Dr. Suppan International Institute

Der Netzwerk Insider

Dezember 2003

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Der Spanning Tree ist tot! – Es lebe der Spanning Tree!

von Markus Schaub

Seit nunmehr über einem Jahr existiert der Nachfolger des klassischen Spanning Trees, der Rapid Reconfiguration Spanning Tree (RSTP). IEEE hat den klassischen Spanning Tree aus 802.1D in der Neuauflage des Standards von 2003 verbannt und nahezu alle Hersteller haben seinen Nachfolger bereits in ihre Produkte implementiert.

Es ist an der Zeit für eine erste Zwischenbilanz. Dazu hat das ComConsult Research Labor Implementierungen von RSTP unter die Lupe genommen und auf ihre Brauchbarkeit hin untersucht.

In diesem Artikel wird nicht der Standard diskutiert, sondern einige Ergebnisse der Untersuchungen werden vorgestellt, ebenso welche Konsequenzen der neue Spanning Tree auf ein modernes, kostengünstiges Netzwerkdesign haben kann. Abschließend wird noch eine Alternative zum RSTP, der HiPER-Ring vorgestellt und mit dem Standardverfahren verglichen.

Die Rückkehr des Spanning Tree

Von einer erschöpfenden Behandlung des Rapid Spanning Trees wird in diesem Artikel abgesehen. Stattdessen wird dem Leser der ComConsult Technologie Report „Design-Varianten Lokaler Netzwerke im Vergleich“ mit beispielhaften Anwendungen oder der Insiderartikel vom Dezember 2002 „Der schnelle Baum“ empfohlen.

weiter Seite 19

Zweitthema

Mobility mit Security in einer unsicheren Welt

Konsequenzen aus den Wurmangriffen in 2003

von Dr. Behrooz Moayeri

Das Jahr 2003 geht nun bald zu Ende. Weltweit wird es als das Jahr der technischen Pannen und Peinlichkeiten in die Annalen eingehen. Die Stromausfälle in den USA und Kanada, Großbritannien, Schweden und Italien waren die aufsehenerregendsten Ereignisse dieser Art.

Insgesamt nicht minder verheerend waren jedoch die Folgen der wiederholten Wurmangriffe dieses Jahres, wovon die Slammer-Attacken ab Januar und der MS Blaster ab August die spektakulärsten waren.

Die Öffentlichkeit nahm eher Kenntnis von dem dunklen Freitag ohne Strom in New York, während ca. 400 km weiter südlich in Washington D.C. in der selben August-Woche die IT in zahlreichen Bundesbehörden durch den MS Blaster praktisch lahmgelegt wurde.

weiter Seite 5

Top-Event

Das Netzwerk-Redesign Forum 2004

auf Seite 3

Zum Geleit

Sicherheit im Netzwerk: wo ist die Grenze?

auf Seite 2

Studie des Monats

Wireless LAN: Interoperabilität zwischen 802.11b und 802.11g

auf Seite 14

Zum Geleit

Sicherheit im Netzwerk: wo ist die Grenze?

Zunehmend werden Sicherheits-Lösungen direkt in das Design und die Konfiguration von Netzwerken einbezogen. Die aktuelle Produktankündigung „Network Admission Control“ von Cisco oder das schon länger existierende UPN-Konzept von Enterasys sind typische Beispiele dafür.

Dabei stellt sich prinzipiell die Frage, ob das Netzwerk der richtige Ort zur Lösung von Sicherheits-Aufgabenstellungen ist. Immerhin nimmt der Konfigurationsaufwand massiv zu und fast immer steigt die Abhängigkeit vom jeweiligen Hersteller durch das Fehlen standardisierter Lösungen.

Bisher standen sich in der Diskussion dieser Frage zwei Extrempositionen gegenüber. Die eine Position vertrat die Ansicht, dass Sicherheit ein Betriebssystem-Thema ist und im Rahmen der Benutzer- und Rechte-Authentifizierung dort geleistet werden muss. Die Gegenposition stellt dem gegenüber, dass ein Angreifer zu einem möglichst frühen Zeitpunkt – also am ersten Switch - abgefangen werden muss, um ihm keine zusätzlichen Informationen für einen Angriff zu geben. Erschwert wurde diese Diskussion noch durch die fehlende praktische Handhabbarkeit einiger zentraler Tools, speziell aus dem Bereich Intrusion Detection oder durch Probleme im Einsatz von IEEE 802.1x, wenn mehr als ein Teilnehmer am Switchport hängt (Telefon mit Mini-Switch).

Die großen Schäden, die die aktuellen Würmer und Viren in den letzten Monaten anrichten konnten (siehe dazu den Artikel von Dr. Moayeri in diesem Heft) und die damit verbundene Änderung der Bedrohungslage haben die Situation nachhaltig verändert. Dies soll an Beispielen ohne Anspruch auf Vollständigkeit dargelegt werden.

Beispiel 1: Notebook

Notebooks sind vielleicht die im Moment gravierendste Risikotechnik in den Unternehmen. Ein einziges infiziertes Notebook, sei es das eines externen Service-Technikers, sei es das einer Führungskraft, die damit auch zu Hause im Internet surft, kann ganze Unternehmen lahm legen. Entsprechende Fälle sind bekannt. Für dieses Problem gibt es nur zwei Lösungsansätze.

In der grauen Theorie sorgen wir dafür, dass es nur sichere Notebooks gibt, die an Unternehmensnetze angeschlossen werden. Zum einen würde dies den Einsatz externer Service-Techniker unmöglich machen, zum anderen würde dies implizieren, dass sich Führungskräfte klaren Regeln in der Nutzung ihres Notebooks unterwerfen. Auch wenn letzteres vereinzelt funktionieren kann, muss für die Mehrzahl der Unternehmen von einer Nicht-Durchsetzbarkeit von Notebook-Sicherheits-Policies auf der Führungsebene ausgegangen werden (man denke an das Verbot einer privaten Nutzung, Internet-Zugang nur über die Firmen-Firewall, kein Besitz des Admin-Passworts, keine Installation von Software durch den Benutzer usw.). Schon der sanfte Hinweis an eine Führungskraft, er/sie würde doch nun wahrlich genügend verdienen, um sich ein eigenes Notebook für 1500 Euro für private Nutzung leisten zu können, kann ungeahnte Energien frei setzen.

Nun wird dem ggf. entgegen gehalten, dass es dann eben Aufgabe des PC- und Server-Betriebs ist, die Umgebung so aktuell zu halten, dass alle denkbaren Angriffe an den darauf vorbereiteten Sicherheits-Einrichtungen scheitern. Hier ist klar festzustellen, dass dies eine gefährliche Illusion ist. Zum einen gibt es Angriffe die kommen, bevor das passende Update des Virenscanners oder von Microsoft vorliegt. Zum anderen haben wir massenweise Problemgeräte, zum Beispiel in der Produktion, die im Extremfall auf Windows 3.1 oder Windows 95 basieren und die technisch gar nicht in einem automatischen Upgrade integriert werden können. Auch sind nicht alle Unternehmen so weit, dass sie eine automatisierte, zentrale Client-Konfiguration umgesetzt hätten. Nur damit lassen sich aber Updates und Konfig-Änderungen in ausreichender Geschwindigkeit flächendeckend umsetzen.

Was ist also zu tun?

Beispiel 2: Wireless LAN

Wireless LANs machen im Moment eine mehr als spannende Entwicklung mit. Waren die Produkte bisher im Spannungsfeld zwischen Konsumer und Enterprise positioniert, so ändern sich die Angebote der Hersteller doch immer mehr in Richtung flächendeckender Profi-Produkte. Wireless-LANs sind, so hat auch das Wireless LAN Forum vor 2 Wochen gezeigt, auf dem Weg zur strategischen Infrastruktur-Technologie.

Was hat das mit Sicherheits-Techniken zu tun? Gerade hier finden herausragende Marktentwicklungen statt. Weil speziell im Wireless-Bereich das Thema Sicherheit von Anfang an als Kernthema angesprochen wurde (Wardriving etc.), wurden speziell für Wireless-Lösungen Sicherheits-Konzepte entwickelt, die zu einer integrierten Sicherheits-Architektur geführt haben. Damit ist etwas durchaus Spannendes passiert. WLANs sind im Sinne dieser Architekturen sicherheitstechnisch an den kabelgebundenen LANs vorbei gezogen. Obwohl das Risiko-Potenzial im Kabel-LAN nicht kleiner ist als im WLAN, hat die starke Konzentration der öffentlichen Diskussion auf die WLAN-Sicherheit hier zu einem erheblichen Zugewinn an sinnvollen Architekturen und Gesamtlösungen geführt (siehe dazu auch die diversen Strategien der Steller: CISCO, Enterasys, Extreme, Nortel). Provokant formuliert: wer heute besondere Sicherheit im Netzwerk will, der soll über WLAN-Technik nachdenken.

Damit entsteht die Möglichkeit, eine flächendeckende Overlay-Infrastruktur zum Beispiel für mobile Endgeräte aufzubauen. Diese wird man differenzieren in Risiko-Klassen und eben für besonders riskante Geräte (dirty devices) ein separates WLAN anbieten. Einige Hersteller wie zum Beispiel Cisco gehen in die Richtung, dies mit einer WLAN-integrierten VLAN-Lösung zu machen. Sinnvoller ist aber ohne Zweifel, eigene Funkkanäle nur für „dirty devices“ vorzusehen. Dies geht technisch allerdings nur mit IEEE 802.1a/h und den dort verfügbaren 19 Kanälen in Kombination mit Access Points, die mehrere separate Radio-Teile beinhalten.

Sicherheit im Netzwerk: wo ist die Grenze?

Beispiel 3:
Personenbezogene Daten im Netzwerk

Die Übertragung personenbezogener Daten ist ein heißes Thema für jedes Netzwerk. Das Bundesdatenschutzgesetz (siehe § 9) verlangt einerseits den vollständigen Schutz der Daten und überträgt andererseits dem Betreiber die komplette Nachweispflicht für den Fall einer Anzeige eines Mitarbeiters. Für wichtige Anwendungsbereiche wie den Einsatz von WLANs im Gesundheitsbereich kann dies nur heißen, dass eine Benutzer-Authentifizierung (keine Geräte-Authentifizierung) zum Beispiel in Kombination mit einem Radius-Server umzusetzen ist. Dieser muss dann ein Logfile über alle Vorgänge führen. War dies früher ein kaum durchsetzbares Thema, so kann man aktuell feststellen, dass die dafür notwendige Architektur genau den gängigen Sicherheits-Konzepten von Wireless-Netzwerken entspricht. Es zeigt sich also, dass Sicherheit und Netzwerk-Architekturen zusammen wachsen und nicht länger als getrennte Technologien betrachtet werden können. Das Problem in diesem Trend ist, dass wir in einer Frühphase dieser Entwicklung sind und viele Produkte noch lange nicht Praxis-tauglich sind. Die Aufgabe besteht also in einer Umsetzung derartiger Architekturen mit Beschränkung auf das heute sinnvoll Machbare.

Was ist das Fazit? Wir brauchen keine isolierten Sicherheits-Komponenten, wir brauchen flächendeckende Sicherheits-Architekturen. Nur diese können den jetzt notwendigen Schutz gewährleisten. Herausragende Gedanken moderner Sicherheits-Architekturen sind die zentrale Rolle der Verzeichnis-Dienste als Speicher- und Authorisierungsort einerseits und die Schaffung von getrennten Netzwerken unterschiedlicher Sicherheitsstufen andererseits. Letzteres ist nicht wirklich neu. Zonenkonzepte gibt es seit Erfindung der Firewall. Neu sind die massiv ausgeweiteten Gestaltungs-Möglichkeiten, die speziell Wireless-Technologien in den Markt gebracht haben speziell in der flächigen Umsetzung von Zonen.

Was ist die Konsequenz? In letzter Konsequenz werden wir unsere gegebenen Netzwerk-Architekturen noch einmal stark überarbeiten. Sicherheits-Overlay-Netzwerke, Authentifizierung, IDS, ein zusätzlicher Bedarf an Datensicherheit für IP-Telephonie müssen in unsere Netzwerk-Architekturen integriert werden. Die zentrale Herausforderung liegt in der Schaffung von Lösungen, die vom Betriebsaufwand und vom Operating her tragfähig sind.

Dieser Themenbereich wird ohne Frage einer der wichtigsten Schwerpunkte des Netzwerk-Redesign-Forums im März 2004 sein. Ich gehe von einer engagierten, kontroversen und konstruktiven Diskussion aus.

Ihr Dr. Jürgen Suppan

Aktueller Kongress

12 % Frühbucherrabatt bis 31.12.03

Netzwerk-Redesign Forum 2004

29.03. - 01.04.04 in Königswinter

4 Tage Netzwerk-Redesign Forum 2004 mit Workshops zum Preis von € 1.690,-- statt regulär € 1.990,-- zzgl. MwSt.

3 Tage Netzwerk-Redesign Forum 2004 ohne Workshops zum Preis von € 1.430.-- statt regulär € 1.690,-- zzgl. MwSt.

Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Kongress-Anmeldung

Ich melde mich an für das
Netzwerk-Redesign Forum 2004

☐ **vom 29.03. - 01.04.04 mit Workshop**
zum Preis von € 1.610,-- zzgl. MwSt.*

☐ **vom 29.03. - 31.03.04 ohne Workshop**
zum Preis von € 1.430,-- zzgl. MwSt.*

*Frühbucherpreise gültig bis 31.12.03

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Top-Event

Netzwerk-Redesign Forum 2004

Analyse und Übersicht der aktuellsten Netzwerk-Technologien und Marktentwicklungen

Vom 29. März bis 1. April veranstaltet die ComConsult Akademie im Maritim Hotel Königswinter das Netzwerk-Redesign Forum 2004.

Wie in jedem Jahr so wird sich hier auch 2004 die Branche treffen. Die Mischung aus hersteller-neutralen Top-Referenten, den neuesten Technologie-Entwicklungen, hochaktuellen Projekterfahrungen und direkt umsetzbaren Empfehlungen aus der Praxis, einer hochaktuellen Ausstellung, der gleichzeitigen Anwesenheit vieler relevanter Hersteller hat diesen Kongress zum jährlichen Treffpunkt der Branche gemacht.

Dieser Spitzenkongress bietet auch in diesem Jahr wieder hochaktuelle Themenblöcke (siehe Kasten).

Auch in diesem Jahr besteht die Möglichkeit, die Veranstaltung 3-tägig oder 4-tägig zu buchen. Am 4. Tag bieten wir den Teilnehmern Spezial-Workshops zu ausgesuchten Top-Themen. Dabei wird der Stand der Technik und der optimale Betrieb wichtiger Technologien intensiv über den ganzen Tag evaluiert. Die Teilnehmer können dabei zwischen den Workshops wechseln. Zurzeit sind folgende Workshops geplant:

- IP-Telefonie: Evaluierung und Marktanalyse
- Sicherheit im Netzwerk: was macht Sinn, was hat sich bewährt, wie sieht eine sinnvolle Integration in ein Gesamt-Szenario aus?
- Produkttests praxisnah und wirtschaftlich durchführen: Methoden, Erfahrungen, Empfehlungen

.

Netzwerk-Redesign Forum 2004 – Die Themen

Standardisierung und Technologie-Entwicklung:
- Was passiert hinter den Kulissen, was ist neu, wie relevant ist es?
- Welche neuen Standards sind verabschiedet, welche stehen vor der Tür?
- Was passiert in den Labors der Hersteller?

Optimierung des Netzwerk-Betriebs:
- Wie kann ein Netzwerk besser betrieben werden?
- Welche neuen Management-Konzepte gibt es?
- LAN-Analyse im Umbruch

Hersteller und Produkte:
- Wie positionieren sich die Hersteller?
- Wie entwickeln sich wichtige Netzwerk-Produkte?
- Welche Vorteile können genutzt werden?

