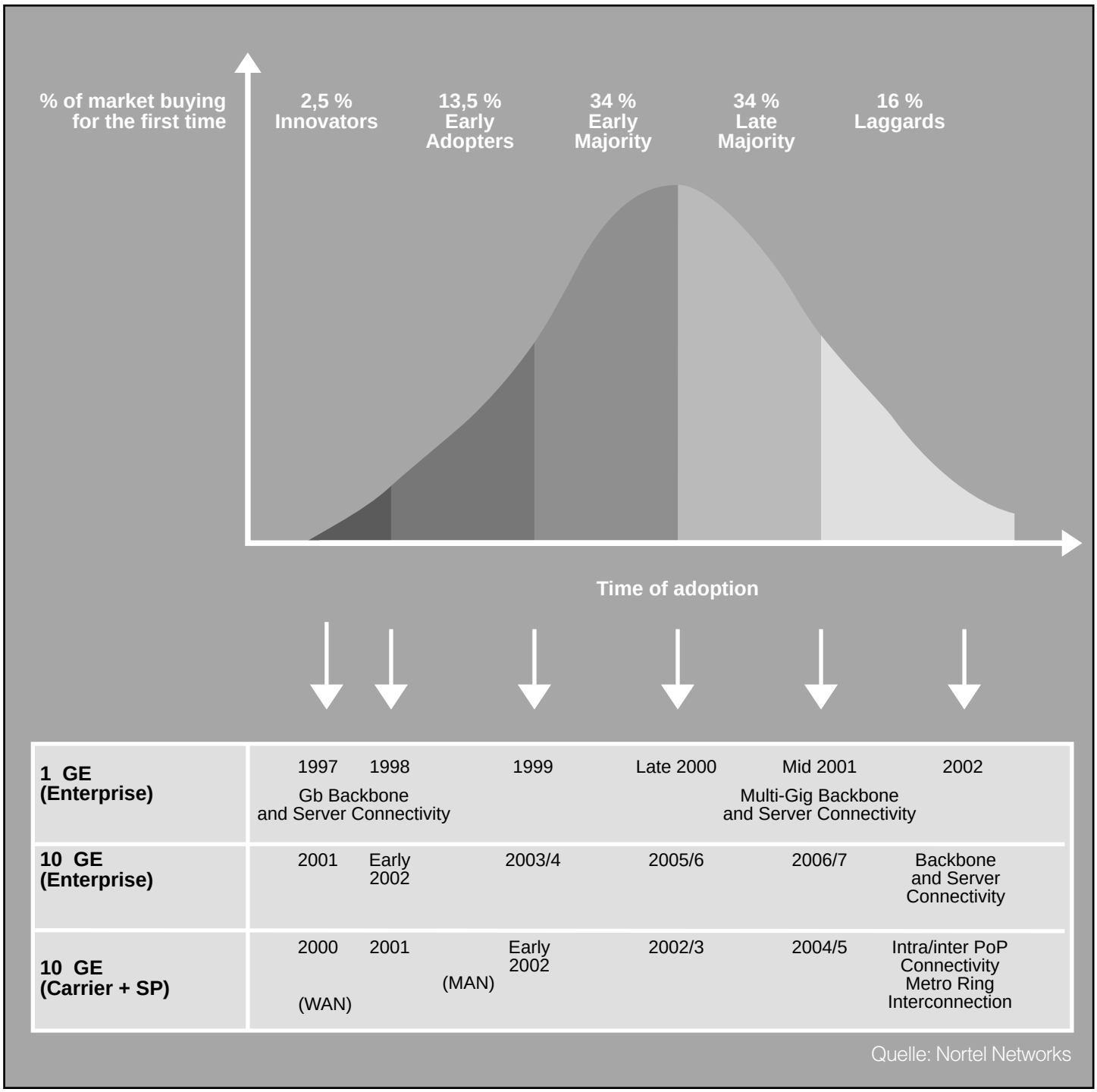
Gestaltung: Zweipfennig

Erscheinungsweise:
Monatlich,
12 Ausgaben im Jahr

Bezug:
Kostenlos
als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie

Für unverlangt
eingesandte Manuskripte
wird keine Haftung
übernommen

Wer ersetzt 3Com, wer gewinnt, wer verliert? 3Com-Produkte noch kaufen oder konsequent aussteigen?



1 GE (Enterprise)	1997 Gb Backbone and Server Connectivity	1998	1999	Late 2000	Mid 2001 Multi-Gig Backbone and Server Connectivity	2002
10 GE (Enterprise)	2001	Early 2002	2003/4	2005/6	2006/7	Backbone and Server Connectivity
10 GE (Carrier + SP)	2000 (WAN)	2001 (MAN)	Early 2002	2002/3	2004/5	Intra/inter PoP Connectivity Metro Ring Interconnection

Quelle: Nortel Networks

Produkt-Lebenszyklus im LAN-Markt

Nachfolgend eine Kurzeinschätzung dieser Hersteller aus meiner rein subjektiven Sicht:

- Alcatel hat durch diverse Käufe (Xylan, Packet Engine usw.) interessante Produkte im Angebot. Hier ist eine Integration dieser Produktreihen erforderlich, um im Markt bestehen zu können. Auch fehlen evtl. die Low-End-Produkte. Positiv ist die Öffnung von Alcatel zu internationalen Investoren zu bewerten, weg von dem provinziellen französichen Klüngel, hin zu einem transparent agierenden, international orientierten Unternehmen.

- CISCO macht in diversen Netzwerk-Märkten den meisten Umsatz und den meisten Gewinn, hat aber eine sehr breite Produktlinie mit sehr unterschied-

Wer ersetzt 3Com, wer gewinnt, wer verliert? 3Com-Produkte noch kaufen oder konsequent aussteigen?

lichen Qualitäten. Nachteil ist im LAN-Switching-Bereich bisher die Orientierung am Großkunden. Vorteile für CISCO können in der allgemeinen Entwicklung des Marktes hin zu Layer-3-Technologien bestehen. Zur Zeit wird durch CISCO einerseits durch Diversifikation der Weg beschritten, speziell im Großkunden-Segment noch weiter Umsatz zu machen und die bestehende Marktposition in diesem Segment weiter auszubauen (typisch Catalyst 6000 als Basis für IP-Telephonie). Andererseits versucht CISCO durch Produkte wie Catalyst 2900 und Catalyst 3500 im Mittelstand Fuß zu fassen. Ebenfalls in neue Märkte geht der Kauf von Aironet mit 802.11-Funknetzen und DSL-Zugangsroutern. Beides sind allerdings Technologien mit erheblichem Wettbewerb. Im Wireless-LAN-Bereich bestehen zudem auch noch technische Risiken (siehe Artikel im letzten Insider zur Überschneidung mit Bluetooth-Frequenzen). CISCO ist in Summe durch seine Produkte und vor allem seine interne Organisation sehr gut für die Zukunft gerüstet, muss sein Angebot aber stärker konzentrieren.

- HP hat in Deutschland sicher Bekanntheitsprobleme mit seinen Netzwerk-Produkten. Aber die Produkte haben ein sehr gutes Preis-Leistungs-Verhältnis und HP hat als Unternehmen einen sehr guten Namen. Damit hat HP gute Chancen auf eine zunehmende Markt-Bedeutung, wenn das TOP-Management weiter zum Netzwerk-Bereich steht (siehe Neuorganisation durch Frau Fiorino). Die notwendigen Absatzkanäle für eine Massenvermarktung sind seit mehreren Jahren vorhanden (Großhandel).

- Lucent hat ähnlich wie Alcatel seine Marktposition durch Aufkäufe errungen (Ascend, Lannet), ist aber in der Integration dieser Produkte weiter als Alcatel. Hier irritiert die Ausgliederung mit der gleichzeitigen Botschaft des Top-Managements, sich im Lucent-Kernbereich nur um stark wachsende und profitable Produkte kümmern zu wollen. Damit ist gleichzeitig die Botschaft verbunden, dass die Netzwerk-Produkte bisher nicht die Ziele des Managements erfüllt haben. Mal abgesehen von der Frage, was von einem Management zu halten ist, das derartige Botschaften offen in den Markt trägt, bietet die Ausgliederung der Netzwerk-Sparte auch Chancen durch die Beseitigung der inneren Abhängigkeiten.

- Nortel Networks hat eine sehr hohe Börsenkapitalisierung und verdient sein Geld vornehmlich als einer der führenden Spezial-Anbieter für hochratige Glasfaser-Übertragungen für Internet-Provider. Zudem ist der TK-Bereich mit den Meridian-Systemen in Kanada und den USA sehr gut aufgestellt. Das neue Enterprise Edge-System als integrierte TK-Lösung für IP- und normale Telephonie mit Software-Vollausstattung (ACD, CTI, Auto-Attendent, Unified Messaging usw.) zum Basis-Preis von 10.000 $ könnte sich zum absoluten Renner entwickeln. Nortel Networks hat sicher den Nachteil, sich in den letzten 2 Jahren nicht sehr um die Netzwerk-Großkunden in Deutschland gekümmert zu haben. Der Accelar 8000 ist sicher nicht in der Lage, einem Catalyst 6000 das Wasser zu reichen. Aber: mit der BayStack-Serie und den dort angekündigten neuen Produkten steht Nortel Networks sehr gut im Mittelstands-Markt. Durch das gleichzeitige Angebot von Netzwerk-Adaptern (NIC) ist Nortel im Produktportfolio sehr gut mit 3Com vergleichbar und und könnte einer der großen Gewinner der Situation sein. Ein Problem in Deutschland ist die diffuse organisatorische Entwicklung der letzten Jahre (Übernahme Dasa zu Nortel Dasa). Hier ist Nortel gefordert, sich stromlinienförmiger und straffer darzustellen (die ersten Schritte in diese Richtung sind sichtbar).

Diese Darstellung ist nicht vollständig. Um Ihnen einen Komplettüberblick zu bieten, werden wir in den nächsten Ausgaben des Netzwerk Insiders zusammen mit Dr. Kauffels einen Überblick über alle relevanten Anbieter geben und dabei auch sehr stark auf deren ökonomische Situation eingehen (Dr. Kauffels Investment Insider).

Einen Hersteller möchte ich noch kurz erwähnen. Dies ist die Firma Extreme Networks. 3Com verweist alle seine Kunden an Extreme und rät zum Ersatz der bestehenden CoreBuilder durch den BlackDiamond von Extreme. Ohne Frage sind die Produkte von Extreme im Layer-3-Switching-Bereich mit das Beste, was der Markt im Moment anbietet. Leider ist das Portfolio von Extreme unvollständig und es fehlen u.a. die Low-End-Massenprodukte. Auch sind die Absatzkanäle für den Massenverkauf nicht so vorbereitet wie es bei HP und Nortel Networks der Fall ist. Interessant sind die Extreme-Aktionäre. Diese sind zwar nicht öffentlich prüfbar, aber man munkelt, dass 3Com und Compaq jeweils über 20% der Anteile halten. Auch Siemens soll im Bereich von 2 bis 3% der Anteil besitzen. Einen weiteren großen Block vermutet man bei Ericsson. Dieses Anteile sind zum Teil aber als Vermögens-Management dieser Firmen zu betrachten und dürfen nicht mit einem strategischen Engagement verwechselt werden.

Näheres zum Angebot von Extreme an die 3Com-Kunden (70% Rabatt auf den BlackDiamont) finden Sie auf dem Web-Server der ComConsult Akademie (www.comconsult-akademie.de) unter "Service-Funktionen>>Material" mit einem durch die Firma Extreme für uns bereitgestellten Papier.

Wer wird nun besondere Vorteile aus dieser Marktsituation ziehen?

Meiner Einschätzung nach wird bei den größeren Kunden CISCO sehr stark von der jetzigen Situation profitieren, auch wenn 3Com- und CISCO-Produkte vom realisierten Umsatz und vom Produktportfolio her nur eine geringe Überlappung hatten. CISCO wird speziell bei Großkunden von der emotionalen Botschaft "bei uns seid ihr in sicheren Händen" profitieren und dadurch auch Firmen wie Alcatel, Extreme und Lucent das Leben schwer machen.

Im Mittelstand, der für die nächsten Jahren den wichtigsten Markt darstellt, da nur hier neben dem Konsumer-Geschäft noch ernsthafte Gewinne gemacht werden können, könnte zudem Gewinner sein, wer eine gesunde Mischung aus Technik, Preis und Vertrauen (Emotion, Vision) vermitteln kann und zudem über die auf den Mittelstand ausgerichteten Absatz-Kanäle verfügt (Großhandel, Zugang zu Installations-Unternehmen vor Ort). Mein Tipp sind hier HP und Nortel Networks aus den zuvor genannten Gründen.

Wir werden die Marktentwicklung weiter intensiv für Sie beobachten und Sie über den Netzwerk Insider und unsere diversen Spezial-Seminare konsequent auf dem laufenden halten.

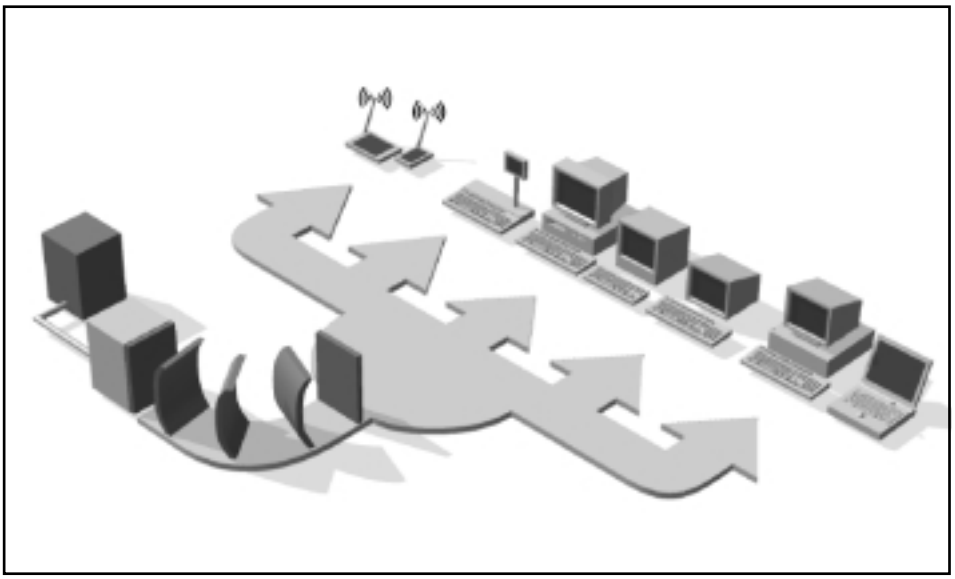
Beachten Sie auch unseren neuen ComConsult Akademie Network Professional Club, der Ihnen weiteres Material zur Technologie- und Markt-Entwicklung bereitstellen wird.

