Dr. Suppan International Institute

Der Netzwerk Insider

April 2003

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

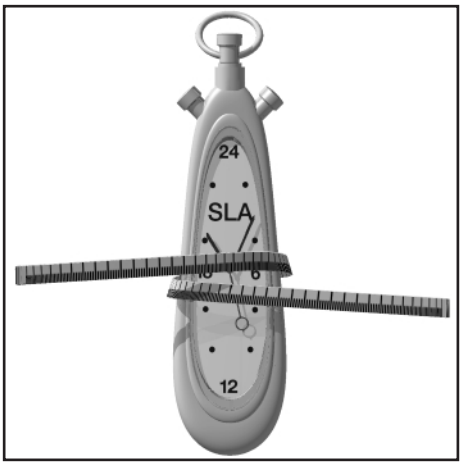
Netzwerk-Management-Lösungen 2003: Schlankheitskur für Enterprise Management

von Petra Borowka

Nachdem etablierte Management-Plattformsysteme jahrelang als Kernelement einer integrativen Management-Lösung hochgehalten wurden, zeichnen sich aktuell neue, schlankere Architekturen ab, die die komplexen API-Lösungen der Plattformen ablösen wollen. Wer wird im Wettlauf um Marktpositionen der Zukunft gewinnen?

Client-Server Betrieb in zunehmend vollvernetzten Systemumgebungen mit zentraler Serverpositionierung und flexibilisierter Arbeitszeit hat zu immer höheren Anforderungen an die Netzwerk-Verfügbarkeit geführt, zu immer schärferen Service Level Vereinbarungen mit den Netzbetreibern:

- 24 Stunden x 7 Tage Zugriff auf viele bis alle Server
- anhaltende Produktivitätssteigerung
- Mischbetrieb von Realzeit- und non-Realzeit-Anwendungen
- niedrige MTTR (Max Time To Repair)



Enterprise Management:
Weniger ist mehr

Als eine der wichtigsten Konsequenzen aus dieser Betriebssituation ergibt sich eine proaktive Informations- und Event-Strategie. Zur Erfüllung ihrer Verantwortlichkeiten/SLA-Verpflichtungen müssen Netzbetreiber nicht mehr nur Auswertungen über den kompletten oder Teilausfall von Netzkomponenten sondern viel weiterreichende Management-Aussagen verfügbar haben, mindestens über:

- Erreichbarkeit und Verfügbarkeit des gesamten Kernnetzes (Gefahrenklasse I und II*)
- Erreichbarkeit und Verfügbarkeit der Server
- Durchsatz-Werte für Einzelkomponenten und Gesamtwege zwischen Clients und Servern
- Antwortzeiten einzelner Server und Anwendungen
- Schwankung von Durchsatz und Delay
- Paketverlustraten, insbesondere für Realzeit-Anwendungen

weiter Seite 8

* Unseren Design- und Management-Strategien liegt eine Einteilung von Netzwerken in drei Gefahrenklassen (I, II, III) zugrunde, wie sie auch im Report "Design-Varianten Lokaler Netzwerke im Vergleich" der ComConsult Technologie Information beschrieben wird.

Zum Geleit

Brisante Technologie-Studie: Wireless verdrängt Kabel!

Die neueste Technologie-Studie von ComConsult Research "Kosten-Analyse: Wireless-LAN kontra kabelbasiertes LAN" ist für jeden Netzwerk-Betreiber und Planer ein absolutes Muss. Sie zählt zu den brisantesten Technologie-Untersuchungen der letzten Jahre. Vor allem beinhaltet sie auch die Präsentation eines Planungsansatzes für ein flächendeckendes WLAN. Im Ergebnis stellt sie die gesamte bisherige Form der Vernetzung in Frage.

Auf Grund der Brisanz und der elementar wichtigen Aussagen der Analyse bieten wir diese Analyse, die einen Umfang von 88 Seiten hat, zu einem Sonderpreis von 198 Euro zzgl. Mwst. an, um sie einem möglichst großen Leserkreis zugänglich zu machen.

Der Kosten-Vergleich wird anhand eines Beispielszenarios aufgesetzt und vergleicht alle bei der Realisierung entstehenden Kosten einerseits einer traditionellen kabelbasierten Lösung und andererseits mit einer reinen Wireless-LAN-Lösung.

Die Analyse macht deutlich, dass bei einer flächendeckenden WLAN-Lösung, die eine Verkabelung von Endgeräten komplett vermeidet, eine völlig neue Netzwerk-Architektur entsteht. Diese wird speziell durch die Elemente Distribution Netzwerk und Sicherheits-Lösung bestimmt.

Neben dem Kostenvergleich wird deshalb der Planungsansatz für eine flächendeckende WLAN-Lösung erklärt. Dieser Teil kann natürlich auch zur Planung einer WLAN-Ergänzungslösung zu einem bestehenden kabelgebundenen Netzwerk genutzt werden.

Die Analyse zeigt aber auch, dass verschiedene Begleitkosten zu berücksichtigen sind, die Einfluss auf die Kostendifferenz und somit die Wirtschaftlichkeit einer WLAN-Lösung haben:

- Art und Aufbau des Distribution-Netzwerks
- Realisierung von Roaming/Handover
- Art und Aufbau der Sicherheits-Lösung
- Lösungsansatz der Telephonie

weiter Seite 2

Brisante Technologie-Studie: Wireless verdrängt Kabel!

Fortsetzung von Seite 1

Geht man beispielsweise von der Notwendigkeit einer Telephonie-Verkabelung aus, so wird man diese in der Regel auf den Grundsätzen der EN50173 basieren lassen. Damit wird einerseits gleichzeitig das Problem der Integration von Hochleistungs-Arbeitsplätzen gelöst, andererseits entstehen natürlich signifikante Kosten. Je nach Umfang der notwendigen Begleitinstallationen dieser Art schmilzt der Kostenvorteil der Wireless-Lösung.

Gleiches gilt für den Bereich der Sicherheits-Lösung. Hier bestehen mehrere Lösungsansätze. Von hoher Attraktivität ist dabei der Einsatz eines VPN, da hiermit herstellerspezifische Sicherheits-Lösungen vermieden werden und gleichzeitig eine allgemeingültige Sicherheits-Lösung entsteht, die auch für andere Aufgaben genutzt werden kann.

Aufgrund der weiterhin rückläufigen WLAN-Kosten wird die Analyse spannend, wenn der Langfristaspekt im Sinne der Kalkulation einer Preis- und Kostenentwicklung in einem Zeitrahmen von 3 Jahren einbezogen wird. Da ein Großteil der Kosten durch Access Points generiert wird, sinken die Kosten der WLAN-Lösung mit sinkenden Marktpreisen. Und diese werden in den nächsten 3 Jahren mindestens um weitere 50% sinken (und dies ist sehr zurückhaltend prognostiziert). Bei mobilen Endgeräten kann dabei in Zukunft generell von einer vorhandenen Wireless-Schnittstelle ausgegangen werden (siehe Intel Centrino). Hinzu kommt, dass speziell die Preise einer VPN-Serverlösung in den nächsten Jahren massiv sinken werden.

Der Aspekt der Betriebskosten wurde in der Analyse nicht bewertet. Hier hat eine Wireless-Lösung natürlich weitere Kostenvorteile. Eine funktionsfähige Roaming-Lösung unterstellt, ist für vorhandene Endgeräte nie wieder eine Umzugs-Rangierung erforderlich. Speziell im Roaming-Bereich wird es auch in den nächsten Wochen noch erhebliche Bewegung geben. CISCO hat mit dem Proxy-Mobile-IP-Ansatz einen durchaus spannenden Ansatz in den Markt gebracht (den wir in einer der nächsten Studien von ComConsult Research auf seine Nutzbarkeit prüfen werden).

Ist eine derartige Analyse überhaupt seriös, werden hier nicht Äpfel mit Birnen verglichen? Immerhin stehen zukünftig Gigabits am Endgerät (siehe neueste Intel-Ankündigung auf der CeBIT mit massiv sinkenden Gigabit-Preisen) auf der Kabelseite einer 20-Megabit-Shared-Lösung auf der Funkseite gegenüber.

Die Analyse geht in der Form auf dieses Thema ein, indem auf der Wireless-Seite verschieden intensive Access-Point-Abdeckungen berechnet werden. So kann der Leser das für ihn passende Szenario auswählen und sich in den Daten positionieren. Vorläufig wird dabei die Wireless-Lösung keine High-Performance-Arbeitsplätze (CAD, Video) abdecken können. Zwar ist mit der 100 Mbit/s-Wireless-Technik durchaus in den nächsten 2 Jahren zu rechnen, doch wird dies real eine Shared-Leistung von 50 Mbit/s bedeuten.

Ansonsten zeichnet sich hier eine Glaubens-Frage ab: Kosten-Optimierung kontra Top-Leistung. Immerhin bietet sich hier speziell dem Mittelstand ein erheblicher Einsparansatz, vor allem wenn die zusätzlichen Potenziale der DECT-Funktelephonie genutzt werden. Ein Telephonie-Ansatz auf Basis eines Wireless-LANs wird in der Studie als nicht sinnvoll bewertet. Gleiches gilt für Filialorganisationen, die vor allem den personalarmen Betrieb in vielen verteilten Filialen anstreben.

Ein Aspekt darf allerdings nicht übersehen werden. Eine Wireless-LAN-Infrastruktur kann durch einen Störsender komplett ausgeschaltet werden. Allerdings ist dies einerseits ein Straftatbestand und andererseits sind derartige Störsender schnell ermittelbar. Von daher darf bezweifelt werden, dass sich potenzielle Störer den damit verbundenen strafrechtlichen Risiken aussetzen werden.

Ich meine: diese Analyse von ComConsult Research muss man gelesen haben. Natürlich werden wir die Ergebnisse auf dem Netzwerk-Redesign-Forum in Königswinter diskutieren. Da dieses Forum leider ausgebucht ist und keine Plätze mehr frei sind, werden wir dieses Thema auch zum Gegenstand der Sommerschule machen (neben anderen brisanten Themen, die sich zur Zeit in der Analyse befinden).

Uns interessiert Ihre Meinung zu diesem Thema. Je nach Art und Umfang der Rückmeldungen werden wir diese im nächsten Insider veröffentlichen. Bitte Meinung an drsuppan@comconsult-research.com mailen.

Ihr
Dr. Jürgen Suppan

Impressum

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

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

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

ComConsult Research

Research Report Wireless LAN Kosten

Der brandneue Report der ComConsult Technologie Information "Wireless LAN Kosten", ist eine Kosten-Analyse: Wireless LAN kontra kabelgebundenes LAN.

Die 88-seitige Studie vergleicht die Kosten für den Aufbau eines traditionellen kabelbasierten Netzwerks mit den Kosten einer Komplettlösung auf der Basis eines WLAN. Das Ergebnis ist eine der brisantesten Technologie-Untersuchungen der letzten Jahre, wird doch die bisher übliche Form der Vernetzung durch die Ergebnisse in Frage gestellt. Die Analyse berücksichtigt unterschiedliche Szenarien, die den Umfang der Kosten und die Vergleichszahlen stark beeinflussen. Somit kann der Leser das für ihn zutreffendste Szenario für seinen Kostenvergleich als Basis nehmen.

In der Studie werden

- die Technologien beider Anschlussverfahren erläutert,
- Unterschiede bei der Konzeption und Planung aufgezeigt
- und die Gesamtkosten beider Lösungen inklusive aller Begleitkosten kalkuliert.

Auf der Grundlage eines umfangreichen und detaillierten Zahlengerüsts werden die wesentlichen Kostenfaktoren beider Lösungen identifiziert und ein äußerst kostensparendes Mischdesign. Die Studie betrachtet hierfür ein sechsgeschossiges Bürogebäude mit ca. 500 Arbeitsplätzen und kommt zu dem Ergebnis, dass über 50% der Investitionskosten gespart werden können,

Kosten-Analyse:
Wireless kontra Kabel

wenn großflächig Funktechnologien eingesetzt werden. Und dabei sind weitere Kostenersparnisse im späteren Betrieb noch nicht einmal berücksichtigt. Solche Ersparnisse sind hauptsächlich im organisatorischen Bereich durch mobile Klienten und Endgeräte zu erwarten, aber auch im administrativen Bereich durch den Wegfall der aufwändigen Umzugsbearbeitung.

Im Einzelnen werden folgende Punkte behandelt:

- Welche Rahmenbedingungen sind bei Wireless LANs zu berücksichtigen?
- Wie sieht eine aktuelle flächendeckende und dienstintegrierte Tertiärverkabelung aus?
- Wie kann ein Planungsansatz für ein flächendeckendes WLAN aussehen?
- Wie wird die Telefonie in eine Wireless-Lösung integriert?
- Sollen Voice-over-IP-Produkte integriert werden?
- Wie sind DECT- und GSM-basierte Telefonielösungen zu bewerten?
- Was ist beim Design des Distribution System für die Access Points zu beachten?
- Welche Redundanzmassnahmen sind im Backbone-Bereich und welche im Funkbereich vorzusehen?
- Welchen Einfluss hat eine zusätzliche Sicherheitsinfrastruktur, um das das WLAN abzusichern?

Um unterschiedlichen Durchsatz- und Performance-Ansprüchen gerecht zu werden, berücksichtigt die Studie verschieden dichte Access-Point-Abdeckungen von 20 m² bis zu 80 m² je Access Point und zeigt die Möglichkeiten und die Grenzen einer umfassenden Wireless-Lösung. Ein Ausblick auf die Kostensituation der nächsten Jahre rundet das Ergebnis ab und eröffnet bis vor kurzem ungeahnte Konsequenzen für den Netzwerkbereich.

Damit ist diese Technologie-Studie ein absolutes Muss für jeden Netzwerkbetreiber und -planer und für jeden Kostenverantwortlichen in diesen Bereichen.

Fax-Antwort an ComConsult 02408/955-399

Reportbestellung
Wireless LAN Kosten

Ich bestelle den Technologie Report

☐ **Wireless LAN Kosten**
88 Seiten zum Preis von € 198,--
zzgl. MwSt. und Versandkosten

_____
Unterschrift

Bestellen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____
Name, Vorname

_____
Firma, Abteilung

_____
Straße

_____
PLZ, Ort

Bedingungen:

Die Ware kann nicht umgetauscht oder zurückgegeben werden. Bei Versand berechnen wir eine Gebühr von € 5,-- zzgl. MwSt. für Porto und Verpackung, bei 2 und mehr Reports € 10,-- zzgl. MwSt. (Bei Versendungen ins Ausland € 25,-- bzw. bei 2 oder mehr Reports € 30,-- zzgl. MwSt.)

ComConsult Certified Trouble Shooter

Die ersten ComConsult Certified Trouble Shooter

Im Herbst letzten Jahres startete die ComConsult Akademie ihre neue Ausbildung und Zertifizierung für den Netzwerk-Profi: Den "ComConsult Certified Trouble Shooter", bestehend aus drei aufeinander abgestimmten Intensiv-Seminaren und einer Prüfung am letzten Tag des dritten Kurses. Nun haben die ersten Teilnehmer die Ausbildung durchlaufen und durch Ablegen der Prüfung den Titel "ComConsult Certified Trouble Shooter" erworben.

Die Ausbildung zum ComConsult Certified Trouble Shooter liefert auf der einen Seite das Wissensfundament für die professionelle Beherrschung von Netzwerken und trainiert auf der anderen Seite die systematische und nachhaltige Beseitigung von Störungen.

Der 1. Kurs "Trouble Shooting in lokalen Netzwerken – Grundlagen" vermittelt das Fundament der erfolgreichen Fehlersuche in Lokalen Netzwerken. Die Teilnehmer lernen, welche elementaren Netzwerk-Fakten zur Fehlersuche zwingend notwendig sind; welchen Einfluss Kabel, Ethernet, Switch und TCP/IP auf Störungen haben; welche Werkzeuge zur Fehlersuche, welche elementaren Methoden der Netzwerk-Analyse, welche Typen von Messungen es gibt und setzen die Störungssuche an Beispielen aktiv und erfolgreich um.

Der 2. Kurs der Ausbildung, "Trouble Shooting in geswitchen Ethernet-Umgebungen" beschäftigt sich mit den Störungen, die durch fehlerhafte Konfiguration von Switching-Verfahren oder durch Fehler in der Firmware von Switch-Systemen entstehen. Hinzu kommen "Konfigurations-Fallen", die in Redundanz-Situationen ein Netzwerk ins Leere laufen lassen können.

Der 3. und letzte Teil der Ausbildung "Trouble Shooting für TCP/IP- und Windows-Umgebungen" beschäftigt sich mit einer weiteren Hauptursache für Netzwerkstörungen, die in der gegenseitigen Beeinflussung von Netzwerk und Betriebssystem. Speziell die Kombination aus Microsoft Windows und TCP/IP ist einer der dominanten Träger von Störsituationen.

Eine qualifizierte Ausbildung beinhaltet auch die praktische Handhabung geeigneter Tools (Die ComConsult Akademie hat sich für diese Ausbildung für Sniffer Basic entschieden.)

Die Trainer Dipl.-Inform. Oliver Flüs und Dr. Joachim Wetzlar leiten das Trouble-Shooting Team der ComConsult Beratung und Planung GmbH und besitzen langjährige Praxiserfahrung in der Beseitigung auch komplexester Fehlersituationen.

Die ersten Prüflinge der Ausbildung zum ComConsult Certified Trouble Shooter: Thomas Arndt, Werner Bonkowski, Beat Boschung, Holger Fink, Stefan Gatz, Johann Geier, Bernd Grieger, Ralf Jessulat, Michael Kemper, Wolfgang Neitzel, Steffen Pollanka, Bernd Reuter, Gabriel Schäfer, Rüdiger Schäfer, Frank Schraml und Marc Westhoff

ComConsult Certified Trouble Shooter

"...da ihr sowieso die einzigen seid, die dieses spezielle Training anbieten"

Wolfgang Neitzel arbeitet bei der Citti Handelsgesellschaft in Kiel in der 35-köpfigen EDV-Abteilung, von denen die Hälfte entwickelt und die Hälfte sich um Server und um Endarbeitsplätze mit integriertem Telefon kümmert. Es gibt 17 Standorte, die alle von Kiel aus verwaltet werden. Der Insider sprach mit ihm unmittelbar nach seiner bestandenen Prüfung zum ComConsult Certified Trouble Shooter.

Insider: Erzählen Sie uns was über sich.

Wolfgang Neitzel: Ich beschäftige mich da seit 10 Jahren mit Netzwerkverwaltung, Systemverwaltung, Unix-Maschinen. Das Netzwerk hatte früher bei uns nur nebenher einen Stellenwert, das hat dann der Unix-Verwalter mitgemacht. Und je mehr das Netzwerk an Bedeutung gewinnt, umso mehr Arbeit stecken wir da rein und umso mehr spezielles Know How wird erforderlich. Verkabelungsthemen kochen hoch, die wir früher in dem Sinne nicht gekannt haben. Und da ich das halt seit 10 Jahren – wenn auch nebenher – betreut habe, fällt dann die Wahl bei solchen Dingen auf mich und man sagt, okay, wir müssen mehr tun, schicken wir den Neitzel mal zur Schulung.

Insider: Brauchten Sie die denn?

Wolfgang Neitzel: Wir haben zur Hälfte geswitchte Umgebungen und die Netzwerkprobleme nehmen dadurch zu, dass wir immer mehr PCs kriegen. Und dann kommen

ComConsult Trouble Shooter
Wolfgang Neitzel

diese Dinge „Mein Netz ist langsam“ und dann kann ich zwar einen von der Endarbeitsplatzarbeitstruppe zusammenfalten, weil der Blödsinn erzählt, aber natürlich kann ich das einem User nicht erzählen, denn der will – egal, was ich ihm erzähle – dass es anschließend schnell geht.