Sicherheit und Netzwerke:
- Welchen Stellenwert haben Sicherheits-Lösungen im Netzwerk?
- Netzwerk, Server, Applikation: wo wird Sicherheit am besten umgesetzt?
- Effizienter SmartCard-Einsatz: vom VPN zur Mail-Verschlüsselung

RZ-Strukturen 2004:
- Integration Server und Netzwerk
- Neue Anforderungen an IP-Management
- Welche Anforderungen an Verzeichnisdienste und IP-Management generiert die neue Generation von Active Directory?
- Integration der Benutzer-Verwaltungen von Windows und Linux

Corporate Networks im Umbruch:
- Welche Alternativen bestehen?
- Remote Access und Standort-Verbindungen neu gestalten
- VPN-Technologien neuester Stand

IP-Telefonie erfolgreich einsetzen:
- Wo steht IP-Telefonie im Markt?
- Wer hat die beste Lösung?
- Siemens versus CISCO: welcher liegt vorne?

Wireless LAN:
- Auf dem Weg zur Massentechnologie
- Wo steht die Produkt-Technologie, was bringen die neuen Produkte
- Senkung der Netzwerk-Kosten durch optimierte Kabel-/Wireless-Kombination
- Szenario: Medizinischer Bereich
- Szenario: Notebooks von Führungskräften
- Szenario: alternative Sicherheits-Konzepte: welcher Ansatz ist betriebstechnisch sinnvoll?

Ethernet in der Industrie:
- Umgebungsanforderungen
- Feldbus-Verdrängung
- Realzeiteignung und Verfügbarkeit
- Verkablung im Produktionsbereich
- Strategien der SPS-Hersteller

Workshops:
- IP-Telefonie
- Sicherheit im Netzwerk
- Produkttests

Der Veranstalter behält sich Änderungen im Programm vor.

Zweitthema Dezember 2003

Mobility mit Security in einer unsicheren Welt – Konsequenzen aus den Wurmangriffen in 2003

Dr. Behrooz Moayeri ist Mitglied der Geschäftsleitung der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrungen zurück. In den letzten Jahren hat Dr. Moayeri zahlreiche führende deutsche Unternehmen bei der Konzipierung und Planung von IT- und Kommunikations-Lösungen erfolgreich beraten.

moayeri@comconsult.com

Fortsetzung von Seite 1

Praktisch das ganze Jahr über dauerten (und dauern) die Wurmangriffe à la Slammer, Blaster & Co. an, wobei die Öffentlichkeit nur von den dramatischen ersten Wellen der Attacken Notiz nahm. Neu bei den Vorfällen war die Tatsache, dass im großen Maße nicht nur Server und Endgeräte, sondern auch Netze von den Würmern des Jahres 2003 in die Knie gezwungen wurden.

Gleichzeitig war 2003 das Jahr der Mobility. Intel startete eine breit angelegte Werbekampagne und brachte damit das Wort Wireless LAN zu bester Stunde ins Fernsehen. Die Verkaufszahlen für Notebooks sind auf dem Weg, die Größenordnung des Absatzes nichtmobiler Rechner zu erreichen. Provider wie die Deutsche Telekom folgten dem Beispiel von Intel und den Notebook-Herstellern. Nicht nur Notebooks mit integrierten WLAN-Chips, sondern eine Vielzahl kleinerer WLAN-Endgeräte sind in diesem Jahr auf den Markt gekommen. WLAN wurde in 2003 zum Inbegriff der Flexibilität und Mobilität. Man versucht an die Erfolgsstory des Mobilfunks anzuknüpfen und nach „Telefonieren überall und ohne Kabel“ nun Kunden für „Internet überall und ohne Kabel“ zu gewinnen. Dabei wird zum Beispiel auf den Werbeplakaten der Deutschen Telekom nicht nur das Internet erwähnt, sondern auch die Möglichkeit, über das Internet auf Unternehmensnetze zuzugreifen. Das Schlagwort dafür war in 2003 WLAN und nicht UMTS.

Jahrzehntelange Erfahrungen zeigen, dass IT-Benutzer neue für sie interessante Möglichkeiten und Features auch dann in Anspruch nehmen, wenn die Fragen der Sicherheit der neuen Technik nicht endgültig geklärt und damit neue Risiken für den Anwender nicht ausgeschlossen sind. Im Falle von „Internet überall“ bzw. „Datenkommunikation und Datenverarbeitung überall“ sind es Mobilität und Flexibilität, die auch auf Kosten der Sicherheit mit offenen Armen aufgenommen werden. Wenn man die beiden großen Entwicklungen des Jahres – mehr schadensstiftende Software und der Trend zu mobilen drahtlosen Endgeräten – nebeneinander betrachtet, erkennt man eine der größten Herausforderungen für die Planer und Betreiber von Unternehmensnetzen. Diese Herausforderung ist in komprimierter Fassung als „Mobility und Security in einer unsicheren Welt“ zu formulieren.

Der vorliegende Artikel beschreibt zunächst in Kurzform einige Angriffsmuster aus dem nun hinter uns liegenden Jahr und zieht daraus Konsequenzen für die Sicherheitsarchitektur in den Unternehmensnetzen. Dabei wird die zunehmende Nachfrage nach Mobilität und Flexibilität berücksichtigt. Mobilität ist ein Produktivitätsfaktor. Nach einer Studie bedeutet die durch den WLAN-Einsatz ermöglichte Flexibilität einen Produktivitätsgewinn von bis zu 14.000,00 US-$ pro Mitarbeiter und Jahr[1].

[1] 2003 Wireless LAN Benefit Study, NOP World Technology im Auftrag von Cisco Systems, November 2003.

Mobility mit Security in einer unsicheren Welt – Konsequenzen aus den Wurmangriffen in 2003

Neue Angriffsmuster

2003 war das Jahr neuer Angriffsmuster, bei denen das Eindringen nur eines einzigen Paketes in ein Unternehmensnetz ausreichte, um lawinenartig eine Vielzahl von Servern und Clients zu verseuchen und gleichzeitig auch LAN und WAN so stark zu belasten, dass in Folge des Angriffs oft stunden- oder gar tagelang „nichts mehr ging".

Der erste Vertreter dieses neuen Angriffstyps war der Slammer. Der Autor hat bereits im März 2003 in einem Artikel als Nachlese zum Slammer-Angriff die Anatomie dieses Angriffs beschrieben[2]. Der Angriff legte erstmalig im Januar 2003 weite Teile des Internet sowie viele Unternehmensnetze lahm. Der Wurm bediente sich einer bereits seit sechs Monaten öffentlich bekannten Sicherheitslücke in zwei weit verbreiteten Microsoft-Produkten, für die es schon die ganze Zeit seit Juli 2002 die korrigierenden Patches gegeben hat. Bei den betroffenen Microsoft-Produkten handelte es sich um den Microsoft SQL Server 2000 und Microsoft Data Engine (MSDE) 2000. Der Slammer provozierte mit einem einzigen Paket einen Pufferüberlauf auf dem Angriffsziel, brachte somit ein Stück Software auf dem Zielrechner zum Laufen und legte ein sehr aggressives Verteilungsverhalten zutage. Es wurden wahllos Pakete an zufällig gewürfelte IP-Adressen gesendet, gerichtet an den UDP-Port 1434. Sowohl Unicast- als auch Multicast-Adressen wurden als Ziel ausgewählt. War ein ungepatchter SQL-Server in einem Netz vom Wurm befallen, brauchte der Wurm nur Sekunden oder gar Sekundenbruchteile, um im selben Netz alle anderen ungepatchten SQL Server zu verseuchen.

Ähnlich ging der MS Blaster vor, mit dem Unterschied, dass statt des Ports 1434 der UDP-Port 135 verwendet wurde, der praktisch auf jedem Windows-System aktiviert ist und der Kommunikation im Rahmen der Microsoft RPC (Remote Procedure Call) dient.

Der Wurm sendete in beiden Fällen viele Pakete, welche die Prozessoren der Netzkomponenten beschäftigten, da die Pakete nicht in die Muster für die Bearbeitung durch die schnelle Forwarding-Hardware der Switches passten. Die Grenzen für die Häufigkeit solcher Pakete waren die Grenzen der Leistungsfähigkeit der befallenen Rechner. Jede moderne PC-Plattform kann Tausende, wenn nicht gar Zehntausende Pakete pro Sekunde senden. Gibt es davon Dutzende in einem Netz, erreicht die aggregierte Last schnell Größenordnungen, welche die Leistungswerte der Prozessoren in den Switches überschreiten. Die betroffenen Netzkomponenten waren nur noch mit der Verarbeitung der vom Wurm gesendeten Pakete beschäftigt. So kam es zum Zusammenbruch der Netze.

Sind nur jene Netze von Computerwürmern gefährdet, die mit dem Internet verbunden sind? Die Erfahrungen von 2003 sagen leider etwas anderes. Die mit Zeitverzögerung im Vergleich zur ersten Verbreitungswelle über das Internet ins Rollen gekommenen Slammer- und MS-Blaster-Lawinen befielen auch Netze ohne jegliche Verbindung zum Internet oder mit einer hinreichend geschützten Verbindung zum Internet. Man stelle sich zum Beispiel eine Umgebung vor, die mit Windows-basierenden Industriesteuerungen arbeitet. Diese Systeme werden oft einmal installiert und dann jahrelang nicht mehr geändert. Das fordern sogar einige Vorschriften der Qualitätssicherung. Folglich werden auf diesen Systemen auch kaum Hofixes und Security Patches installiert. Dann reicht oft ein einziges Paket, um die Systeme zu verseuchen und die ganze Umgebung zum Erlahmen zu bringen. Gleiches gilt für viele IP-Telefonie-Server.

Wie soll das erste verseuchende Paket in ein isoliertes Netz gelangen? Man brauche nur an folgendes Szenario zu denken: Ein Techniker (vielleicht von einer Fremdfirma) reist an und hat die Lösung für ein dringendes Problem oder eine Software-Erweiterung auf seinem Notebook. Gemäß den Sicherheitsrichtlinien wird der Techniker gefragt, ob er den aktuellsten Virenscanner auf seinem Notebook habe. Nachdem der Techniker dies versichert, wird sein Rechner an das Netz angeschlossen. Binnen Sekunden ist das ganze Netz lahmgelegt. Der Techniker hatte kurz vor seinem Einsatz aus dienstlichen oder privaten Gründen sein Notebook an das Internet angeschlossen. Er hat zwar den aktuellsten Virenscanner darauf, aber der aktuellste Virenscanner taugt nichts gegen das aktuellste Virus. Das Notebook ist verseucht. Wie Notebook-Benutzer es häufig tun, fährt der Techniker seinen Rechner nicht herunter, sondern versetzt ihn lediglich in den „Schlafmodus". Damit wird der vollständige Inhalt des Arbeitsspeichers einschließlich auch jener Würmer konserviert, die sich nicht auf der Festplatte verewigen (von den anderen Viren zu schweigen). Beim Erwecken des Rechners aus dem Schlafmodus ist der Wurm wieder aktiv.

[2] B. Moayeri, „Slammer und die Lehren" in Der Netzwerk Insider, Security Special 2003

Mobility mit Security in einer unsicheren Welt – Konsequenzen aus den Wurmangriffen in 2003

Dieses Szenario kann nicht nur von mobilen Rechnern der Fremdfirmenmitarbeiter, sondern auch von den firmeneigenen Notebooks verursacht werden, die wechselweise an das Internet und das Unternehmensnetz angeschlossen werden. Dies ist im Verlauf des Jahres 2003 genau gemäß dem dargestellten Ablauf eingetreten.

Vor solchen Angriffen kann sich nur ein Unternehmen schützen, welches das dargestellte Szenario und alle ähnlichen Szenarien ausschließen kann. Da reicht nicht eine superfeste Firewall oder gar die völlige Trennung vom Internet.

Die Internet-Firewalls der meisten dem Autor bekannten Firmen standen so fest, dass sie den Angriffen wacker standhielten. Es waren oft die „Hintertürchen", die von den Würmern ausgenutzt wurden.

Zielkonflikt: Flexibilität und Sicherheit

Nicht als Spielzeug, sondern als mittlerweile unverzichtbare Werkzeuge zum flexiblen und mobilen Arbeiten mit IT-Anwendungen werden Notebooks und andere mobile Endgeräte in immer größerer Zahl eingesetzt.

Aber es hat immer einen Zielkonflikt zwischen Flexibilität und Sicherheit gegeben. Statt sich für Flexibilität ohne Sicherheit oder Sicherheit ohne Flexibilität zu entscheiden, bleibt den meisten Unternehmen nichts anderes übrig, als mehr in Mobilität und Flexibilität mit Sicherheit zu investieren.

Die IT-Abteilungen können die Nachfragen der Benutzer nach mehr Mobilität unter Nutzung moderner Verfahren wie WLAN nicht mehr mit dem stereotypen Satz „das Verfahren ist nicht sicher genug" beantworten. Sie sind vielmehr gefordert, eben sichere Lösungen zu finden.

Die Erfahrungen des Autors zeigen, dass es angesichts der enormen Produktivitätsvorteile für Unternehmen durch die Nutzung von mobilen Endgeräten sowie mit Hinweis auf die Erfahrungen mit schadensstiftender Software in 2003 gelingen kann, die Entscheiderebene für größere Anstrengungen im Bereich IT-Sicherheit unter Wahrung der geforderten Flexibilität der Benutzer zu gewinnen.

Nachfolgend wird ein Maßnahmenkatalog dargestellt, der aufgrund der Erfahrungen dieses Jahres entwickelt worden ist.

In dem bereits erwähnten Insider-Artikel „Slammer und die Lehren" vom März 2003 wurde auf einige erforderliche Maßnahmen hingewiesen:

- Gestaltung aller Internet-Zugänge über statusbewusste Firewalls, damit das Eindringen von schadensstiftenden Paketen in das Netz erschwert wird
- Installation der wichtigen Hotfixes und Security Patches auf allen betroffenen Systemen, zum Beispiel unter Zuhilfenahme solcher Werkzeuge wie Microsoft Software Update Services (SUS)
- Firewall-Schutz für das eigene Netze gegenüber allen Bereichen, in denen man nicht sicherstellen kann, dass die Securtiy Patches wirklich installiert, die Virenscanner aktualisiert und die Internet-Zugänge hinreichend abgesichert werden
- Installation von Software im möglichst eingeschränkten Sicherheitskontext und nicht immer unter mächtigen Konten
- Lückelose Übersicht darüber, wo im eigenen Netz welche Software installiert ist
- Strikte Trennung zwischen Test- und Hauptnetz
- Strukturierter Netzaufbau mit Layer-3-Instanzen zwischen verschiedenen Bereichen, in denen beispielsweise provisorische Filter aktiviert werden können
- Aufbau eines vom Hauptnetz strikt getrennten Outband-Management-Netzes, das auch bei Angriffen und Netzausfällen verfügbar bleibt und den Zugriff auf Netzkomponenten erlaubt
- Planung und regelmäßige Übung von Incident Response
- Definition von Zuständigkeiten für die Sicherheit in der IT-Organisation und Vorsehen von Kapazitäten für die Erfüllung der damit verbundenen Aufgaben

Alle o. g. Maßnahmen sind weiterhin dringend zu empfehlen. Hinzu kommen aus den weiteren Erfahrungen des Jahres 2003 die nachfolgend beschriebenen Schritte.

Verzicht auf die Default-Route in Netzkomponenten

Auf Netzkomponenten sollte auf die so genannte Default-Route möglichst verzichtet und stattdessen dedizierte statische Routen, Proxy-Server und ähnliche Zwischenstationen bei ausgehenden Zugriffen verwendet werden.