Ihr
Dr. Jürgen Suppan

Sonder-Seminar

Terminal Server Technologie – Multiuser Systeme unter Windows NT / 2000

Multiuser-/Thin-Client-Systeme kommen im IT-Umfeld immer mehr zum Einsatz und das Interesse daran steigt stetig.



Viele Arbeitsplätze in Buchhaltung, Logistik und Fertigung sind jedoch technisch überdimensioniert und unterliegen trotzdem einem enormen Wartungs- und Pflegeaufwand, obwohl sich die tatsächlichen Anwendungen auf ein Minimum beschränken. Hier finden sich konkrete Ansätze des Thin-Clients als Alternative zur Workstation, die den sogenannten Power Usern vorbehalten bleibt. Die Verlagerung der lokalen Systemressourcen vom Arbeitsplatz zum zentralen "Frontend-Server" erfordern leistungsstarke Serversysteme, die die Hardware-Hersteller mittlerweile bieten können.

Die Motivation zum Einsatz von Windows-Terminal-Lösungen liegt in den hohen Investitions- bzw. Upgradekosten einer Client-/Server-Infrastruktur sowie deren immens hoher Aufwand in Betrieb und Unterhaltung. Letzteren wirken Desktopmanagementsysteme im Sinne des TCO Gedanken entgegen und die Intelly Mirror Technology von Microsofts jüngstem Sprössling - Windows 2000.

Mit der Einführung von Windows 2000 ist der Terminalserver kein eigenständiges Produkt mehr, sondern ein integrierter Bestandteil der Windows 2000 Server Familie. Die Administration ist technisch noch beherrschbarer und durch einen erweiterten Funktionsumfang leistungsfähiger geworden. Zudem gibt es wie unter dem Windows NT Terminal Server auch hier die adaptive Lösung Metaframe der Firma Citrix, die das Leistungs- und Funktionsspektrum nochmals erhöht.

Der Erfolg eines derartigen Projekts ist jedoch mit einer Reihe wichtiger Fragen verbunden:

Welche Applikationen laufen, welche nicht?

Wie muss der Client mit HW und SW aussehen? Kann ein derartiger Client vollautomatisch installiert werden? Wie kann SMS 2.0 dazu eingesetzt werden?

Wie sieht der Drucker-Betrieb aus?

Welche Anforderungen entstehen an den Server? Wie viele User für den oben genannten Client-Umfang können betrieben werden auf einem Server?

Ist der Zugang über ein WAN möglich, wenn ja, mit welcher Performance?

Vom 3. - 4. Juli veranstaltet die ComConsult Akademie ein Seminar, das diese Fragen beantwortet: Terminal Server Technologien – Multiuser Systeme unter Windows NT / 2000.

IT-Entscheidern und Projektmitarbeitern, die diese nicht neue, jedoch nun populär gewordene Technologie kennen- und einschätzen lernen wollen, wird eine rechtzeitige Anmeldung dringend empfohlen, da die Teilnahmeplätze begrenzt sind.

Es werden die unterschiedlichen Architekturen vorgestellt und die Funktionsweise live demonstriert.

Neben Wirtschaftlichkeitsbetrachtungen werden realitätsbezogene Einsatzszenarien aufgezeigt.

Zudem wird ein Argumentationsleitfaden aufgebaut, jedoch auch die Defizite und Grenzbereiche genannt. Darüber hinaus werden konkrete Lösungsansätze erörtert und die konzeptionelle Vorgehensweise aufbereitet.

Die Konfigurationen reichen von Grafikterminals über Handhelds bis zu Mischkonstellationen auf Power Workstations.

Geleitet wir das neue Seminar von Dipl.-Ing. / MCSE Martin Barbian von der ITC GmbH. Martin Barbian zählt mit seinem Team zu den führenden deutschen SMS-Experten. Darüber hinaus befasst sich das anerkannte Beratungshaus mit aktuellen Themen, die einer betriebswirtschaftlichen Optimierung der IT-Landschaft Rechnung tragen. Dazu zählen das Netzwerk- und Systemmmanagement sowie E-Mail- und Informationssysteme, User Help Desk-Lösungen und Client-/Server-Netze unter Windows NT / 2000.

Die ITC GmbH blickt auf eine Vielzahl realisierter Projekte mit unterschiedlichsten Schwerpunkten zurück, so dass die erforderliche Praxisnähe eingehend vermittelt werden kann.

Im Sinne eines unternehmerischen Investitionsschutzes und der Aufwandsoptimierung des IT-Betriebes gewinnen die Multi-user-Systeme unter Windows NT / 2000 besondere Bedeutung im Portfolio des bundesweit etablierten Consulting-Unternehmens.

Terminal Server Technologie – Multiuser Systeme unter Windows NT / 2000

Im einzelnen hat das Seminar folgenden inhaltlichen Aufbau:

Einleitung	• Definition Multiuser Betriebssystem versus Client-/Server-Architektur • Motivation, Zielsetzung und Positionierung Multiuser NT OS
Die Technik im Überblick	• Hersteller und Anbieter (Microsoft, Citrix) • Clienttypen • Funktionsübersicht und konkrete Technik • Vergleich RDP versus ICA • Lizensierungsmodelle • Einsatzszenarien und Wirtschaftlichkeitsbetrachtung (TCO)
Konzeption	• Analyse, Test, Planung, Dimensionierung, Parametrisierung
Realisierung	• Installation, Konfiguration und Administration im Überblick • Einrichtung Benutzerumgebungen
Produktivbetrieb	• Remote Installation Desktopanwendungen • Ausfallsicherheit und Loadbalancing • Erweiterung und Optimierung • Praxiserfahrungen
Resüme und Ausblick	• Vor- und Nachteile • Empfehlungen

Fax-Antwort an ComConsult 02408/149233

Anmeldung

Terminal Server Technologie – Multiuser Systeme unter Windows NT / 2000

☐ Ich melde mich an für das Seminar **Terminal Server Technologie – Multiuser Systeme unter Windows NT / 2000.**
vom 03.07. - 04.07.00 in Bonn
zum Preis von DM 2.480,-- (EUR 1.268,--)
zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Holiday Inn Bonn
(Übernachtung/Frühstück DM 199,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/149233** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

ComConsult Certified Network Engineer

"Was heute Zukunft ist ist morgen Standard"

Achtzig Prozent der Top 500 der deutschen Industrie sind Kunden von ComConsult. Auch die Firma Bosch lässt ihre Ausbilder in der ComConsult Akademie ausbilden. Jürgen Herder führt seit 4 Jahren bei Bosch Telecom Schulungen durch und hat jetzt seine eigene Schulung zum ComConsult Certified Network Engineer im Rekordtempo, quasi als Crash-Kurs absolviert. Nach seiner bestandenen Prüfung gab er uns folgendes Interview.

Insider: Wie sieht Ihr derzeitiges Beschäftigungsfeld aus?

Jürgen Herder: "Ich bin bei der Firma Bosch Telecom beschäftigt. Und da ist meine Aufgabe die Einführung neuer Produkte auch im Datennetz-Bereich. Und dafür brauche ich auch Informationen. Neue Produkte werden da vorgestellt und Leistungsmerkmale, die jetzt im Bereich Voice over IP eingesetzt werden, werden dann unseren Teilnehmern vermittelt, quasi habe ich auch eine Schulungstätigkeit – natürlich nicht so intensiv, wie das in der Ausbildung zum Certified Network Engineer durchgeführt wird."

Insider: Was war Ihre Motivation die Ausbildung zum ComConsult Certified Network Engineer zu machen?

Jürgen Herder: "Ich wollte tiefergehende Informationen im Bereich Datennetze, weil das Thema jetzt von der Telekommunikation in den Bereich Internet-Telefonie geht und man ist danach auch fitter im Bereich Datennetze."

Insider: Wie lange hat die Ausbildung zum CCNE für Sie gedauert?

Jürgen Herder: "Das ging eigentlich ziemlich schnell hintereinander, vielleicht waren es jetzt bis zum Abschluss drei bis vier Monate."

Insider: Wie beurteilen Sie die einzelnen Kurse?

Jürgen Herder: "Also: Sehr gut. Die Seminare haben mir sehr gut gefallen. Ich habe viele hilfreiche Informationen bekommen, viele fachliche Informationen und vor allem auch Informationen, die zukunftsausgerichtet sind, denn was heute Zukunft ist ist morgen Standard und mit dem Standard muss man dann umgehen."

Petra Borowka gratuliert Jürgen Herder zur bestandenen Prüfung

Insider: Welche Auswirkung hat die Zertifizierung auf Ihren weiteren beruflichen Werdegang?

Jürgen Herder: "Vielleicht hat die Zertifizierung jetzt noch keine direkte Auswirkung, aber das wird noch kommen, wenn ich vom Bereich Telekommunikation mehr in den Datennetz-Bereich rübergehe."

Wir gratulieren an dieser Stelle nochmal zur bestandenen Prüfung und wünschen ihm, dass er dieses Tempo bei seinem weiteren beruflichen Werdegang beibehalten kann.

Die mündliche Prüfung wurde bei Jürgen Herder zum ersten Mal in der Geschichte der Zertifizierung zum ComConsult Certified Network Engineer nicht von Dr. Jürgen Suppan persönlich abgehalten, sondern von Petra Borowka.

Die bekannte Netzwerkexpertin, Buchautorin und Referentin (auch des zweiten Seminars der Ausbildung zum ComConsult Certified Network Engineer, "Internetworking") gehört seit langem zur Creme de la Creme der deutschen Netzwerkszene.

Auf die Bitte von Dr. Suppan stellte sie sich bereitwillig zur Verfügung, sich die Gruppe der Prüflinge in der mündlichen Prüfung zu teilen, um die Wartezeiten zwischen der schriftlichen und der mündlichen Prüfung für den einzelnen Teilnehmer zu verkürzen. "Auf die Weise kann ich selber mal sehen, was die Teilnehmer sich aus meinen Seminaren mitnehmen." Sie ließ es sich dann auch nicht nehmen, ihr Autogramm unter die Zertifikate der von ihr geprüften Teilnehmer zu setzen. Und das ist in diesem Falle ganz genauso viel wert wie das von Dr. Jürgen Suppan.

ComConsult Akademie Network Professional Club

Der Club im Gesamtprofil

Wie können wir unseren langjährigen Stammkunden für ihre Treue und Begeisterung danken?

Wie können wir unsere erfahrenen Kunden noch besser über neue Technologien und Einsatzerfahrungen auf dem laufenden halten?

Unsere Antwort für Sie ist:

Der ComConsult Akademie Network Professional Club.

Mit dem ComConsult Akademie Network Professional Club bauen wir konsequent unser Leistungsprofil einer umfassenden Informationsleistung rund um alle Netzwerk-Technologien aus. Vom Einstieg in den Netzwerk-Markt bis zum erfahrenen Netzwerk-Profi: wir bieten Ihnen die Informationen, die Sie für Ihren beruflichen Erfolg benötigen. Wir arbeiten für Sie an der zentralen deutschen Informations-Drehscheibe für Netzwerk-Technologien.

Unser Gesamtprofil bietet Ihnen:

- Grundlagenseminare mit dem Wissen erfahrener Praktiker, auf höchstem Niveau mit vielen Tipps und Tricks, die in keinem Lehrbuch stehen. Dazu umfangreiches Lehrmaterial und viele Anregungen für die Nachbearbeitung zu Hause
- Mit der Prüfung zum ComConsult Certified Network Engineer eine systematische Ausbildung und einen Leistungsnachweis für erfolgreiches Arbeiten und professionellen Netzwerk-Betrieb
- Mit unseren Spezialseminaren die Weiterbildung für erfahrene Netzwerk-Betreiber. Von Experten werden Sie in ausgewählte Themen eingeführt und diskutieren Vor- und Nachteile für den täglichen Einsatz
- Mit unserem monatlich erscheinenden Netzwerk Insider die fortlaufende Information über die aktuellen Entwicklungen des Marktes: technische Hintergründe, aber auch kritische Bewertungen derselben
- Mit unserem VIP-Verteiler sofortige Information über aktuelle wichtige Marktänderungen (über den VIP-Verteiler haben Sie sofort erfahren, dass IBM aus dem Netzwerk-Markt aussteigt und 3Com sich aus dem Firmenkunden-Geschäft zurückzieht). Darüber hinaus erfahren Sie über diesen Verteiler immer zuerst über Sonderveranstaltungen und neue Themen und haben so die Möglichkeit, rechtzeitig und vor der Masse zu buchen

Und nun zur Abrundung dieses Angebots:

der ComConsult Akademie Network Professional Club für die deutschen Netzwerk-Profis und die, die es werden wollen.

Was bietet Ihnen der Club?

- ein Bonus-System mit Kundenkarte und Punkte-System a la Miles-and-More. Mit jedem Seminar- und Kongressbesuch sammeln Sie Punkte, die Sie später in attraktive Leistungen umwandeln können (zum Beispiel ein Wochenende mit Partner/in in London, Mailand, Paris oder einen Sprachkurs Business-English in London oder Business-Spanisch in Palma de Mallorca oder einen Besuch im Netzwerk-Entwicklungs-Labor führender Hersteller)
- einen separaten Web-Server (nur für Club-Mitglieder zugänglich) mit ausgewählten White-Papers zu aktuellen Technologie-Entwicklungen, Hintergrundberichten und der ComConsult-Selection: unsere brandheißen Buchempfehlungen: was gibt es, was muss man gelesen haben
- Sonderveranstaltungen, die sich primär an erfahrene Netzwerk-Betreiber wenden, um Sie aktuell und tiefgreifend über die heißesten Themen zu informieren

Wie werden Sie Mitglied?

Anmeldeformular (siehe unten oder auf dem Web-Server der ComConsult Akademie) oder entsprechend formulierte Mail ausfüllen und abschicken.

Was kostet die Mitgliedschaft?