Insider: Wieso haben Sie den ComConsult Certified Trouble Shooter gewählt?

Wolfgang Neitzel: Ich habe andere Veranstaltungen von ComConsult besucht, die haben mir alle sehr gut gefallen, keine Frage. Und da ihr sowieso die einzigen seid, die dieses spezielle Training anbieten, hab ich mich dann dazu angemeldet. Und ich muss sagen, ich hab unheimlich viel Wissen mitgenommen. Und ich denke auch, dass die Dozenten über ein ungeheures Know How verfügen. Auf das Ziel hin am Ende eine Prüfung zu machen, waren die Unterlagen leider nur mäßig geeignet. Da waren zu wenig detaillierte Informationen drin um sich damit gut auf die Prüfung vorbereiten zu können. Aber es gab ja noch den Report dazu, und der hat dann doch einiges abdecken können. Das, was die Dozenten anbieten, kann man eh nicht in die Tasche stecken und einfach so mitnehmen. Da wird viel passives Wissen bleiben, das ich dann hoffentlich im Extremfall auch hervorholen kann.

Insider: Dann war das eine Investition in die Zukunft? Oder können Sie das auch so gebrauchen?

Wolfgang Neitzel: Ja, nach dem ersten Kurs kam ich mit dem Sniffer schon ganz gut klar und da hatten wir bei uns auch gleich ein Problem, wo ich meine Leute dann auch direkt in die richtige Spur schicken konnte.

Insider: Und wie haben Sie sich auf die Prüfung vorbereitet?

Wolfgang Neitzel: Wenn man mit den anderen Teilnehmern 3 Wochen zusammen ist, findet sich ja schon ein Kreis zusammen, der sich untereinander austauscht und wir haben dann die Fragen so zusammen bearbeitet und diskutiert.

Aktueller Kongress

Security-Event 2003: Das Netzwerk Sicherheits-Forum

Vom 19. bis 22. Mai 2003 veranstaltet die ComConsult Akademie zusammen mit der GAI NetConsult im Maritim Königswinter das diesjährige "Netzwerk Sicherheits-Forum".

Das "Netzwerk Sicherheits-Forum" ist im Laufe der letzten Jahre für Sicherheitsverantwortliche und -interessierte die herausragende Plattform für aktuellste Informationen, Produktvergleiche und Fachdiskussionen geworden. Hier trifft sich die Branche. Es beginnt am ersten Tag mit einem (optionalen) Tutorium. Darauf aufbauend werden dann die Referenten an den folgenden drei Tagen inhaltlich stärker in die Tiefe gehen (siehe Kasten).

Neben Moderator Detlef Weidenhammer und Frank Breitschaft von der GAI NetConsult referieren Dr. Simon Hoff, Dr. Behrooz Moayeri und Hans Peter Mohn von der ComConsult Beratung und Planung, Stefan Strobel, Steffen Gundel und Marco Lorenz von cirosec, Dieter Pietsch (UB-Pietsch), Dr. Frank Bourseau (FinanzIT), Uwe Naujoks (WestLB AG), Frank Schlottke (Applied Security), Jens Lorenz und Guido Alexius (Döres AG), Rob Suurland (Consecur), Helmut Honermann (BDG), Jürgen Wege (Group Technologies), Ulrich Emmert (esb Rechtsanwälte), Oliver Baumgart (immutec), Thorsten Bruchhäuser (F-Secure) und Sven Schumann von der HUK Coburg.

Netzwerk-Sicherheits-Forum 2003 – Die Inhalte

Tutorium

Sicherheitsmanagement
- Übersicht zu Bedrohungsszenarien
- Aufbau einer Sicherheitsorganisation
  - SecPol
  - Richtlinien
  - Konzepte
- Vorgehen bei einer Sicherheitsanalyse

Schutz von Netzübergängen
- Sicherung der Netzgrenzen
  - Firewalls
  - Proxies
  - DMZ-Server
- Maßnahmen gegen Malware
  - Viren
  - Würmer
  - Active Contents
- Sichere Konfiguration von Webbrowsern

Sicherheitsüberprüfungen
- Vorgehensweise, Zertifizierungen
- Einsatz von Security-Scannern
- Intrusion-Detection und Intrusion-Prevention

Einsatz von kryptographischen Methoden
- Grundlagen der Kryptographie
- VPN: Gesichert kommunizieren über unsichere Netze
- Sichere E-Mail mit S/Mime und PGP
- Datei- und Festplattenverschlüsselung
- Public Key Infrastrukturen

Sicherheit im internen Netz
- LAN/WLAN und WAN-Anbindungen
- Sicherer Betrieb von Servern und Desktops
- Sichere Administrationsumgebung

IT-Security – Anspruch und Wirklichkeit
- Einschätzung aktueller und zukünftiger Bedrohungen
- Grenzen heutiger Schutzsysteme
- Der Mensch als "Sicherheitsrisiko Nr. 1" • Ausblick

Entwicklungstrends bei Firewalls
- Neue Anforderungen an Firewalls
- Lock Keeper Technologie als Firewallarchitektur
- Einsatz in High-Speed Netzen
- Lösungen zur Hochverfügbarkeit

Durchlässige Brandmauern?
- Grenzen klassischer Firewalls bei der Applikationskontrolle
- Port-80 als Tunnel in das Unternehmens-LAN
- Kritische Bewertung von IDS-, IPS- und Shield-Lösungen
- Neue Anforderungen an Sicherheitsüberprüfungen

Sind moderne Mainframes sicherer als ein PC?
- Penetrationstests von z/OS- und zLinux-Systemen
- Code-Einschleusung bei Buffer Overflow-Schwachstellen
- Denial-of-Service Angriffe gegen Mainframes
- Konsequenzen für ein Mainframe-Securitykonzept

Implementierung der Security Policy bei einem IT-Dienstleister
- Sicherheitsziele in einem Rechenzentren-Verbund
- Anwendung des BS-7799
- Erfahrungen bei der Umsetzung in Organisation und Technik
- Risikomanagement

Risk Management und Business Continuity
- Anforderungen an ein Risk Management System
- Rechtliche Probleme
- Etablierung einer Notfallorganisation
- Notfalltests, Wartung, Krisenmanagement

ROSI – praktischer Nutzen oder Marketinggag?
- Modelle zur Berechnung von Return on Security Investment
- Kritische Untersuchung der Modelle
- ROSI-Berechnungen anhand von Beispielen

Netzwerk-Sicherheits-Forum 2003 – Die Inhalte

Workshops

Hacking Extreme: Web Server und Applikation
- Einbruch auf Webserver • Installation von Hintertüren
- Durchgriff auf interne Systeme • Applikations-Hacking
- SQL Injection

Windows Sicherheitsfeatures im praktischen Einsatz
- Sicherheitsmanagement mittels PKI-Einsatz
- Umgang mit Group Policies und Security Templates
- Patchlevel-Management mit Software Update Service und Systems Management Server
- Neuerungen und Alternativen bei Windows Server 2003

Wireless LAN-Security in der Praxis
- Überblick zur aktuellen Situation
- Praxisbeispiel 1: Rapid ReKeying von Enterasys
- Praxisbeispiel 2: LEAP von CISCO
- Praxisbeispiel 3: Einsatz eines IP-VPNs
- Diskussion der Aufwände, der Vor-und Nachteile

Intrusion Detection Systeme
- IDS in Aktion: Welche Angriffe werden erkannt?
- IDS im Alltag: Bewertung der Risiken erkannter Angriffe; Reduktion von Fehlalarmen
- Zusatznutzen von Intrusion Prevention Lösungen
- Diskussion: IDS - Segen oder Fluch?

Sicherung einer modernen Hostumgebung
- Einbindung des Mainframes in IP-Netze
- Sicherung der Alt-Anwendungen (TN3270, SNA über IP)
- Konzepte für (webbasierte) E-Commerce Anwendungen
- Nutzung von z/OS-Features und Zusatzprodukten

Der Weg zum BSI-Grundschutzzertifikat
- Was ist das BSI-Grundschutzzertifikat?
- Unterschiede zu einer BS 7799 Zertifizierung?
- Praxisteil: Datenbank-gestützte Erstellung von IT-Sicherheitskonzepten; Anwendung des BSI-Grundschutztools und der SAVe-Datenbank von infodas; Was wird bei einer Zertifizierung geprüft?

Slammer Incident Response Team
- Anatomie eines Angriffs
- Warum die Netze zusammenbrachen
- Technische Konsequenzen
- Organisatorische Konsequenzen

Security Policy als moderierter Prozess
- Die Crux mit der Security Policy: Anspruch und Wirklichkeit
- Wie kann man den Prozess besser und effektiver gestalten
- Praxisbericht: Security Policy Entwicklung in einem mittelständischen Unternehmen
- Erfahrungen und Ausblick

Sichere und effiziente E-Mail Kommunikation
- Gefahren beim Einsatz von E-Mail im Unternehmen
- Wie kann und sollte man sich davor schützen?
- Gibt es einen ROI?

Rechtliche Risiken für Unternehmen im Internet
- Haftung im Netz • Organisationspflichten
- Mitarbeiterüberwachung • Datenschutz

Telefonnetzanbindung:
Risikofaktor TK-Anlage und Nebenstellen
- Methodik des TK-Scans ("wardialing")
- Vorstellung kommerzieller und freier Tools
- Protokolle, Systeme und typische Schwachstellen
- Risikoanalyse und Maßnahmen

Security Monitoring –
eine unternehmensweite Herausforderung
- Gleichzeitige und automatisierte Überwachung aller Sicherheitsmechanismen in Echtzeit
- Unternehmensübergreifende Architektur und Organisation
- Kopplung mit Alarm- und Eskalationsmechanismen als Grundlage für "Incident Response" Verfahren
- Trennung von Geräte- und Sicherheitsmanagement

Sicherheit bei Mobilen Systemen
- Typische Sicherheitprobleme
- Zugriffsschutz und Datenintegrität • Vertraulichkeit
- Einbindung in ein zentrales Management

Der Veranstalter behält sich Änderungen im Programm vor.

ComConsult Akademie – Telefax: 02408/955-399

Kongress-Anmeldung

Ich melde mich an für das
Netzwerk Sicherheits-Forum 2003

☐ **vom 19.05. - 22.05.03 mit Tutorium**
zum Preis von € 1.790,-- zzgl. MwSt.

☐ **vom 20.05. - 22.05.03 ohne Tutorium**
zum Preis von € 1.590,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ PLZ, Ort _____

Straße _____ eMail _____

Telefon, Fax _____ Unterschrift _____

Netzwerk-Management-Lösungen 2003: Schlankheitskur für Enterprise Management

Fortsetzung von Seite 1

Evolution von Management-Lösungen: Phasen 1 und 2

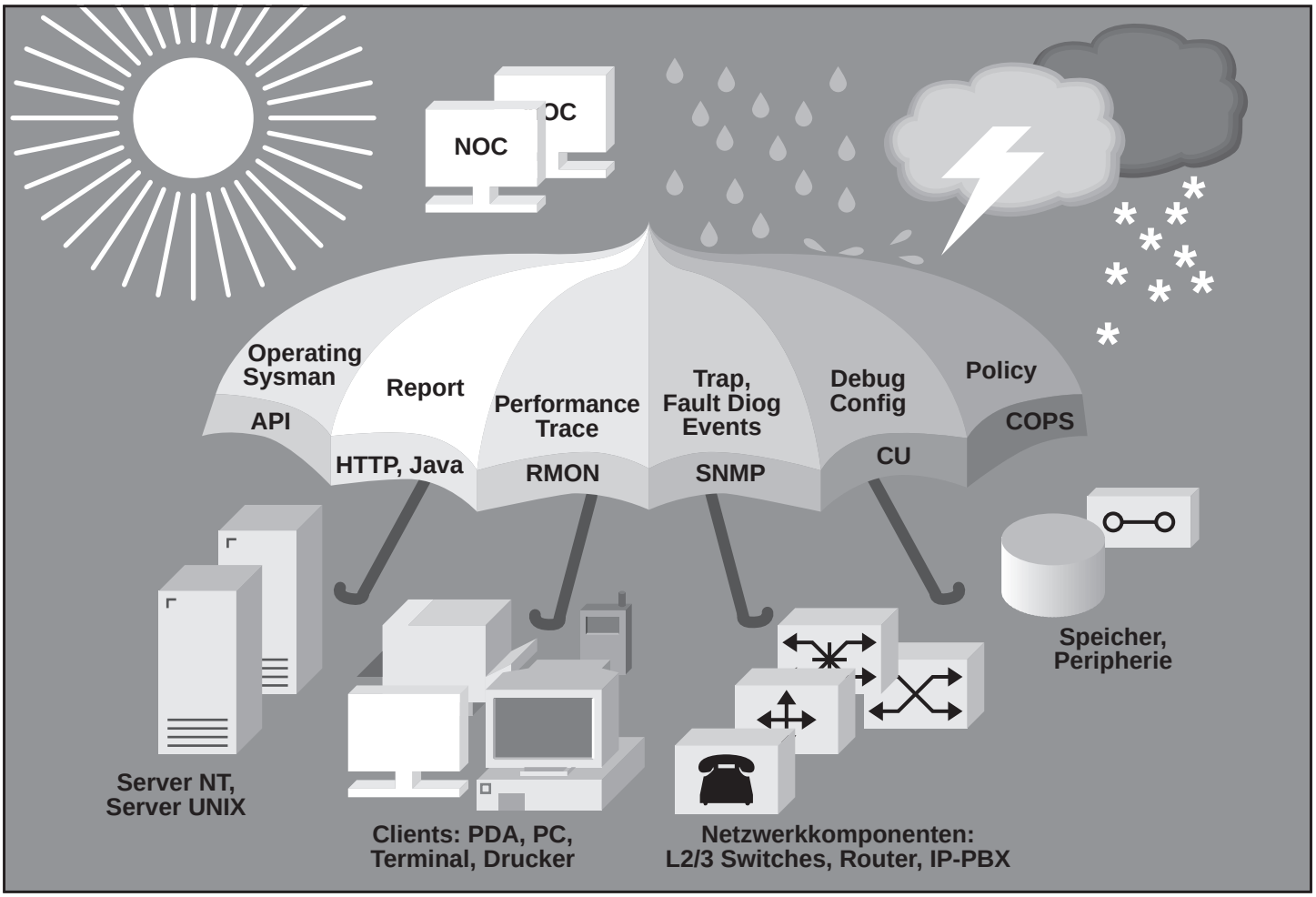
Von 1990 bis 1995 rückte Netzwerkmanagement mit steigender Netzgröße zunehmend ins Interesse der Fachwelt. In einer ersten Produkt-Phase entstanden Tools für einzelne Betriebssegmente wie Kabeltester und Netzwerk-Analysatoren für Shared LANs, gefolgt von SNMP Managern und RMON Probes für Konfiguration, komfortableren remote Zugriff und Monitoring. Die zweite Phase brachte Integrations-Ansätze mittels Management-Plattformsystemen wie HP OpenView, IBM NetView/Tivoli Enterprise Manager, Sun Solstice Manager, CA's TNG (The Next Generation) und ähnliche. Allerdings erwies sich die Zusammenfassung und Einbindung aller System- und Netzmanagement-Tools in eine gemeinsame Menü- und Datenstruktur über komplizierte Schnittstellen (siehe Bild 1) als sehr aufwändig, sowohl für die Hersteller von

Netz- und Systemkomponenten als auch für die Betreiber / Bediener der Management-Konsolen, und die etablierten SNMP und RMON Standards waren mit ihrer Ausrichtung auf Einzelparameter-Abfrage und Shared LANs zur Überwachung voll geswitchter Netzwerke nur mittelmäßig geeignet. Insbesondere im Marktsegment der Enterprise Netzkomponenten zeigten sich seit 1999 verstärkt separatistische Tendenzen mit betonter Vermarktung der herstellereigenen Tools für die eigene Komponentenwelt und nur noch mangelhafte Unterstützung der Umbrella Systeme.

Die Autorin

Dipl.-Inform. Petra Borowka leitet das Planungsbüro UBN; langjährige Projekterfahrung mit herstellerunabhängiger standardbasierter Netzwerk-Planung in Beratungsprojekten für verschiedenste Industrie- und Dienstleistungsunternehmen; Schulungen, Veröffentlichungen

Bild 1 Integrative Netzwerkmanagement-Plattformsysteme



Evolution von Management-Lösungen: Phase 3

Seit 2000 ist eine Trendwende in Richtung Funktionstrennung und Reduzierung der Bedienkomplexität festzustellen. Die Märkte für System- und Netzwerkmanagement haben sich auseinanderentwickelt, zunehmend kommt eine bedarfsgerechte Kombination von Tools und Verfahren für Konfiguration, Betrieb und Überwachung von Clients, Servern und Netzkomponenten zum Einsatz, wie in Bild 2 dargestellt:

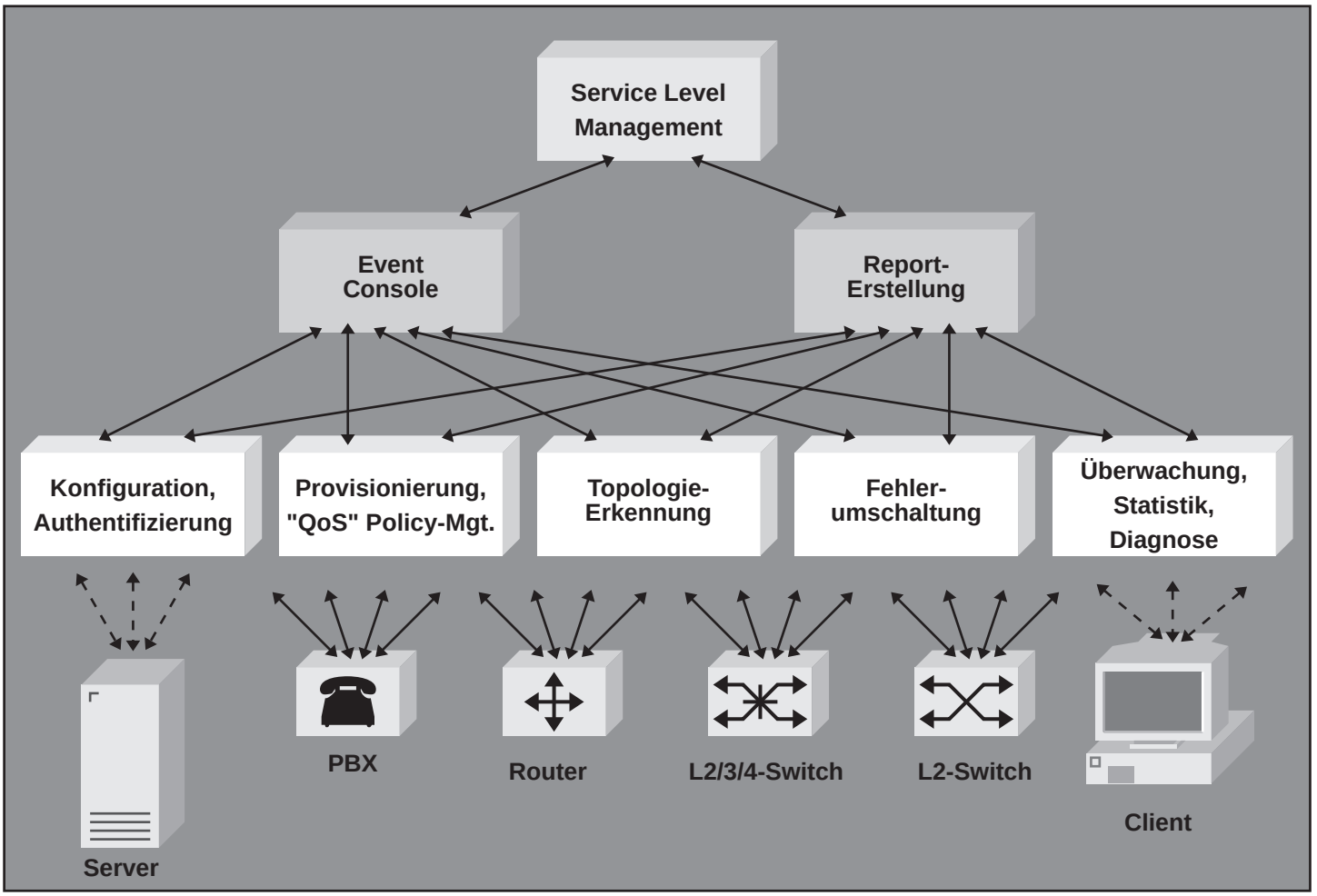
- Event-Konsole zur Minimal-Integration von grafischer Netzdarstellung und Event-Handhabung
- Konfiguration und Dienst-Provisionierung über Webbrowser oder CLI
- Automatische Fehlerumschaltung bei Netzwerk-Ausfällen durch Einsatz von Redundanzverfahren

garantierte Verfügbarkeit	Ausfallzeit (Minuten/Monat)	Ausfallzeit (Stunden/Monat)
97 %	1314	21,9
98 %	876	14,6
98,5 %	657	10,95
99 %	438	7,3
99,9 %	43,8	0,73
99,99 %	4,38	0,073
99,999 %	0,438	0,0073
100 %	0	0