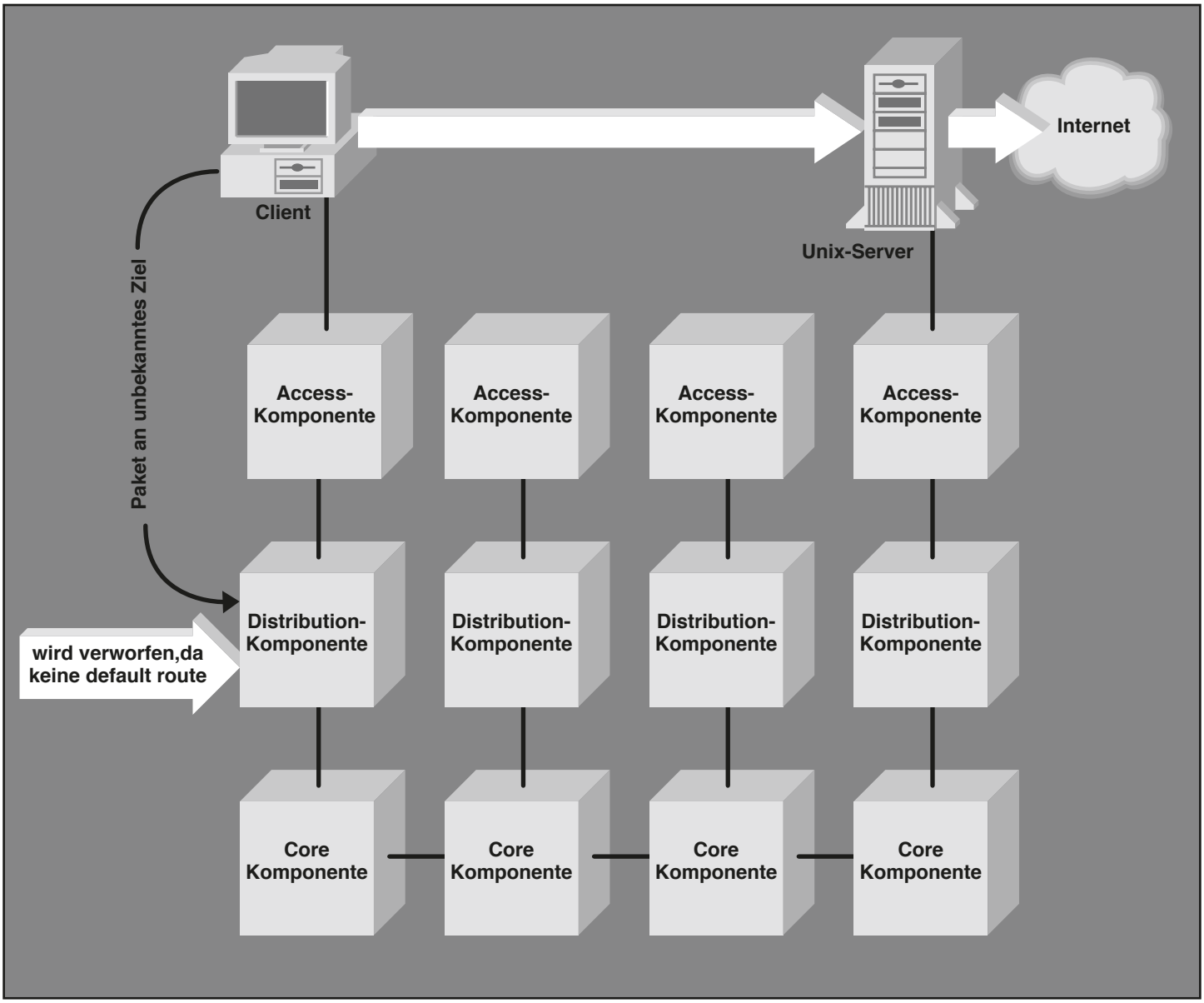
Die Default-Route führt nämlich dazu, dass die von den Würmern typischerweise willkürlich gesendeten Pakete das ganze Netz bis zur Internet-Firewall durchwandern und auf ihrem Weg alle Layer-3-Instanzen mit Paketen an unbekannte Ziele in CPU-Lastbereiche nahe 100 % treiben.

Die Default-Route wird in vielen Unternehmen für Zugriffe von innen auf das Internet benötigt, welche ohne Proxy-Funktion arbeiten, wie beispielsweise Einloggen auf Unix-Rechnern, File Transfer mit diesen von der Windows- oder Unix-Kommandozeile aus etc.

Es ist zunächst einmal zu analysieren, welche Rechner die Default-Route nutzen. In einigen Fällen werden dediziert eingestellte Routen das Problem lösen. Für die anderen Fällen muss beispielsweise ein interner Unix/Linux-Server mit einer Default-Route in Richtung Internet-Firewalls als Zwischenstation beim Zugriff auf beliebige Rechner im Internet dienen. Analog ist bei den Web-Proxy-Servern sicherzustellen, dass deren Default-Route ebenfalls in Richtung Internet-Firewalls zeigt (s. Bild 1).

In Bild 1 ist ein LAN dargestellt, das in vielen Unternehmen nach diesem Muster aufgebaut ist, nämlich bestehend aus Core-, Distribution- und Access-Switches, davon die ersten beiden mit Layer-3-Funktionalität. Dringt ein Wurm in das dargestellte Netz und befällt einige Clients, werden vom Wurm an wahllose Ziele gesendete IP-Pakete bereits von der Distribution-Komponente verworfen, da die meisten willkürlich gewählten Ziele keinem Routing-Eintrag entsprechen (bei aktiver Default-Route auf dem Distribution-Switch würde dieser die Pakete weiterleiten und zentrale Komponenten belasten).

Bild 1: Deaktivierung der Default-Route im Netz



Public-Netz

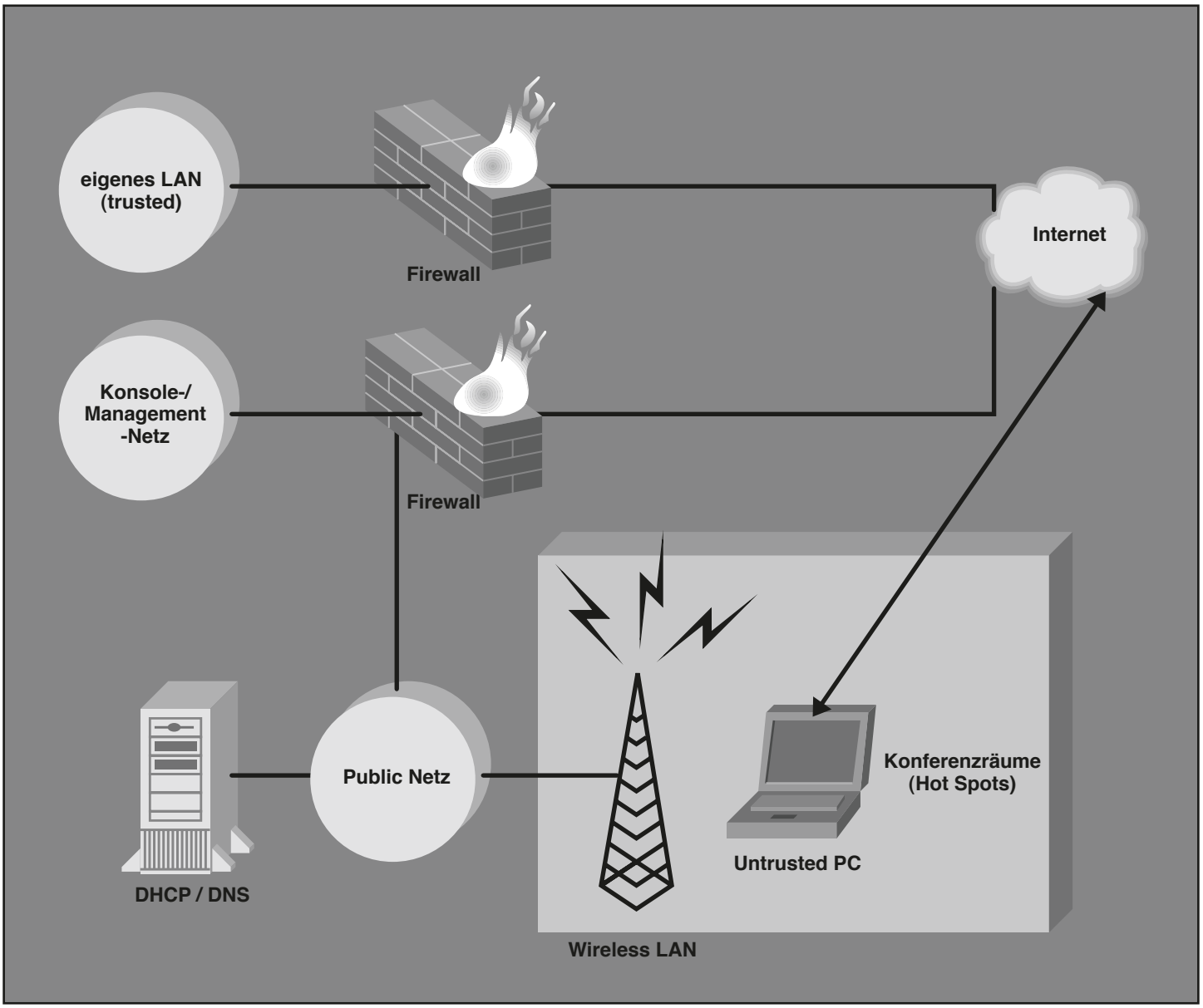
Viele Firmen müssen Gästen und Fremdfirmen die Möglichkeit gewähren, in den firmeneigenen Gebäuden Rechner an das Netz anzuschließen (um z. B. auf das Internet zuzugreifen). Diese Rechner sind in der Regel nicht vertrauenswürdig in dem Sinne, dass sie nach dem erforderlichen Standard vor schadensstiftender Software geschützt sind. Der Anschluss solcher Rechner an das unternehmensinterne Netz stellt somit ein Risiko dar.

Die Schaffung eines Public-Netzes inkl. WLAN und Hot Spots zum Beispiel in Besprechungsräumen dient der Trennung von nicht vertrauenswürdigen Rechnern mit Kommunikationsbedarf vom Hauptnetz. Das Public-Netz ist in Bild 2 dargestellt.

Das Public-Netz verbindet über drahtgebundene und drahtlose Verfahren die internen Hot Spots mit dem Internet und ist vom Hauptnetz getrennt. Das Public-Netz ist über ein Firewall-System mit dem Internet verbunden, damit die untrusted PC vom Public-Netz aus auf das Internet zugreifen können. Die trusted PC können über das Public-Netz und das Internet auf das VPN der eigenen Firma und damit auf sämtliche interne Anwendungen zugreifen, ohne vom Public-Netz gefährdet zu sein, da sie nur einen verschlüsselten Tunnel zum VPN Gateway unterhalten. Somit können auch eigene Mitarbeiter der Firma das Public-Netz sinnvoll nutzen, wenn sie zum Beispiel im Firmengelände unterwegs sind und in Besprechungsräumen das Public-LAN bzw. Public-WLAN nutzen. Vom Management-Netz aus kann das Public-Netz über das dargestellte Firewall-System administriert und überwacht werden.

Damit die angeschlossenen Geräte mit passender IP-Konfiguration versehen werden und Namen in IP-Adressen auflösen können, ist ein eigener DHCP/DNS-Server im Public-Netz erforderlich.

Bild 2: Public-Netz



Eigene mobile Clients

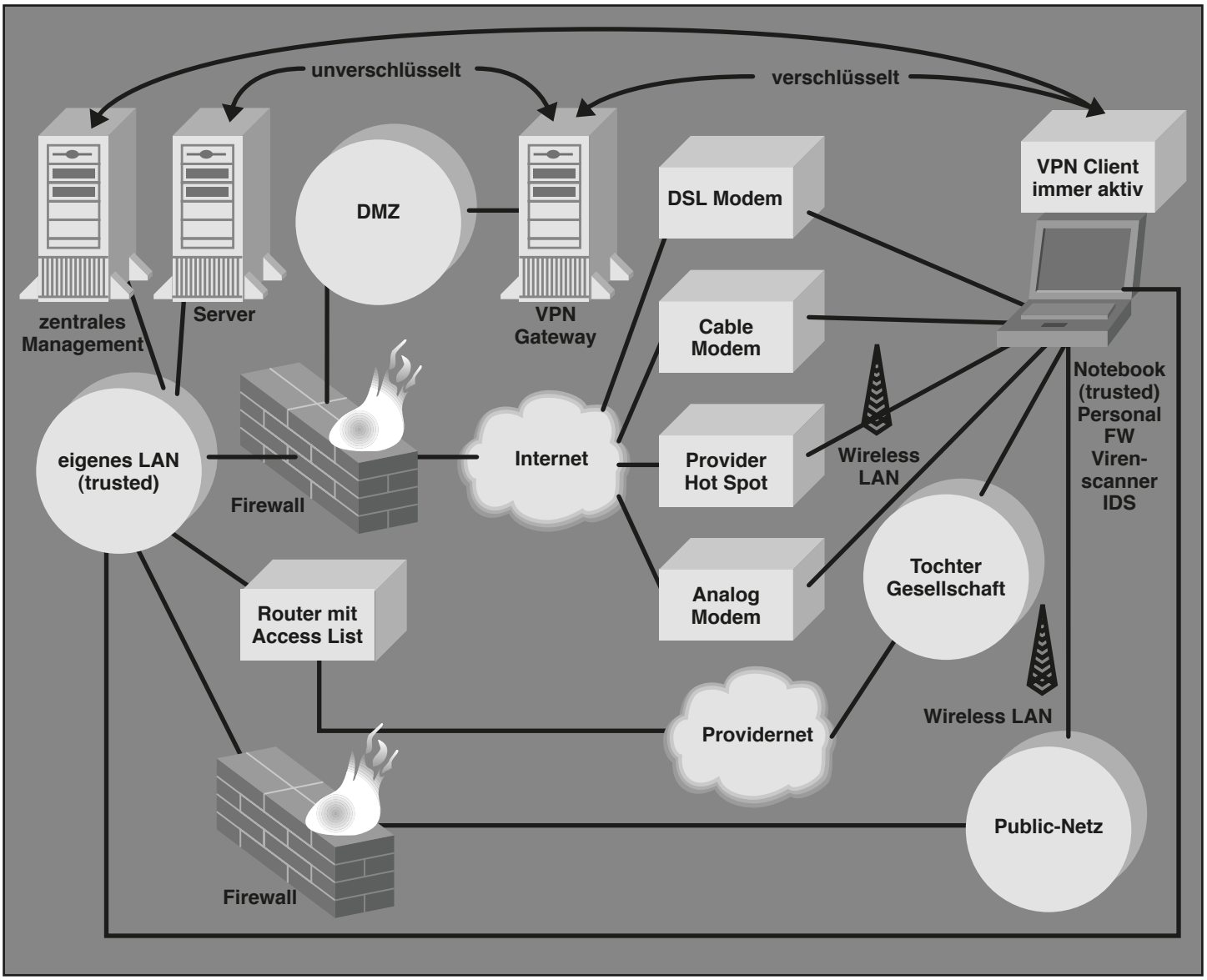
Damit die eigenen mobilen trusted Clients eines Unternehmens bei Anschluss an nicht ganz vertrauenswürdige Netze (Internet, Netze anderer Firmen, internes Public-Netz) nicht gefährdet bzw. infiziert werden, müssen sie mit den ständig aktiven Modulen VPN Client, Personal Firewall, Virenscanner und Intrusion Detection System versehen werden. Zentrales Management aller dieser Komponenten ist von essenzieller Bedeutung.

Der mobile Standard-Client ist in Bild 3 dargestellt.