Der ComConsult Akademie Network Professional Club ist eine Service-Leistung für unsere Kunden, die Mitgliedschaft ist kostenlos.

Nutzen Sie unser Gesamt-Leistungsprofil für Ihren beruflichen Erfolg. Profitieren Sie von unserem Wissen und unseren Beziehungen für Ihren beruflichen Erfolg und den professionellen Netzwerk-Einsatz in Ihrem Unternehmen.

- Grundlagenausbildung
- Spezial-Seminare
- Sonderveranstaltungen zu ganz heißen Themen
- Prüfung zum ComConsult Certified Network Engineer
- VIP-Verteiler für sofortige und aktuellste Information
- Der Netzwerk-Insider mit detaillierten Technologie-Analysen und Bewertungen
- Der ComConsult Akademie Network Professional Club als Forum für unsere Stammkunden und als Kommunikations-Plattform für die deutschen Netzwerk-Spezialisten

Ihre
ComConsult Akademie

Fax-Antwort an ComConsult 02408/149233

Beitrittserklärung

☐ Ja, ich möchte Mitglied im ComConsult Network Professional Club werden und kostenfrei die Vorteile nutzen. Senden Sie mir meine persönliche Clubkarte zu.

Name, Vorname	eMail
Firma	Telefon, Fax
Straße	PLZ, Ort
Unterschrift	

Faxen Sie uns einfach diesen Abschnitt an **02408/149233** oder schicken Sie eine eMail an **akademie@comconsult.de**

Neuer Bestandteil des Netzwerk Insiders

Dr. Kauffels Investment Insider

von Dr. Franz-Joachim Kauffels

Sehr geehrte Kunden. Der Markt der Netzwerk-Technologien befindet sich im ständigen Wandel. Kurze Lebenszyklen der Produkte und ein zum Teil sehr harter Wettbewerb führen dazu, dass eine rein technische Bewertung der Anbieter zu kurz greift. Entwicklungen, wie wir sie bei IBM und 3Com beobachten mussten, machen deutlich, dass Investitionssicherheit nur durch eine vermehrt auch betriebswirtschaftliche Sicht auf den Anbieter entsteht. Im Zeitalter des Shareholder Values ist dies gleichbedeutend mit einer Börsen-Bewertung der Anbieter. Um dabei gleichzeitig dem steigenden Interesse der Leser nach interessanten Anlagemöglichkeiten zu entsprechen, werde ich neben einer Bewertung der Netzwerk-Hersteller auch die Frage der Sinnvolligkeit in ein entsprechendes Investment aus der subjektiven Sicht des Autors behandeln. Generell stelle ich dabei rein subjektive Standpunkte dar, um einen weiteren Baustein neben vielen anderen in der Bewertung der Hersteller bzw. für eine denkbare Anlageentscheidung zu bieten. Auf keinen Fall haften ich oder der Netzwerk Insider für Investments der Leser, die sich aus diesen Darstellungen ergeben. Eine Haftung, weder für Verluste noch für entgangene Gewinne, wird absolut ausgeschlossen. Ich kann und will nicht eine seriöse Anlageberatung ersetzen und verweise dazu auf Ihre jeweilige Hausbank bzw. die diversen Online-Banken im Internet oder die einschlägigen Spezialisten aus diesem Bereich.

Der Dr. Kauffels Investment Insider greift als regelmäßiger Bestandteil des Com-Consult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends. Dabei beschränke ich mich ganz klar auf Dinge, die wir gemeinsam verstehen können, also die Entwicklung um die vernetzte Informationsverarbeitung im weitesten Sinne. Über z.B. Biotech werden Sie hier nichts lesen, denn wenn ich in meinen vielen Jahren an der Börse eines gelernt habe, ist es das machtlose Gefühl der kalten Füße bei Aktien von Firmen, bei denen man keinerlei Durchblick hinsichtlich Produkten und Aktivitäten hat. Dies möchte ich Ihnen ersparen.

Meinen Schwerpunkt setze ich eindeutig in den USA, manchmal werden sicherlich auch europäische oder asiatische Firmen erwähnt.

Die Empfehlungen, die ich gebe, sind immer positiv zu verstehen. Aus rechtlichen Erwägungen werde ich niemandem von einem Investment direkt abraten, außer vielleicht in sehr pauschalem Maßstab. Die Empfehlungen und Bewertungen stellen meine persönliche Meinung dar. Sie können danach handeln oder es lassen. Es entstehen für Sie keinerlei Kosten. Meine generelle Unabhängigkeit, die Sie auf dem Technologiebereich bereits schätzen gelernt haben, werde ich auch weiterhin wahren.

Viel Erfolg!
Ihr Dr. Franz-Joachim Kauffels

Dr. Kauffels Investment Insider

Generelle Beurteilung der Märkte

In den Kern-Märkten kämpfen zur Zeit alte und neue Ökonomie gegeneinander.

Die schweren Tagesverluste im NASDAQ und NEMAX sind hauptsächlich durch Umschichtungen zu sehen. Ein traditioneller Wert wie Coca Cola (NYSE:KO) legt innerhalb weniger Tage 15% zu, so viel wie ein High Tech High Flyer, um es dann auch wieder schnell abzugeben. Das Herz der Anleger schlägt aber nach wie vor für die Werte der New Economy, und das mit gutem Grund. Es gibt aber einen wesentlichen Unterschied zwischen NASDAQ und NEMAX. Bei letzterem sind noch sehr viele "Milchmädchen" aktiv, die ohne jeden Anlass für Panik in jeder Richtung sorgen können. Ein Index, der mehrfach hintereinander an einem Tag locker mehr als 10% steigt oder fällt, zeigt auf einen wirklich nicht ganz ernstzunehmenden Markt. Warum werden diese Aktien nicht direkt bei eBay versteigert? Ich denke, dass sich mit Ausnahme des NEMAX die Kern-Märkte auch wegen der leicht versiegenden Kapitalzuflüsse seitwärts mit leicht negativer Tendenz bewegen. Ich rechne auf 3 Monate mit einer möglichen Korrektur um ca. 10% nach unten für DAX und DowJones. Die kann aber auch noch bis in den Sommer auf sich warten lassen. Der NEMAX muss noch Milchmädchen ausschütteln, es würde mich nicht wundern, wenn er dabei in den Bereich bis um 4000 Punkte abstürzt.

Der Euro stellt für alle Anlagen in Aktien ein grundsätzliches Problem dar, da viele der für uns relevanten Hersteller in Form von Dollar-Aktien gehandelt werden und auch ein Handel in Euro nur auf der Umrechnung basiert. Ich habe bereits im Vorfeld des Euro immer auf "1$ = 1? = 2DM" spekuliert, aber jetzt sehe ich das Ding noch gegen 75 US-Cents fallen. Einige Experten sehen in der Unfähigkeit wichtiger europäischer Länder (primär Deutschland, Frankreich, Italien) zu wirklichen Reformen den Grund für diese Entwicklung (die Unklarheiten in der Gesundheits- und Renten-Reform können nach heutigen Prognosen die Lohnnebenkosten um weitere 5 bis 10% der Gesamtlohnkosten in den nächsten 10 Jahren steigen lassen). Was hilft? Sachwertanlagen in US$ wären eine denkbare Spekulation, um diesen Trend zu nutzen.

Meine Empfehlung: schwache Tage sind Kauftage, aber nur für substanzstarke Wachstumswerte, die bereits eins aufs Mützchen bekommen haben. Verschießen Sie nicht Ihr ganzes Pulver, halten Sie über die Hälfte Liquidität.

Dr. Kauffels Investment Insider

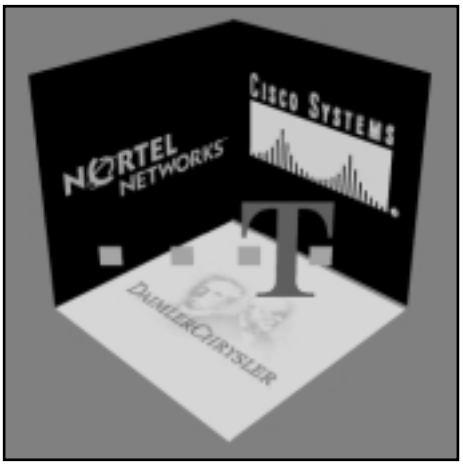
Fundamentals: Old and New Economy

Halten Sie sich vor Augen: nur 3 % der Weltbevölkerung sind schon "drin", im Internet. Selbst wenn wir in den nächsten paar Jahren nur weitere 3% hineinbekommen, ist dies ein immenser Zuwachs.

Eine gewisse Verlangsamung des Wachstums könnte es erst in den USA geben, wo gegen Ende des Jahres etwa die Hälfte der Bevölkerung vernetzt sein wird. Dies macht aber gar nichts, denn noch sind praktisch alle Anschlüsse quälend langsame Modemverbindungen.

Es ergeben sich also direkt zwei Richtungen des Wachstums: Anzahl der Anschlüsse und Geschwindigkeit pro Anschluss.

Während man hierzulande noch um Fragen wie ISDN oder ADSL ringt, werden noch in diesem Jahr die US-Backbones nach Angaben führender Hersteller wie Cisco Systems (NASDAQ:CSCO) oder Nortel Networks (NYSE:NT) mit Terabit-Glasfaserverbindungen hochgerüstet.



Eine Deutsche Telekom kann sich nur deshalb mit einem vergleichsweise langsamen 30 Gbps-Backbone brüsten, weil auf der Teilnehmerseite keine nennenswerte Netzwerkleistung verbraucht wird.

Zum ersten Male seit 1973 ist in Europa ein gewisser Aufschwung zu verzeichnen, weil auch hier pfiffige kleine Firmen mit neuen Ideen für Bewegung sorgen. Langsam lockert sich der eiserne Griff der Regulation, aber Vorsicht: überall in Europa sind Regierungen in undurchschaubare Interessensgeflechte eingebunden, die sich schnell neue Maßnahmen zur Gängelung der unternehmerischen Freiheit einfallen lassen könnten. Nichtsdestotrotz: auf diesem Sektor geht die Musik ab. Bei den Firmen Old Economy ist es eine Frage, inwieweit sie sich den neuen Herausforderungen stellen können oder dabei versagen. Wenn sie versagen, werden sie von einem Herausforderer aus dem Netz gecancelt! Immerhin gehen ernsthafte Beobachter davon aus, dass 40% der Firmen, die heute im S&P 500 gelistet sind, innerhalb der nächsten fünf Jahre aufgeben müssen. Viele davon sind sicherlich nicht so träge wie manche europäischen Companies.

Dr. Kauffels Investment Insider

Unter der Lupe: Cabletron (NYSE:CS)

Wie viele von Ihnen vielleicht wissen, hatte ich oftmals keine besonders großen Sympathien für diesen bekannten Hersteller von Netzwerk-Komponenten und dazu passender Software.

Dabei waren es vor allem organisatorische Mängel, die schwer ins Gewicht fielen. Gerade hier wurde aber in den letzten Monaten viel getan. Die Umstrukturierung in vier Business-Bereiche könnte hier einiges bewegen. Außerdem zeigt es, dass man nicht wie andere Hersteller an Aufgabe des Geschäftes denkt. Nachdem die Firma 3Com auf dem Bereich der professionellen Netze das Handtuch geworfen hat, wird der Markt dieser Kundschaft (das sind: Sie) neu gemischt.

Das Angebot der Firma "Enterasys", wie sich der betreffende Cabletron-Bereich jetzt

nennt, an 3Com Wechselkunden, ist zumindest in den USA interessant.

Technisch hat Cabletron vor allem im Bereich Layer-3-Switching eine Reihe von Test-Erfolgen aufzuweisen, die die Investoren beeindrucken.

Enterasys wurde von einer entsprechenden Business-Zeitschrift unter die "Top 100 Places to Work in IT" gesetzt. Die Firma ist Anfang April ca. 4,2 Mrd US$ wert - von der Bewertung her ist Cabletron ein echtes Schnäppchen: mit einem Kurs/Gewinn-Verhältnis von ungefähr 10 rund zwanzigmal "billiger" als Cisco Systems. 55% der Aktien sind bei 469 institutionellen Anlegern.

Das Umsatzwachstum ist zwar 84% schlechter als der Branchendurchschnitt und der Cash Flow ist negativ. Dennoch ist die Firma deutlich unterbewertet. Das Risiko ist limitiert, viel weiter kann es nicht mehr abwärts gehen.

Dr. Kauffels Investment Insider

Unter der Lupe: Extreme Networks (NASDAQ:EXTR)

Extreme Networks ist der von 3Com für seine CoreBuilder-Produktreihe empfohlene Nachfolger hinsichtlich der professionellen internen Netzwerke.

Der spezialisierte Hersteller von Power-Switches, deren pure Leistung so ist, wie der Firmenname in Aussicht stellt, wird in seiner Rolle als Herausforderer vom Markt recht hoch bewertet, Anfang April mit fast 3,9 Mrd. US$ fast genau so hoch wie Cabletron, leider auch mit einem Kurs/Gewinn-Verhältnis von ca. 100. Extreme ist sicherlich momentan Technologieführer bei Gigabit Ethernet über Twisted Pair. Es sei darauf hingewiesen, dass es genau das ist, was man bei Hochleistungs-E-Business Server-Farmen dringend benötigt: satte Bandbreite über Kupferkabel. Hier fragt niemand danach, wie lange eine Lösung exakt so bleiben kann, wie sie ist, sondern wie schnell sie Geld verdient und, fast noch wichtiger, wie schnell man sie umbauen kann. Auf dem Netzwerk Redesign Forum haben die meisten Referenten für solche Anwendungsfälle eine dreistufige strukturierte Architektur mit Layer-2-Switches am Rand, Layer-3-Switches im Kern und ggf. Layer 4-7-Switches vor den Servern umrissen. Weil man aus Gründen der Ausfallsicherheit hierfür mindestens sechs Komponenten benötigt, wird diese Architektur auch als "Six-pack" bezeichnet. Extreme möchte diese Sixpacks ablösen durch schwere Switches, die auf der einen Seite mit dem Internet-Zugang, und auf der anderen Seite direkt mit den Servern verbunden sind und dabei Layer 2,3, und 4-7-Switching auf einmal machen. Damit könnten sie großen Erfolg haben, weil sich der Betriebsaufwand deutlich verringert und die Zuverlässigkeit deutlich steigt. Eigentlich ist der Wert schon etwas hoch bewertet, aber die Produktlinie ist rein und klar.