Tabelle 1 SLA Zahlen und ihre Bedeutung

- Vorbeugende Überwachung der Server und aller Netzkomponenten des Kernnetzwerks
- Reporterstellung zum Nachweis der Einhaltung der vorliegenden Betriebsanforderungen bzw. der getroffenen SLA-Vereinbarungen

Bild 2 Neues Funktionsmodell für "Lean Management"



Die gewünschten Funktionen sind vielfach durch eine Kombination von drei Bausteinen realisierbar: einem Basis-Managementsystem, oft als Basis-Suite oder Element Manager eines Herstellers erhältlich, einem oder zweier Zusatztools für Monitoring und Reporterstellung sowie in ausgeprägten SLA-Umgebungen einem übergeordneten Service Level Management Tool zur Zusammenführung der Einzelaktionen und Ergebnisse. Diese relativ simple 3-Baustein-Architektur ist in Bild 3 gezeigt. Nachfolgend gehen wir auf die einzelnen Elemente dieser Architektur näher ein, mit besonderem Fokus auf neue Entwicklungen im Bereich Monitoring.

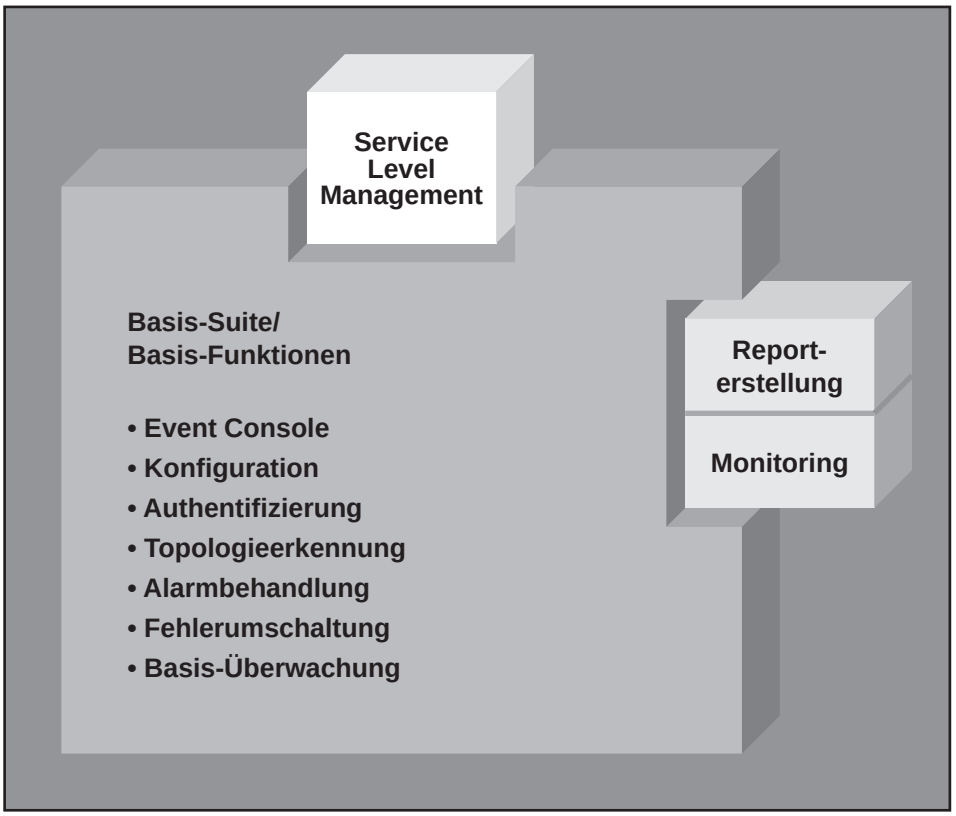
Der Element Manager (Basis-Suite)

Ein Element Manager System enthält meistens eine Funktion zur Topologieerkennung des Netzwerks, eine Event-Datenbank für grafische und/oder textuelle Störfallanzeigen, Anzeige der Umleitung einzelner Komponenten-Logs auf eine zentrale Konsole, Komponenten-Meldungen und Poll-Ergebnisse. Gleichermaßen ist über einen Element Manager die Überwachung wichtiger Betriebsparameter und Schwellwerte möglich wie

- Auslastung einzelner Ports, Verbindungen oder Wege
- CPU-Auslastung und CPU-Überlastung von Switches und Routern
- Speicher- / Puffer-Auslastung und Überlastung von Switches und Routern
- Paketfehler (falsche Länge, Bitfehler, Kollisionen, Duplex Konflikte)
- Protokollfehler wie Einzel- oder Blockwiederholung, Fluten oder Adress-Duplizierung

Mehr oder weniger detailliert lassen sich auch Aktionen zur Alarmbehandlung über Skripte oder Aktions-Bibliotheken programmieren. Konfiguration einzelner Komponenten oder auch Mehrfach-Konfiguration (Bulk Action) gleicher Komponententypen können über eine grafische oder Browser-Oberfläche durchgeführt und teilweise auf erfolgreiche Aktivierung überprüft werden. Allerdings ist hier anzumerken, dass der Umfang der Browser-Oberfläche das CLI meistens nicht voll sondern nur zu 60 bis 90 Prozent ersetzt. SNMP als Träger-Protokoll für den (grafischen) Konfigurationszugriff nimmt jedoch mehr und mehr ab.

Bild 3 Bausteine der neuen Management-Architektur



Authentifizierung des Management-Zugriffs, mindestens über CHAP oder RADIUS gehört heute vielfach schon zum Standard-Lieferumfang. Verschlüsselung oder SSL / SSH sind nicht ganz so häufig verfügbar. Soweit die eingesetzten Switches dies unterstützen, kann die Provisionierung von Diensten für Realzeit- und non-Realzeit-Anwendungen über so genannte Policy Manager als Zusatztool oder Menü des Element Managers durchgeführt werden.

Betreiber sollten hier entsprechend konsequent die Implementierung des neuen Sicherheitsstandards IEEE 802.1X einfordern, der die Überprüfung des autorisierten Zugriffs schon am ersten Etagen-Switchport vornimmt, an den ein User- oder Managementsystem angeschlossen ist.

Zusätzlich zur Authentifizierung ist die Nutzung eines Outband Management LANs günstig, soweit die eingesetzten Switches einen solchen separaten Port unterstützen. Andernfalls unterstützen inzwischen alle etablierten Switches die Konfiguration eines separaten, isoliertes Management VLANs über 802.1Q.

Als Weiterentwicklung der Element Manager zeichnet sich aktuell die Integration eigener weiterführender Monitoring Tools ab sowie die Entwicklung zur konvergenten Lösung d.h. Management-Integration von Datennetz und TK-Lösung, soweit bei einem Hersteller eine eigene Lösungspalette in beiden Welten verfügbar ist (z.B. bei Alcatel, Avaya, Cisco, Foundry / Mitel, Nortel Networks).

Etablierte Element Manager Lösungen sind

- OmniVista von Alcatel
- CajunView bzw. sein Ablöse-Tool Visability von Avaya
- CiscoWorks 2000 von Cisco
- EPICenter von Extreme Networks
- Optivity von Nortel Networks.

Automatische Fehlerumschaltung

Soweit Hardware-Störfälle und (in begrenztem Umfang) Software-Störfälle vorliegen, ist der Netzbetrieb nicht auf manuelle Störfall-Behebung mittels Element-Manager-basierter Konfiguration angewiesen, sondern es können bei Betrieb entsprechender Redundanzverfahren auf Layer 1, 2 oder 3 automatische Fehlerumschaltungen greifen.

Solche Verfahren sind auf Layer-1 Herstellerverfahren wie HIPERRing, Resilient Links, LinkSafe, Link Redundancy u.a., auf Layer-2 Standards wie 802.1D Spanning Tree (STP) und Rapid Reconfiguration Spanning Tree (RSTP), 802.1s Multiple Spanning Tree (MSTP), 802.3ad LACP und auf Layer-3 OSPF, BGP und VRRP der IETF.

Soweit die genannten Verfahren mit angemessenem Aufwand realisierbar sind (d.h. von den eingesetzten Komponenten funktionierend unterstützt werden), ist die automatische Fehlerumschaltung der reinen Überwachung / Anzeige stets vorzuziehen.

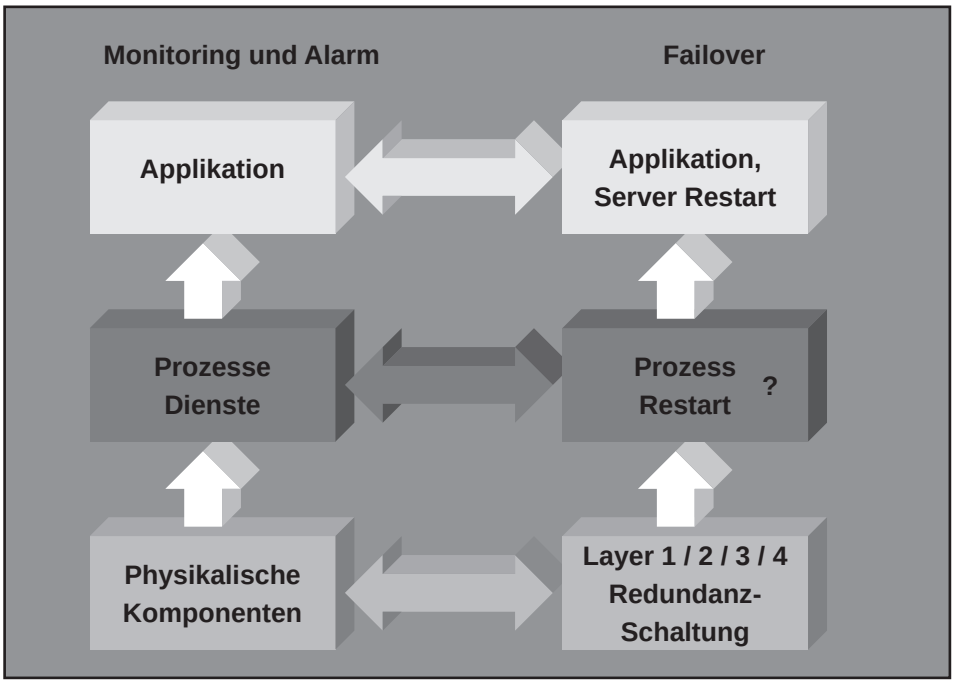


Bild 4 Komplementäres Zusammenspiel von Monitoring und Fehlerumschaltung

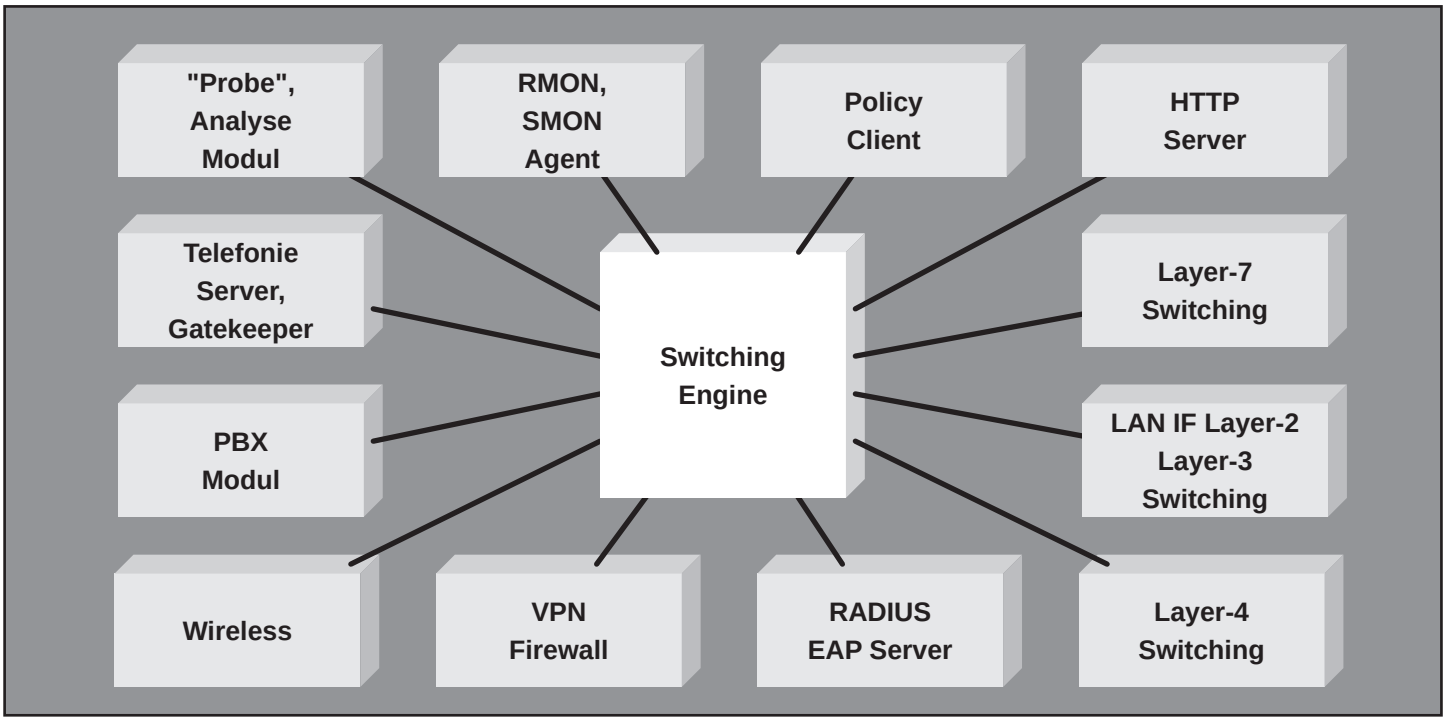
Monitoring ist jedoch insofern als komplementäre Maßnahme zu Redundanzverfahren zu betrachten, als dass Monitoring selbst bei eingehenden Meldungen oder schlechten Monitoring-Werten eine Fehlerumschaltung initiieren kann, wie in Bild 4 gezeigt wird. Außerdem lassen sich mit Monitoring alle oder zumindest sehr viele Störfälle überwachen und feststellen, die nicht durch automatische Fehlerumschaltung behebbar sind.

Ist der SNMP Manager noch zeitgerecht?

Die Komplexität der Switches / Router und resultierende Anzahl der MIB Parameter führt zu immer mehr SNMP Parametern, die nicht mehr sinnvoll vollständig und parallel überwacht werden können. Mehr und mehr werden Zusatzfunktionen (siehe Bild 5) und Sicherheitsmechanismen in diese Netzkomponenten eingebaut, die einfache Überwachungsmechanismen sehr erschweren bis verunmöglichen, so z.B.

- Wireless
- Security
- Authentifizierung
- Firewall
- VPN
- DNS Cache
- u.a.

Bild 5 Ihr Switch, das unbekannte Wesen ...



Hinzu kommt, dass die Abfrage einzelner Parameter, wenn sie denn überhaupt möglich ist, oft nicht viel Mehrwert bringt. Was hat ein Netzbetreiber in einer konkreten Störfall-Situation davon, wenn er weiß, dass an Slot 3, Port 22 seit dem letzten Restart 47.369 ARP Requests gesehen wurden? Anstelle der Abfrage einzelner Parameter einzelner Komponenten wird zunehmend die Auswertung von Logfiles gewünscht, da sie mehr auf situative Fehlermeldungen fokussiert sind. Dieser Trend macht intelligente Tools zur Umleitung der Logdateien auf System- und Backup-Server sowie zur Auswertung der Logfiles erforderlich. Die Anforderung nach Logfile-Umleitung besteht, weil in vielen Switches die Logdatei nur dynamisch / volatil gespeichert wird und bei einem Reboot (wie er zur spontanen Fehlerklärung oder Behebung bei "Software-Hängern" sehr oft durchgeführt wird) verloren geht (!).

Aus den genannten Gründen ist sowohl nutzer- als auch insbesondere herstellerseitig eine Trendwende weg vom SNMP Manager hin zum HTTP Server, zu Java oder noch zukunftsträchtiger zur XML-Applikation festzustellen. Wenden wir uns daher nun den Tools für weiterführende Funktionen einer Management-Lösung zu wie Durchsatz-Messungen, Antwortzeit-Messungen, Jitter-Messungen, Event-Weiterleitung und Korrelation, Störfall-Analyse, Reportwesen und Dokumentation, SLA-Überwachung und Abgleich, Langzeitstatistik und Historienverfolgung sowie Accounting.