Der mobile Standard-Client ist mit einem ständig aktiven VPN-Client ausgestattet. Verbindungen dieses Clients mit dem VPN Gateway der eigenen Firma und darüber mit allen internen Ressourcen sind über folgende Wege möglich (Bild 3 in der Reihenfolge von unten nach oben):

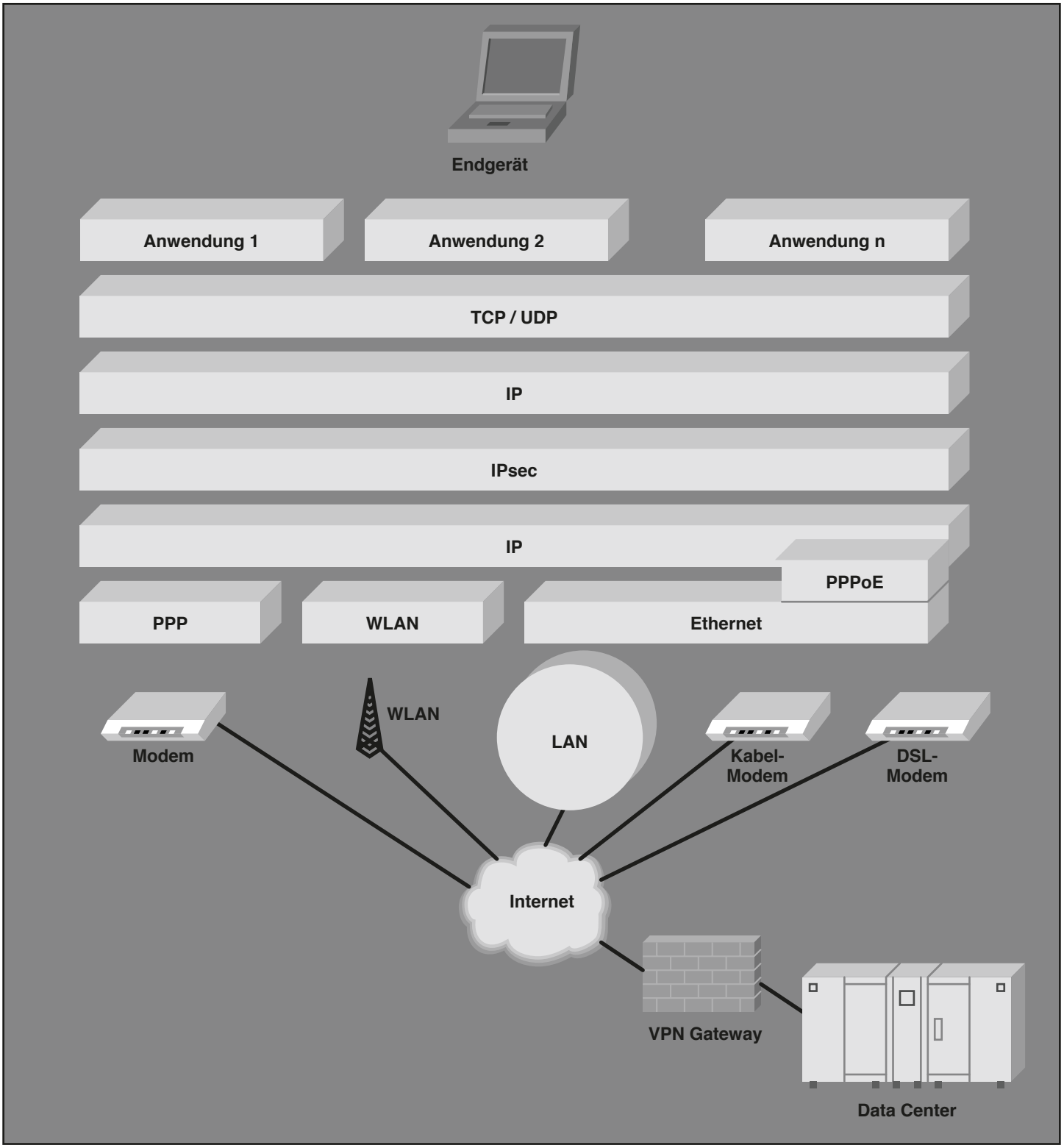
- Direktanschluss an das LAN der eigenen Firma: Dazu ist eine 10/100BaseT-Karte erforderlich.
- Anschluss an das Public-Netz der eigenen Firma: Dazu ist eine 10/100BaseT-Karte oder eine WLAN-Karte erforderlich.
- Anschluss an das Netz einer anderen Firma wie zum Beispiel einer ausländischen Tochtergesellschaft mit abweichendem Sicherheitsstandard: Dazu ist eine 10/100BaseT-Karte oder eine WLAN-Karte erforderlich.
- Anschluss an das Internet über einen Provider mit Dial-In-PoPs: Dazu ist ein analoges Modem erforderlich.
- Anschluss an das Internet über einen Provider mit WLAN-Hotspot: Dazu ist eine WLAN-Karte erforderlich.
- Anschluss an das Internet über ein Cable Modem: Dazu ist eine 10/100BaseT-Karte erforderlich.
- Anschluss an das Internet über ein DSL-Modem: Dazu ist eine 10/100BaseT-Karte erforderlich.

Bild 3: Mobiler Standard-Client



Das heißt, dass der mobile Standard-Client mit den drei physikalischen Netzschnittstellen analoges Modem, Ethernet und WLAN auskommt und weltweit eine VPN-Verbindung zur eigenen Firma aufbauen kann. Diese drei Komponenten sind Bestandteile der meisten heute verkauften Notebooks. Unter den Schnittstellen, die in Bild 4 dargestellt sind, gewinnt WLAN aufgrund der damit verbundenen Flexibilität und Benutzerfreundlichkeit zunehmend an Bedeutung.

Bild 4: VPN über verschiedene Schnittstellen



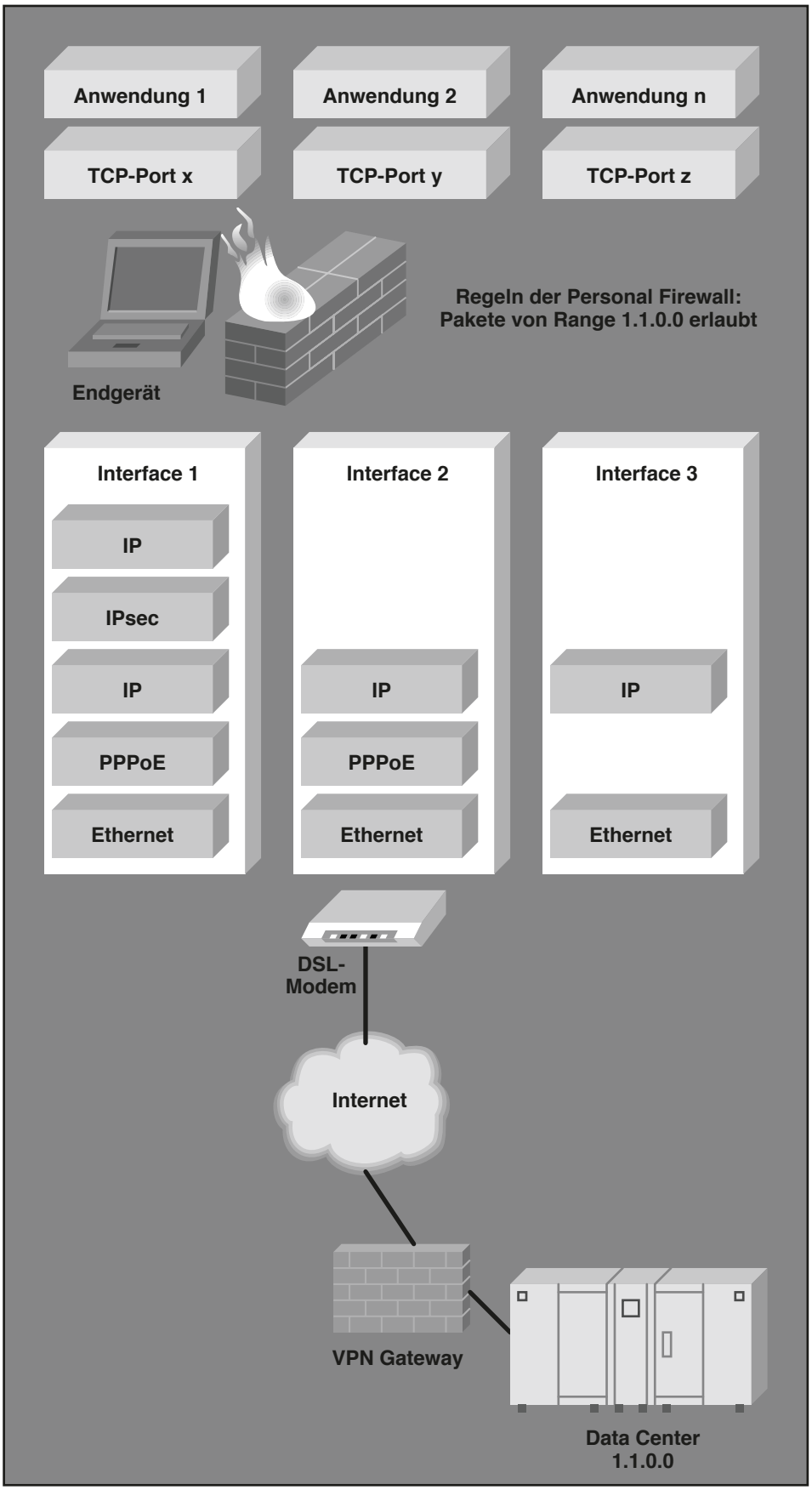


Bild 5: Unterbindung aller Kommunikation bis auf solche über den VPN-Tunnel

Der ständig aktive VPN Client schützt den Rechner vor allen mit Verbindungen zu untrusted-Netzen zusammenhängenden Gefahren, da eine Kommunikation nur über den Tunnel möglich ist. Andere Kommunikationsbeziehungen müssen unterbunden werden (s. Bild 5).

Der VPN-Tunnel führt zum Firmennetz. Auch Zugriffe über das Internet müssen über diesen Tunnel getätigt werden. Die Clients müssen mit zentral managebaren Personal Firewalls, Virenscannern und Intrusion Detection Agents geschützt werden. Wichtig ist auf jeden Fall das zentrale Management für Virenscanner, Personal Firewalls und Intrusion Detection Agents auf den Notebooks. Die Komplexität eines solchen Vorhabens im Zusammenhang mit den Applikationen ist nicht zu unterschätzen, wie auch die Erfahrungen vieler Firmen mit dem Virenschutz zeigen.

Im Zusammenhang mit der Nutzung von IPsec-basierenden VPN dürfen natürlich die technischen Herausforderungen nicht unterschätzt werden. Auf einige dieser Herausforderungen wurde in einem Artikel der November-Ausgabe des Netzwerk Insider eingegangen[3].

Weitere Herausforderungen sind:

- Benutzerverwaltung
- Schlüsselverwaltung
- Zertifikatsverwaltung
- Client Management

Allen diesen Herausforderungen muss bei gleichzeitiger Einbindung in die unternehmensweite Verzeichnisstruktur begegnet werden. Unlösbar sind die damit verbundenen Probleme nicht. Die Lösung erfordert jedoch sorgfältige Planung und teilweise die Investition in neue Werkzeuge.

---

[3] Andreas Meder, „Problematische VPN-Aspekte – Redundanz und NAT“, veröffentlicht in Der Netzwerk Insider, November 2003.

Neues Seminar

Storage-Netze: Technologie und Lösungen in der Analyse

Vom 9. bis 11. März 2004 veranstaltet die ComConsult zum ersten Mal ihr neues Seminar "Storage-Netze: Technologie und Lösungen in der Analyse" im Hilton Hotel in Bonn.

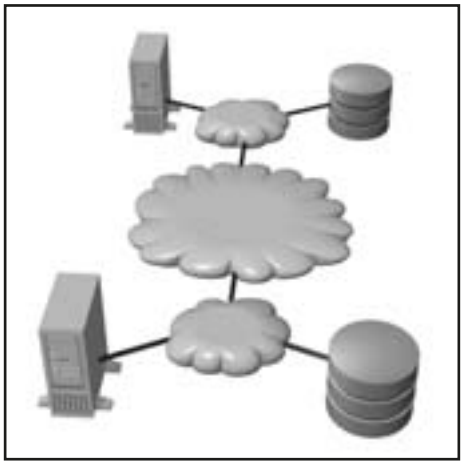
Die Zentralisierung von Speicher in der Form von Storage-Netzen ist die unverzichtbare Basis fast aller Konsolidierungs- und Optimierungs-Projekte. Die Vorteile reichen von der Kostensenkung über die flexiblere Nutzung bis hin zu vereinfachtem Backup und Disaster Recovery.

Die angebotenen Produkte basieren auf unterschiedlichen Technologien, selbst innerhalb einer Technologie ist Interoperabilität zwischen Herstellern nicht die Regel. So erfordert die Planung und Umsetzung von Storage-Netzen eine sorgfältige Analyse der konkurrierenden Lösungsansätze.

Dieses hochaktuelle Seminar arbeitet die verfügbaren Technologien und Produktansätze auf und analysiert ihre Nutzbarkeit und die damit erreichbare Lösungsqualität.

Im Einzelnen beinhaltet das Seminar folgende Themen:

- Storage-Netze: Stand der Technik, Entwicklungstrends, Motivation
- Standardisierung: wer macht was, was ist relevant
- Standards im Überblick: FibreChannel, SCSI, FCIP, Infiniband
- Reichweiten und Performance: wo liegen die Grenzen



- Lösungsansätze in der Analyse: DAS; NAS; SAN, iSCSI
- SAN-Lösungen: Technologie-Alternativen und Komponenten im Vergleich, für wen ist wann was geeignet
- Schlüsselfaktor Sicherheit: Zoning, Masking, ACLs
- Virtualisierung: was leistet sie, macht sie überhaupt Sinn, wo liegen Vor- und Nachteile
- Management: InBand kontra OutBand
- Migration: was ist zu beachten
- Datensicherung: Konzepte und Lösungen in der Analyse
- Hochverfügbarkeit: 2-Standort-Lösungen, Clustering, Disaster Recovery

Aus dem Inhalt

Motivation: Daten als Unternehmensressource, Datenexplosion, Storage-Kosten

Standards und Protokolle: Erläuterung der Standards und der Drafts, Theoretische Performancewert und Reichweiten

Varianten und deren Gegenüberstellung: DAS, NAS, SAN, iSCSI

Darstellung der unterschiedlichen SAN-Topologien, die realisierbar sind: Single-Fabric, Dual-Fabric, Arbitrated Loop, Vermaschte Netze, Trunking

SAN-Komponenten: HBA, Hub, Switch, Bridge, Director, Speichersystem

Sicherheit: Zoning, Masking, ACLs

Virtualisierung auf den unterschiedlichen Ebenen: Server, SAN, Storage

Management: InBand/OutBand

Realisierbare Heterogenität: Open Systems und Mainframe, Herstellervielfalt

Migration: Umstellung im laufenden Betrieb

Datensicherung und –wiederherstellung: Virtuelle Sicherungssysteme, Dezentrale/Zentrale Sicherung, LANless Backup, ServerFree Backup, Cloning, Snapshot, Virtualisierung, Archivierung, HSM , Einsatz des NDMP

Hochverfügbarkeit: 2-Standorte Konzept, Clustering, Disaster Recovery

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Storage-Netze

Ich buche das Seminar
Storage-Netze: Technologie und Lösungen in der Analyse
zu folgendem Termin

☐ 09.03. - 11.03.04 Bonn
☐ 14.06. - 16.06.04 Berlin
(Preis € 1.690,-- zzgl. MwSt.)

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

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ, Ort
eMail	Unterschrift

Studie des Monats

Wireless LAN : Interoperabilität zwischen 802.11b und 802.11g

Aus dem neuen ComConsult Research Wireless LAN Grundlagen Report*

Lesen Sie eine Zusammenstellung aus den Kapiteln
4.3 Übertragungstechnik (PHY-Layer)
4.3.3 Extended High Rates nach 802.11g
4.3.3.1 Optionale Modulationen im 802.11g
4.3.4 Interoperabilität zwischen 802.11b und 802.11g

Übertragungstechnik (PHY-Layer)

Der Physical Layer (PHY) des IEEE 802.11 ist in zwei Sublayer aufgeteilt. In der ersten Schicht „Physical Medium Dependent" sind die schnittstellenspezifischen Funktionen der verschiedenen physikalischen Schnittstellen und die zugehörenden Übertragungstechniken festgelegt. In der zweiten Schicht stellt das PLCP (Physical Layer Convergence Protocol) dem übergeordneten, gemeinsamen MAC-Layer einheitliche, technologie-spezifische Schnittstellen zur Verfügung.