Dr. Kauffels Investment Insider

Schnäppchenecke

An düsteren Börsentagen gibt es immer wieder Kaufgelegenheiten:

Broadvision (NASDAQ: BVSN, auch Neuer Markt WKN 901599) ist für mich immer noch einer der wichtigsten Hersteller wirklich professioneller One-to-One E-Business-Software. 90% der in meinen Büchern erwähnten Erfolgsstories arbeiten mit dieser Software. Um 40 $: kaufen!

SAP (DAX30 WKN 716463) wird stark davon profitieren, dass die B2B-Software im Zusammenhang mit der bestehenden Installationsbasis eingesetzt wird. Ich habe schon 1997 das Kursziel 1000? ausgegeben. Dabei bleibe ich, zu den jetzigen Kursen schon mal vorsichtig wieder kaufen.

Sun Microsystems (NASDAQ: SUNW WKN 871111) hat sich als einziges wirkliches Gegengewicht zu IBM Hosts im Markt der E-Business Power Server Farms etabliert. HP und IBM müssten erst einmal nachlegen. Solaris ist hier das führende OS. Durch die Indexshocks jetzt preiswert bei geringem Risiko.

Texas Instruments (NYSE: TXN WKN 852654) ist bei Chips im Mobilfunk und auch insgesamt besser positioniert als die hierzulande hochgejubelte Infineon, kostet aber nach fundamentalen Gesichtspunkten nur die Hälfte. Hier ist ein günstiger Einstieg möglich.

ADVA Optical (Neuer Markt WKN 510300) ist zwar eine echte Zockeraktie und optisch teuer, hat aber ganz wunderschöne Gewinnperspektiven, auch durch die Zusammenarbeit mit CISCO Systems. Bei Kursrückschlägen unter 600? in kleinen Mengen zupacken. Ein Risiko besteht in der neuen Zusammenarbeit zwischen JDS Uniphase und Alcatel, beide Marktführer im Bereich Wellenlängenmultiplex - sie wollen gemeinsame Standards definieren.

Cisco Systems (NASDAQ: CSCO WKN 878841) muss man einfach haben. Wer noch nicht dabei ist, sollte Kursrückschläge nutzen. Aber: Anfang April waren sie mal richtig günstig, aber nur für eine Stunde, dann ging es wieder aufwärts. Kurse unter 70 $ sind Kaufkurse.

Dr. Kauffels Investment Insider

Trostecke

Niemand kann von sich behaupten, ohne Verluste durch das Börsenleben zu gehen.

Ich will Ihnen echte Verluste von mir oder Bekannten vor Augen führen, und neben dem Trost auch versuchen, eine Lehre zu ziehen.

Mein größter Flop waren Aktien von CAI-Wireless, einer Firma für drahtlosen Internet-Zugang. Zu 11 $ gekauft setzten sie danach zum ungebremsten Sinkflug an. Was war passiert? Die Firma hatte mit dem Vorhandensein von Lizenzen geworben, die aber gar nicht vorhanden waren. Mein Fehler war dann, nicht einfach bei drei oder vier US$ zu verkaufen, sondern stur dabei zu bleiben. Es ist sicher oft richtig, Verluste aussitzen zu wollen, aber eben nicht immer. Jetzt schwimmt ein Schreiben der Bank, dass die Firma nicht mehr existent sei und die Aktien somit völlig wertlos, in einem Haufen Krokodilstränen!

Bis zum nächsten Mal wünsche ich Ihnen viel Erfolg!

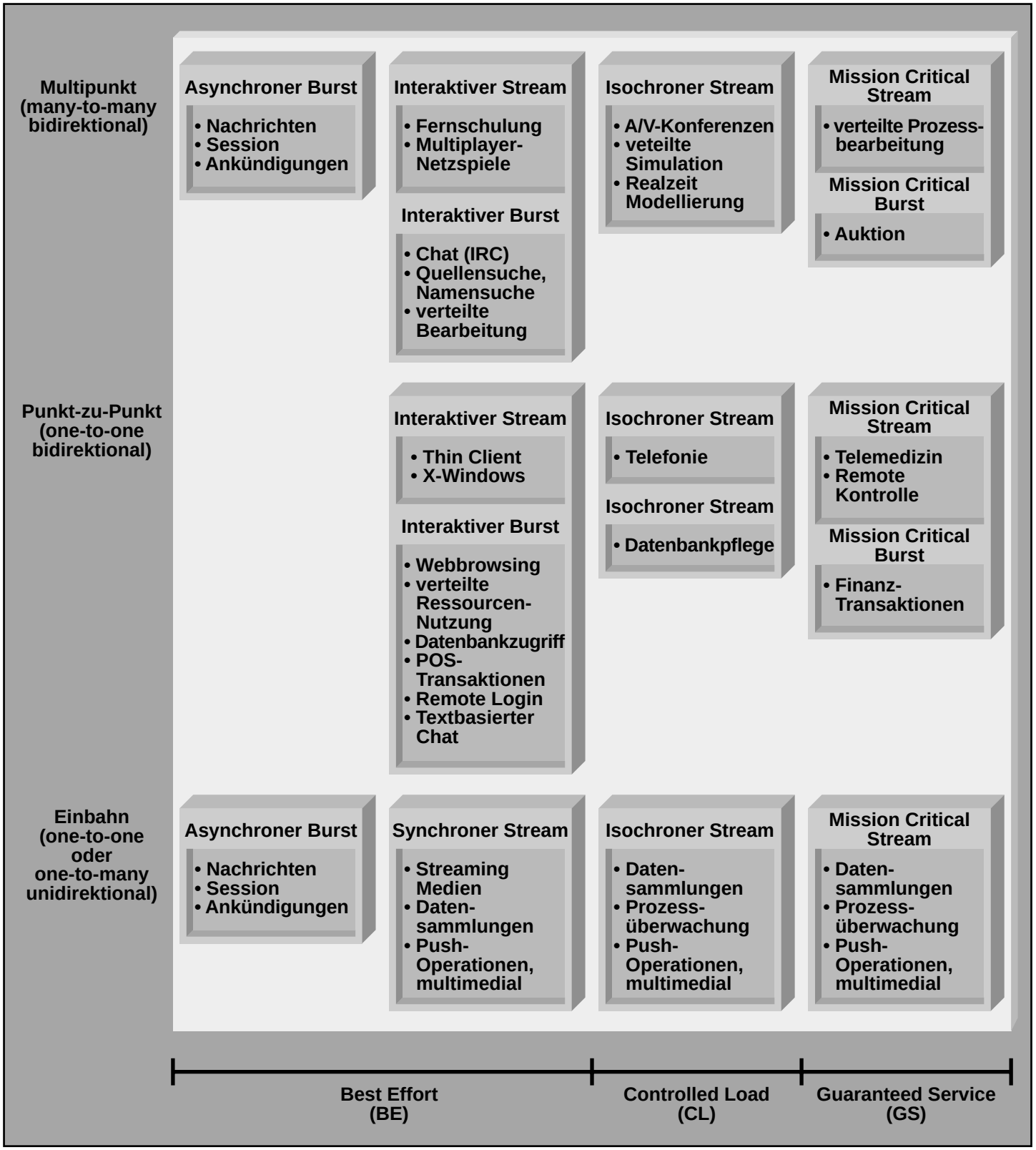
Ihr

Dr. Franz-Joachim Kauffels

Anspruch und Realität von Policy Konzepten

Fortsetzung von Seite 1

Bild 1 Anwendungstypen und technische Dienstgüte-Anforderungen



Anspruch und Realität von Policy Konzepten

Anforderungen an Netzwerk-Infrastruktur und Betrieb

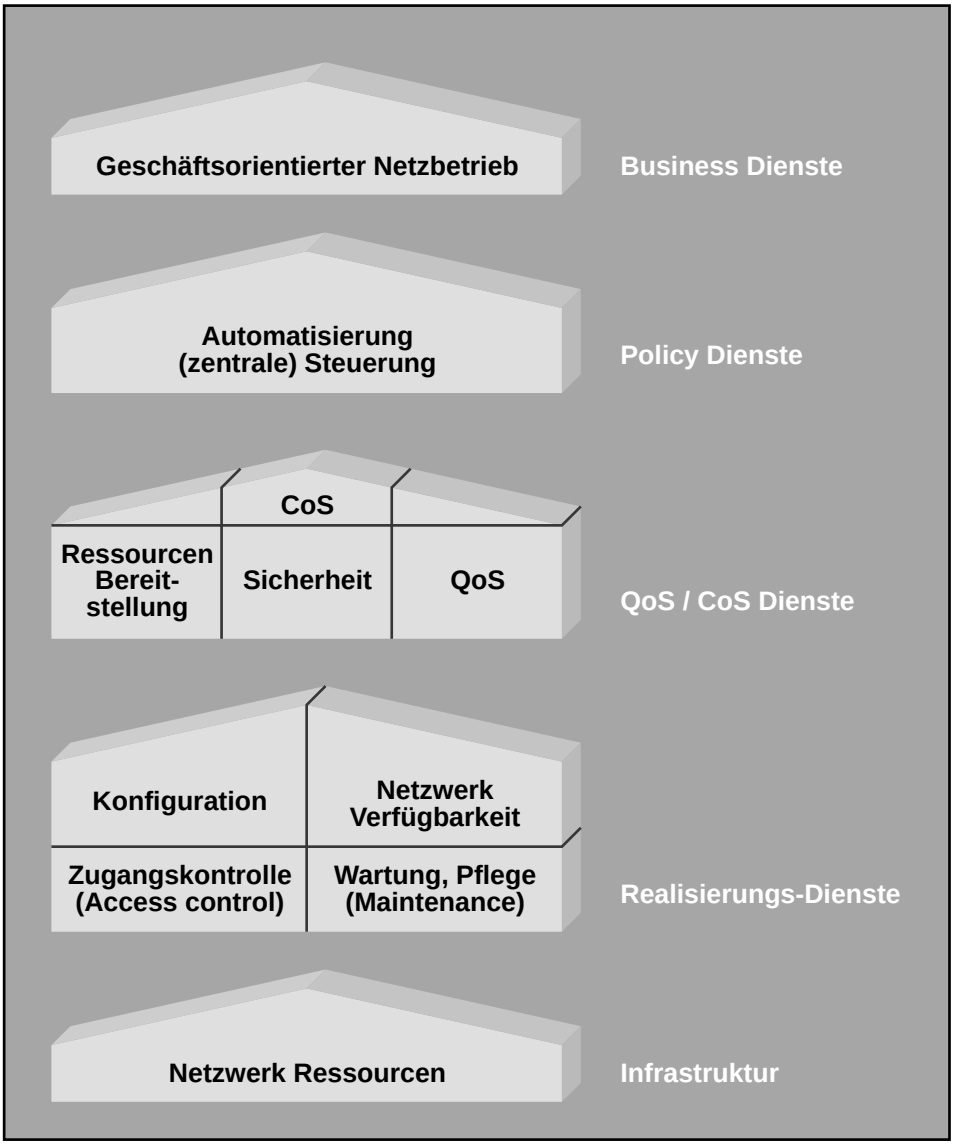
Etwa zwei Drittel der Netzbetreiber fordern von der Netzwerkinfrastruktur inzwischen eine Verfügbarkeit von 99,5% bis 99,99% mindestens im Backbone, in einigen Fällen liegen die Anforderungen auch bei 99,999%; bedingt sind solche Forderungen in der Regel durch zentral betriebene Serverpools, die ohne verfügbaren und leistungsstarken Netzwerk-Backbone nicht mehr zugreifbar sind. Datenraten von 100 Mbit bis 500 Mbit am Server sind keine Seltenheit und führen zu entsprechendem Bedarf an Port-Konzentration und Kapazität für Switches zur RZ-Backbone-Anschaltung. Die Forderung nach niedrigen Antwortzeiten kommen bei kritischen ERP-Transaktionssystemen und allen ernsthaft produktiv eingesetzten Applikationen mit Realzeit-Anteil (IP-Telefonie, Konferenzschaltungen) hinzu. Verschiedene Anwendungstypen und resultierende technische Anforderungen sind in Bild 1 dargestellt.

Parallel zur technischen Infrastruktur-Bereitstellung besteht der Bedarf nach stabilem Netzverhalten, insbesondere auch bei Lastprofilen, die sich dynamisch ändern und nur bedingt vorhersehbar sind. Daraus ergibt sich einerseits die Anforderung nach dynamischer Bereitstellung von Bandbreite und ggf. bevorzugter Bearbeitung einzelner Anwendungen, andererseits ein wachsender Druck nach Automatisierung der Komponentenkonfiguration durch geeignete Management-Tools sowie in der Folge die automatisierte und bedarfsangepasste Reportgenerierung.

Insgesamt erfordert verstärkter Kostendruck Optimierung sowohl der Personalkapazitäten als auch der Investitionen für Hardware, Sofware und Wartung. Konsequenz ist in einer Reihe von gewachsenen Netzwerken weiterhin eine Vermeidung von Überkapazität (insbesondere hoher Kosten im WAN) bei gleichzeitiger Anstrengung, den Betriebs-Aufwand zu verringern oder mindestens nicht zu erhöhen. Diese teilweise widersprüchlichen Rationalisierungsziele führen zu einem Tauziehen zwischen selektivem Einsatz von Verfahren zur Dienstgüte-Steuerung (QoS, CoS) und der Implementierung von Policy-Konzepten zur Automatisierung der Dienstgüte-Steuerung. Insofern lässt sich die Implementierung eines Policy Konzeptes als "Zwischenschicht" zwischen Infrastruktur, QoS-Verfahren und geschäftsorientierten Anwendungen beschreiben wie in Bild 2 dargestellt.

Zur Autorin
Dipl.-Inform. Petra Borowka, Studium Universität Dortmund. Langjährige Projekterfahrung mit verschiedensten Industrie- und Dienstleistungsunternehmen im Bereich Beratungsprojekte, standardbasierte Netzwerk-Planungen, Schulungen, Veröffentlichungen.
Unternehmensberatung Netzwerke UBN

Bild 2 Zusammenspiel zwischen Netzwerkinfrastruktur, QoS, CoS, Policy und Anwendung



Anspruch und Realität von Policy Konzepten

Definitionen für QoS, CoS und Policy

Unter Quality of Service (QoS) wird die erreichbare oder garantierte Dienstgüte verstanden, oft für eine einzelne Session.