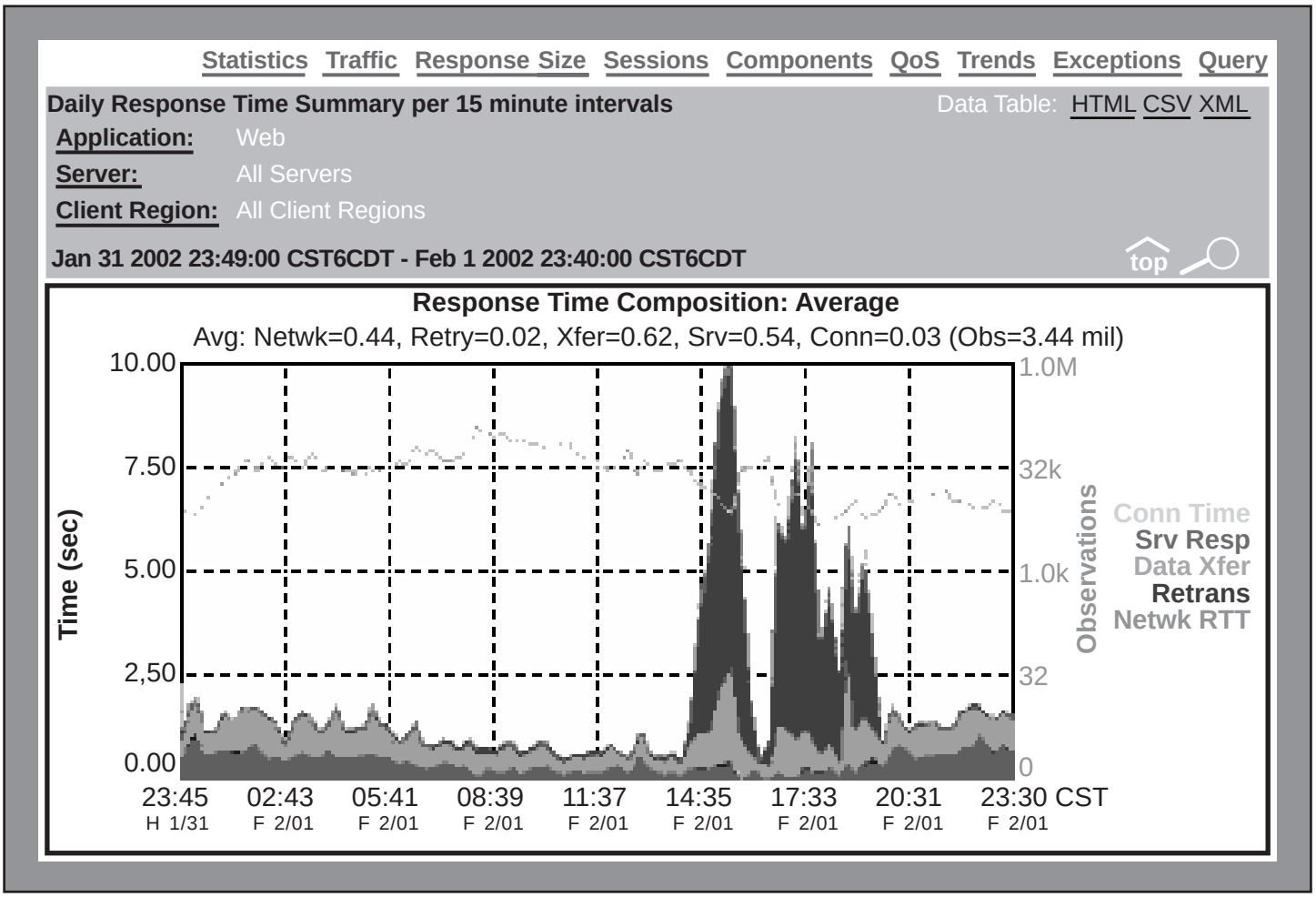
Monitoring weiterführender Parameter

Nicht nur der Durchsatz, sondern auch Verzögerung, Antwortzeit und Schwankung von Leitstungsparametern (Jitter) sind wichtige Informationen, die Aufschluss über dauerhafte und burstbedingte Leistungs-Engpässe (siehe Bild 6) geben können. Aktuell verfügbare Tools leisten mittels verschiedener Detailtests eine intelligente Aufsplittung in Antwortzeit-Anteile nach Verbindungs-Aufbau, Server-Antwortzeit, Datentransfer-Antwortzeit, Gesamt-Retransmission-Zeit und Netzwerk-Retransmission-Zeit. Zu untersuchen sind insbesondere die nachfolgend genannten Netzwerk-Elemente:

- Einzelswitches
- Einzelverbindungen
- Teilstrecken
- Ende-zu-Ende-Verbindungen
- LAN-WAN-Verbindungen

Software- und Treiberfehler sowie fehlerhaftes Anwendungs-Design lassen sich durch Messungen / Mitschneiden (Traces) bestimmter Protokoll-Aktionen und Prozesse eingrenzen und diagnostizieren. Mindestens sollten die eingesetzten Tools folgenden Funktionsumfang unterstützen: Analyse der Layer-3 Verbindungen für IP, Analyse der Layer-4 Verbindungen für TCP und UDP, Trace-Eingrenzung auf bestimmte TCP/UDP Portnummern, Analyse der Layer-7 Verbindungen für HTTP, NBT, POP3 und andere eingesetzte IP Anwendungen.

Bild 6 Aufzeichnung eines Antwortzeit-Peaks, aufgesplittet in die verschiedenen Transaktions-Anteile



Netzwerk-Management-Lösungen 2003: Schlankheitskur für Enterprise Management

Die Analyse sollte sowohl für Unicast als auch für Broadcast und Multicast separat durchführbar sein. Besonders Multicast-Analyse wird mit zunehmendem Einsatz von Konferenz- und anderen verteilten Anwendungen immer wichtiger. Zur Beurteilung des ganzheitlichen Netzverhaltens sollten die Messungen im Produktivumfeld gemischter Anwendungs-Szenarien mit Transaktionssystemen (SAP/R3, Oracle), Datentransfer-Bursts (NT-Profile, Mischdokumente, 3D-Grafiken), Produktion (Sinec AP) und Automatisierungstechnik sowie Realzeit-Anteilen (Sprache, Video) durchgeführt werden.

Monitoring Konzepte

Für die Implementierung von Monitoring Lösungen kommen verschiedene Alternativen mit jeweils unterschiedlichen Vor- und Nachteilen in Frage. Grundsätzlich ist zwischen Server- und Client-Monitoren zu unterscheiden, die jeweils auf oder in physikalischer Nähe der zu überwachenden Systeme installiert werden und entsprechende Werte über Systemparameter, Transaktions-Anzahl und Antwortzeiten liefern.

Server-Monitore: Server-Monitore werden, wie ihr Name schon sagt, zur Überwachung der Server eingesetzt und liefern die genaueste Anzeige von Server-Delays, Server-Transaktionen sowie Anzahl der erfolgten Client-Zugriffe. Sofern der Monitor nicht als Agent direkt auf dem Server läuft, wird er günstigerweise an einem Monitorport des Switches angeschlossen, an dem der zu überwachende Server angebunden ist. Der Monitorport wird als Spiegelport für den betreffenden Switchport konfiguriert, an dem der Server betrieben wird. Im gezeigten Beispiel Bild 7 sind die Messwerte eines Oracle Servers aufbereitet, der mit 98% Speicherauslastung und 81% Swap-Auslastung erkennbar an der oberen Grenze seiner Leistungsfähigkeit arbeitet.

Client-Monitore: Client-Monitore erfordern bei einer flächendeckenden Implementierung deutlich höhere Kosten als Server-Monitore, da die erforderliche Anschlusszahl sehr viel höher ist. Client-Monitore wird man daher stets nur an ausgewählten signifikanten Referenzpunkten implementieren wie das am weitesten entfernte Netzsegment, das System mit der höchsten (vermuteten) Aktivität oder einer zeitkritischen Anwendung.

Ein Client-Monitor kann in der Regel nicht zur Server-Überwachung genutzt werden, da er bei den heute üblichen zentralen Serverkonzepten entweder in großer Netzentfernung zum Client oder zum Server angebunden ist und hierdurch die Messwerte für Client- oder

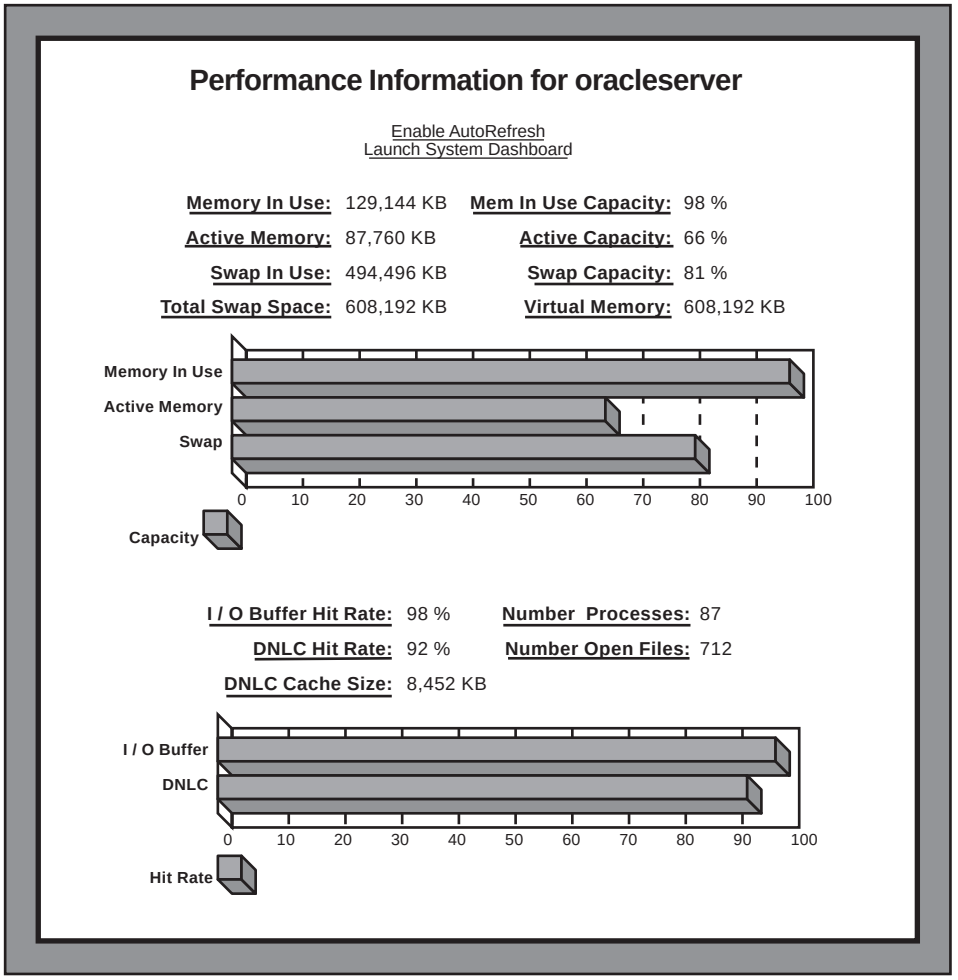


Bild 7 Monitoring Auswertung eines Oracle Servers am Kapazitäts-Limit

Serverdelay entsprechend ungenau werden.

Client- und Server-Monitore sind verfügbar als aktive oder passive Monitore**.**

Passiver Monitor: Ein passiver Monitor ist ein dediziertes Gerät mit eigenem Netzanschluss, mit dem die Messungen durchgeführt werden, im Regelfall durch passives Mitprotokollieren in Kombination mit der Nutzung von Monitorports der entsprechenden LAN Switches. Vielfach arbeiten passive Monitore auf der Basis von Paket-Decodierungs-Software ("Analysatoren") oder der Application Response Time Monitoring Schnittstelle (ARM API) und messen die vom Benutzer bzw. Client-System generierten Datenströme. Der Vorteil ist, dass durch passives Monitoring keine Beeinflussung des Benutzersystems und des Netzwerks stattfindet. Der Nachteil ist, dass bei fehlender Benutzer-Aktivität (Meeting, Urlaub, ...) keine oder keine brauchbaren Messwerte zustande kommen.

Aktiver Monitor: Ein aktiver Monitor, auch Agent genannt, ist ein dediziertes Gerät in physikalischer Nähe des zu überwachenden Systems und emuliert ein Clientsystem oder einen Serverprozess. Im Regelfall werden vordefinierte oder mitprotokollierte simulierte Aktionen in vorgebbaren Zeitintervallen abgespielt, die entsprechend kontrollierbare Aktions- / Reaktionsschemata und somit kontrollierbare Ergebnisse erzeugen wie z.B. der Verbindungsaufbau zum Login Server, ein Dateitransfer oder Datenbank-Zugriff. Aktive Monitore generieren also zusätzliche Netzlast, die jedoch im Normalfall so gering ist, dass die Beeinflussung der Netzwerkleistung vernachlässigbar bleibt. Weitere Nachteile sind darin zu sehen, dass die einzuspielenden Simulationen für jede Applikation separat erzeugt werden müssen und Verfälschungen der Messergebnisse dadurch entstehen können, dass bei regelmäßiger Wiederholung gleichartiger Requests Caching Prozesse aktiv werden, die zu günstigeren Ergebnissen als im Normalfall führen.

Fehlertolerantes Monitoring: Für alle eingesetzten Monitore gilt: Ein Monitor kann ausfallen! Gemäß der ersten Murphy'schen Ableitung wird genau nach dem Ausfall eines Monitors zusätzlich ein Störfall bei der überwachten Komponente auftreten. In diesem Fall ist der Betreiber genau dann auf dem Monitoring Auge blind, wenn es am dringendsten erforderlich ist. Wesentlich für alle kritischen und wichtigen Überwachungsprozesse ist daher eine fehlertolerante Auslegung mindestens der Monitoring Systeme selbst. Eine zusätzliche Absicherung solcher Störfälle bietet auch die lokale Abspeicherung von Events auf den betroffenen Switches, Client- oder Serversystemen (Vorsicht bei Switches: Der Event-Log kann durch ein Reboot gelöscht werden!).

Monitoring Möglichkeiten (1): Einsatz von RMON Probes

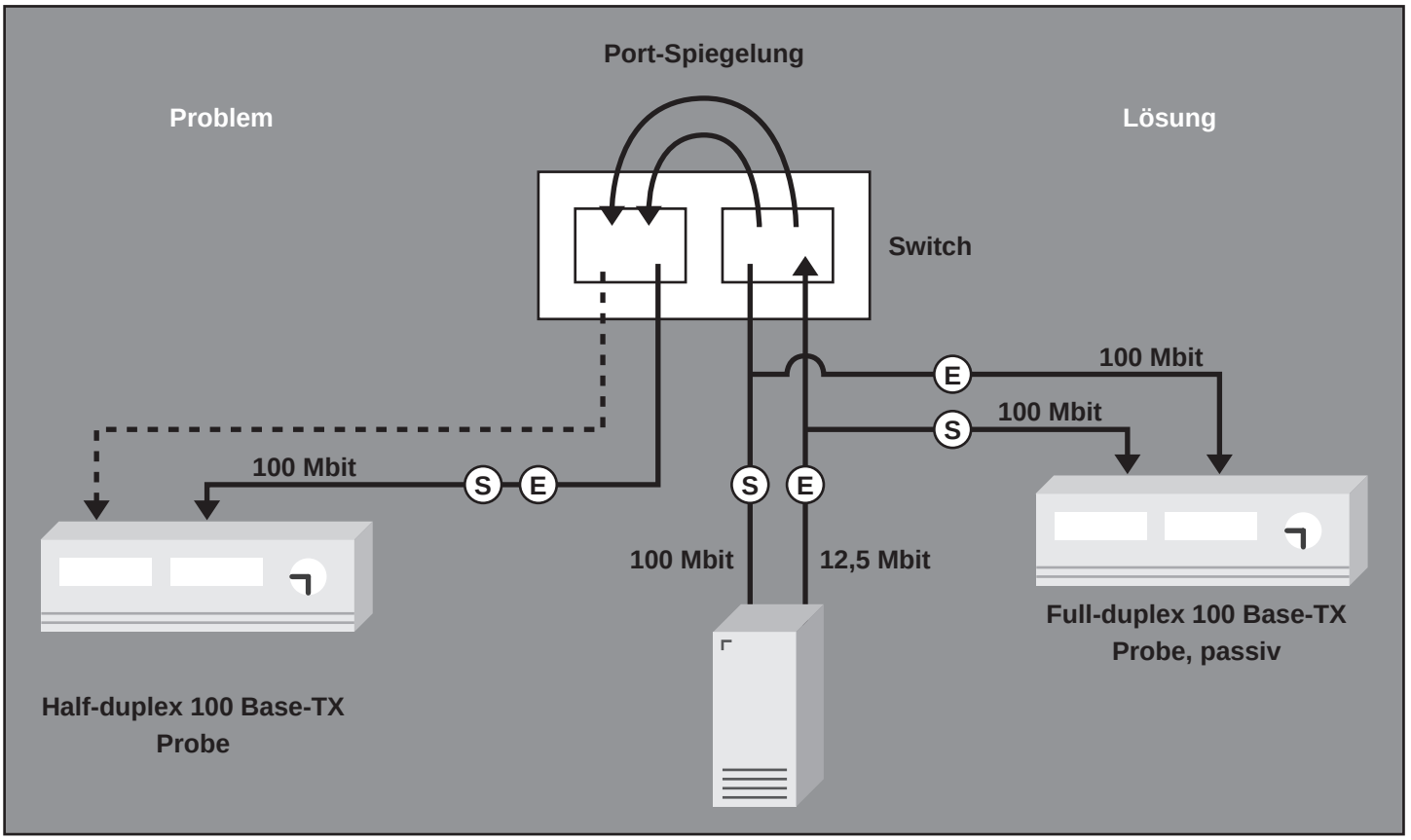
Für die Überwachung von Basiswerten können die RMON Standards genutzt werden. Teilweise ist eine einfache RMON Funktionalität auf den eingesetzten Switches implementiert, die die vier am wenigsten aufwändigen RMON MIB-Gruppen 1, 2, 3, und 9 (statistics, history, alarm, event) umfasst und Messwerte für übertragene Paketzahlen und Bytezahlen sowie Fehlerraten und Schwellwertüberschreitung liefert sowie bei der Überschreitung gesetzter Schwellwerte zur Auslösung eines RMON Alarms / Traps genutzt werden kann. Die Abfrage der Werte und Alarme erfolgt dann über eine RMON Applikation auf dem Element Manager System, einem separaten RMON Mastersystem oder einem Plattformsystem..

Vollfunktionale Unterstützung von RMONv1 oder dem weitergehenden Standard RMONv2 (Layer-3 und Layer-7 Werte und Verteilungen) ist nur über separate Probes erreichbar, die über Monitorports an das Netzwerk angeschlossen oder passiv über Verbindungsleitungen eingeschleift werden. Separate Switcheinschübe oder Tochterkarten, die als vollfunktionale Monitore arbeiten, sind zwar in Einzelfällen (z.B. Cisco) auch verfügbar, haben jedoch eine sehr viel niedrigere Performance als etablierte dedizierte Probes, da es sich bei den switchinternen Probes vielfach um einmal aufgekaufte und in der Entwicklung weitestgehend eingefrorene Produkte handelt, die nicht zum Kerngeschäft des Netzkomponenten-Herstellers gehören.

Der Einsatz von Probes führt zu folgenden Problemen:

- Für das Mitschneiden von full duplex Verkehr sind passive (eingeschleifte) Probes erforderlich, da Monitorports nur in einer Richtung spiegeln können (vom Switch zur Probe) und daher nur die Hälfte des Maximaldurchsatzes erreichen (siehe hierzu Bild 8).
- Auswertungen über VLAN- und/oder Prioritäts-getagte Frames sind in RMONv2 erst sehr viel später und zudem sehr umständlich nachdefiniert worden, weshalb viele RMON Produkte diese Auswertungen nicht unterstützen. Zur Auswertung von VLAN- oder Prioritäts-getagten Frames hat sich der SMON Standard im Markt etabliert, der jedoch von den meisten Herstellern nicht voll unterstützt wird.
- Sollen mehrere Ports parallel überwacht werden, darf der Datentransfer in Summe nicht höher sein als die Leistung des Monitorports in einer Richtung
- Ansonsten müssen Probes mit Mehrfach-Schnittstellen und mehrere Monitorports auf dem entsprechenden Switch aktivierbar sein.