Im ursprünglichen Standard 802.11 von 1997 sind drei physikalische Schnittstellen definiert:

- DSSS im 2,4-GHz-Band,
- FHSS im 2,4-GHz-Band und
- eine Infrarot-Schnittstelle.

Daneben definiert der Standard 802.11a eine vierte Schnittstelle im 5-GHz-Band mit Übertragungsraten bis 54 Mbit/s.

Nach 1999 wurde dann in mehreren Schritten das DSSS-Interface im 2,4-GHz-Band erweitert. Zunächst wurden mit dem Standard IEEE 802.11b die Übertragungsraten auf 11 Mbit/s erweitert. Hierzu wurde mit CCK ein erweitertes Modulationsverfahren definiert, welches mit derselben Taktrate arbeitet wie das DSSS-Interface. Optional beschreibt der 802.11b ein zweites Modulationsverfahren PBCC mit denselben Übertragungsraten. Darüber hinaus sieht der Standard für beide Modulationen ein optionales, kürzeres Headerformat vor.

Dieser 11b-Standard wird 2003 durch den Standard 802.11g nochmals erweitert. Hier wird die gesamte OFDM-Technologie des 802.11a mit allen Formaten in das 2,4-GHz-Band übernommen. Damit werden auch hier Übertragungsraten bis 54 Mbit/s zur Verfügung gestellt. Zusätzlich können alle Systeme nach 802.11g kompatibel zu 802.11b betrieben werden und unterstützen daher beide Header-Formate des 11b.

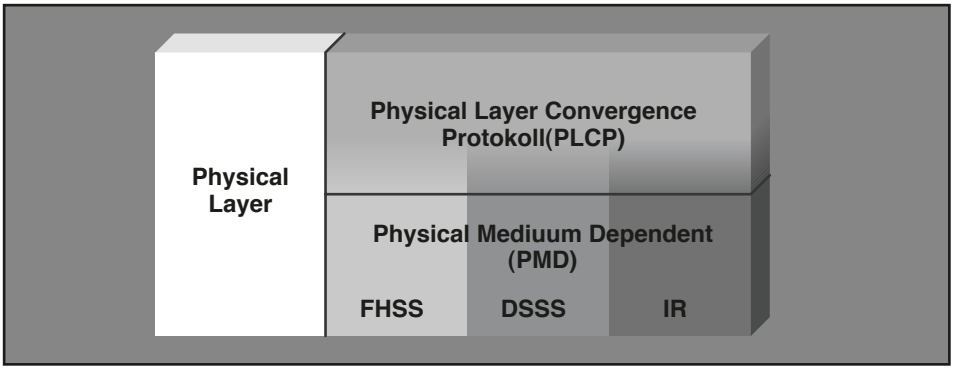


Bild 1: Physical Layer

Zwei weitere Modulationsverfahren ergänzen das Portfolio: eine Erweiterung der PBCC-Modulation unterstützt Übertragungsraten bis 33 Mbit/s und eine Mischform aus 11b-Header und OFDM-Datenteil mit den OFDM-Raten bis zu 54 Mbit/s. Beide optionale Formate werden mit beiden 11b-Headerformaten unterstützt.

Die folgende Tabelle fasst die zurzeit definierten Schnittstellen zusammen.

Tabelle1: Physikalische Schnittstellen des 802.11

IEEE 802.11:		
I.	DSSS	
II.	FHSS	
III.	Infrarot	
IEEE 802.11b:		
IV.	DSSS/CCK	umfasst I.
V.	DSSS/CCK/short	optional, umfasst IV.
VI.	DSSS/PBCC	optional, umfasst IV.
VII.	DSSS/PBCC/short	optional, umfasst VI.
IEEE 802.11g:		
VIII.	OFDM	umfasst V.
IX.	DSSS/PBCC	optional, umfasst VII. und VIII.
X.	CCK-OFDM	optional, umfasst VIII.
IEEE 802.11a:		
XI.	OFDM	

* Wireless LAN Grundlagen, ComConsult Research Technologie Report,
zu beziehen über den Verlag ComConsult Technologie Information (weitere Informationen unter **www.comconsult-research.com**)

Extended High Rates nach 802.11g

Mit der zweiten Erweiterung von 2003 wurden weitere Modulationsverfahren für das Interface festgelegt. Verpflichtend für alle Systeme nach 802.11g wird das OFDM-Verfahren aus dem Standard IEEE 802.11a aus dem 5-GHz-Band in das 2,4-GHz-Band übernommen. Dieses Verfahren stellt acht weitere Übertragungsraten mit 6, 9, 12, 18, 24, 36, 48 und 54 Mbit/s zur Verfügung, wobei lediglich 6, 12 und 24 Mbit/s verpflichtend für alle Systeme vorgeschrieben sind.

OFDM (Orthogonal Frequency Division Multiplexing) verwendet eine gänzlich andere Modulationstechnologie als die bisher beschriebenen Verfahren. OFDM unterteilt prinzipiell den verfügbaren Frequenzbereich in mehrere Unterkanäle (Carrier). Das Datensignal wird meist über geeignete fehlertolerante Kodierungen abgesichert und dann auf den Unterkanälen parallel übertragen.

Der Standard 802.11a legt pro Kanal 52 Unterkanäle fest, von denen jedoch vier zur Synchronisation genutzt werden und nur 48 zur Datenübertragung zur Verfügung stehen. Der Datenstrom wird über Vorwärtsfehlerkorrektur-Codes im Verhältnis 1:2, 2:3 oder 3:4 gesichert, auf die Unterkanäle verteilt und dort mit vier möglichen Modulationsverfahren übertragen. Die vom Standard unterstützten Modulationen und die daraus resultierenden Übertragungsraten sind in der folgenden Tabelle 2 aufgelistet.

Zusätzlich zu den OFDM-Verfahren fordert der 802.11g-Standard, dass alle Systeme auch die DSSS/CCK-Modulation nach 802.11b unterstützen, und zwar sowohl in der Long-Header-Version als auch mit Short Headers. Damit muss bei 11g-Produkten das Short-Header-Format verpflichtend von allen Systemen unterstützt werden.

Optionale Modulationen im 802.11g

Wie im 802.11b-Standard führt auch der 802.11g-Standard die optionalen PBCC-Modulationsverfahren weiter. Nach den 5,5- und 11-Mbit/s-Varianten nach 802.11b definiert der neue Standard zwei weitere Varianten mit 22 Mbit/s und 33 Mbit/s. Für beide Verfahren wird die 1/2-Kodierung durch eine 2/3-Kodierung ersetzt. Das hiermit aus je zwei Datenbits entstehende Trible wird jeweils einem Symbol zugeordnet und über eine 8-wertige PSK übertragen.

Kodier-Verhältnis	Modulation	Kodierte Chips pro Carrier	Bits pro Symbol
1 : 2	BPSK 1	24	6 Mb/s
3 : 4	BPSK 1	36	9 Mb/s
1 : 2	QPSK 2	48	12 Mb/s
3 : 4	QPSK 2	72	18 Mb/s
1 : 2	16-QAM 4	96	24 Mb/s
3 : 4	16-QAM 4	144	36 Mb/s
2 : 3	64-QAM 6	192	48 Mb/s
3 : 4	64-QAM 6	216	54 Mb/s

Tabelle 2: Modulationsverfahren und Datenraten nach IEEE 802.11a

Bleibt man also bei der bekannten Taktrate von 11 MChip/s erhält man eine Datenübertragungsrate von 22 Mbit/s. Um die Datenrate von 33 Mbit/s zu erreichen, muss die bis dahin unveränderte Taktrate auf 16,5 MChip/s angehoben werden.

Insgesamt werden im 802.11g also drei verschiedene PHY-Headerformate unterstützt:

1. das Long-Header-Format nach 802.11,
2. das Short-Header-Format nach 802.11b und
3. OFDM-Header.

Das Long-Header-Format ist interoperabel mit den DSSS-Formaten mit 1 und 2 Mbit/s, mit den 802.11b-Formaten mit 5,5 und 11 Mbit/s und mit den PBCC-Formaten mit 5,5 bis 33 Mbit/s. Das Short-Header-Format wird wie im 802.11b mit Datenraten von 2 Mbit/s bis 11 Mbit/s und den PBCC-Formaten unterstützt.

Um auch die hohen Übertragungsraten der OFDM-Modulationen mit einem kompatiblen Header ausrüsten zu können, wurde ein drittes, ebenfalls optionales Verfahren definiert, welches die DSSS-Header mit einem OFDM-Datenteil kombiniert. Dieses CCK-OFDM-Verfahren hat die Besonderheit, dass unmittelbar nach dem Header von einer Single-Carrier-Transmission auf eine Multi-Carrier-Transmission umgeschaltet werden muss, um den OFDM-Datenteil zu senden.

Interoperabilität zwischen 802.11b und 802.11g

Zusammenfassend kann man feststellen, dass der Standard 802.11g im Wesentlichen die Technologien aus 802.11a und 802.11b in einem Gerät und einem Frequenzband zusammenführt. Leider sind diese Technologien jedoch nicht kompatibel und daher müssen zusätzliche Vorkehrungen getroffen werden, damit sich die technologische Kompatibilität der Geräte, die im Standard ja gefordert ist, auch praktisch durch einen gleichzeitigen Betrieb im selben WLAN auszahlen kann. Was nützt ansonsten ein Access Point, der zwar beide Übertragungsformate beherrscht, wenn in einem WLAN nicht auch beide Formate tatsächlich eingesetzt werden können.

Wie am Ende des vorigen Kapitels bemerkt, sind zunächst einmal die Header der beiden verpflichtend vorgeschriebenen Modulationen OFDM und DSSS/CCK nicht interoperabel. Der Standard fordert zwar, dass 11g-Geräte sowohl OFDM- als auch DSSS-Sendungen erkennen können und damit genau wissen, wann andere Systeme senden und wann das Medium frei ist. Das können aber 11b-Geräte nicht! Zwar gibt es mit CCK-OFDM ein Verfahren, das diesen Konflikt lösen kann, da es einen kompatiblen 11b-Header benutzt, aber leider ist dieses Verfahren nur optional. Das heißt, man kann sich nicht darauf verlassen, dass alle Produkte dieses Verfahren unterstützen werden. Die Erfahrung lehrt im Gegenteil, dass die Unterstützung optionaler Verfahren eher die exotische Ausnahme bleibt. Die Intension der IEEE an diesem Punkt ist klar: Weg mit den Altlasten, hin zu OFDM, und zwar in Reinkultur.

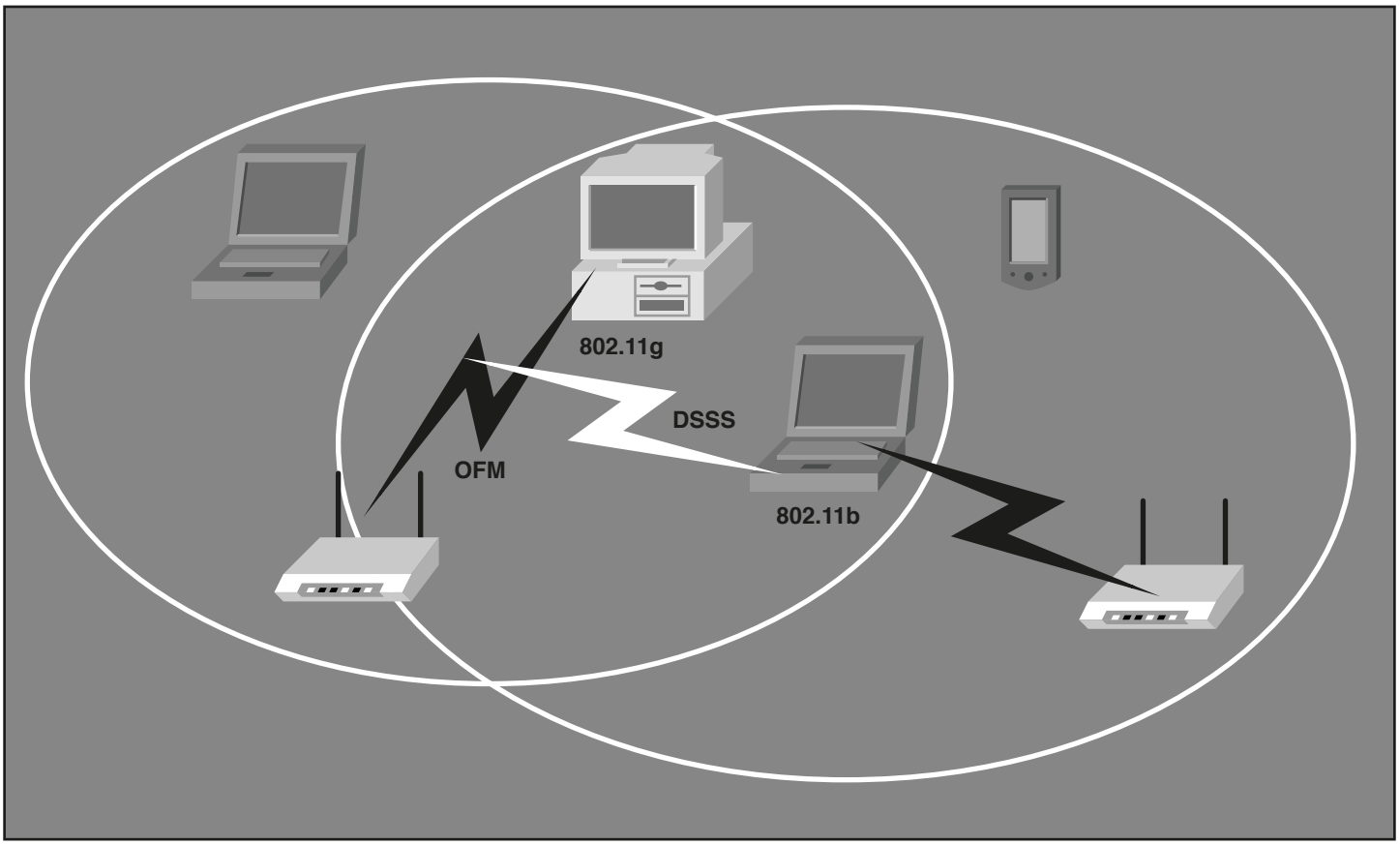


Bild 2: Interferenzen durch 802.11b im 802.11g-Netz

Damit sind aber in einem gemischten WLAN mit 11g- und 11b-Geräten die OFDM-Frames hochgradig gefährdet von den 11b-Geräten abgeschossen zu werden, da diese die OFDM-Frames nicht sehen können. Der Standard empfiehlt (!) an dieser Stelle, dass die Access Points alle 11g-Systeme dynamisch in einen Kompatibilitätsmodus schalten. In diesem Modus werden alle OFDM-Frames durch einen vorangehenden RTS-CTS-Handshake im (langsamen!) 11b-Format geschützt. Diese RTS- und CTS-Frames informieren das WLAN darüber wie lange das Medium belegt sein wird und werden von den 11b-Systemen verstanden. Der zu erwartende Overhead dieses Kompatibilitätsmodus wird enorm sein.

Ungünstigerweise überlässt es der Standard auch noch den Herstellern Entscheidungskriterien zu implementieren, ob und wann dieser Modus eingeschaltet wird, oder ob es günstiger sein kann, das Risiko einzugehen und die OFDM-Frames nicht zu schützen. Wichtig bei diesen Überlegungen ist in jedem Fall, dass dieser Mechanismus auch Funkzellen übergreifend funktionieren muss. Es nützt nämlich nichts, wenn Sie in einem reinen 11g-Netzwerk auf den RTS-CTS-Schutz Ihrer OFDM-Frames verzichten, solange ein überlappendes Netz mit 11b-Geräten für massive Interferenzen sorgt.