Sie definiert sich aus den Messwerten für

- garantierte / erreichte Bandbreite
- garantiertes / erreichtes Delay (Antwortzeit)
- garantierte / erreichte Begrenzung von Bandbreiten-Schwankung (Jitter)
- garantierte / erreichte Begrenzung von Delay-Schwankung (Jitter)
- bevorzugte Bearbeitung relativ zu anderen (konkurrierenden) Datenströmen

aber auch

- Verfügbarkeit
- Fehlertoleranz
- Effizienz
- Sicherheit

Class of Service (CoS) bedeutet im Regelfall die Zusammenfassung von "irgendwie" gleichartigen Kommunikationsbeziehungen (Sessions) zu einer gemeinsamen Gruppe oder Klasse, wobei innerhalb einer Klasse die einzelnen Sessions gleichwertig bearbeitet werden. Dies wird auch als aggregierte Dienstgüte bezeichnet.

Die Pakete einer Dienstgüte-Klasse werden mittels Klassifizierung erkannt und entsprechend eingeordnet. Eine individuelle Dienstgüte-Vereinbarung für einzelne Sessions gibt es nicht mehr, weshalb CoS-Konzepte erheblich weniger Overhead erfordern und deutlich besser skalieren.

Ein typisches Vorgehen ist die Zusammenfassung aller Anwender, die eine bestimmte Applikation auf Basis TCP/IP nutzen. Die Klassifizierung erfolgt in diesem Fall über die TCP Portnummer,

z.B.

80 für Websurfen mit HTTP,

161 für Management mit SNMP,

103 für POP3.

Der Begriff Policy (übersetzt: Politik, Strategie) ist nicht neu und wird je nach Bedarf und Hersteller für beliebige regelbasierte Steuerungsverfahren benutzt. So kann es eine Policy zur Auswahl von Netzkomponenten / Anbietern geben, eine Policy für schichtweisen Netzbetrieb und Störfall-Eskalation, ebenso eine Policy für Sicherheit und Benutzerprofile und eine Policy für die Ressourcen-Auslegung, -Zuteilung, Bandbreitenmanagement und deren Automatisierung. Womit wir beim Schlagwort Policy-Networking oder Policy-basiertes Netzwerkmanagement gelandet sind. In unserem Zusammenhang soll gelten:

Definition

Policy: Zentrale Konfiguration von QoS-Regeln und resultierend daraus QoS-Parametern zur Steuerung und Überwachung der Dienstgüte eines vernetzten Systems. Jede Regel besteht aus einer oder mehreren Bedingungen und Aktionen. Die Bedingungen definieren die Parameter, auf die die Regel angewendet wird.

Konzepte und benutzte Standards

Wenn Sie nach langem Grübeln und noch längerem Studium der Menüs (für Hacker) oder Handbuch-CD's (für Systematiker) Ihre Policies definiert haben und sie nun aktivieren, sendet der Policy Server passende Konfigurationskommandos an Ihre Switches. Standardkonform tut er dies mit dem COPS Protokoll, das seit Januar endlich in der ersten Version fertig ist (RFC 2748, RFC 2751, beide Proposed Standard).

Um QoS/CoS zu realisieren, müssen Pakete "im Netz" unterschiedlich behandelt werden. Um zuerst einmal erkennen zu können, wie ein Paket zu behandeln ist, lesen die beteiligten Switches und Router Informationen der verschiedenen Protokoll-Header und ordnen entsprechend der gesetzten Policies einzelne Pakete bevorzugten oder auch benachteiligten Prozessen bzw. Warteschlangen zu. Dieser Vorgang wird auch als Klassifizierung bezeichnet. Es gibt viele Möglichkeiten zur Klassifizierung:

- Physikalischer Port
- Layer 2 MAC Ziel-/Quelladresse
- Layer 2 MAC VLAN Tag
- Layer 3 IP Ziel-/Quelladresse, Adressbereiche
- Layer 3 IP TOS Feld (3 Bit)
- Layer 3 IP DS Feld (6 Bit)
- Layer 3 MPLS Tag
- Layer 3 IPX Ziel-/Quelladresse, Adressbereiche
- Layer 3 AppleTalk Socket
- Layer 4 IP Protocol Number
- Layer 4 TCP Ziel-/Quell-Portnummer
- Layer 4 UDP Ziel-/Quell-Portnummer
- Layer 7 HTTP URL

Am häufigsten werden TCP/UDP Portnummern oder IP Adressen (von Servern) verwendet. Einige Klassifizierungen des IP TOS/DS Byte sind in IETF Standards RFC's 2597 und 2598 spezifiziert. Beim Aufbau einer Session kann mit RSVP als Signalisierungs-Protokoll zusätzlich zur Klassifizierung eine Reservierung geschaltet werden - was allerdings wegen des hohen Aufwands sehr restriktiv genutzt werden sollte. Die überwiegende Kommunikationslast wird eher ohne Reservierung aber dennoch nach unterschiedlicher Wichtigkeit gehandhabt werden. Die aktuellen Standardtrends sehen RSVP+ in Verbindung mit DiffServ, d.h. Reservierungen werden nur für aggregierten Class of Service Verkehr geschaltet, nicht mehr für einzelne Sessions.

Sind die Pakete klassifiziert, erfolgt eine Priorisierung und bei Bedarf eine passende Markierung mittels Tagging auf IP Ebene und/oder auf MAC Ebene. Geht es nach Microsoft, so wird auch auf Ebene 2 Reservierung genutzt, die hierfür notwendige Spezifikation (SBM) ist jedoch noch im Draft-Status mit der aktuellen Version 10 vom Januar 2000, und von der restlichen Herstellerwelt ist wenig über eine SBM-Unterstützung zu hören. Eine aktualisierte Übersicht der Standards zeigt Tabelle 1 (für eine detailliertere Beschreibung der QoS Techniken: "P. Borowka: Quality of Service mit etablierten Frame-Technologien; Netzwerk Insider April 1999").

QoS Ansätze für Frame Technologien				
Protokoll	**Bedeutung**	**Arbeitsgruppe**	**Zielsetzung**	**Informationen**
COPS	Common Open Policy Service Protocol	IETF/RSVP Admission Policy (RAP)	Client/Server Modell, um Policy Kontrolle über DS/CoS und QoS Signalisierungs-Protokolle, z.B. RSVP, zu unterstützen	RFC's 2748, 2751
RSVP	Resource ReSerVation Setup Protocol (früher: Resource Reservation Protocol)	IETF/RSVP	QoS Signalisierung: Schaltung einer Ende-zu-Ende Reservierung zwischen Netzknoten (Client/Server)	http://ietf.org/ids.by.wg/rsvp.html RFC's 2207, 2208, 2210, 2430, 2746, 2747, 2749, 2750, 2751...
DS	Differentiated Services	IETF/DIFFSERV	Class of Service, SLA's durch Setzen von Prio Bits im TOS-Byte, DS-Byte	http://ietf.org/ids.by.wg/diffserv.html RFC's 2474, 2475, 2597, 2598
MPLS	Multi Protocol Label Switching	IETF/MPLS	Class of Service, SLA's durch Einfügen eines zusätzlichen "Labels" (Tagging)	http://ietf.org/ids.by.wg/mpls.html RFC's 2430, 2547
ISSLL Framework	Integrated Services over Specific Link Layer Architektur	IETF/ISSLL	Realisierung von Dienstgüte in Form von Dienstklassen (CoS) auf Link Protokolle mit reinen Frame Technologien	http://ietf.org/ids.by.wg/issll.html
CL	Controlled Load	IETF/ISSLL	Bevorzugte Bearbeitung	RFC 2211
GS	Guaranteed Service	IETF/ISSLL	Reservierung/Garantie einer maximalen Arbeitszeit (Delay)	RFC 2212

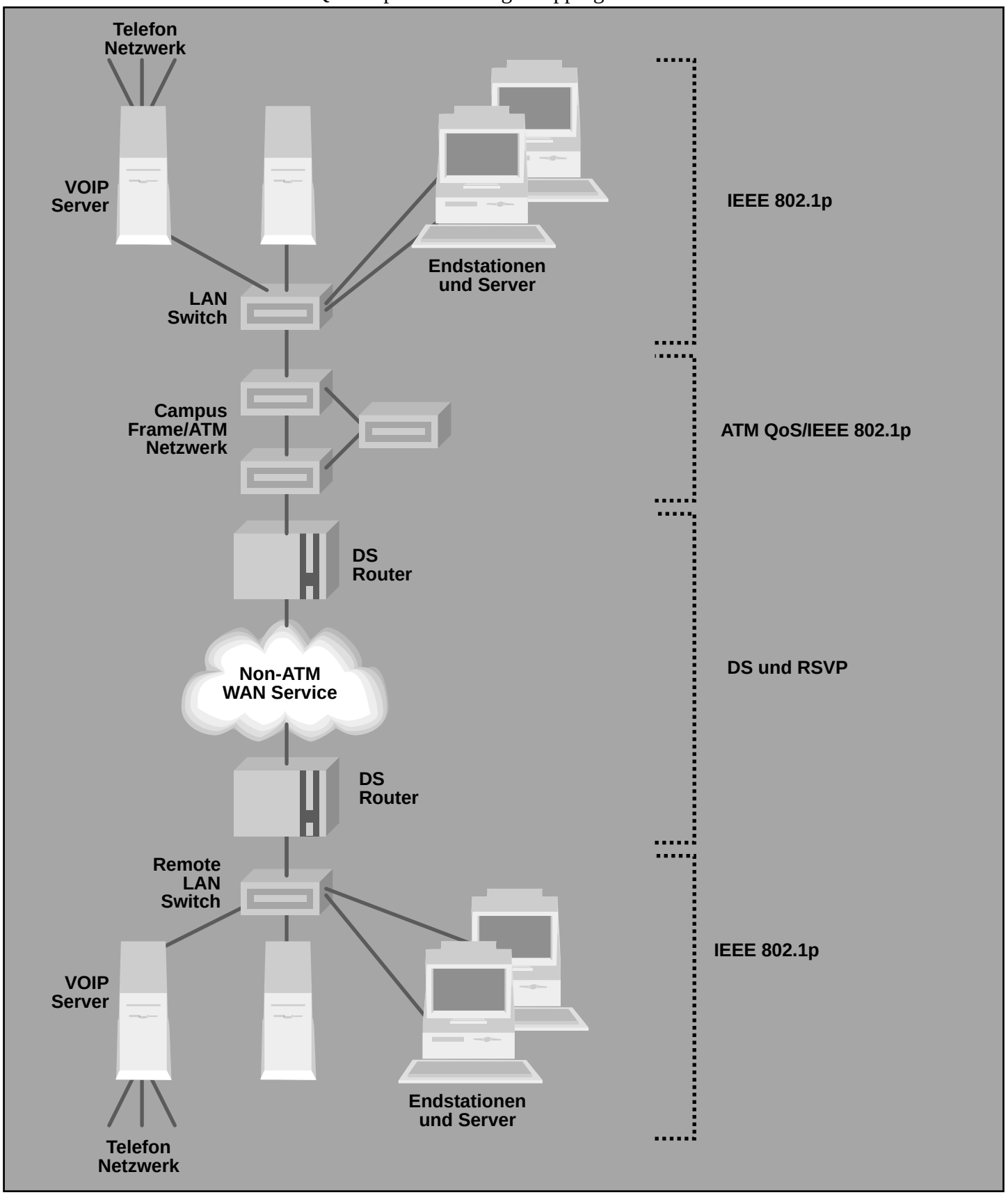
Tabelle 1 Verfahren für Quality of Service mit Frame Techniken

Um Ende-zu-Ende tatsächlich eine Chance für eine korrekte Umsetzung der definierten Policies zu haben, müssen die genutzten QoS-Techniken für LAN-Zugang, LAN Backbone, LAN-WAN-Übergang und WAN Backbones sinnvoll ineinander überführt werden. Mit den jetzt verfügbaren Standards lässt sich eine einigermaßen durchgängige Klassifizierung und Priorisierung von der Applikation bis zur MAC-Ebene implementieren: URL's oder Portnummern werden auf TOS/DS Tag's abgebildet, diese wiederum auf Prioritäts-Tag's der MAC Ebene. Bei Einsatz von ATM-Backbones lassen sich MAC Tag's auf ATM ELAN-Kennungen mappen. Beim Übergang vom LAN zum WAN bzw. Providernetz kann Mapping von IP TOS Bits auf DS Bits erfolgen. Für einzelne DS-Klassen können am LAN-WAN Übergang zusätzlich RSVP Reservierungen geschaltet werden (siehe Bild 3).

Ein Beispiel: Die Bestellwesen-Applikation auf Basis SAP/R3 ist für Sie wichtig und soll mit hoher Priorität gefahren werden. Sie analysieren, mit welchen Portnummern Ihre SAP Server arbeiten und definieren Policy-Regeln, nach denen diese Ports mit "Gold" Priorität behandelt werden. Dies führt dazu, dass Ihre Layer-3 Switches SAP-Pakete im IP TOS Feld mit "110" markieren und im erweiterten MAC Header die Prioritäts-Bits auf "110" setzen. Falls die Layer-3 Switches nur das IP Feld, nicht aber den MAC Header markieren, sind die beteiligten Layer-2 Switches entweder blind oder müssen selbst die Intelligenz haben, Pakete zu klassifizieren und darüber hinaus möglicherweise auf MAC Ebene zu markieren (für die Layer-2 Switches, die Layer-2 Tags nur lesen, nicht setzen können). Markieren von Paketen wird von Layer-2 Switches im Regelfall aktuell nicht unterstützt! Nun zur WAN-Ankopplung mit Provider-Übergang: Der Router Ihres Providers mappt die gesetzten IP TOS Bits auf die unteren drei DS Bits, damit er für Sie als Kunde entsprechend Ihres Kundentarifs in den oberen DS Bits eine Markierung eintragen kann. Falls Sie Geld sparen wollten und mit dem Provider nur einen "Lite"-Tarif abgeschlossen haben: Pech! Die Markierung ist jetzt z.B. "001110", durch die oberen auf "001" gesetzten Bits werden Sie bei Hochlast im Vergleich zu allen Kunden mit teureren Tarifen benachteiligt. Zum Trost für Sie: Ihre SAP-Applikation wird im Rahmen der für Sie verfügbaren Leistung gegenüber den Ihren anderen über WAN betriebenen Applikationen bevorzugt. Am Ausgang des Providernetzes mappt der Provider-Router die DS Bits wieder auf den ursprünglichen IP TOS Wert "110", so dass die beteiligten Layer-3 Switches in Ihrem LAN die Policy "SAP/R3 = Gold" korrekt handhaben können. Unterstützen die Provider-Router dieses Mapping nicht, so verschwindet am LAN-WAN-Übergang die von Ihnen gesetzte Gewichtung, übrig bleibt nur die Provider-Klassifizierung aufgrund Ihres Tarifs "001000". Dann müssen Sie den Layer-3 Switches in allen Standorten per Policy Konfiguration beibringen, die von gewünschte Markierung IP TOS "110" aktiv zu setzen.