Bild 8 Spiegelung von Produktivdaten eines Servers auf einen Monitorport mit angeschlossener Probe sowie auf eine passiv eingeschleifte Probe



Monitoring Möglichkeiten (2): Hersteller MIB's

Da RMON in den meisten Routern schlecht oder nicht unterstützt wird, kann – zumindest für Systeme des Marktführers Cisco – die herstellereigene NetFlow MIB genutzt werden, sofern eine Probe diese MIB unterstützt (z.B. NetQos). Auch hier gilt wieder: Die separate Probe ist leistungsfähiger als der NetFlow Prozess im Router. Wie bei standardkonformen RMON Probes können auch die Werte von NetFlow Probes über eine zentrale Master-Station abgefragt und aufbereitet werden, wie in Bild 9 dargestellt.

NetFlow spezifiziert folgende Parameter:

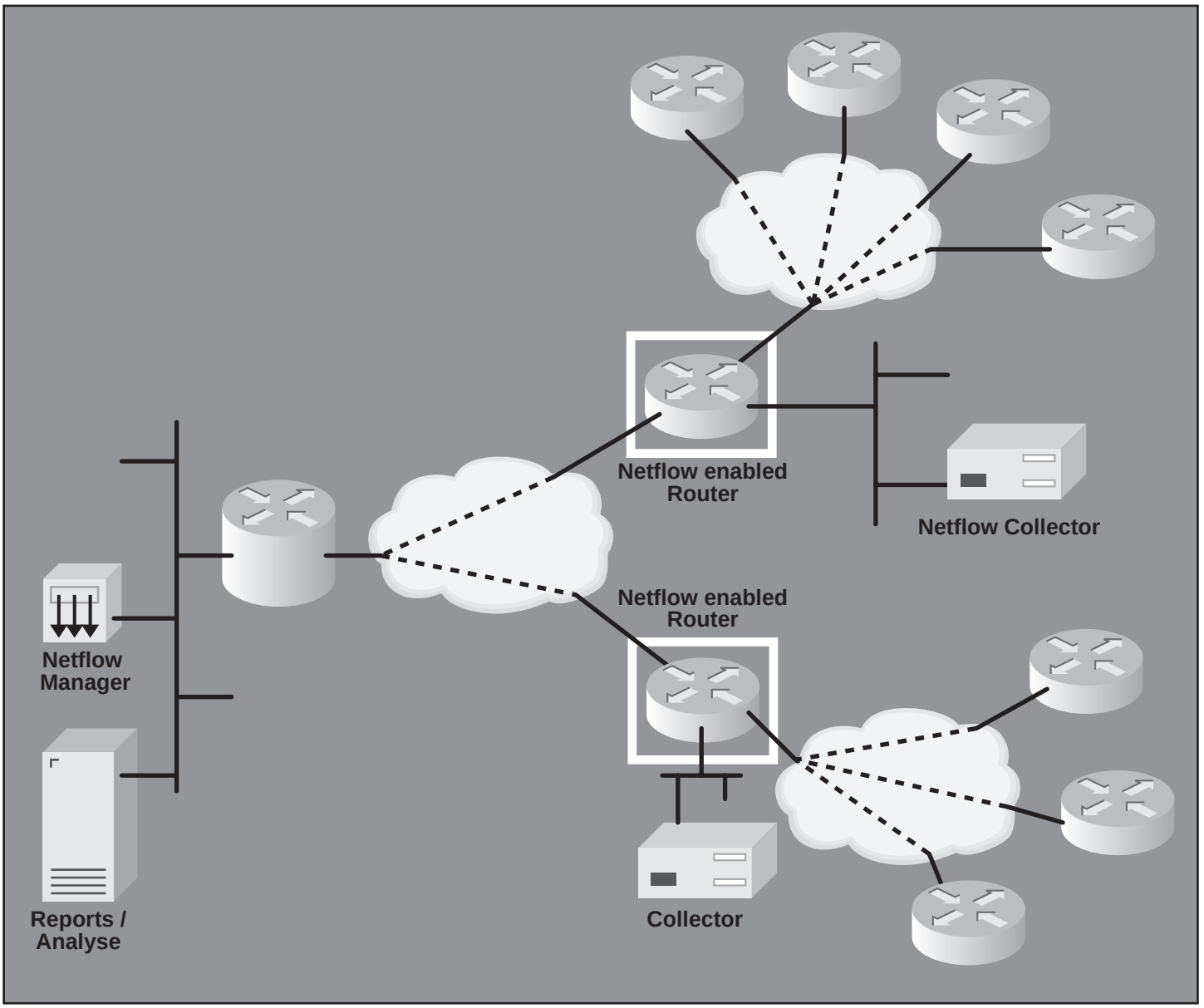
- IP Quelladresse
- IP Zieladresse
- Quellport (TCP/UDP)
- Zielport (TCP/UDP)
- Protokolltyp (IP, ICMP)
- TOS Byte (nicht: DS-Byte !)
- logisches Input Interface

mit folgenden RMON-ähnlichen Auswertungsmöglichkeiten

- Top N Talkers
- Top N Conversations
- Top N Applications

- Volumen per Entity (Verbindung, Standort, Region, ...)
- Datenrate per Entity (Verbindung, Standort, Region, ...)
- Volumen per AS
- QoS Markierungen per Applikation oder per Entity

Bild 9 Einsatz von NetFlow zur Router-Überwachung



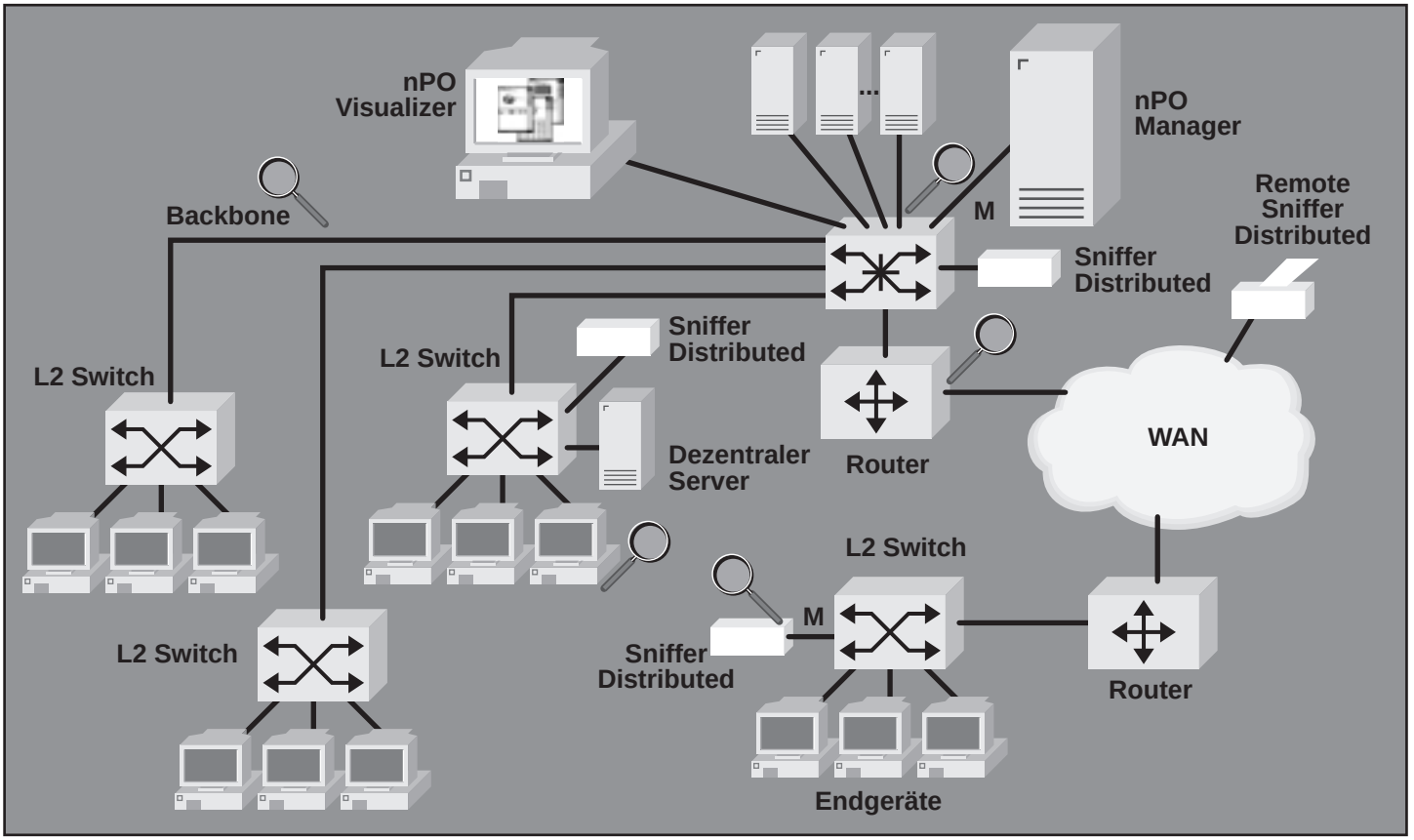
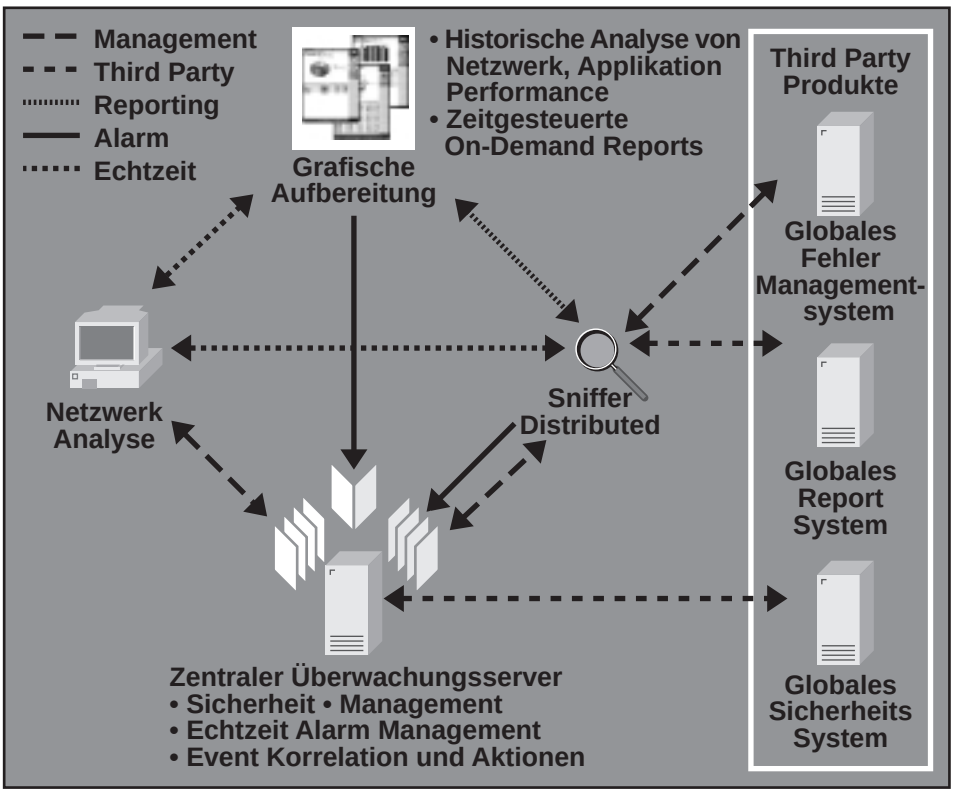


Bild 10 (oben): Einsatz-Szenario für verteilte Probes, Bild 11 (unten): Verteilte Probes, zentraler Steuer-Server und grafische Aufbereitung

Monitoring Möglichkeiten (3): Verteilte Probes

Verteilte Probes sind eine Weiterentwicklung der dedizierten Probe-Lösungen zur Einsparung von Hardware-Kosten und Vereinfachung des Betriebsaufwands. Das Konzept funktioniert so, dass an allen wichtigen Messpunkten verteilte Probes installiert werden wie in Bild 10 gezeigt, die über einen zentralen Server gesteuert und über eine separate grafische Aufbereitung / Reporterstellung von beliebig vernetzten Arbeitsplätzen aus abfragbar sind (siehe Bild 11). Typische Anschlusspunkte sind Monitorports von nichtmodularen und modularen Layer-2 und Layer-3 Switches, teilweise kann auch ein Einschleifen in die WAN-Anschaltung eines Routers erfolgen. Vorteilhaft ist hierbei der zentrale Bedien- und Abfragepunkt, der erhöhte Zugangssicherheit, vereinfachte Bedienbarkeit, Echtzeit Alarmbehandlung, Event Korrelation und Aktionsprogrammierung bietet und insbesondere im NOC betreibbar ist. Die separate grafische Aufbereitung erzeugt zeitgesteuert (historisch) und anforderungsgesteuert Reports mit Analysen für Netzwerk- und Anwendungen. Auch die Aufbereitungs-Konsole kann bei der Erreichung entsprechend definierter Schwellwerte im Rahmen der Auswertung Alarme an den zentralen Abfrageserver generieren.



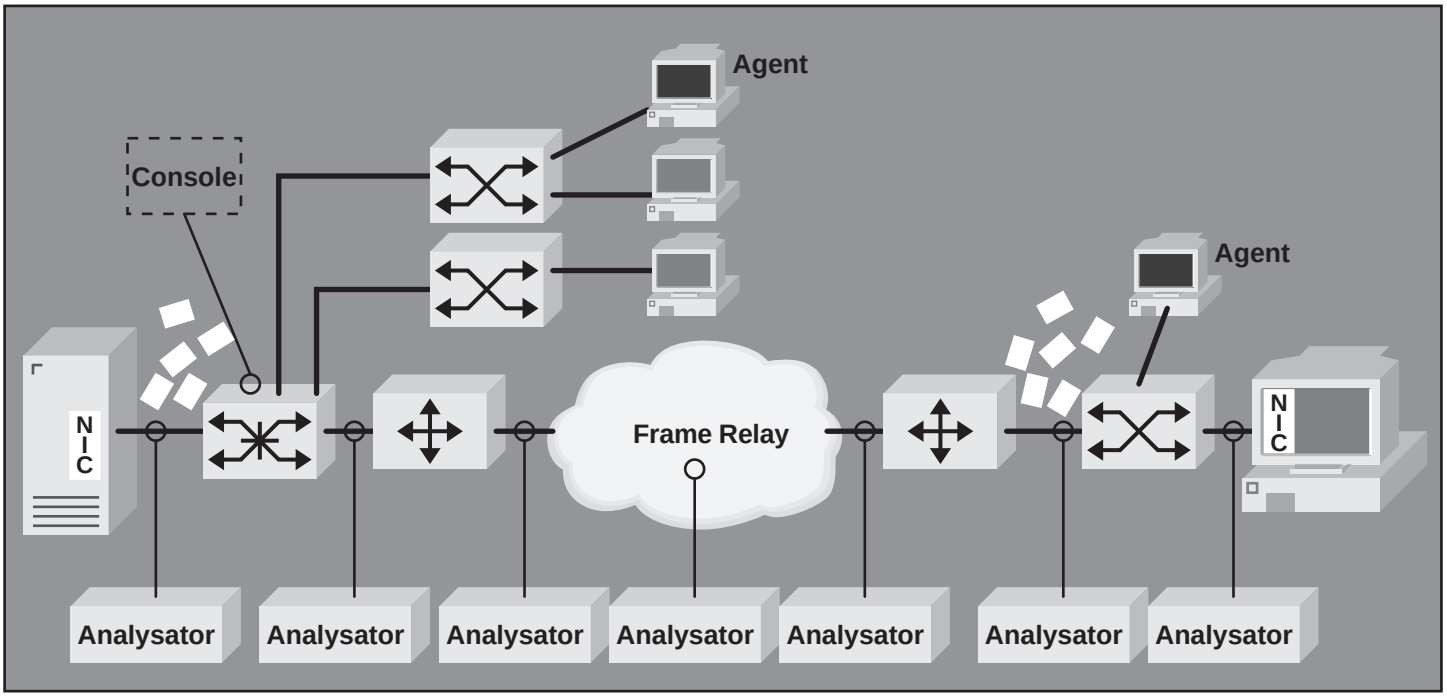


Bild 12 Einsatzszenario einer Agenten-Implementierung

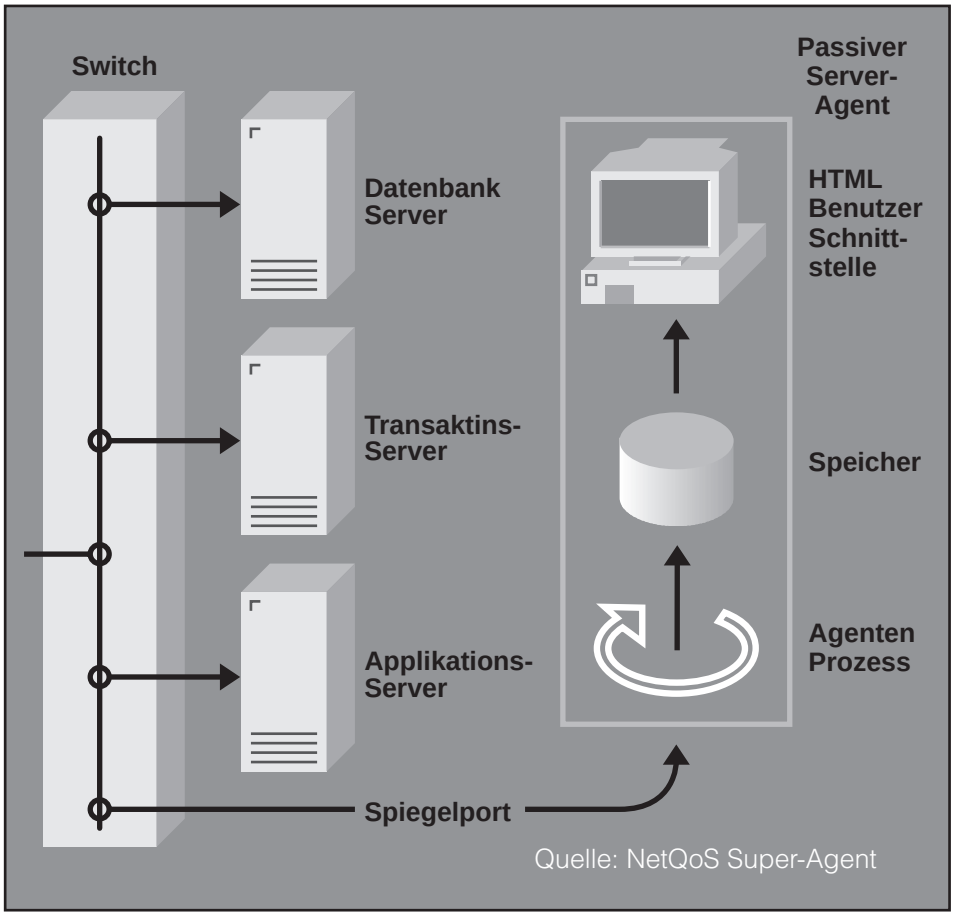
Probe-Lösungen sind z.B. bei Acterna (früher Wandel und Goltermann), Fluke, NetScout, Network Associates (Sniffer als eines der bekanntesten Tools), Cisco und NetQos zu finden.

Monitoring Möglichkeiten (4): Agenten Konzepte

Agenten-Konzepte sind eine Alternative dazu, an vielen Einzelmesspunkten Analysatoren zu installieren, denn sie liefern über mehrere Netzkomponenten hinweg Ende-zu-Ende Messergebnisse (siehe Bild 12) und eignen sich insbesondere für eine Permanent-Überwachung oder einen SLA-Abgleich. Je nach Produkt benutzt ein Agent einfache TCP/IP Aktionen wie Ping oder SNMP Get oder aber komplexere Skripte für Aktionen höherer Protokollschichten. Teilweise ist es möglich, Mitschnitte aus dem eigenen Netz wieder einzuspielen und so die spezifische eigene Umgebung kontrolliert zu simulieren.