Die Zusammenführung von 802.11a und 802.11b führt jedoch noch zu einem weiteren Problem. Das bei Wireless LANs verwendete Medienzugangsverfahren CSMA/CA setzt auf verschiedenen Timern auf (für Details zum Verfahren siehe Wirless LAN Grundlagen Report, Kapitel 4.4.2), einer davon ist die so genannte Slot Time. Anhand dieser Slot Time berechnet jede Station die Zeit, die sie warten muss bis sie endlich senden darf, nachdem das Medium von einer anderen Station belegt war. Im 802.11 und unverändert auch im 802.11b wird die Slot Time für das DSSS-Interface auf 20 µs festgelegt, im 802.11a dagegen für die OFDM-Verfahren auf 9 µs. Es ist nun aber offensichtlich, dass in einem Netzwerk alle aktiven Systeme die gleiche Slot Time verwenden müssen. Ansonsten werden nämlich die Systeme, die die höhere Slot Time verwenden, im Mittel länger warten und damit deutlicht benachteiligt.

Im Mischbetrieb müssen also alle Stationen in einer Funkzelle auf 20 µs zurückschalten, sobald sich eine einzige 11b-Station anmeldet. Dieses Zurückschalten sollte standardgemäß dynamisch während des aktiven Netzwerkbetriebs möglich sein, allerdings gibt es Produkte (bzw. Firmwareversionen), die im gemischten Modus von Anfang an quasi mit gezogener Handbremse fahren.

Auch dieser Punkt muss zellenübergreifend funktionieren, da sonst die Zelle mit den höheren Timern ins Hintertreffen gerät. Konfigurationsparameter wie „11g-only“ oder „Mixed Mode“ scheinen die angesprochenen Probleme zu adressieren, wobei die genaue Bedeutung dieser Einstellungen in den meisten Fällen nicht klar wird. Zumindest im „11g-only-Modus“ lassen die getesteten Access Points keine 11b-Clients mehr zu und setzen dann in der Regel die kürzere Slot Time von 9 µs ein.

Aktueller Report

Studie des Monats: Wireless LAN Grundlagen

Bedingt durch den Übergang von der Ergänzungs-Technologie zur strategischen Technologie sind WLANs einem erheblichen Wandel unterworfen. So werden die bisherigen 11b-Produkte in vielen Bereich innerhalb von wenigen Wochen durch 11g abgelöst, in einer Reihe von professionellen Installationen wird schnell der Einzug von 11a/h zu beobachten sein. Dies immer in Kombination mit Sicherheits-Lösungen, die gerade in den letzten Wochen noch einmal einer erheblichen Überarbeitung unterworfen waren.

Wireless-LANs entwickeln sich zu einer strategischen Infrastruktur-Technologie. Sie bieten extrem interessante Lösungen für eine Reihe wichtiger Aufgaben-Stellungen, davon seien nur einige genannt

- Logistik-Lösungen im Produktions-Bereich
- Neue Service-Konzepte im Gesundheitsbereich
- Einbindung von „Dirty Devices“
- Overlay-Strukturen zum bestehenden Kabel-LAN
- Mobility-Lösungen mit niedrigsten Betriebskosten

Unser neuer Report bietet als umfassendes Standard-Werk, das in keinem Unternehmen fehlen darf, einen kompletten Überblick über die WLAN-Technologie, von der grundsätzlichen Arbeitsweise bis hin zur Installation:

Wireless WLAN:
• Arbeitsweise
• Varianten
• Schwachstellen
• Planung
• Installation

Einleitung
Anwendungsgebiete: Büroumfeld, Notebook-Einbindung, Kaufhäuser, Krankenhäuser, LAN-Koppelung
Grundlagen von Funktechniken: Frequenzbänder, elektromagnetische Wellen, Interferenzen (Rauschen, Reflexionen, Mehrwegeausbreitung), Modulationsverfahren (AM, FM, PM), Spread Spectrum, Multiplexing, Multiple Access, Funk Standards (DECT, GSM, UMTS, Bluetooth, 802.11, HiperLAN/2)
Antennentechnik: Einführung (EM-Wellen, Fresnel, Polarisation, Kenngrößen), Bauformen von Antennen (Diversity, Dipole, Patch)

Der Standard IEEE 802.11: Die Struktur des Standards, Konzepte und Aufbau von Wireless LANs (Grundbegriffe), Übertragungstechnik (PHY-Layer), DSSS nach 802.11, CCK und PBCC nach 802.11b, 802.11g, Interoperabilität zwischen 802.11b und 802.11g, OFDM nach 802.11a (und 802.11h), FHSS, Infrarot, MAC-Layer, Medienzugang (CSMA/CA), Distribution Coordination Function, Point Coordination Function, RTS/CTS, Fragmentierung, Frameformate, Scanning, Authentication und Association, Roaming, Management im BSS, Powermanagement, Inter-Access Point Protocol (802.11F)
Sicherheit in WLANs: Gefährdungspotentiale, Sicherheit nach 802.11, WEP, Authentisierung, Verbindungsaufbau, Angriffsszenarien, Tools, Ein Anforderungskatalog, Neue Kryptographieverfahren (CCMP, TKIP, WPA), Frameformate, Authentisierung, Der Standard 802.1X,Pre-Shared Keys, Schlüsselverwaltung, Roaming, Migrationsmöglichkeiten
Messtechnik und Tools: Spektrumanalysator, Client Utilities, Protokollanalysatoren
Produkte: Ausstattung und Installation, Konfigurationsparameter, Testverfahren, Delay und Reichweite, Interoperabilität, Overhead spezieller Einstellungen, Auswahlkriterien
Einsatz externer Antennen: Deckenantennen, Wandantennen, Vertikalstrahler, Verbinder, Kabel, Pigtails
Aufbau von Wireless-LANs: Konfigurationsaufgaben, Antennen und ihre Positionierung, Typische Installationen, Strukturierte Netze, Die Rolle des Distribution System, Die Rolle des Client
Rechtliche und gesundheitliche Aspekte
Anhang: Tabellen, Kanäle, Frequenzen

Fax-Antwort an ComConsult 02408/955-399

Bestellung Wireless LAN Grundlagen

☐ Ich bestelle den Research Report
Wireless LAN Grundlagen
(Preis € 398,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Bestellen Sie auf unserer Web-Seite
www.comconsult-research.com

Neues Seminar

IP-Telefonie: Projektleitfaden

Vom 15. bis 17. März 2004 veranstaltet die ComConsult Akademie im Radisson SAS in Düsseldorf zum ersten Mal ihr neues Seminar "IP-Telefonie: Projektleitfaden".

Nachdem die Frage ausreichender Funktionalität und professioneller Nutzbarkeit für IP-Telefonie geklärt ist, stellt sich nun zunehmend die konstruktive Frage, wie ein entsprechendes Projekt erfolgreich umgesetzt wird. Dabei sind eine Reihe wesentlicher Einflussfaktoren zu berücksichtigen, von der Anlagenarchitektur über den Umbau des LAN bis hin zur erforderlichen Sicherheits-Lösung.

Dieses Seminar erarbeitet einen Leitfaden zur Umsetzung von IP-Telefonie in der Praxis. Alternativen werden verglichen, bekannte Probleme aufgezeigt, erfolgreiche Konzepte vermittelt.

Aktuelle Projekte und Betriebserfahrungen mit vielen Tipps und Tricks bieten unverzichtbare Zusatzinformationen, die in keiner Literatur zu finden sind.

Im Einzelnen lernen Sie in diesem Seminar:

- Wie ein Unternehmens-Standard für IP-Telefonie aufgebaut sein sollte
- Welche Architekturen von IP-PBX-Lösungen zur Wahl stehen
- Welche Infrastrukturdienste zu integrieren sind: Redundanz, IP, Verzeichnisdienste, Rufnummernpläne

- Was VoIP-Endgeräte leisten müssen, was die angebotenen Geräte können
- Welchen Einfluss ein VoIP-Projekt auf ein bestehendes LAN hat, wo Änderungen sinnvoll sind, was bei der Integration der Server und Gateways zu beachten ist
- Wie IP-Telefone in der Praxis konfiguriert werden
- Was CTI leistet, warum fast jedes VoIP-Projekt CTI braucht
- Welche neuen Anwendungen den Mehrwert von VoIP ausmachen
- Was Call Center, IVR, ACD, UM für das Projekt bedeuten
- Was bei einer Ausschreibung beachtet werden muss
- Was VoIP für das Corporate Network bedeutet, welche Änderungen erforderlich und sinnvoll sind
- Wie VoIP über VPN realisiert wird, was sie im WAN dabei zu beachten haben
- Voice over Wireless: warum dies für bestimmte Projekte wichtig ist und was bei der Wireless-Konfiguration zu leisten ist
- Security-Maßnahmen und Lösungen: wie Sicherheit von VoIP im LAN/WAN erfolgreich umgesetzt wird
- Sprachqualität und Messtechnik: was wird benötigt, wie sind Ergebnisse zu bewerten
- Quality of Service: Standards, Lösungen, Messergebnisse, Empfehlungen zur Nutzung
- Management-Lösungen: was leisten sie, was wird wirklich gebraucht
- Betriebskonzepte: wie sieht ein erfolgreicher und zuverlässiger Betrieb aus, Werkzeuge, Personal, Organisation

Der Referent Dr. Behrooz Moayeri ist Mitglied der Geschäftsleitung der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrungen zurück. In den letzten Jahren hat Dr. Moayeri zahlreiche führende deutsche Unternehmen bei der Planung von Telekommunikations- und VoIP-Lösungen erfolgreich beraten.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung IP-Telefonie

Ich buche das Seminar
IP-Telefonie: Projektleitfaden
zu folgendem Termin

☐ 15.03.-17.03.04 Düsseldorf
☐ 21.06.-23.06.04 Berlin
(Preis € 1.690,-- zzgl. MwSt.)

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

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ, Ort
eMail	Unterschrift

Schwerpunktthema Dezember 2003

Der Spanning Tree ist tot! – Es lebe der Spanning Tree!

Fortsetzung von Seite 1

Markus Schaub ist seit vielen Jahren für die ComConsult Technologie Information GmbH tätig. Seine Aufgabenbreiche umfassen die Evaluierung, Konfiguration und Inbetriebnahme neuster Hard- und Software aus dem Netzwerkumfeld. Er verfügt über langjährige Betriebs- und Praxiserfahrung.

schaub@comconsult-research.com

Wesentlich ist bei dem neuen Verfahren, dass es nicht mehr timerbasiert arbeitet (siehe Bild 1 und 2, wie der klassische Spanning Tree, sondern durch Aktionen, die eventgesteuert ausgelöst werden. Fällt eine Leitung aus, kann das Rapid Spanning Tree Verfahren sofort auf den Ausfall reagieren und so die Umschaltzeit sehr gering halten. Nach Wiederherstellung einer neuen, stabilen Topologie werden alle Switches des Baumes darüber informiert, die notwendigen Einträge ihrer Bridge-Tabellen zu löschen.

Bild 1: Timerbasierte RSTP Reaktion auf einen Ausfall

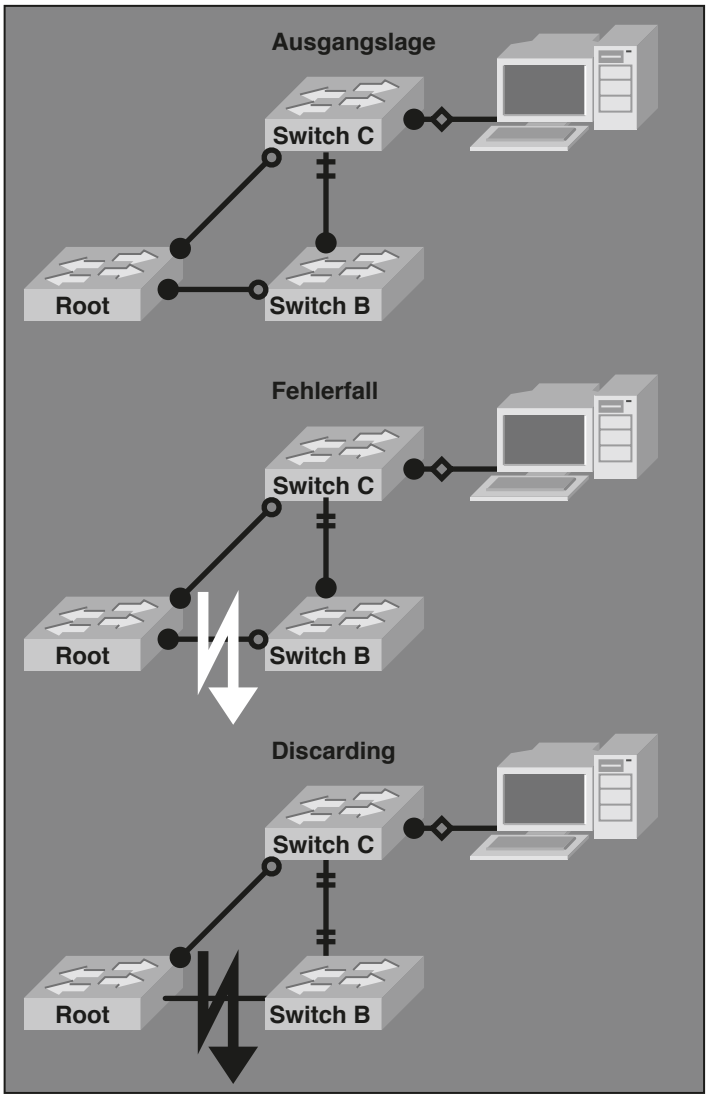
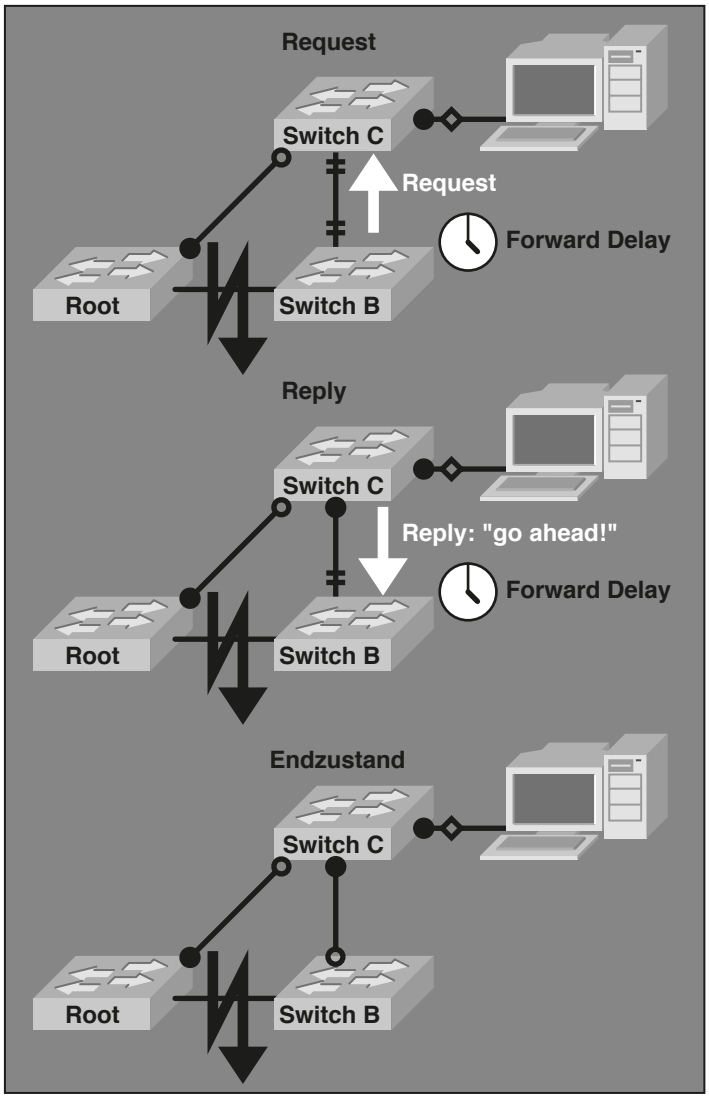


Bild 2: Timerbasierte RSTP Reaktion auf einen Ausfall



Drei Besonderheiten sind beim RSTP Verfahren zu beachten, die eine Ende-zu-Ende Kommunikation deutlich verzögern können

1. Ein Switch muss einen Link-Ausfall oder eine Link-Aktivierung durch einen Link-Up bzw. Link-Down bemerken. Ist beispielsweise ein Medienkonverter zwischen zwei Switches geschaltet, der den Link-Status nicht weitergibt, so dauert es bis der Ausfall durch Ausbleiben der BPDUs bemerkt wird.