Diese Vorstellung entsetzt Sie? Mich auch - bei einem Netz mit 20 bis 200 oder 2000 Switches und Routern.

Bild 3 Ende-zu-Ende QoS Implementierung: Mapping verschiedener Verfahren



Und genau hier kommen die Hersteller und Standardisierer mit ihren Policy-Konzepten ins Spiel: Mittels zentraler Netzsteuerung über Policy-Server soll eine vernünftig automatisierte Handhabung der nötigen Switch-/Router-Konfigurationen und zukünftig außerdem Überwachung per Monitoring erreicht werden.

Gesamtszenario: Komponenten eines policy-basierten Netzwerks

Mit der Standardisierung von Policy-basiertem Management befassen sich sowohl IETF als auch DMTF (früher Desktop Management Task Force, jetzt Distributed Management Task Force). Zu verfügbaren Produkten lässt sich jedoch im jetzigen Status lediglich lapidar feststellen:

Vision und Wirklichkeit klaffen auseinander.

Die Vision

Eine Netzkomponente (Layer2/3/4-Switch, Router, PC / NIC, ...) agiert als Policy Client (PEP Policy Enforcement Point) und stellt bei Sessionaufbau eine Anfrage an einen Policy Server, ob die Session in der gewünschten Form (priorisiert, mit Reservierung, ...) gefahren werden darf. Der Policy Server arbeitet als PDP (Policy Desision Point) und gleicht die Anfrage-Inhalte mit einer Datenbank ab, in der Profile für Netzkomponenten, Server und Benutzer abgelegt sind. Auf Basis der Daten entscheidet er über die Anfrage und beantwortet sie entsprechend mit Ja oder Nein. Das Ganze spielt sich über das COPS Protokoll ab. Die Einhaltung der definierten Policies wird mittels paralleler Monitorfunktion überwacht, bei Nichteinhaltung erhält der Policy Server eine Rückmeldung und kann die Komponentenkonfigurationen oder aber die Policies dynamisch anpassen. Eine solche Implementierung hat das ehrgeizige Ziel, eine Art vollautomatische Netzsteuerung umzusetzen und wird als signalisierte Policy bezeichnet. Eine Übersicht zeigt Bild 4.

Die Wirklichkeit

Die Wirklichkeit sieht heute anders aus (siehe Bild 5)

Bild 4 Architektur für dynamische Policy-Steuerung

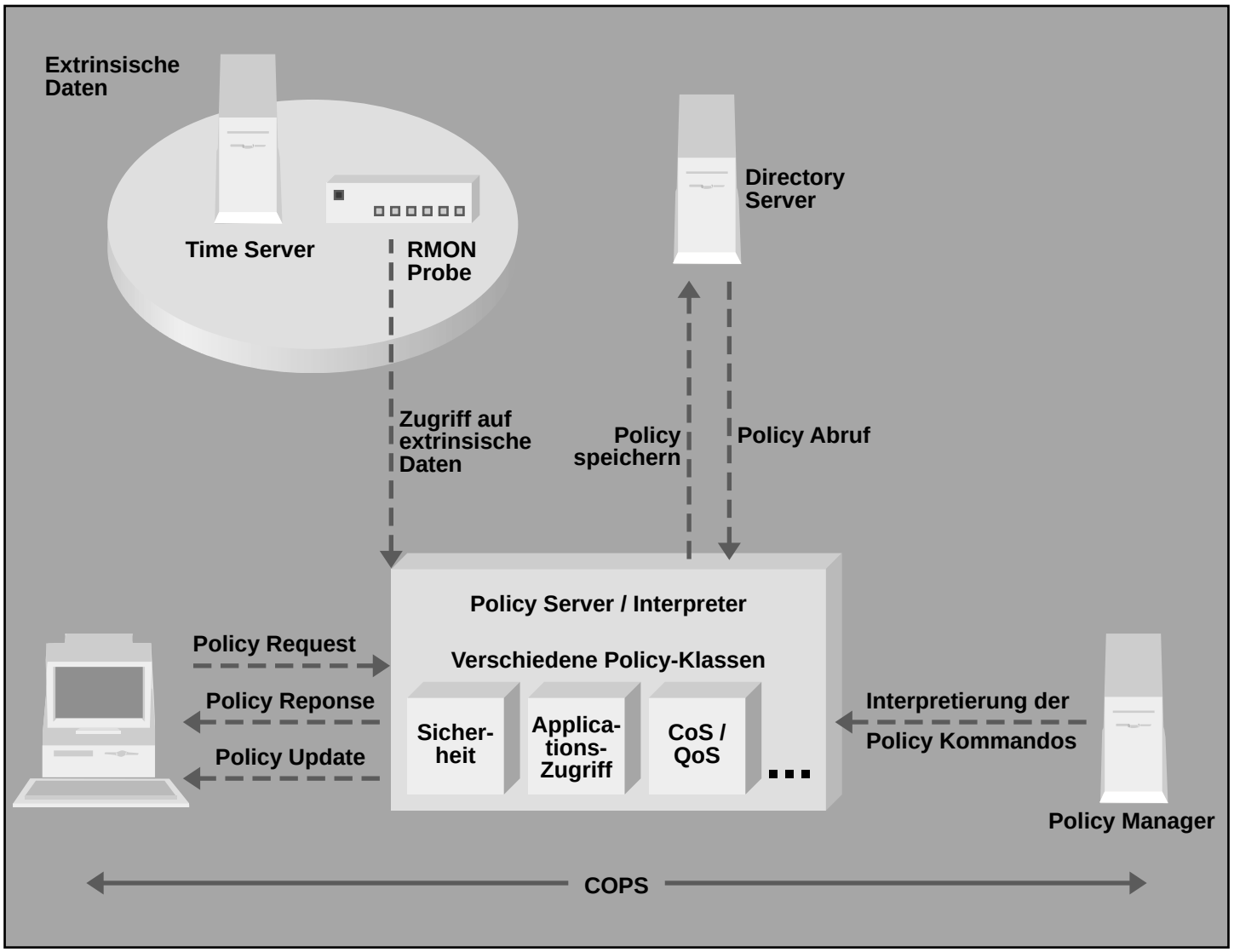
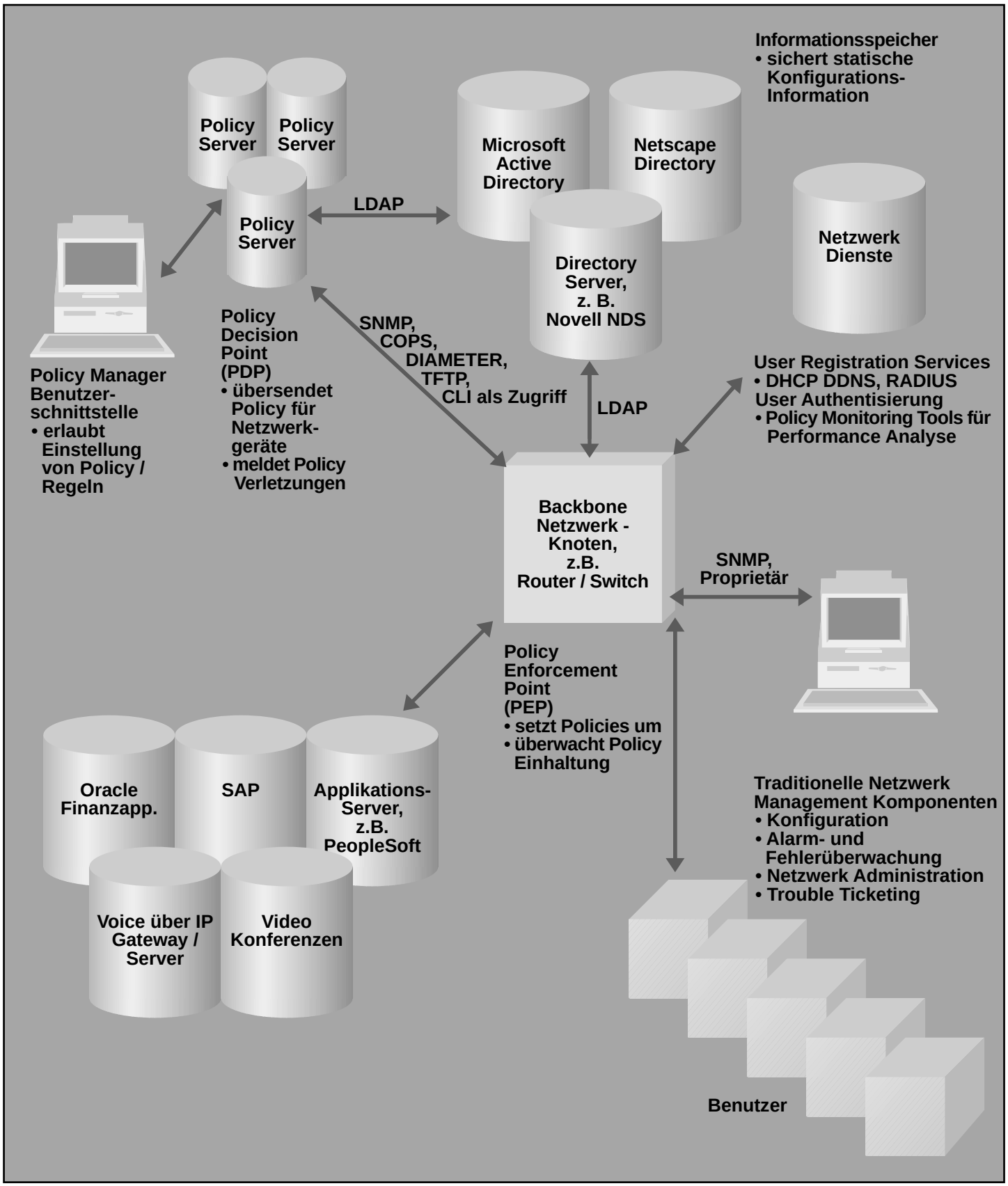


Bild 5 Gesamtszenario eines Policy-gesteuerten Netzwerks



Anspruch und Realität von Policy Konzepten

In einem Netzwerk mit Policy-Steuerung können Sie zentral über eine Policy Konsole die Regeln für Bandbreiten-Management eingeben. Bei einigen Herstellerlösungen lassen sich zusätzlich Regeln für Sicherheits-Management setzen. Die Regeln landen bei einem Policy Server, der sie in eine Datenbank oder ein Directory schreibt und in seiner Funktion als PDP aus den Regeln Konfigurationsparameter für die Netzkomponenten generiert, die er ebenfalls in Dantenbank / Directory schreibt. Die neu definierten Regeln bzw. Konfigurationsparameter werden durch einen Download (Push) zu den Netzkomponenten aktiviert, die als PEP arbeiten. Einen abweichenden Ansatz hat Lucent gewählt: Nach erfolgter Definition der Policies werden die Netzkomponenten durch eine SNMP-Nachricht getriggert, der tatsächliche Download wird jedoch durch die Komponenten gestartet (Pull-Konzept). Dadurch ergibt sich eine etwas verbesserte Skalierbarkeit. Push und Pull-Lösungen werden auch als provisionierte Policy bezeichnet. Dieser Ansatz arbeitet mit statischen, vordefinierten Policies, die sich nicht zu häufig ändern dürfen (Konfigurations- und Push-Aufwand!). Mit provisionierten Policies kann daher keine Steuerung unvorhergesehener dynamischer Netzlasten erfolgen. Problematisch bei Push-Lösungen ist die "Black-Hole" Zeit, während der ein Update auf vielen Komponenten erfolgt und sich das Netz in einem inkonsistenten Zustand befindet. Ein weiteres Problem sind nicht erkannte Policy-Konflikte, die entweder dazu führen, dass die Policy auf bestimmten Komponenten nicht aktiviert werden kann und damit zu schwarzen Löchern im Gesamt-Policyschema führt (das kleinere Übel) oder die dazu führen, dass sich widersprüchliche Policies gegenseitig behindern und das gewünschte Tuning-Resultat ausbleibt (das größere Übel).

Unterstützte Netzkomponenten bei verfügbaren Policy Servern sind meistens nur (Cisco) Router und Layer-3 Switches. Layer-2 Switches, Load Balancer und Firewalls sollen in zukünftigen Versionen unterstützt werden (Ausnahme: Cisco hat seinen Load Balancer "Local Distributor" integriert). Das einzige Konzept mit erkennbarer Multivendor-Unterstützung ist der PolicyXpert von HP/Intel, bei dem ein SDK für integrationswillige Komponentenhersteller ausgeliefert wird. Die Vielfalt tatsächlich unterstützter Komponenten ist jedoch auch hier schlichtweg mager (HP Switches, Intel Switches, Cisco Router). Eine Kopplung des Policy Servers mit vorhandenen Tools wie DNS, DHCP, Netzwerkmanagementsystem oder RMON Monitoren ist wenn überhaupt nur sehr lose implementiert. Bestenfalls lassen sich Reports über die aktiven Policies erstellen (z.B. Cisco).

Fazit:

Von der Vision einer vollautomatisierten Netzsteuerung ist aktuell lediglich eine Hilfe für Konfiguration und Verwaltung der Policies umgesetzt.