Im Beispiel von Bild 13 ist ein einzelner passiver Serveragent an dem Monitorport eines "Serverswitches" angeschaltet, der den Netzzugang für mehrere Server realisiert. Je nachdem, welcher Server (Datenbank, Transaktionsserver, Applikationsserver) gerade überwacht oder geprüft werden soll, wird der Monitorport als Spiegelport für den entsprechenden Switchport konfiguriert und der Serveragent erhält sämtlichen Datenverkehr, um die notwendigen Messwerte zu berechnen.

Bild 13 Überwachung mehrerer Server durch einen einzelnen passiven Agenten mittels Switch-Monitorport



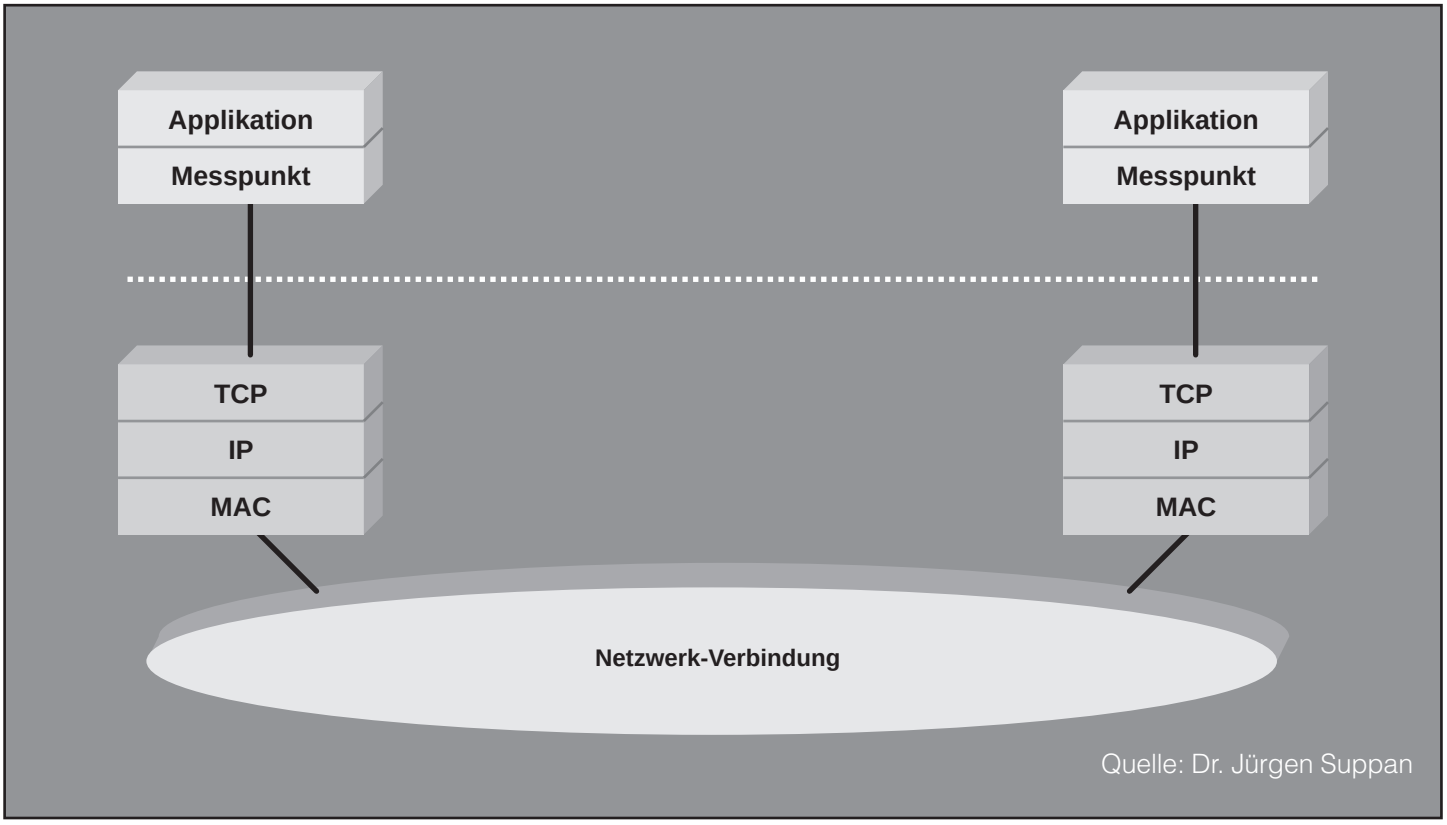


Bild 14 Einsatzszenario einer Lösung mit Kunstlast-Erzeugung

Laufen auf einem Server mehrere Anwendungen, kann die Auswertung der am Monitorport anliegenden gesamten Daten für die Auswertung eingeschränkt werden. Für einen Citrix Terminalserver könnte die Überwachung z.B. auf den Server Port 1494 und einen dynamisch zugewiesenen Client Port begrenzt werden, die Anwendung der ART MIB auf die Kommunikation zwischen MetaFrame Server und Datenbank Servern lässt sich auf die Auswertung der TCP Ports 139, 443, 1433 und 1521 reduzieren.

Produkte für Lösungen mit Monitoring-Agenten liefern z.B. AppDancer Networks (AppDancer/FA), Chevin (Tevista), Concord (eHealth), Finisar (Surveyor), Jaalam (AppareNet), Lucent (VitalSuite), NetIQ (AppManager) oder NetScout (nGenius).

Monitoring Möglichkeiten (5): Kunstlasten

Ein Spezialfall von Agenten-Konzepten sind Tools, die konfigurierbare Bibliotheken für die Generierung von Kunstlasten anbieten, wobei im Regelfall auf Geräten mit beliebigen TCP Protokollstacks als lasterzeugende Probes die Generator-Software läuft, während die zentrale Steuer- und Anzeigekonsole ein dediziertes Gerät ist wie in Bild 14 dargestellt. Die definierten Kunstlasten werden als vordefinierte und dann angepasste Lastprofile und in konfigurierbar vorgegebenen Zeitabständen im Agenten erzeugt und an die Auswertungs-Station gesendet. Die Ergebnisse hängen hierbei immer auch davon ab, wie performant der TCP Stack der eingesetzten Agenten ist ! Eines der am längsten etablierten Kunstlast-Tools ist z.B. Chariot von NetIQ, andere Lösungen sind bei Radcom und NetAlly zu finden.

Praxis-Erfahrungswerte und Planung von Messpunkten

Legen Sie den Fokus auf Ende-zu-Ende Ergebnisse, d. h. testen Sie zuerst stets gegen Client- oder Serversysteme, nicht gegen Router oder Switches, da diese nicht an den Endpunkten einer Netzverbindung liegen. Falls sich herausstellt, dass Sie einzelne Netzkomponenten näher untersuchen müssen, weil der Leistungsengpass nachweislich im Netzwerk liegt, testen Sie Netzkomponenten zuerst an den Punkten, wo das Netzdesign oder die Systemauslegung der Komponenten Leistungsengpässe vermuten lässt. Hierbei gilt das Prinzip "der Schein trügt": Überprüfen Sie vermutete Bottlenecks jedenfalls nochmals durch einen kontrolliert gesteuerten Leistungstest. Isolieren Sie Leistungsengpässe, die nicht genau geklärt sind, mittels Eingrenzung nach dem "Hop by Hop" Prinzip.

Überprüfen Sie bei Leistungsengpässen grundsätzlich die nachfolgend genannten häufigen Fehlerursachen

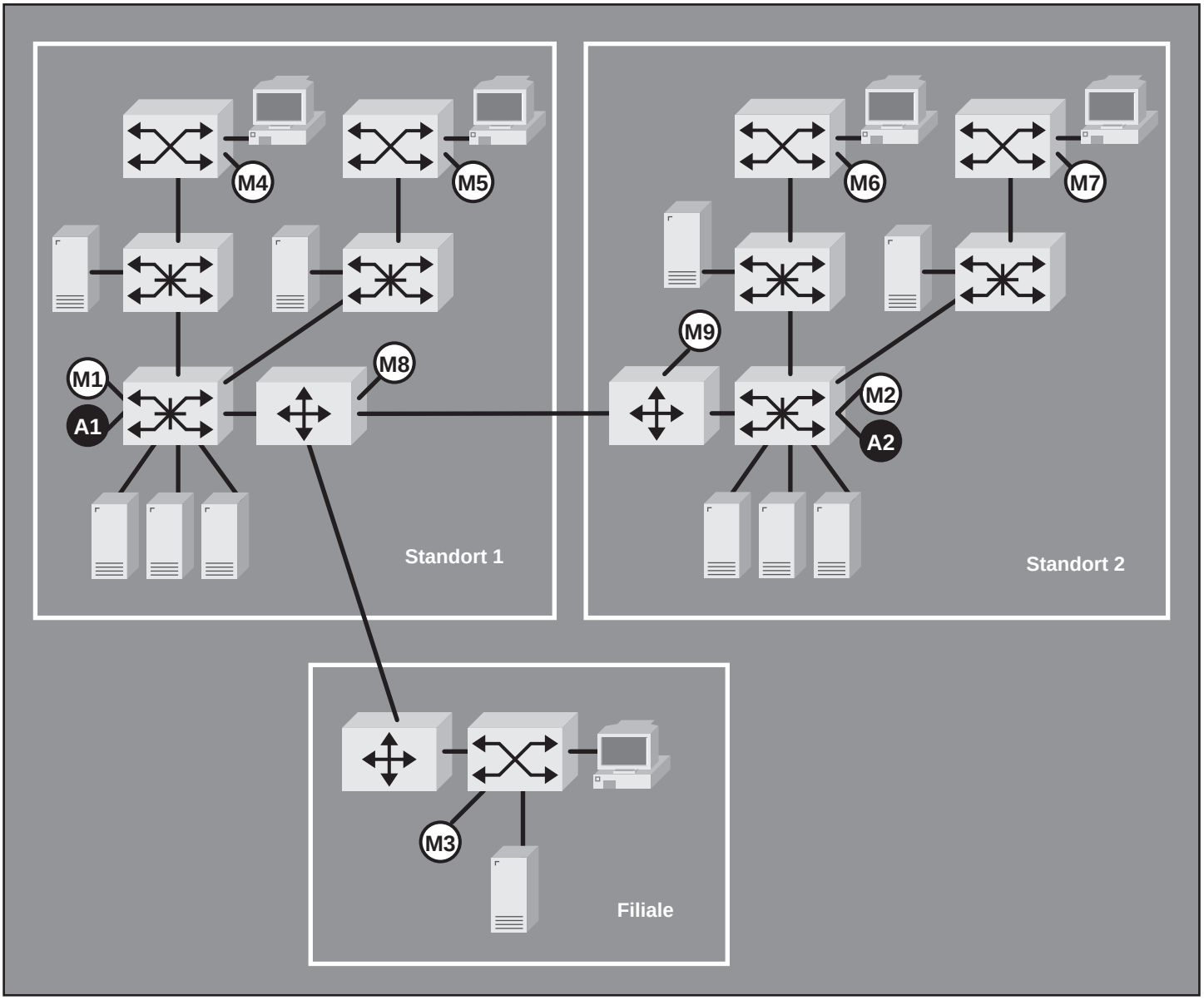
- MTU Konflikte
- hdx / fdx Konflikte
- Seiteneffekte durch Multiprotokoll Betrieb
- langsame NIC's
- langsame Router
- fehlerhafte Raten-Limitierung aufgrund von falsch konfigurierten QoS-Profilen
- WAN-Verbindungen mit hohem Delay (z.B. über Satellit)

Zur Detailplanung eines Netzwerks gehört die Festlegung von Messpunkten zur Berechnung und Überwachung der Betriebs- und Leistungsparameter für alle erforderlichen bzw. gewünschten Messungen. Ein Beispiel-Szenario zeigt Bild 15.

Für alle festgelegten Messpunkte sind Switch-Anschlüsse einzuplanen und im laufenden Betrieb dauerhaft (!) freizuhalten oder aber mit fest installierten Probes / Agenten zu belegen. Nachfolgend werden exemplarisch wichtige Messungen mit den hierfür zu nutzenden Beispiel-Messpunkten skizziert:

- M1 – M4, M1 – M5, M2 – M6: Gebäude-Erreichbarkeit, Qualität der Verbindung
- M4 – M5, M6 – M7: Qualität der Peer-Verbindung, Ende-zu-Ende Delay
- M1 – M2, M1 – M3: Standort-Erreichbarkeit, Qualität der Verbindung
- M4 – M6 / M7: Standortübergreifende Ende-zu-Ende Qualität
- M4 – M5: Eignung eines Standorts für Voice über IP (VoIP) Anwendungen
- M4 – M6: Standortübergreifende VoIP Eignung
- M4 - M1: Qualität der Verbindung zu einem zentralen Server
- A1 - A2: Applikations-Datenströme für Accounting
- M1, M2, M3: Belastung einzelner Server, Lastanteile einzelner Applikationen

Bild 15 Typische Messpunkte für Überwachung und Accounting in einem LAN-WAN-Szenario



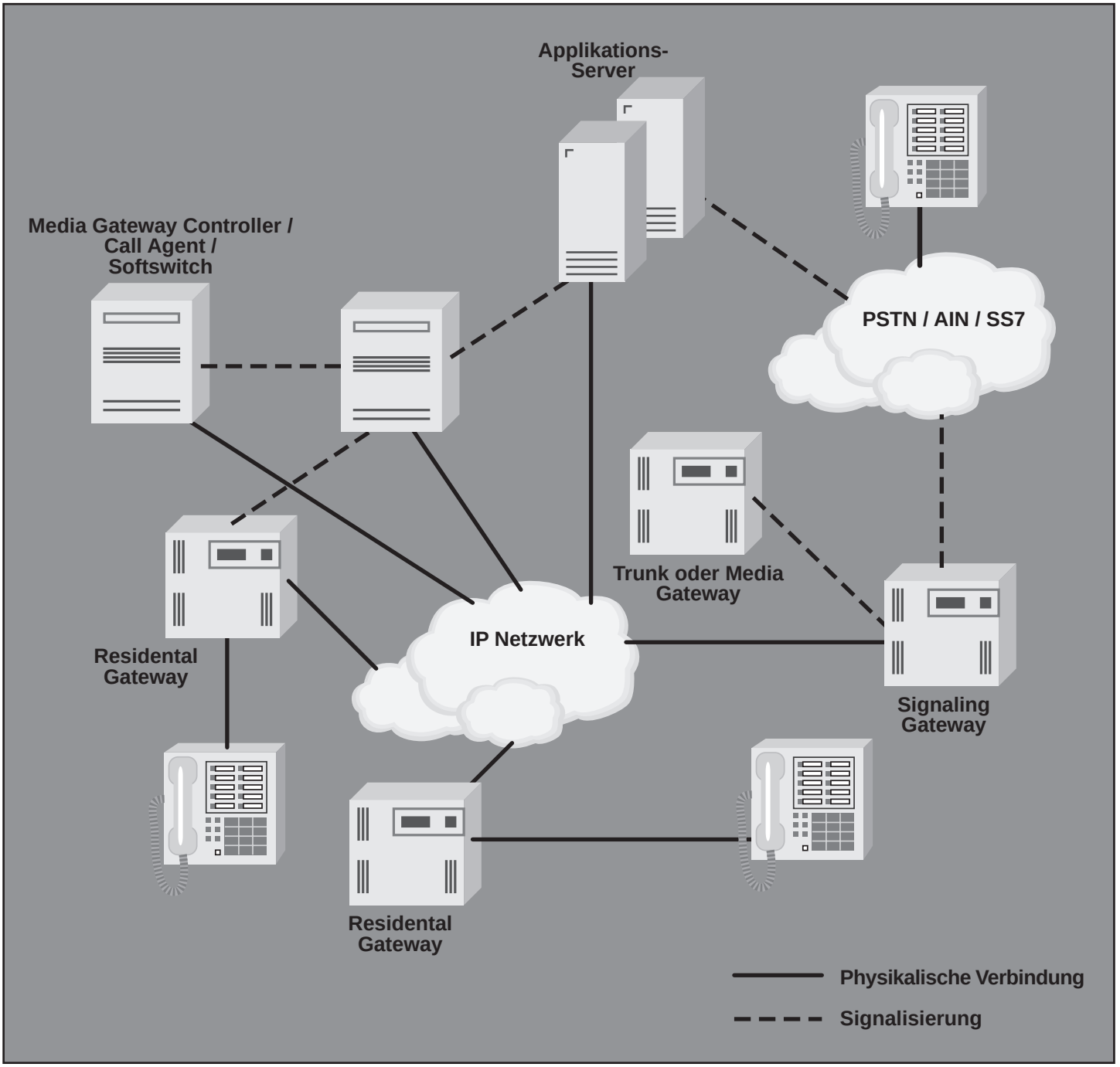


Bild 16 Komponenten für den Betrieb von Sprachanwendungen in IP Netzwerken

Der Neue Markt: Voice Monitoring

Mit zunehmender Anforderung nach dem Betrieb von Sprache in IP Netzen wurden neue Tools oder Module für existierende Tools entwickelt, die Leistungs-Messungen für und Überwachung von Sprachanwendungen abdecken. Die Bandbreite von Komponenten, die hier überprüft werden müssen, zeigt Bild 16, sie reicht vom Telefonserver über Signaling, Residental,Trunk oder Media Gateways, Media Controller / Call Agenten bis zum IP Hardware Telefon oder Softphone.

Hierfür werden Messverfahren für die physikalischen Verbindungen (dies sind dieselben wie für die Datenkommunikation), Datentransfer und Signalisierung bzw. die entsprechenden Kommunikations- und Signalisierungsprotokolle benötigt.