2. Nicht alle Hersteller nutzen zur Verbreitung von Änderungen eventgetriggerte BPDU Pakete, sondern nutzen statt dessen die regelmäßig versendeten BPDUs. Damit kann die Umschaltung im ungünstigsten Fall jedoch mehrere Sekunden dauern.

3. Ebenso werden die Topology Change Meldungen häufig in den regulären BPDUs gesendet, so dass auch hierfür gilt, dass es verhältnismäßig lange dauern kann, bis alle Switches die Information erhalten haben.

Ferner ist zu beachten, dass es beim Rapid Spanning Tree durch eine Umschaltung zu Frame-Verdopplungen oder zu einer Änderung der Frame-Reihenfolge vom Sender zum Empfänger kommen kann.

Testaufbau RSTP

Das Labor von ComConsult Research hat in diesem Jahr das Umschaltverhalten des Rapid Spanning Tree getestet. Im Folgenden werden einige der Ergebnisse kurz vorgestellt. Weitere Testergebnisse können von der ComConsult Research Homepage unter http://www.comconsult-research.de/ im Bereich Produkt Analysen herunter geladen werden. Das Dokument heißt „Redundanzverfahren bei Hirschmann Switches“ und enthält sowohl die Ergebnisse zum Rapid Spanning Tree wie auch einen Vergleich mit den von Hirschmann eingesetzten Verfahren.

Für die Tests des Rapid Spanning Trees wurden je vier 2950er Workgroup-Switches und vier 2955er Industrie-Switches von Cisco genutzt. Um die später im Artikel noch vorgestellte Kaskade testen zu können, wurden die Switches als Ring verschaltet. Für die Tests wurde nur die Root durch Konfigurationsänderung festgelegt, die anderen Defaultwerte bezüglich des RSTP blieben unverändert.

Es wurden sowohl die Zeiten für die Unterbrechung des Ringes wie auch für seine Wiederherstellung gemessen. Sender und Empfänger waren für alle Tests an die Root und einen benachbarten Switch angeschlossen. Um die Umschaltung auszulösen, wurde die Verbindung zwischen den beiden Switches getrennt, an denen die Messrechner angeschlossen waren.

Eingesetztes Testverfahren

Da es schwierig ist, die „echte“ Umschaltzeit zu ermitteln, wurde ein indirektes Messverfahren gewählt, das für die Praxis auch von größerer Relevanz ist: gemessen wird die Zeitperiode, in der ein Clientsystem keine Pakete erhält. Dafür wird mittels des Lastgenerators Chariot von der Firma Ganymede ein kontinuierlicher Datenstrom zwischen zwei PCs auf UDP/RTP Basis initiiert. Da die Parameter des Datenstroms vorgegeben wurden, konnte aus der Verlustrate die Dauer der Verbindungsunterbrechung ermittelt werden.

Umschaltzeit-Verhalten von RSTP über acht Switches

Zunächst wurde die Ausfallzeit gemessen, die sich über einen Ring mit acht Switches ergibt. Insgesamt wurde der Versuch zehn Mal wiederholt.

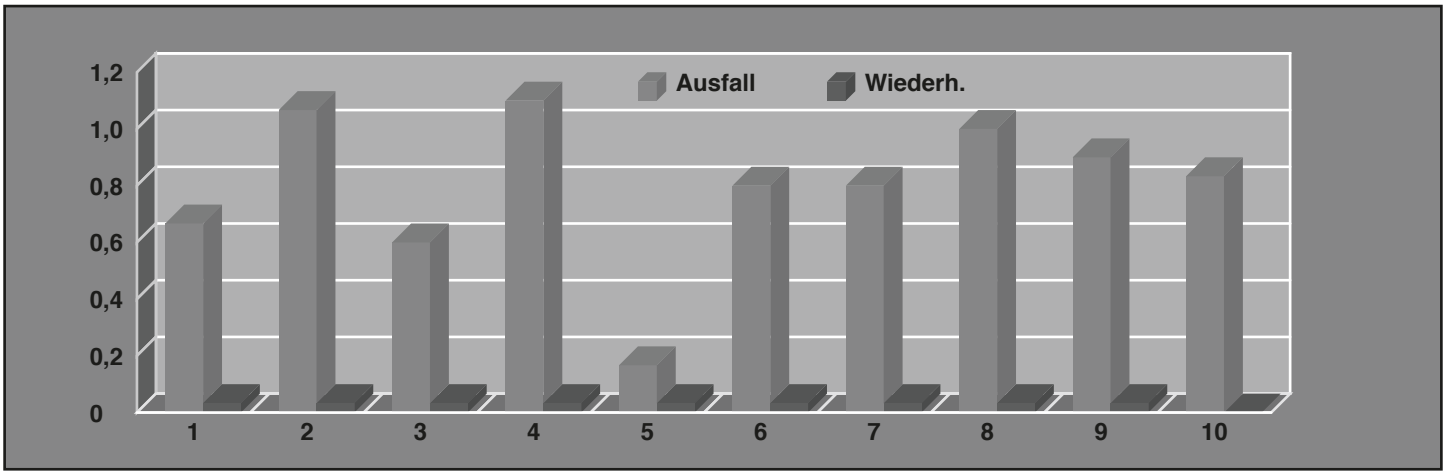
Es fallen zwei Punkte sofort ins Auge:

1. Das RSTP-Verfahren benötigt bedeutend weniger Zeit zur Wiederherstellung der Ausgangstopologie als zur Recovery im Fehlerfall. Der Grund dafür ist, dass bei der Wiederherstellung der Ende-zu-Ende-Kommunikation „nur“ der Link zwischen der Root und ihrem Nachbarn wiederhergestellt werden musste und keine Pakete im Speicher der Switches gelöscht werden. Dadurch kann es jedoch zu einer Vertauschung der Paketreihenfolge beim Empfänger kommen. Was insbesondere bei einer Ringschaltung nicht sehr unwahrscheinlich ist.

2. Die Zeit für das Recovery ist starken Schwankungen unterworfen und liegt zwischen knappen 200 ms und mehr als einer Sekunde bei acht Switches. Die Ausfalldauer ist somit nicht als deterministisch anzusehen, sondern sie kann sehr stark schwanken. Bei Messungen während des Versuchsaufbaues ist es sogar zu Ausfällen von über zwei Sekunden gekommen, die jedoch nicht dokumentiert wurden und deswegen in die Messauswertung nicht mit aufgenommen wurden.

Im Folgenden werden immer nur Durchschnittswerte von Versuchsreihen angegeben. Von daher ist es interessant zunächst zu betrachten, wie aussagekräftig solche eine Durchschnittsermittlung überhaupt ist. Der Durchschnitt dieses Versuches lag bei 794 Millisekunden (ms).

Bild 3: Ausfall und Wiederherstellung eines Ringes mit RSTP Komponenten



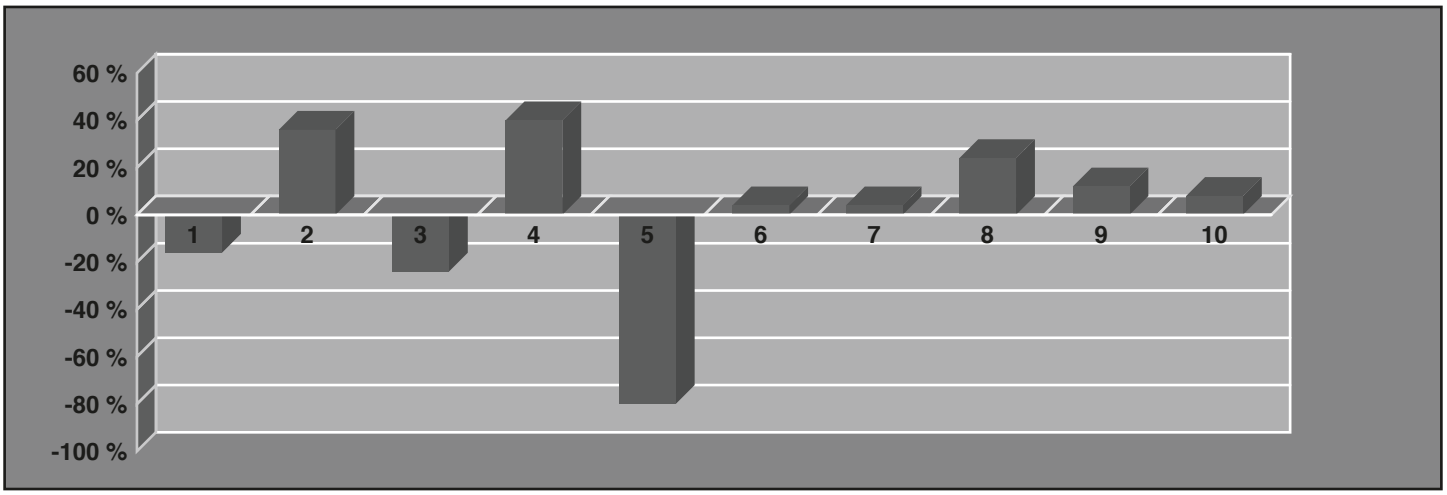


Bild 4: Schwankung von 10 Messergebnissen

Bild 4 zeigt die prozentuale Abweichung der 10 Einzelmessungen vom Mittelwert. Es sticht sofort ins Auge, dass vier von zehn Messwerten über 20% vom Durchschnitt abweichen. Die durchschnittliche Abweichung liegt bei rund 25%. Eine der Messungen weicht sogar um 80% ab. Nimmt man diese extreme Abweichung aus der Berechnung heraus, so ergibt sich ein Mittelwert von 864 ms, also 70 ms mehr als der als der Durchschnitt über alle 10 Versuche. Damit kann eine solche Durchschnittsangabe nur als Daumenwert gelten, man sollte jedoch davon ausgehen, dass die Umschaltzeiten in Einzelfällen auch weit über diesen Werten liegen können.

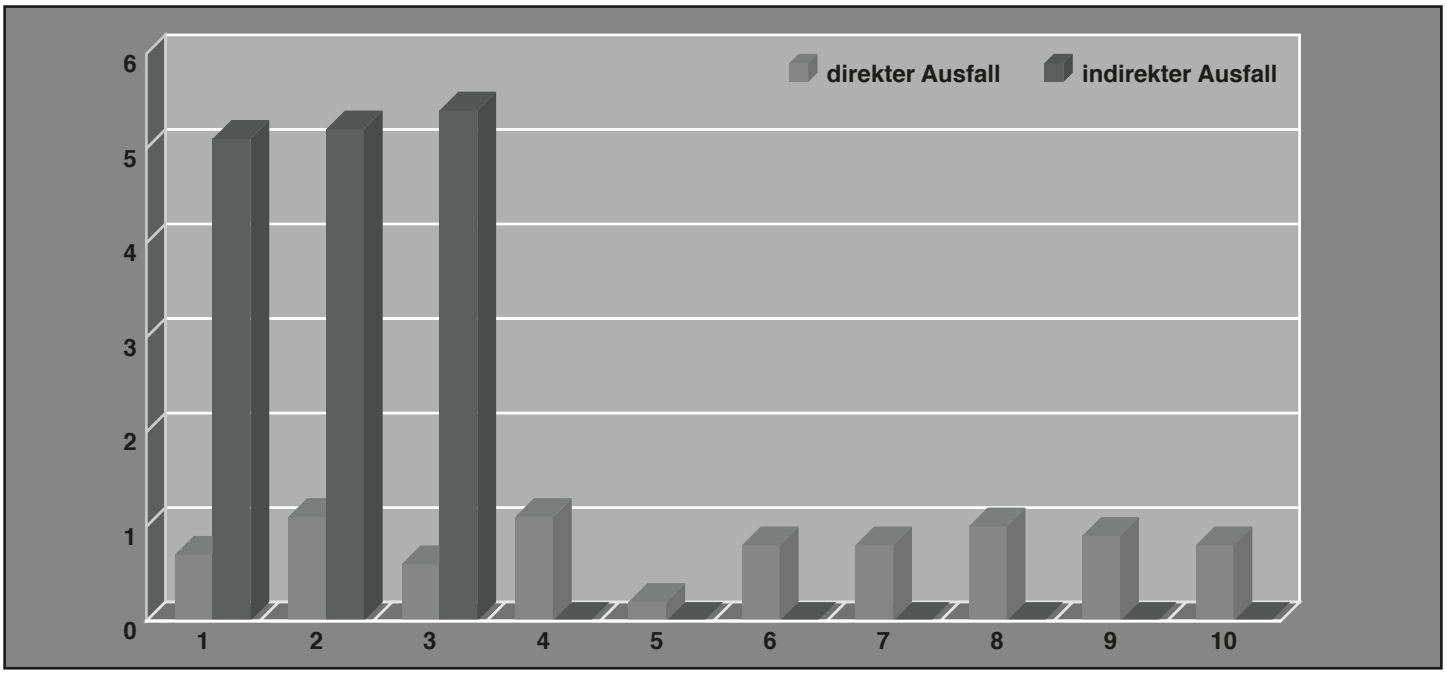
Worst-Case Ausfall bei RSTP

Die im vorhergehenden Versuch gemachten Messungen spiegeln nicht den absoluten Worst-Case des Rapid Spanning Trees wieder, da der Link-Down von zwei Switches sofort erkannt und gemeldet wird. Es kann jedoch sein, dass Medienwandler oder Systeme im Ring angeschlossen sind, die einen Link-Down an die Switches nicht weitergeben können und selbst keine RSTP Geräte sind. In diesem Fall muss der Ausfall durch das Ausbleiben der BPDU Pakete erkannt werden. Um diese Fehlersituation nachzustellen, wurden zwei Geräte in den Ring eingebaut, die zwar selbst kein RSTP sprechen, BPDUs jedoch weiterleiten. Anschließend wurde das Kabel zwischen diesen beiden Komponenten gezogen.

Abbildung 5 stellt den Ausfall, der von Switches direkt festgestellt werden kann, dem Linkausfall der nur durch fehlende BPDUs bemerkt wird gegenüber. Es fällt auf, dass die Zeit sich ca. um den Faktor fünf erhöht und die Unterbrechung bei über 5 Sekunden liegt.

Damit ist sie zwar bedeutend besser als beim klassischen Spanning Tree, liegt jedoch auch weit über einer Sekunde, die vielfach als Umschaltzeit des RSTP genannt wird.

Bild 5: Direkter und indirekter Leitungsausfall bei RSTP



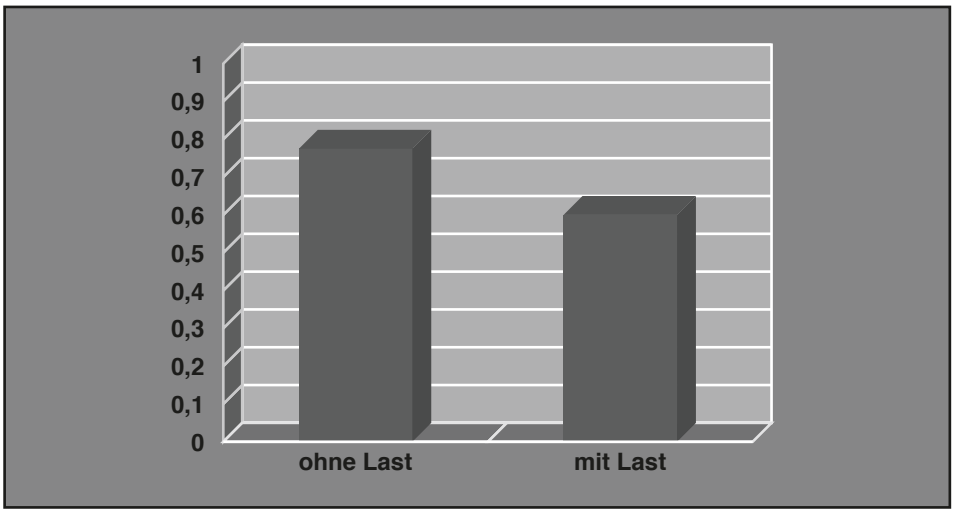


Bild 6: RSTP Lastvergleich

Eine weitere spannende Frage ist, ob sich das Umschaltverhalten des Rapid Spanning Trees unter Last anders verhält als bei einem unbelasteten System. Dazu wurde zusätzlich zum Testdatenstrom ein TCP Transfer zwischen den Testsystemen initiiert, so dass die Leitung zwischen den Switches insgesamt zu ca. 56% ausgelastet war, ein Wert, der auch in der Praxis nicht überschritten werden sollte.