Tabelle 2 Gesamtszenario eines Policy-gesteuerten Netzwerks

	Policy Konsole	Policy Server	Directory Server	End-system	Server	Layer-2 Switch	Layer-3 Switch	Layer-4 Switch	Router	Probe	NMS
Policy Konfiguration	X										X
Policy Decision (PDP, COPS)		X									
Policy Enforcement (PEP, COPS)				X	X	X	X	X	X		
Top-Down Policy Konfiguration	X	X				X	X	X	X		
Policy Konfig. durch Signalisierung		X		X	X						
RSVP Signalisierung				X	X		X		X		
SBM Signalisierung				X	X	X					
Layer-4 Klassifizierung				X	X		X	X	X		
Layer-3 Klassifizierung				X	X		X	X	X		
Layer-2 Klassifizierung				X	X	X					
DS Markierung				X	X		X	X	X		
IP TOS Markierung				X	X		X	X	X		
802.1p Markierung				X	X	X	X	X	X		
DS Shaping							X	X	X		
Priorisierung nach IP TOS / DS							X	X	X		
Priorisierung nach 802.1p						X	X	X	X		
LDAP	X	X	X			X	X	X	X		
RMON						X	X	X	X	X	X
SMON						X	X	X		X	X

Anspruch und Realität von Policy Konzepten

Nachfolgend werden die beteiligten Komponenten näher betrachtet. Eine Übersicht, welche Policy-Funktion auf welchen Komponenten zu finden ist, zeigt Tabelle 2.

Die Policy Konsole, auch Policy Manager genannt, realisiert mittels GUI oder WUI die Benutzerschnittstelle. Meistens ist sie unter Windows 98/NT realisiert, selten unter Unix, Linux wird in keiner Lösung offiziell unterstützt; nicht alle Lösungen sind multiuser-fähig.

Die Policy Konsole wird teilweise auf derselben Maschine wie der Policy Server betrieben, teilweise über einen beliebigen Arbeitsplatz mit Webbrowser. Eingebbare Regeln betreffen im wesentlichen Klassifizierung, Markierung für relative oder strikte Priorisierung, typischerweise mit drei oder vier Stufen (critical, high, medium, best effort oder Gold, Silber, Bronze, ...) sowie eingesetzte Queueing Verfahren. RSVP kann generell zugelassen oder geblockt werden. Ein kompletter Regelsatz lässt sich mit Namen als "Gesamt-Policy" speichern und bei Bedarf aktivieren. Somit ist die komplette Definition mehrerer Policy-Strategien möglich, z.B. für verschiedene Betriebssituationen (z.B. Normalbetrieb, Quartalsabschluss, Jahresendbetrieb).

Policy Server sind im Regelfall als Software auf NT oder Unix (falls Linux, dann nicht offiziell) realisiert, teilweise als Modul der sowieso vorhandenen Netzwerkmanagementsoftware, seltener ist eine Implementierung in der Betriebssoftware von Netzkomponenten (Switches, Load Balancer).

Je nach Lösung ist es möglich, die resultierenden Konfigurationen vor der Verteilung an die Switches und Router einzusehen, damit Sie in der Lage sind, gegebenenfalls Unfug gleich vorher zu löschen, falls Sie Konfigurationsdateien soweit lesen können, dass Sie ihn erkennen.

Die Herstellerangaben für die maximale Anzahl steuerbarer Komponenten liegen bei etwa 200 bis 2000 Komponenten je Policy Server. Je nach Lösung leistet der Policy Server sehr einfache Konsistenzprüfungen, ob die definierten Policies von den Netzkomponenten überhaupt unterstützt werden. Nach dem Aktivieren steht in einigen Fällen eine Liste zur Verfügung, bei welchen Komponenten der Download erfolgreich ausgeführt wurde und bei welchen nicht.

Vielfach gibt es genau einen Policy Server, bei einigen Produkten lassen sich sogenannte Policy Domänen definieren, die von je einem Policy Server bedient werden. Die verschiedenen Policy Server kommunizieren jedoch untereinander nicht und es gibt auch keinen Standardansatz dafür. In wenigen Lösungen wird ein Backup Server unterstützt, der mit dem produktiven Policy Server synchronisiert läuft und im Fehlerfall per Umschaltung aktiv wird.

Die breiteste Skalierbarkeit ist aktuell in der Architektur von Nortel erkennbar: Hier ist ein Server Manager vorgesehen, der auf mehrere Policy Server und ggf. DHCP/DNS Server zugreifen kann. Jeder einzelne Server kann "im Zweierpack" konfiguriert, d.h. durch Backup abgesichert werden. Clusterlösungen von mehr als zwei gekoppelten Servern für einen Funktionsbereich (Policy, DHCP, DNS) sind noch nicht möglich.

Bei Lucent ist eine Kopplung des Policy Servers mit dem Tool QIP für Management der IP Adressen / DHCP / DDNS vorhanden.

Die Policy Datenbank ist teilweise proprietär und liegt auf der Maschine, auf der die Policy Server Software läuft (z.B. Cisco, Extreme). Datenbanken verschiedener Policy Server (verschiedene Domänen) sind nicht synchronisiert.

Obwohl in den ersten Policy-Lösungen etablierte Datenbanken eingesetzt werden (z.B. Nortel: Oracle v8), geht der Trend und auch die Standardisierung in Richtung Verzeichnisdienst als Basis für Poplicy-Informationen und Profile: Der hierarchische Aufbau von Directories ermöglicht effiziente Abfragen auf Gruppen- und Einzelinformationen, die objektorientiere Natur erleichtert die Definition konsistenter Policies. Die Verbindung bestimmter Profile mit Benutzern oder Nutzergruppen ist seit jeher eine Kernfunktion von Verzeichnisdiensten, somit bietet sich ihre Nutzung für Bandbreitenmanagement- und Sicherheits-Profile geradezu an.

Einige Hersteller unterstützen LDAPv3 oder LDAP-artige Directories wie NDS von Novell, Netscape Directory, ADS von Microsoft (Cabletron, Lucent, Marconi). In diesem Fall ist die Skalierbarkeit für den Zugriff auf Policy-Informationen höher als bei den proprietären Datenbanken.

Trotzdem stellt sich auch hier das Problem Skalierbarkeit für sehr große Netze, in denen mehrere verteilte Verzeichnisse synchronisiert werden müssen, um bei vielen Komonenten gleichzeitige Anfragen performant bearbeiten zu können. Replikation könnte hier ein Ausweg sein, kann aber zu Datenverlust-Problemen führen.

Als Protokolle tauchen im Policy-Umfeld verschiedene Varianten auf, die Implementierung von Standards ist längst nicht überall gegeben. So wird zwischen Policy Server und Netzkomponenten nicht nur COPS, sondern auch das gute alte CLI, TFTP oder SNMP verwendet. Die RSVP-Weiterentwicklung DIAMETER, die Aspekte wie Authentisierung, Autorisierung und Accounting zwischen Policy Client und Server behandelt, muss noch als Zukunftsmusik bezeichnet werden.

Zwischen Policy Server und Datenablage läuft nicht nur LDAPv3 sondern gegebenenfalls das jeweils spezifische Protokoll für den Datenbankzugriff.

RSVP zwischen PDP und PEP, das vom Standard für die Signalisierung dynamischer Policy-Informationen vorgesehen ist, wird heute noch bei keiner Lösung unterstützt.

Überwachung des Netzverhaltens bzw. der Einhaltung von Policies erfolgt zur Zeit gar nicht oder nicht mit dem Policy Server und/oder Directory gekoppelt.

Vielfach wird von Herstellern auf die in den eigenen Managementsystemen vorhandenen Überwachungstools oder Dritt-Anbieter verwiesen. Bestenfalls liegen Absichtserklärungen einer zukünftigen Integration von Monitoring und Accounting vor, und der Anwender steht noch im April-Regen.

Bewertung von Policy-Konzepten

Die Betrachtung der verschiedenen Policy-Komponenten und ihres Zusammenspiels macht deutlich:

In jedem Fall ist eine sorgfältige Auswahl erforderlich.

Daher nachfolgend einige Kriterien zur Bewertung von Policy-Lösungen. Die genannten Kriterien sind für eine spezifische Netzumgebung jeweils unterschiedlich zu gewichten.

Eine Bewertungs-Übersicht verfügbarer Herstellerlösungen zeigt Tabelle 3.

Anspruch und Realität von Policy Konzepten

Bewertungen von Policy Lösungen							
	Cabletron	Cisco	Extreme	HP / Intel	Lucent	Marconi	Nortel
Verteilte Policy Server	(+)	(+)	-	+	+	-	+
Server Backup	(+)	-	-	+	-	-	+
Manager of Manager	-	-	-	-	-	-	+
Policy Domänen	-	+	-	-	-	-	+
Mehrere Konsolen	(+)	-	0	+	+	-	+
resultierende Skalierbarkeit	+	(+)	-	+	(+)	-	++
Einbindung aller Switches	+	-	++	+	-	+ / -	-
Weitere Komponenten	-	-	+	(+)	-	-	(+)
Cisco Router	+	+	+	+	+	-	+
Protokolle	SNMP, CLI, LFAPv4	CLI	CLI	COPS, SNMP, CLI	SNMP, TFTP	CLI, LDAPv3	COPS, CLI, LDAPv3
QoS Signalisierung	-	-	-	(+)	-	-	-
QoS Provisionierung	+	+	+	+	+	+	+
Klassifizierung	+	+	++	+	+	+	+
Markierung	+	+	++	++	+ / -	+	+
Queueing	+	++	+	+	+	-	-
Zugangssteuerung	-	-	(+)	-	+	-	+
Directory Unterstützung	+	-	-	-	+	++	+(+)
Integration DHCP / DNS	-	+ / -	-	-	+	-	+
Integration von Monitoring	-	-	-	-	-	-	-

Tabelle 3 Bewertungs-Übersicht verfügbarer Policy-Lösungen

- Ist der Policy Server standalone oder in den Switches realisiert?
- Welche CPU / RAM Ausstattung benötigt der Policy Server?
- Ist der Betrieb verteilter und redundanter Policy Server möglich?
- Ist ein hierarchisches Konzept möglich?

- Lassen sich verschiedene Policy Domänen einrichten?
- Wieviele Netzkomponenten steuert ein Policy Server?
- Sind alle Switches und Router in die Policy-Steuerung einbindbar?
- Werden Multivendorkomponenten oder im wesentlichen Komponenten eines Herstellers integriert?
- Sind Endsysteme in die Policy Steuerung einbindbar?
- Welche Bereiche werden unterstützt: WAN, LAN, beides?
- Wie wird die Policy Information zu Policy Clients und zum Informationsspeicher übertragen: COPS, SNMP, LDAP, TFTP, CLI?

- Wird nur der Download (Push) unterstützt oder auch Signalisierung von Policy-Steuerung?
- Welche Funktionen lassen sich für Klassifizierung, Markierung, Shaping definieren?
- Lassen sich Regeln für Überbuchung definieren?

- Welche Verzeichnisdienste / Datenbanken werden unterstützt?
- Welche CPU / RAM Ausstattung benötigen Datenbank / Directory?
- Sind Monitoring und IP Tools integriert?
- Werden Basismessungen (Baselining) unterstützt?

Anspruch und Realität von Policy Konzepten

Schrittweise Einführung von Policy Networking

Die stufenweise Einführung von Policysteuerung des Netzwerks lässt sich in folgende Schritte aufteilen:

- Zieldefinition
- Überprüfung der Netzvoraussetzungen
- WAN-Lösung
- Implementierung provisionierter Policies mit Policy Server als Push Server
- Bereitstellung von Konfigurations-Infrastruktur
- LAN-Lösung
- Implementierung provisionierter Policies mit Policy Server als Push Server
- Implementierung dynamischer Policies
- Überwachung

Zieldefinition

Erarbeiten Sie, zusammen mit den Mitarbeitern, die die Lastmuster Ihres Netzwerks am besten kennnen, die vorrangigen Ziele, die Sie durch Quality of Service erreichen wollen, nach Dringlichkeit abgestuft.

Auch wenn es unangenehm ist: Klären Sie intern in aller Offenheit ab, dass die Definition von "Gewinnern" automatisch dazu führt, dass es auch "Verlierer" gibt!

Legen Sie zu jeder Stufe fest: Welche Applikationen sind betroffen und wie sehen die technischen Anforderungen dafür aus? Spezifizieren Sie die notwendigen Klassifizierungen und resultierende Regeln. Beschränken Sie die Policies auf wenige Grundklassen, z.B. kritisch, zeitsensitiv, wichtig, best effort (unwichtig).

Netzvoraussetzungen

Fahren Sie Basismessungen, um die aktuelle Dienstgüte festzustellen. Stellen Sie ggf. durch Netzerweiterung die erforderliche Verfügbarkeit und Gesamtkapazität sowie einen verträglichen Überbuchungs-Faktor sicher. Überprüfen Sie, ob Ihre Netzkomponenten Klassifizierung, Markierung, Priorisierung und Policy Agenten (Client Funktion) unterstützen.

Policy Server (1)

Definieren Sie die gewünschten WAN-Policies. Generieren Sie entsprechende Konfigurations-Befehle für Router und ggf. Layer-3 Switches. Starten Sie einen Download der Konfigurationen (Push). Führen Sie eine Kontrollmessung zur Überprüfung der Wirksamkeit durch.

WAN-Lösung

Belegen Sie die Geräte am LAN-WAN-Übergang mit QoS-Funktionen durch Download vom Policy Server und/oder indem Sie Tagging aktivieren, Priorisierung konfigurieren, Mapping zwischen IP TOS / DS / ATM für die Komponenten definieren, die vom Policy Server nicht unterstützt werden. Beachten Sie, dass Provider über SLA's eingebunden werden müssen, wenn Sie Ende-zu-Ende eine Policy durchsetzen wollen. Machen Sie eine Kontrollmessung, um die Auswirkungen der konfigurierten QoS-Funktionen zu überprüfen.

Konfigurations-Infrastruktur

Implementieren Sie DHCP, falls nicht schon vorhanden. Implementieren Sie Verzeichnisdienste unter Berücksichtigung von LDAPv3 als (zukünftigem) Standardprotokoll. Integrieren Sie Benutzerprofile und Informationen über Netzkomponenten in das/die Verzeichnis/se.

Policy Server (2)

Definieren Sie die gewünschten LAN-Policies. Generieren Sie entsprechende Konfigurations-Befehle für Layer-3 und zukünftig Layer-2 Switches. Starten Sie einen Download der Konfigurationen (Push). Führen Sie eine Kontrollmessung zur Überprüfung der Wirksamkeit durch.