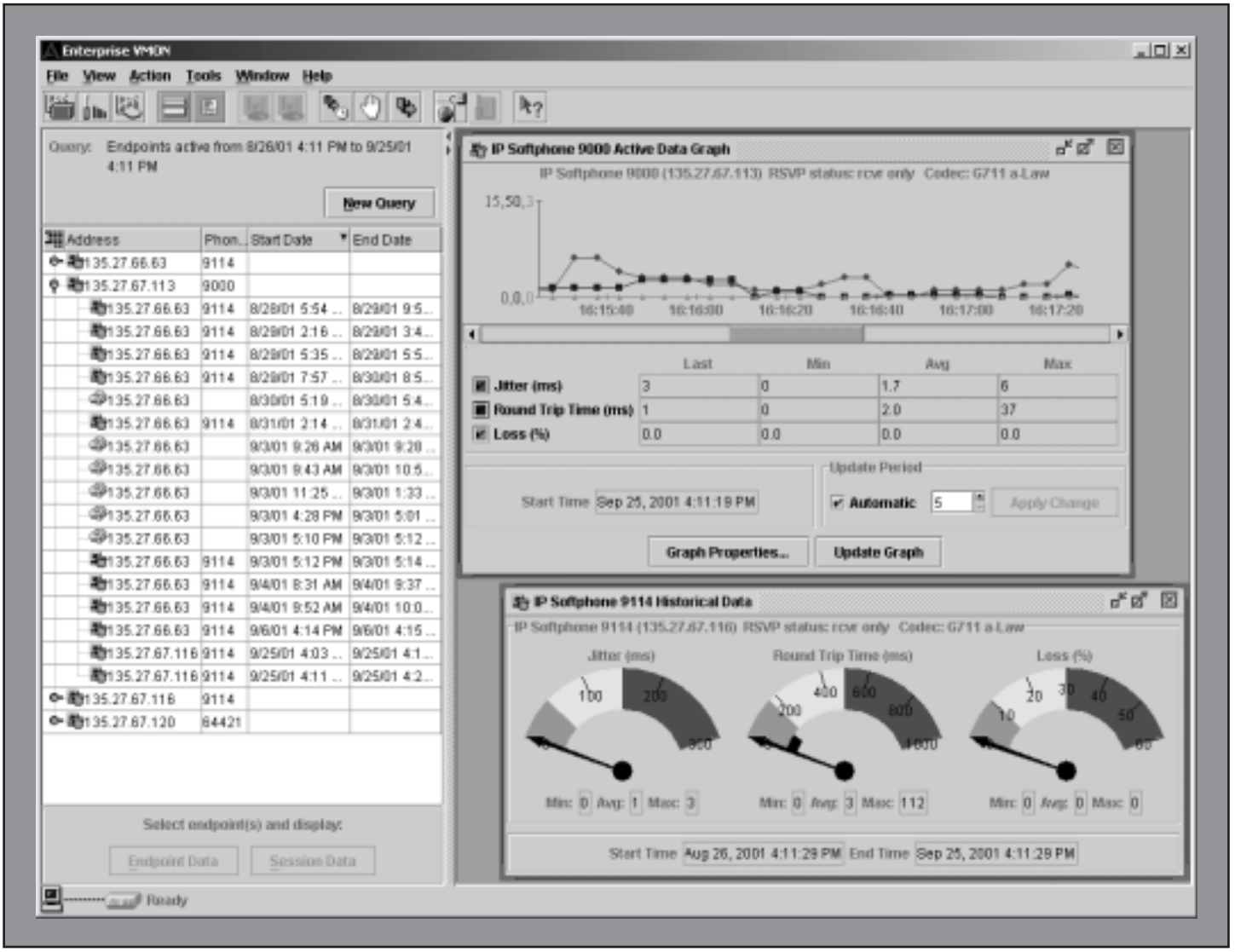


Bild 17 Überwachung eines IP Softphone im LAN mit dem Avaya VoIP Monitoring Manager

Bild 17 zeigt beispielhaft für ein im LAN betriebenes IP Softphone die historische Überwachung von Antwortzeit-Schwankung, Round Trip Delay und Verlustrate sowie die aktuelle Schwellwert-Überwachung dieser Parameter nach dem bekannten Ampel-Schema (grün, gelb, rot) mit dem Avaya VoIP Monitoring Manager.

Die zum Einsatz kommenden Messtools müssen sowohl die private Betriebsseite als auch den Übergang zum öffentlichen Betreiber-Netzwerk (NGN) abdecken. Eine Übersicht über die wichtigsten Protokolle, die auf beiden Seiten zum Einsatz kommen, sowie die Komponenten, zwischen denen sie ablaufen, ist in Bild 18 gezeigt.

Ähnlich wie für Datenapplikationen werden im Voice-Umfeld Funktionen für Simulation (Kunstlasten), Messung der erreichten Sprachqualität (PESQ, PAMS, PSQM), Monitoring von Durchsatz, Delay und verstärkt auch Jitter für Einzelkomponenten und Ende-zu-Ende Verbindungen, priorisierte und nicht-priorisierte Verbindungen, für reine LAN- und LAN-WAN-Verbindungen benötigt.

Tabelle 2 zeigt eine Übersicht über verfügbare Hersteller / Produkte und ihren funktionalen Einsatzbereich.

Empfehlungen

Nicht jeder Kuchen wird nach dem selben Grundrezept gebacken und dasselbe Rezept erzielt nicht in jedem Ofen das selbe Resultat: Die hier aufgezeigten Lösungs-Möglichkeiten müssen auf jede spezifische Betriebsumgebung individuell angepasst werden. Auch hier gilt wie so oft: Viele Köche verderben den Brei! Soll heißen: Günstigerweise sollte zusammen mit allen erforderlichen Betriebsgruppen ein ganzheitliches Management-Konzept erarbeitet werden, das in Stufe 1 den zwingend erforderlichen Funktionsumfang abdeckt und in aufeinanderfolgenden Schritten auf wichtige und wünschenswerte Funktionen erweiterbar ist. Wir empfehlen hier eine klassische Drei-Phasen-Lösung:

1. Legen Sie die Ziele für den Einsatz von Management Tools fest: Welche Kernaussagen wollen Sie mittels Tool-Einsatz treffen können? Welche Funktionen ergeben sich hieraus als zwingend, welche als wichtig, welche als wünschenswert? Erarbeiten Sie eine entsprechende Gewichtung mit resultierender Implementierungs-Reihenfolge.

2. Legen Sie den Tool-Bedarf fest: Welche Funktionen sollen mit welchem Tooltyp erfüllt werden? In welchem Maß und wie soll eine Integration verschiedener Ergebnisse sowie Informations-Weiterleitung erreicht werden? Welche Schnittstellen sollen hierfür genutzt werden?

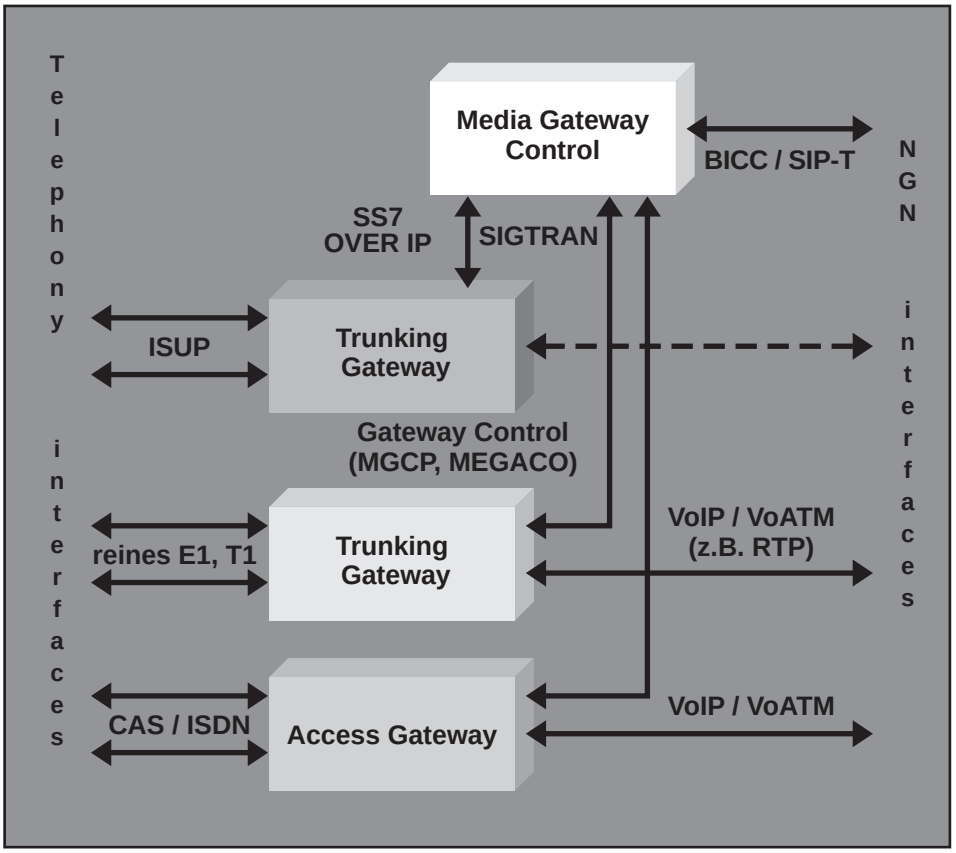


Bild 18 Protokolle und Schnittstellen von Sprachanwendungen

3. Treffen Sie die Produktauswahl für einzusetzende Element Manager, Probes / Agenten, Reporterstellung und so weit erforderlich eine in Richtung SLA-Management erweiterte Event-Konsole.

Fazit: Weniger ist mehr

- Insgesamt ist ein deutlicher Trend zur Trennung von Netz- und Systemmanagement erkennbar.
- Die klassischen Frameworks oder Plattformsysteme haben in der Praxis zu der Erfahrung geführt, dass ihre Bedienung zu komplex ist, die zu tätigenden Investitionen zu hoch sind und notwendige Funktionen im Bereich Monitoring und Reporting fehlen.
- Die Element Manager etablierter Hersteller wurden über Jahre hinweg konsequent ausgebaut und entwickeln sich aktuell zu Ablösetools für die Frameworks, da sie einfacher bedienbar und kostengünstiger sind, aber trotzdem die wesentlichen Kernfunktionen besitzen.
- Weiterreichende Tools für Monitoring, Reporting, SLA-Management müssen entsprechend der spezifischen Bedarfe als ergänzende Bausteine einer Management-Architektur ausgewählt werden.
- Eine erweiterte Event-Konsole und SLA Tools sind nicht für jede Management-Lösung und nicht immer in der ersten Stufe erforderlich.

Tabelle 2 Hersteller und Tools für Voice Monitoring

Hersteller	Produkt	SM	M	EEM	K
Agilent	Network Advisor		x		
Appdancer Networks	AppDancer		x		
	FA / VoIP		x		
Avaya	VoIP Monitoring Manager		x		
Delta Information Systems	VoIP Bulk Call Generator				x
Finisar	Nettest InterWATCH	x		x	
	Surveyor MultiQoS				
GN	Nettest InterWATCH				x
NetAlly	VoIP				
NetIQ	Chariot Voice Modul				
Network Associates	Sniffer		x		
RADcom	VoIP Manager	x	x		x
Viola Networks	NetAlly DART				

SM = Speech Measurement, M = Monitoring, EEM = Ende-Ende Monitoring, K = Kunstlast

Netzwerk-Management-Lösungen 2003: Schlankheitskur für Enterprise Management

Abkürzungen

A	
API	Application Programming Interface
ARM	Application Response Time Monitoring
ATM	Asynchronous Transfer Mode
AUI	Attachment Unit Interface
B	
B	Bit
BC	Broadcast
BGP	Border Gateway Protocol
BICC	Bearer Independent Call Control
C	
CAS	Common Access Signaling
CHAP	Challenge Handshake Protocol
CLI	Command Line Interface
C/S	Client / Server
D	
DS	Differentiated Services
DSL	Digital Subscriber Line
DWDM	Dense Wavelength Division Multiplexing
F	
FDDI	Fibre Distributed Data Interface
FC	Fibre Channel
fdx	full duplex
G	
GbE	Gigabit Ethernet
Gbps	Gigabit per second
H	
HDSL	High Speed DSL
HSSG	High Speed Study Group
hdx	half duplex
HTTP	Hyper Text Transfer Protocol
I	
IEEE	Institute for Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRTF	Internet Research Task Force
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN User Part
ITU-T	International Telecommunications Union for Telecommunication Standards
L	
LACP	Ling Aggregation Control Protocol
LWL	Lichtwellenleiter
M	
MAC	Media Access Control
Mbps	Megabit per second
MC	Multicast
MD5	Message Digest 5
MeGaCo	Media Gateway Control Protocol (IETF)
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MMF	Multimode Faser
MTBF	Mean Time Between Failure
M	
MTTR	Max Time To Repair
MTU	Maximum Transfer Unit
MSTP	Multiple Spanning Tree Protocol
N	
NBT	NetBios over TCP/IP
NEBS	Network Equipment Building Systems
NGN	New Generation Network
NIC	Network Interface Card
NOC	Network Operating Center
O	
OSPF	Open Shortest Path First
P	
PAMS	Perceptual Analysis/Measurement System
PESQ	Perceptual Evaluation of Speech Quality
POP3	Post Office Protocol Version 3
PSQM	Perceptual speech Quality Measurement
Q	
QoS	Quality of Service
R	
RADIUS	Remote Authentication Dial In User Service
RMON	Remone MONitoring (SNMP)
RSTP	Rapid Reconfiguration Spanning Tree
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
S	
SAN	Storage Area Network
SDH	Synchrone Digitale Hierarchie
SIGTRAN	Signaling Transport (IRTF WG)
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMF	Single Mode Faser
SMON	Remote Network MONitoring MIB Extensions for Switched Networks
SNMP	Simple Network Management Protocol
SS7	Signaling System #7
SSL	Secure Socket Layer
SSH	Secure SHell
STP	Spanning Tree Protocol
T	
TCP	Transmission Control Protocol
TOS	Type of Service
U	
UDP	User Datagram Protocol
V	
VoATM	Voice over ATM
VoIP	Voice over IP
VRRP	Virtual Router Redundancy Protocol
W	
WAN	Wide Area Network
WG	Working Group
WWDM	Wide(band) Wavelength Division Multiplexing

Netzwerk-Management-Lösungen 2003: Schlankheitskur für Enterprise Management

Links

www.acterna.com
www.altaworks.com
www.appdancer.com
www.aprisma.com
www.arula.com
www.avaya.com
www.bmc.com
www.brixnet.com
www.caw.com
www.chevin.com
www.cisco.com
www.clairvoyant.com
www.ca.com
www.concord.com
www.delta-info.com
www.dirig.com
www.edge-technologies.com
www.empirix.com
www.entuity.com
www.fidelia.com
www.flukenetworks.com
www.hp.com
www.infovista.com
www.ipswitch.com
www.itmasters.com
www.jaalam.com
www.logec.com
www.lucent.com
www.magnum-tech.com
www.managedobjects.com
www.merc-int.com
www.micromuse.com
www.netiq.com
www.netqos.com
www.netscout.com
www.nettest.com
www.nai.com
www.networkharmoni.com
www.networkphysics.com
www.net-reality.com
www.open.com
www.opnet.com
www.opticom.com
www.orchestream.com
www.packeteer.com
www.panacya.com
www.peakstone.com
www.peregrine.com
www.precise.com
www.productivitynet.com
www.quallaby.com
www.responsenetworks.com
www.resonate.com
www.riversoft.com
www.silverbacktech.com
www.sitaranetworks.com
www.smarts.com
www.tavve.com
www.tivoli.com
www.violanetworks.com
www.visualnetworks.com

Literatur

Berger, Stephen:
An Overview of eHealth for System & Applications Management, Concord, 2002

Dubie, Denise:
Finding the Suite Spot, NetworkWorld, 18.03.2002

Jaalam:
Duplex Conflicts: How a Duplex Mismatch can cripple a Network, August 2002

NetQos:
Monitoring Application Response Time, 2001

NetQos:
Cisco NetFlow or RMON2: Considerations for Enterprises, 2002

RFC 2205: Resource RSVP Version1 Functional Specification; September 1997

RFC 2207:
RSVP Extensions for IPSEC Data Flows; September 1997

RFC 2208:
Resource RSVP; September 1997

RFC 2613:
Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0, June 1999

RFC 2819:
Remote Network Monitoring Management Information Base, May 2000

RFC 3395:
Remote Network Monitoring MIB Protocol Identifier Reference Extensions, September 2002

RFC 3287:
Remote Monitoring MIB Extensions for Differentiated Services, July 2002

RFC 3273:
Remote Network Monitoring Management Information Base for High Capacity Networks

RFC 2021:
Remote Network Monitoring Management Information Base Version 2 using SMIv2, January

Walker, John Q., Hicks, Jeff:
Evaluating Data Networks for VoIP, NetIQ, 2001

Aktuelle Sonderveranstaltung

ComConsult Technologie-Meeting: Neueste Entwicklungen der Ethernet-Technologie: 10 GbE, 100 GBE, EFM

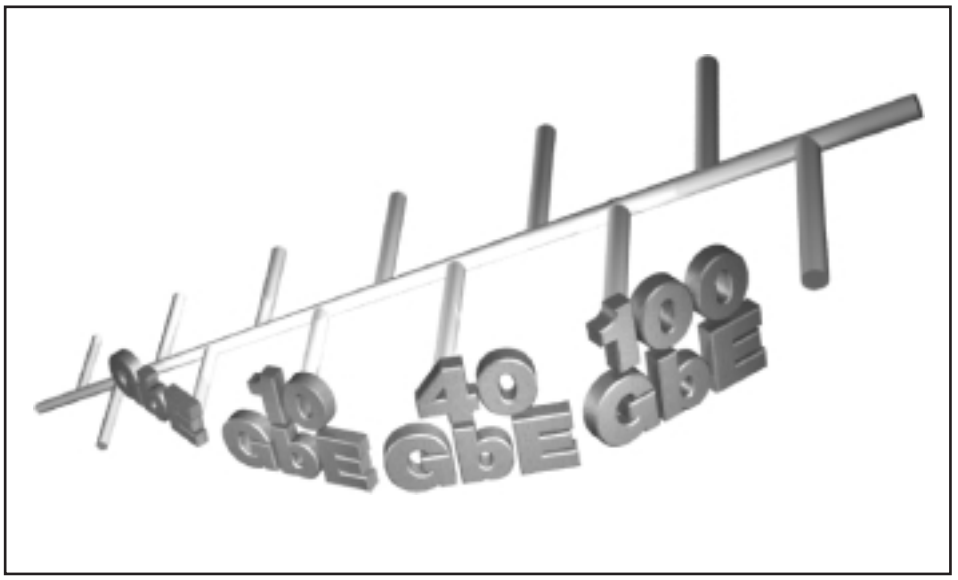
Die ComConsult Akademie präsentiert vom 14. bis 15. Mai im Excelsior Berlin die Ergebnisse der Technologie-Studie "Ethernet Evolution – Die neuesten Entwicklungen der Ethernet-Technologie: 10 Gigabit, 100 Gigabit, EFM" durch den Autor Dr. Franz-Joachim Kauffels.

Zum Thema

In den letzten Wochen hat es erneut einen Entwicklungsschub in der Ethernet-Technologie gegeben. Die neuen Meilensteine heißen:

- 10 Gigabit über Kupfer
- 100 Gigabit Glasfaser
- First Mile Technologie

Ethernet baut damit seine Stellung als dominierende, allumfassende Netzwerktechnologie weiter aus und erschließt immer mehr auch den Weitverkehrsbereich. Dort gibt es eine immer stärkere Bündelung mit neuesten optischen Technologien, die extrem wirtschaftliche WAN-Lösungen generieren werden. Im lokalen Bereich prägt die stark aufkommende Einführung von 10 Gigabit-Ethernet immer mehr den Komponentenmarkt. Träger des Bedarfs sind Speichertechnologien einerseits (immer stärkere Zunahme der Platten-/Systemtransferraten in den Gigabitbereich, resultierende Backup-Leistungsanforderungen) und der Systemwechsel auf Gigbit-Technik im Clientenbereich innerhalb der nächsten Jahre. Letztlich ist es vor allem die Kontinuität der Entwicklung, die auch zu einem wirtschaftlichen Netzwerkbetrieb führt, weil es von der Analyse und dem notwendigen Ausbildungsgrad der Betriebsmannschaft her keinen wirklich wesentlichen Unterschied macht, ob die Ethernet-Päckchen nun mit 0,1, 1 oder 10 Gigabit herumsausen. Im Endeffekt führt die kontinuierliche Weiterentwicklung von Ethernet zur Senkung der Betriebs- und Beschaffungskosten und macht dadurch gerade die Einführung neuer Technologien zu einer auch wirtschaftlich sinnvollen Maßnahme.



In dieser Sonderveranstaltung geben wir zunächst einen Überblick über die möglichen Anwendungsbereiche für 10 und 100 Gigabit Ethernet, die sich im Bereich der Corporate Networks vor allem im strukturellen Wandel innerhalb der Rechenzentren manifestieren.