LAN-Lösung

Belegen Sie Layer-3/4 Switches mit QoS-Funktionen durch Download vom Policy Server und/oder indem Sie Tagging aktivieren, Priorisierung konfigurieren, Mapping zwischen GQoS / 802.1p / IP TOS / DS für die Komponenten definieren, die vom Policy Server nicht unterstützt werden. Belegen Sie analog Layer-2 Switches mit QoS-Funktionen, sobald möglich. Binden Sie Endgeräte in die Policy-Konfiguration mit ein, soweit es sich nicht vermeiden lässt. Machen Sie eine Kontrollmessung, um die Auswirkungen der konfigurierten QoS-Funktionen zu überprüfen.

Dynamische Policies (zukünftig)

Legen Sie fest, für welche Applikationen Reservierungen erlaubt sein sollen. Begrenzen Sie diese auf verträgliche maximale Raten. Aktivieren Sie RSVP und COPS für Signalisierung von Policy-Information.

Überwachung (zukünftig)

Implementieren Sie Permanent-Überwachung auf Einhaltung der Policies an allen kritischen Netzpunkten (über Probes, Switchagenten, ARM, Trendtools, ...). Definieren Sie eine regelmäßige Reporterstellung. Sehen Sie die erstellten Reports regelmäßig ein (!). Passen Sie gegebenenfalls die Policies oder aber (Kosten!) die Zielsetzungen an.

Pflege

Denken Sie nicht, dass Sie jetzt fertig sind. Ihr Client/Server-Netzwerk ist erfahrungsgemäß einem ständien Wandel unterworfen. Das bedeutet, dass Sie Ihre Policies mindestens im selben Intervall wie normale Netzwerk-Redesign-Zyklen überprüfen und anpassen müssen.

Praxisbeispiel: Handelsunternehmen mit mehreren Standorten

Ein Handelsunternehmen mit ca. 50 Standorten und einer Zentrale betreibt einen LAN-WAN-Verbund. Alle LANs sind mit Ethernet realisiert. In den Filialen sind die PC's sowie jeweils ein Filialserver über Ethernet Switches mit 10 Mbit (Server: 100 Mbit) angebunden. Ein Router leistet die WAN-Kopplung zur Zentrale über Frame Relay und ISDN Backup, zusätzlich gibt es Backup Links zu Visa für Kunden, die mit Kreditkarte bezahlen wollen. In der Zentrale laufen die Routerverbindungen der Filialen zusammen. Hier wird der Mainframe betrieben, ebenso ein Netzwerkmanagementsystem (siehe Bild 6).

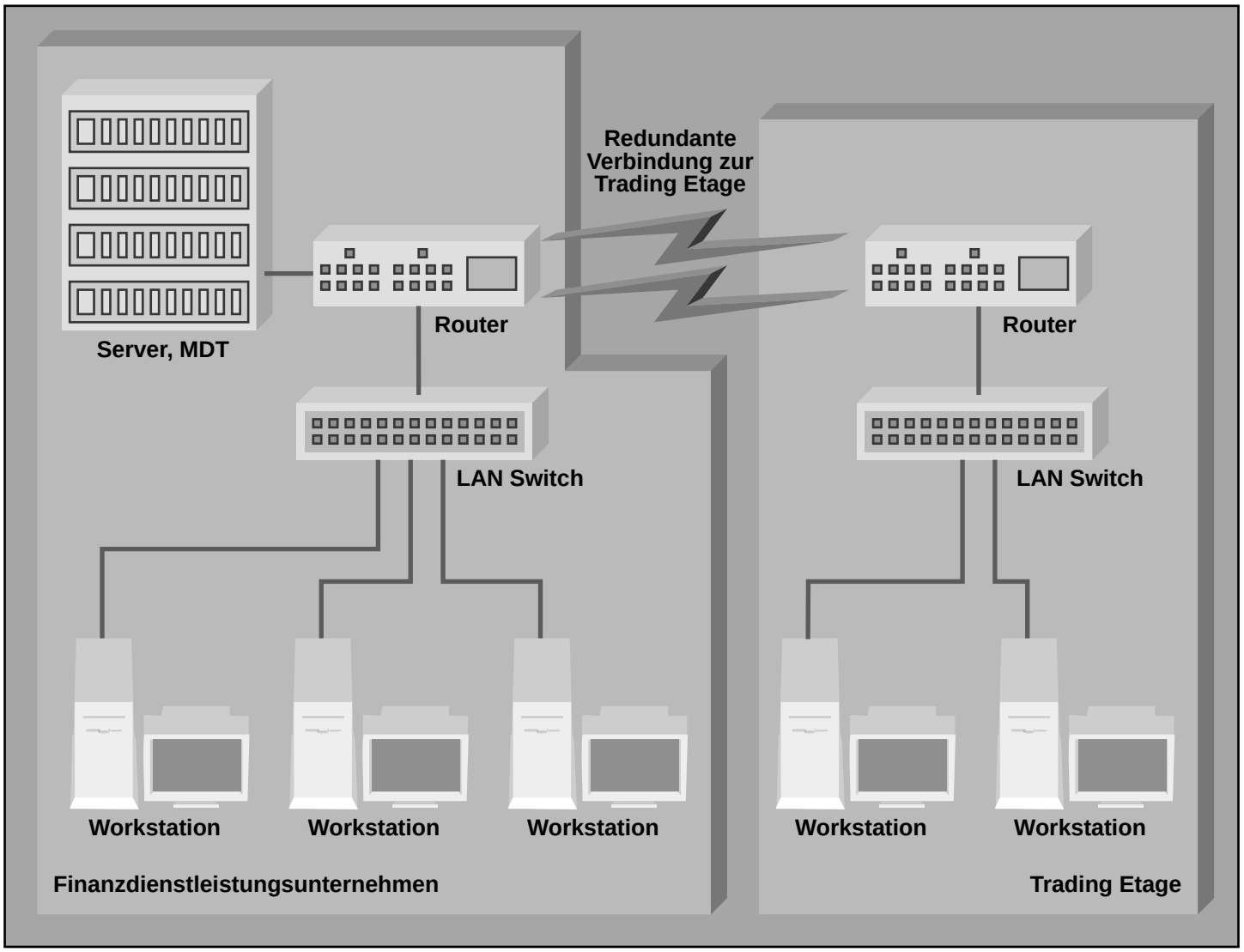


Bild 6 Einsatzbeispiel Policy: Handelsunternehmen mit ca. 50 Filialen

Die drei Hauptanwendungen sind erstens Transaktionen mit Kassensystemen (POS) als IP-Anwendung: zeitsensitiv, da direkt umsatzbezogen; zweitens Intranet (IP) mit E-Mail, nachts Backup und Preislisten-Update: nicht zeitsensitiv, jedoch verlustsensitiv, muss am Morgen verfügbar sein; drittens Preisgestaltung, Marketing, Bestellwesen und Auftragsbearbeitung mit TCP: diese sind zwar kritisch für das operative Geschäft, arbeiten aber angepasst an die verfügbare Bandbreite mit begrenzter Delaytoleranz.

Aktuelle Anforderungen

Aktuelle Anforderungen sind: Just-in-Time Management und Telefonie-Integration; POS soll gegenüber Lager / Bestellwesen / Marketing bevorzugt werden, aber bei 50% Bandbreiten-Nutzung soll ein SNMP Trap generiert werden; Lager / Bestellwesen / Marketing ist gegenüber Volumentransfer (Faxe, E-Mails) zu priorisieren; in Planung ist monatliche abzuhaltende Videokonferenz für Mitarbeiter in der Stadthalle (Bursts, hoher Bandbreitenbedarf, zeitsensitiv).

Die Lösung

POS Verkehr wird über den IP TOS Tag / DS Tag "101000" priorisiert, aber mit einer oberen Schranke von 50% der Interface-Kapazität belegt (tatsächliche Messungen haben gezeigt, dass an Hochlast-Tagen nicht mehr als 20% Bandbreite benötigt wird). Überbuchung wird ohne Priorisierung bearbeitet und erzeugt einen SNMP Trap. Lager / Bestellwesen wird mit IP TOS Tag / DS Tag "011000" priorisiert. Routing Informationen können von den Routern mit Priorisierung belegt werden, ebenso SNMP (Network Control, "111000"). POS-Überbuchung, Lager / Bestellwesen und Best Effort Verkehr werden mit Interleaving entsprechend einem gewichteten RR-Schema bearbeitet. Das LAN in der HV wird ohne Priorisierung gefahren, der Host wird allerdings mit mehreren Interfaces direkt an LAN- und WAN-Zugang angeschaltet, um eine Beeinflussung des Filialzugriffs durch LAN-Verkehr zu vermeiden. IP Telefonie wird mittels RSVP signalisiert, jedoch auf eine Rate von 128 kbps je Filiale begrenzt. Überbuchung wird als Best Effort Verkehr eingestuft.

Anspruch und Realität von Policy Konzepten

Vorteile für Netzbetreiber

Falls Bandbreitenmanagement und Implementierung von Quality of Service Funktionen für Sie als Netzbetreiber ein Thema sind, kann der Einsatz einer Policy-Steuerung einige Vorteile bieten - sobald die Produktreife verfügbarer Lösungen gestiegen ist (empfohlene Wartezeit ca. 6 Monate):

- konsistente Anpassung des Netzwerks an den Betrieb verschiedenster Applikationen
- schnellere Anpassung an wechselnde Anforderungen (durch Aktivierung einer vordefinierten alternativen Gesamt-Policy)
- Aufwands-Reduzierung für Konfiguration von QoS-Parametern in den beteiligten Komponenten
- Sicherstellung einer identischen Konfiguration für gleiche Gerätetypen
- bessere Übersicht über die konfigurierte Gesamtsteuerung

Fazit

Wer ernsthaft größere Netze mit Quality of Service betreiben will, ist dringend auf Automatisierungwerkzeuge wie Policy Server angewiesen, um den Aufwand für Konfiguration der Netzkomponenten sowie ihre Verwaltung in erträglichen Grenzen zu halten.

Verfügbare Lösungen sind allerdings überwiegend in einem "Version-1-Status", d.h. stehen ganz am Anfang ihrer Entwicklung und sind entschieden verbesserungsbedürftig.

Insbesondere die Kopplung zu Überwachungstools fehlt fast vollständig, die Skalierbarkeit ist erheblich eingeschränkt und unterstützte Netzkomponenten bewegen sich überwiegend in einer homogenen Herstellerwelt. Fehlende Interoperabilität verschiedener Lösungen hat bisher eine stärkere Verbreitung zusätzlich verhindert.

Dies gilt auch für LDAP als Directory-Protokoll, da die LDAP Spezifikation nicht detailliert genug ist, um Interoperabilität zwischen verschiedenen Verzeichnissen zu garantieren.

Für die Implementierung von Policy-Konzepten sollten mindestens folgende Design-Regeln beachtet werden: erstens klare und übersichtliche Zielsetzung, zweitens Anforderungs- und Produktanalyse, drittens die Beachtung des KISS Prinzips (Keep It Simple & Stupid).

Literatur

Borowka, P.: Quality of Service mit etablierten Frame-Technologien; Netzwerk Insider April 1999

Borowka, P.: InterNetworking - Konzepte, Komponenten, Protokolle, Einsatzszenarios; mitp Verlag, Bonn 3. Aufl. 2000

HP OpenView Management Division: A Primer on Policy-based Network Management; Sept. 1999

Nortel Networks: Optivity Policy Enabled Networking; White Paper 1999

RFC 2472: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers; obsoletes RFC 1455, RFC 1349; K. Nichols, S. Blake, F. Baker, D. Black; Dez. 1998

RFC 2597: Assured Forwarding PHB Group; J. Heinanen, F. Baker, W. Weiss, J. Wroclawske; Juni 1999

RFC 2598: An Expedited Forwarding PHB; V. Jacobson, K. Nichols, K. Poduri; Juni 1999

RFC 2748: The COPS (Common Open Policy Service Protocol); J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, A. Systry; Jan. 2000

Internet Draft: SBM - A Protocol for RSVP-based Admission Control over IEEE 802-style Networks; draft-ietf-issll-is802-sbm-10.txt; Jan.2000

Policy Links

http://www.stardust.com/policy

http://www.cisco.com/univercd/.../qpm1_1

http://www.lucent.com/ins/library/whitepap.htm

http://www.nortelnetworks.com

http://www.openview.hp.com/products/policy/

Seminare

Aufbau und Design hochverfügbarer Netzwerke (QoS-LANs)

Voice und Video über IP

Anspruch und Realität von Policy Konzepten

A	ADS	Active Directory Service
	API	Application Programming Interface
	ARM	Application Response Time Monitoring
	ATM	Asynchronous Transfer Mode
C	CL	Controlled Load
	CLI	Command Line Interface
	COPS	Common Open Policy Service
	CU	Currently Unused
D	DHCP	Dynamic Host Configuration Protocol
	DMTF	Distributed Management Task Force
	DNS	Domain Name Service
	DS	DiffServ, Differentiated Services
	DSCP	Differentiated Services Code Point
E	ERP	Enterprise Resource Planning
G	GARP	Generic Attribute Registration Protocol
	GMRP	GARP Multicast Registration Protocol
	GQoS	Generic QoS (Microsoft Windows 2000)
	GS	Guaranteed Service
	GUI	Graphical User Interface
H	HTTP	HyperText Transfer Protocol
I	IEEE	Institute for Electrical and Electronic Engineers
	IETF	Internet Engineering Task Force
	IPX	Internetwork Packet eXchange
	ISSLL	Integrated Services over Specific Link Layers
L	LDAP	Lightweight Directory Access Protocol
M	MPLS	Multi-Protocol Label Switching
N	NDS	Netware Directory Services
	NIC	Network Interface Card
P	PDP	Policy Decision Point
	PEP	Policy Enforcement Point
	PHB	Per Hop Behavior
	POP3	Post Office Protocol v3
R	RED	Random Early Discard
	RMON	Remote Network MONitoring
	RR	Routnd Robin
	RSVP	Resource ReSerVation Setup Protocol
S	SBM	Subnet Bandwidth Manager
	SDK	Software Development Kit
	SLA	Service Level Agreement
U	URL	Universal Resource Locator
W	WFQ	Weighted Fair Queueing
	WUI	Webbased User Interface
	WRED	Weighted Random Early Discard
	WRR	Weighted Round Robin

Anzeige