Den Standard für 10 Gigabit Ethernet mit optischer Übertragung kann jeder von IEEE beziehen und ggf. sogar gratis aus dem Internet laden. Deshalb konzentrieren wir uns bei der standardisierten Variante auf die technologischen Eigenheiten und Unzulänglichkeiten, die der Standard in seiner heutigen Form bietet. Für die Teilnehmer aus dem Provider-Bereich dürften vor allem die Zusammenhänge zu SONET von Interesse sein.

Für 10 GBASE -T gibt es jetzt eine eigenständige Interessengruppe bei IEEE 802.3. In dieser Sonderveranstaltung werden wir die Machbarkeit von 10 GBASE-T untersuchen und zeigen, wie weit die aktuellen Arbeiten sind. Erste Simulationen und Prototypen zeigen, dass die gesteckten Ziele erreicht werden können. Das wäre ein enormer Durchbruch auch im Bereich der Speicher-Technologien und der RZ-Restrukturierung.

Für 100 Gigabit Ethernet gibt es zur Zeit der Reporterstellung noch keine Standardisierungs-Initiative. Dennoch kann man anhand der heute schon vorhandenen optischen Komponenten für 10, 40 und 100 Gigabit nachweisen, dass 100 GbE durchaus machbar ist. In diesem Report zeigen wir, wie 100 GbE aussehen würde, wenn man es heute sofort bauen wollte. Das übliche wirtschaftliche Ziel der Ethernet-Entwicklung "zehnfache Leistung zum dreifachen Preis" wird allerdings erst dann erreicht, wenn die Integration optischer Komponenten weitere Fortschritte macht. Wir zeigen Entwicklungen, die auf der ECOC 2002 präsentiert wurden und bald serienreif sein werden. Die Provider drängen sehr stark in Richtung 40 Gigabit Line Rate. Auf dieser Grundlage entwerfen wir erste mögliche Ausführungsformen für 100 Gigabit Ethernet-Komponenten und leiten daraus Handlungsempfehlungen für die Netzwerk-Planung ab.

Abgerundet wird die Veranstaltung durch die Darstellung von EFM, wo die Arbeiten noch laufen. Auch hier zeigen sich interessante Konsequenzen nicht nur für den eigentlichen Einsatzbereich im Providermarkt, sondern auch für völlig neue Gestaltungsansätze im Umfeld der Corporate Networks.

ComConsult Technologie Meeting

Neueste Ethernet-Technologien – Die Inhalte

Anwendungsbereiche für 10 und 100 Gigabit
- Anforderungen und Märkte für 10 Gigabit Ethernet
- Der besondere Charme einer 10 GbE-Kupferlösung
- 10 Gigabit vor dem Hintergrund der RZ-Restrukturierung
- Anwendungsbereiche für 100 Gigabit Ethernet
- Neue Perspektiven der Wirtschaftlichkeit von MANs/RANs/WANs

10 Gigabit Ethernet mit optischer Übertragung
- Ziele bei der Entwicklung des 10GbE Standards
- Struktur des Dokumentes IEEE 802.3ae
- LAN-PHY
- IEEE 802.3ae WAN PHY
- XAUI, XGSS und XGMII
- Der 10 GbE-Standard Stand ECOC 2002
- Exkurs: Netzwerk-Prozessoren

10 GBASE-T
- Zur Anwendung von 10 GBASE-T und Ziele der Standardisierung
- 10 Gigabit auf UTP – setzt Shannon unüberwindbare Grenzen?
- Verkabelungsfragen: Cat 5e, 6 oder 7
- Zum Aufbau der Kompensationsschaltkreise

100 Gigabit Ethernet
- Triebfedern und Anwendungsbereiche für 100 GbE
- Wichtige technologische Entwicklungen
- Optische integrierte Schaltungen für 100 GbE
- 100 Gigabit Ethernet und die Glasfasern
- Modellvarianten für 100 Gigabit Ethernet
- 100 GBASE-SX12 CWDM
- 100 GBASE-LX12 CWDM
- 100 GBASE-EX12 DWDM
- 100 GBASE-LX3 CWDM
- Fazit für die Unternehmensnetze

Ethernet in the First Mile, IEEE 802.3ah EFM
- Hintergrund und Entwicklung des Standards, Übersicht
- Das Projekt IEEE 802.3ah
  – Weitere Ziele und architekturelle Einbindung
- Entwicklung bei MPCP - P2MP
- Entwicklung bei der Optischen P2P-PMD
- Entwicklung bei der Kupfer-PHY
- Entwicklung bei OAM

Der Technologie Report zur Sonderveranstaltung: Ethernet-Evolution

In ihrer neuesten Technologie-Studie analysiert die ComConsult Research die aktuellen Entwicklungen und Aussichten der zukünftigen Ethernet-Technologien: 10 Gigabit über Kupfer, 100 Gigabit über Glasfaser und Ethernet First Mile.

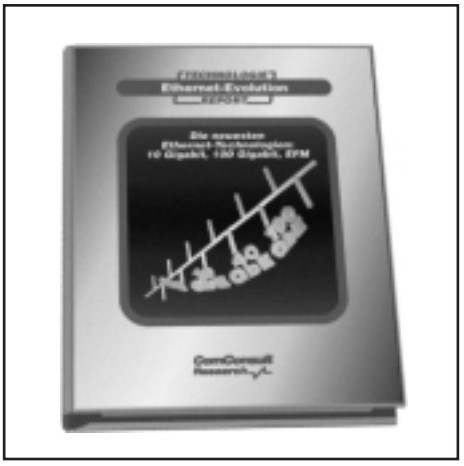
Mit dieser Entwicklung entstehen für Netzbetreiber, Serviceprovider, Dienstleister und Berater neue Herausforderungen und Geschäftsfelder:

- Ethernet erschließt immer mehr den Weitverkehrsbereich, es werden äußerst wirtschaftliche WAN-Lösungen realisierbar, die auf neueste optische Technologien aufbauen.

- Neue 10-Gigabit-Ethernet-Komponenten verändern den Markt im LAN-Bereich, mit Reduzierung der Preise werden sie im Backbone Standard werden.

- Datensicherungsabläufe und Speicher-Zentralisierung/-Konsolidierung lassen sich deutlich besser skalieren und in Netzwerke integrieren.

- Der durch die zunehmende Umstellung der Server und Clienten auf Gigabit-



Technik entstehende Bedarf an Spitzenlast-Bandbreite, um Stausituationen und Überbuchungen der Switchsysteme zu verhindern, wird abgedeckt.

- Standortverbindungen und Remote-Kopplungen von Rechenzentren sind nun ohne Leistungseinbußen für alle Anwendungsbereiche von der Notfall-Absicherung über den zentralen Datenbankbetrieb bis zur verteilten Cluster-Bildung möglich.

Im Einzelnen untersucht die Studie:

- welche Anwendungsbereiche sich für 10- und 100-Gigabit Ethernet eröffnen,

- wie insbesondere die Infrastrukturen von Rechenzentren durch eine 10-Gigabit-Kupferlösung verändert werden,

- welche Kabel nutzbar sein werden,

- welche technologischen Eigenheiten und Unzulänglichkeiten der Standard zu 10-Gigabit Ethernet mit optischer Übertragung hat,

- welche Zusammenhänge und Besonderheiten in Verbindung mit SONET bestehen,

- welche Konsequenzen sich auf die Planung und das Design von Unternehmensnetzen ergeben.

Diese Studie ist eine wertvolle und zukunftsweisende Lektüre für alle Betreiber und Entscheider von Ethernet-Netzwerken, die Ihnen zeigt, wohin sich Ethernet entwickelt und wie Sie Ihre Netzwerke und Ihre Investitionen sicher in die 100-Gigabit-Zukunft führen.

ComConsult Research

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung

ComConsult Technologie-Meeting: Neueste Entwicklungen der Ethernet-Technologie: 10 GbE, 100 GBE, EFM inklusive Technologie Report Ethernet-Evolution

☐ Ich melde mich an für das ComConsult Technologie-Meeting:
Neueste Entwicklungen der Ethernet-Technologie: 10 GbE, 100 GBE, EFM inklusive Technologie Report Ethernet-Evolution

vom 14.05. - 15.05.03 in Berlin
zum Preis von € 1.490,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Excelsior Berlin

vom_____bis_____

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Abteilung _____

Position _____ Funktion _____

Telefon, Fax _____ eMail _____

Straße _____ PLZ, Ort _____

Telefon, Fax _____ Unterschrift _____

Fax-Antwort an ComConsult 02408/955-399

Reportbestellung Ethernet-Evolution

Ich bestelle den Technologie Report

☐ **Ethernet-Evolution**
zum Preis von € 298,-- zzgl. MwSt. und Versandkosten

_____
Unterschrift

Bestellen Sie über unsere Web-Seite
www.comconsult-akademie.de

Name, Vorname _____

Firma, Abteilung _____

Straße _____

PLZ, Ort _____

Bedingungen:

Die Ware kann nicht umgetauscht oder zurückgegeben werden. Bei Versand berechnen wir eine Gebühr von € 5,-- zzgl. MwSt. für Porto und Verpackung, bei 2 und mehr Reports € 10,-- zzgl. MwSt. (Bei Versendungen ins Ausland € 25,-- bzw. bei 2 oder mehr Reports € 30,-- zzgl. MwSt.)

Anzeige

Ausbildung zum ComConsult Certified Network Engineer

Jetzt mit HP 5450 oder Sony Clie NX70V als Bestandteil der Ausbildung

Komplett-Paket: Für die komplette Ausbildung mit allen vier Seminaren zum ComConsult Certified Network Engineer zahlen Sie statt € 7.960,-- nur den Paketpreis von € 6.690,-- zzgl. MwSt. und erhalten zusätzlich wahlweise ein HP 5450 oder ein Sony Clie NX70V als Bestandteil des Ausbildungspakets bis zum 30.06.03.

Termine 2003

Lokale Netze

Einzelpreis: € 1.990,-- zzgl. MwSt.

- **19.05. - 23.05.03 in Aachen**
- **21.07. - 25.07.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**
- **10.11. - 14.11.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

TCP/IP und SNMP

Einzelpreis: € 1.990,-- zzgl. MwSt.

- **05.05. - 09.05.03 in Bonn**
- **21.07. - 25.07.03 in Berlin**
- **22.09. - 26.09.03 in Berlin**
- **13.10. - 17.10.03 in Berlin**
- **08.12. - 12.12.03 in Berlin**

Internetworking

Einzelpreis: € 1.990,-- zzgl. MwSt.

- **05.05. - 09.05.03 in Aachen**
- **30.06. - 04.07.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

Neue Ethernet Technologien

Einzelpreis: € 1.990,-- zzgl. MwSt.

- **12.05. - 16.05.03 in Aachen**
- **30.06. - 04.07.03 in Aachen**
- **15.09. - 19.09.03 in Aachen**
- **13.10. - 17.10.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

LAN-Praxis-Intensiv-Seminar:

Praktischer Aufbau von lokalen Netzen und Umsetzung typischer Netzwerk-Konfigurationen

Einzelpreis: € 2.290,-- zzgl. MwSt.

Zusätzlich zum Komplett-Paket: € 1.890,-- zzgl. MwSt.

- **05.05. - 09.05.03 in Aachen**
- **15.09. - 19.09.03 in Aachen**

ComConsult Akademie

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Meta-Directories - ein rentabler Ausweg aus dem Verzeichnis-Chaos? 05. - 06.05. Bonn

Das Seminar macht die Teilnehmer neben den theoretischen Grundlagen einer PKI auch mit der grundsätzlichen Installation, Konfiguration, Administration und dem Betrieb einer Windows 2000 / .Net PKI im Rahmen von Live-Präsentationen vertraut.
Referent: Dipl.-Ing. Martin Barbian (ITC GmbH) Preis: € 1.290,-- zzgl. MwSt.

Optische Netze und 10 Gbit Ethernet, 05. - 07.05.03 in Aachen

Das Seminar führt in die faszinierende Welt der 0ptischen Netze, die ausgehend von den Aufrüstungen der Carrier auch für die Bereiche SAN, LAN-Backbone, MAN und Access eine bisher ungeahnte Leistungsdimension erschließen.
Referent: Dr. Franz-Joachim Kauffels Preis: € 1.590,-- zzgl. MwSt.

.NET Server 2003 – plan: Windows Active Directory..., 05. - 09.05.03 in Aachen

Das Seminar befasst sich mit der Strukturierung des Active Directory unter Windows .NET-Server 2003, wobei auch Mischszenarien mit Windows 2000 erläutert werden. Ein weiterer grundlegender Bestandteil ist das erforderliche IP-Management, insbesondere DNS.
Referenten: Markus Holländer, Dipl.-Inform. Michael van Laak, Frank Neunzig, Dipl.-Ing. Lars Kuhl Preis: € 2.290,-- zzgl. MwSt.

Security-Meeting: Windows-Security, VPN und Wireless, 06. - 07.05.03 in Bonn

Diese Sonderveranstaltung beschäftigt sich mit dem Haupt-Sicherheitsrisiko der gesamten IT-Infrastruktur: dem Netzwerk-Clienten – typischerweise ein PC mit Windows-Betriebssystem – im Zusammenhang mit der Planung und Umsetzung von VPN-Lösungen und Wireless Security. Preis incl. Technologie Report "Windows Sicherheit € 1.980,-- zzgl. MwSt., Paketpreis mit den 3 Reports "Windows Sicherheit", "Virtual Private Network" und Wireless LAN Sicherheit" € 2.248,-- zzgl. MwSt.

Optimale Netzstrukturen für hochverfügbare Serverfarmen, 12. -14.05.03 Düsseldorf

diskutiert die bestehenden Alternativen in der Anbindung von Servern und Speicher an Netzwerke. Denkbare Architekturen werden speziell unter dem Blickwinkel Performance, Verfügbarkeit und Betrieb gegenüber gestellt und bewertet.
Referent: Dr. Behrooz Moayeri (ComConsult Beratung und Planung) Preis: € 1.590,-- zzgl. MwSt.

Integrierte Lösungen ... 12. -14.05.03 in Bonn

Das Seminar beschäftigt sich mit der Voraussetzung für die Sicherstellung der Verfügbarkeit und der Performance der Unternehmens-wichtigen Applikationen am Arbeitsplatz: eine funktionale und datentechnische Integration der einzelnen Management-Lösungen für Netzwerke, Server, Clienten und Applikationen.
Referenten: Dipl.-Verwaltungswirt Jürgen Dierlamm, Dr. Jürgen Suppan Preis: € 1.590,-- zzgl. MwSt.

Cisco-Router erfolgreich einsetzen, 12. - 16.05.03 in Aachen

Das Seminar lehrt den Aufbau und die Arbeitsweise von Cisco-Routern an Cisco 2600 Routern, an denen die Teilnehmer aktiv arbeiten können. Referent: Markus Schaub Preis: € 2.590,-- zzgl. MwSt.

Mobile und drahtlose Datenkommunikation..., 19. - 20.05.03 in Köln

Das Seminar gibt am 1. Tag einen Überblick über mobile und drahtlose Kommunikation, behandelt vertieft die GSM-Datendienste und zeigt die Möglichkeiten für die Unternehmenskommunikation auf und widmet sich am 2. Tag schwerpunktmäßig dem Wireless LAN.
Referenten: Andreas Meder, Dr. Simon Hoff, Dr. Joachim Wetzlar Preis: € 1.290,-- zzgl. MwSt.

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung

Titel des Seminars _____ Vorname _____ Nachname _____

Termin _____ Firma _____ PLZ, Ort _____

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Straße _____ eMail _____

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Telefon, Fax _____ Unterschrift _____

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerkkomponenten

Die Spielregeln

Sie melden uns ihr Angebot oder Gesuch per Mail, mit dem Fax-Formular (unten) oder über den Web-Server. Wir veröffentlichen es unter einer Anzeigen-Nr. im Netzwerk Insider und auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her.

Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Gebote

Adapter

IBM, Novell PCI TR Karten, ISA TR Karten, Anzahl 355 und 77, Preis VB, Anzeigen-Nr. B30205

Xylan / Alcatel OSR, Anzahl 1, Preis VH, Bemerkung: war bis zum 6.03.03 produktiv im Einsatz, 2 MGM Module SW 4.X 1 GSX (4 Port), 3 ESX (32 Port 10/100), Anzeigen-Nr. B30301

Erweiterungseinheit

Erweiterungseinheit à 20 ICS-Ports (PN: 53F5501), Anzahl 19, Preis VB, Anzeigen-Nr. B30103

Steuereinheit

IBM 5394-01B, BOS e-Twinax (IP) Controller B044656 für 56, Anzahl 1, Preis VB, Geräteadressen mit 8-Port Controller-Adapter B04500, Kaufpreis Euro 11.400 /Okt 2000, Anzeigen-Nr. B30101

Gebote

Ringleitungsverteiler

IBM Modell: 8230-001, Anzahl 8, Preis VB, Anzeigen-Nr. B30102

Router

Cisco ISDN Router 761 M neuwertig, Anzahl 1, Preis 230 Euro, Bemerkung: war Demo-Gerät
Anzeigen-Nr. B30302

Switch/Brücke

XYLAN (SEL-Alcatel) Omniswitch9, Omniswitch5, Omniswitch 5w, Anzahl 5, 3, 2, Preis VB, Bemerkung: Modulkare Switchsysteme diverse Switchkaten vorhanden: FastETH, modular ETH, FDDI, TR, Anzeigen-Nr. B30304

Cisco Module für Cat 6500, Anzahl mehrere, Preis LKP - 43%, Bemerkung: 4 x CIO:WS-CAC-1300W= , 3 x CIO:WS-X6K-S2MSFC2, 1 x CIO:WS-X6416-GBIC=, 4 x CIO:WS-G5484= (nicht original Cisco), 13 x CIO:WS-G5486= 2 x CIO:WS-X6548-RJ-45=, 1 x CIO:WS-C6500-SFM, Anzeigen-Nr. B30203

Sonstige

NetScout Modell: TR 7103R/TR, Anzahl 1, Preis VB, Bemerkung: FDDI DAS/Token Ring - Probe, Anzeigen-Nr. B30204

IBM Lanstreamer, Anzahl 31, Preis VB, Anzeigen-Nr. B30206

NetScout Dolch, Anzahl 1, Preis 20.000 Euro, Bemerkung: Protokoll Analysator für Gigabit Ethernet, PAC 65, Pentium II 400 MHZ Mit NT 4.0 Softwareversion Sniffer Pro Version 4.0.12 ist aufgespielt und funktional. Zusätzlich Sniffer Predictor Release 2.0.1.1203, Anzeigen-Nr. B30201

Gebote

Sonstige

NetScout Modell: 8211ET/128 mit Zubehör, Anzahl mehrere, Preis verschieden, Bemerkung: 4 x NetScout: 8211ET/128 (7.500,00 Euro/St.), 4 x NetScout: TX-Tap-Copper Tap Kit (820,00 Euro/St.), 8 x NetScout: 60/40 Singlemode Fiber Optic Splitter (1.100,00 Euro/St.), Anzeigen-Nr. B30202

Fax an ComConsult 02408/955-399

☐ **Ich suche**

☐ **Ich biete**

☐ **Antwort auf Anzeigen-Nr.** ☐ ☐☐☐☐

Produkt/Komponente/Release/Software

Preisvorstellung

Ansprechpartner

Firma

Ort

Straße

Telefon

Fax

eMail

Weitere Anzeigen

finden Sie auf dem Web-Server der ComConsult Akademie

www.comconsult-akademie.de