Wie man sieht ist die Umschaltzeit unter Last sogar scheinbar geringer als bei einem ansonsten unbelasteten RSTP-Ring. Jedoch liegt der belastete Ring mit rund 600ms immer noch im Toleranzbereich der „natürlichen“ Schwankungen des RSTP. Man kann also davon ausgehen, dass es keinen Unterschied macht, ob die getesteten unter Last arbeiten oder nicht, zumindest solange die Auslastung der Uplinks die 50% Marke nicht überschreiten.

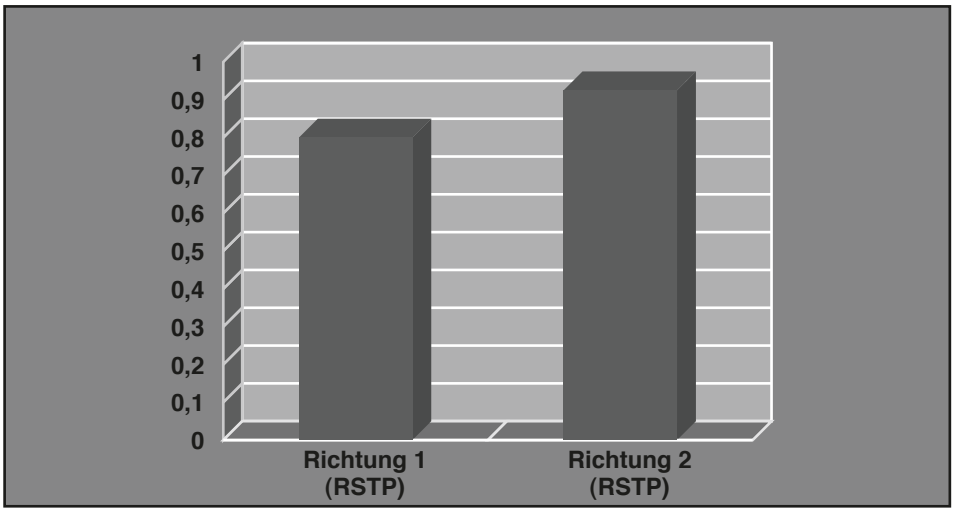
RSTP Umschaltverhalten bei bidirektionalem Datenstrom

Im nächsten Versuch wurde bei gleichem Aufbau untersucht, ob die Richtung der Übertragung von Bedeutung ist.

Für diesen Test wurde je ein Datenstrom von einer Teststation zur anderen und umgekehrt gleichzeitig übertragen. In Bild 7 sind die Ergebnisse für die Wiederherstellung des Ringes für beide Richtungen einander gegenübergestellt.

Das Ergebnis zeigt, dass es erwartungsgemäß keinen Unterschied macht, in welche Richtung der Datenstrom fließt, ebenso wenig ob man eine oder zwei Richtungen zur selben Zeit untersucht. Auch die hier auftretenden Unterschiede liegen wieder im Toleranzbereich der RSTP Schwankungen.

Bild 7: RSTP Vergleich der Richtung des Datenstroms



Ansteigen der Umschaltzeit in Relation zur Anzahl der Switches

Gerade für die im Folgenden diskutierte Kaskadierung (Hintereinanderschaltung) von Switches ist die Frage nach der Abhängigkeit der Umschaltzeit von der Anzahl der hintereinander geschalteten Switches von Bedeutung. Darum wurde im nächsten Versuch die Anzahl der Switches schrittweise von acht auf drei reduziert. Es wurden je drei Messungen durchgeführt.

Es verwundert auf den ersten Blick, dass vier Switches scheinbar schneller schalten als drei und sechs schneller als fünf. Das liegt jedoch an den stark schwankenden Umschaltzeiten von RSTP, die sich bei drei Messungen statistisch stark auswirken. Quantitativ kann wegen der geringen Anzahl von Wiederholungen des Versuches zwar keine sinnvolle Aussage getroffen werden, qualitativ legen die Ergebnisse jedoch nahe, dass die Anzahl der Switches die Umschaltzeit stark beeinflusst. Da die Umschaltzeit zum einen von den eingesetzten RSTP Komponenten abhängt und zum anderen ohnehin sehr starken Schwankungen unterliegt, wurde auf eine genauere Messung verzichtet.

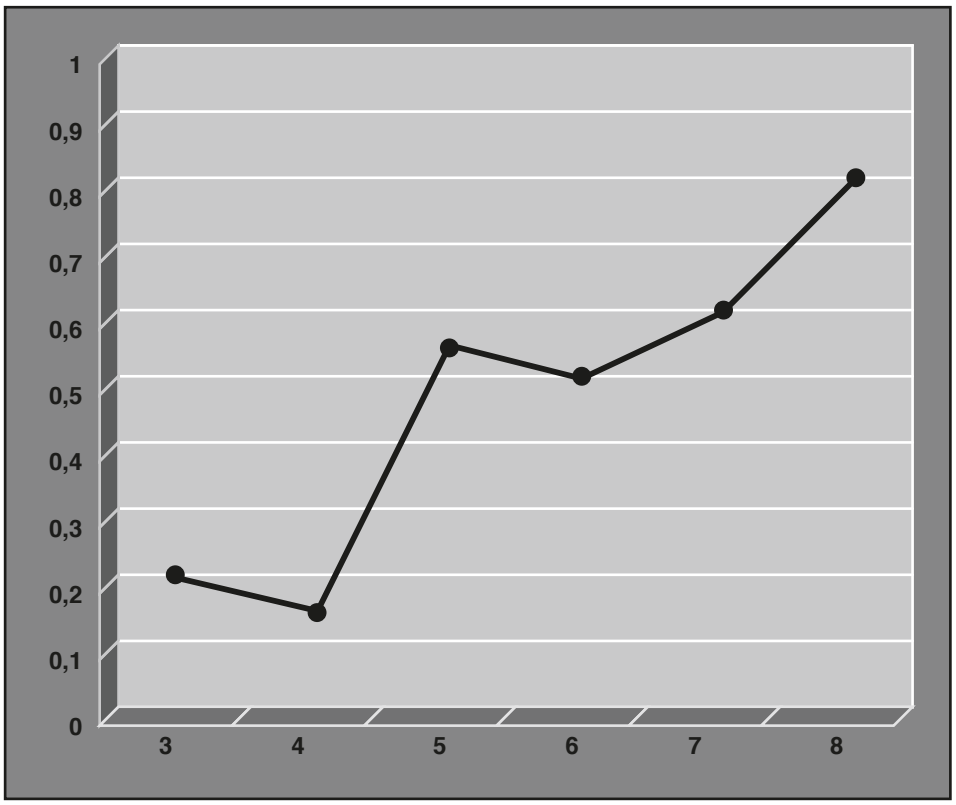


Bild 8: Einfluss der Anzahl von Switches auf die Umschaltzeit

Zusammenfassung der Ergebnisse

Gegenüber seinem Vorgänger ist der Rapid Spanning Tree, was die Umschaltzeit angeht, haushoch überlegen. Allerdings ist die Recoveryzeit starken Schwankungen unterlegen und sowohl von der Art und dem „Ort“ des Ausfalles wie auch vom dem Design des Netzes abhängig. Bei guten Implementierungen kann man jedoch davon ausgehen, dass der Rapid Spanning Tree einen Fehler schneller beheben kann, als dass ein darüber liegendes Layer 3 Verfahren wie VRRP oder OSPF den Ausfall überhaupt bemerkt. Das ist ein erheblicher Vorteil gegenüber dem klassischen Spanning Tree, da sich zumindest bei einem Routing Protokoll eine Recovery nicht auf ein Subnetz beschränkt, sondern über das gesamte Layer 3 Netz mindestens bis zu den Area-Grenzen hin auswirkt.

Für viele Anwendungen dürften Umschaltung im 1-3 Sekunden Bereich auch völlig ausreichen, zumal es sich ja ohnehin um Ausnahmesituationen handelt und nicht um ein regelmäßige stattfindendes Ereignis. Sollte man jedoch Anwendungen haben, die vorhersagbare und vor allem kürzere Umschaltzeiten zwingend erfordern, so ist man jedoch weiterhin auf proprietäre Verfahren angewiesen.

WARNUNG: Schlechte Implementierungen des RSTP

Zudem muss ausdrücklich davor gewarnt werden, die vorgestellten Ergebnisse zu verallgemeinern. Wie dieses Jahr auf der Sommerschule der ComConsult vorgestellt wurde, gibt es auch Implementierungen des RSTP, die scheinbar nicht mit event-getriggerten Updatemeldungen arbeiten, sondern auch Änderungen mittels der regelmäßig alle zwei Sekunden gesendeten BPDUs verbreiten. Das führt natürlich zu deutlich höheren Umschaltzeiten und die Abhängigkeit von der Anzahl der Switches steigt ernorm. Neben Umschaltzeiten von 10-15 Sekunden bei 7 Switches war es bei dieser Implementierung auch nicht möglich, Netze mit mehr als 7 Switches im Durchmesser noch stabil zu betreiben.

> Vor dem Einsatz von RSTP sollte man zum aktuellen Zeitpunkt unbedingt entweder selbst intensive Tests durchführen oder solche Test in Auftrag geben, um sicherzustellen, dass die geplanten Komponenten die Anforderungen erfüllen.

Kostenersparnis durch RSTP-Design

Der alte STP hatte design-technisch zwei gravierende Nachteile:

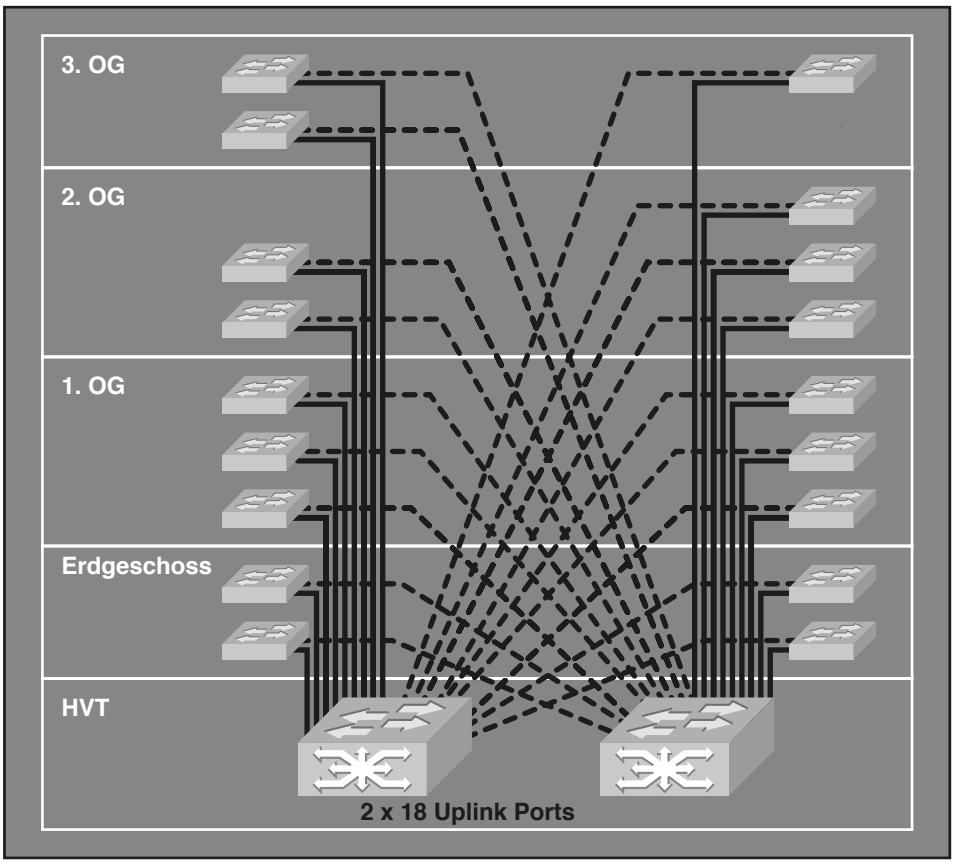
1. Er war zu langsam.
2. Über mehr als sieben Brücken durfte man nicht gehen.

Beim Netzwerkdesign mit dem klassischen Spanning Tree versuchte man diese beiden Restriktionen dadurch in den Griff zu bekommen, dass man Layer 2 Switches in einer Dreieckschaltung mit den Layer 3 Switches im Hauptverteiler verband.

Bild 9 zeigt ein solch klassisches Design.

Die meisten Hersteller hatten proprietäre Verfahren entwickelt, um für genau diese Dreieckschaltung schnellere Umschaltzeiten zu erreichen, indem bei dem Ausfall des aktiven Uplinks die alternative Leitung mehr oder weniger sofort durch den Etagenswitch aktiviert wurde. Damit war das erste Problem gelöst. Das zweite, die sieben Brücken Restriktion, ergab sich erst gar nicht, da jeweils nur drei Switches beteiligt waren.

Bild 9: Sternförmiges Netzwerkdesign



So praktisch und funktional diese Lösung auf den ersten Blick auch erscheinen mag, sie hat einen gravierenden Nachteil: sie ist immens teuer!

Die Kosten ergeben sich aus der hohen Anzahl benötigter Uplinkports auf den teueren, modularen Geräten im HVT. Im gewählten Beispielgebäude benötigt man 18 Gigabit-Uplinks pro HVT-Switch. Die Kosten werden auch durch den Einsatz von reinen Layer 2 Komponenten im HVT überhaupt nicht oder zumindest nur sehr gering gesenkt.

Beide Nachteile stellen sich in einer reinen RSTP Umgebung jedoch grundsätzlich nicht mehr, was neue Möglichkeiten des Designs eröffnet.

Bild 10 zeigt einen solchen Designansatz, die Layer 2 Kaskade:

Anstatt jeden Etagenswitch einzeln mit den beiden HVT-Switches zu verbinden, werden bei der Kaskade, analog zu einem Stack, die Switches auf der Etage hintereinander geschaltet. Dazu wird je ein Uplink Port eines Etagenswiches mit dem eines anderen Etagenswiches verbunden. Die beiden Endswiches dieser Reihenschaltung werden nun auf die beiden HVT-Swtiches geschaltet. Dabei ist es problemlos möglich zwei getrennte Steigbereiche aus Redundanzgründen zu nutzen. Die jeweils „mittlere“ Leitung der in Reihe geschalteten Etagenswichtes ist nicht aktiv, d.h. einer der beiden Ports ist im Discarding Modus, um einen Loop auszuschließen. Die beiden Seiten des Gebäudes werden durch einen Link zwischen den HVT-Switches miteinander verbunden.

Im stabilen Zustand, in dem keine Redundanz genutzt werden kann, ergibt sich damit folgendes Bild: die maximale Entfernung von einem PC zum HVT beträgt 3 Etagenswitche und die Maximale Entfernung von einem PC zu einem anderen PC 8 Swichtes (3x Etage + 2x HVT). Damit das funktioniert, muss jedoch gewährleistet sein, dass die sieben Brücken-Regeln nicht mehr eingehalten werden braucht. Schlimmer noch, wenn es zu einem, oder gar zwei Leitungsausfällen kommt, dann kann es bei der dargestellten Kaskade zu einer Entfernung von bis zu 13 Switches kommen, wie in Bild 11 dargestellt.

Bevor man sich zu solch einer Konstruktion entschließt, sollte man ausführlich testen, dass die sich im vorgestellten Ernstfall ergebende Topologie noch stabil ist und in einer vernünftigen Zeit ergibt.

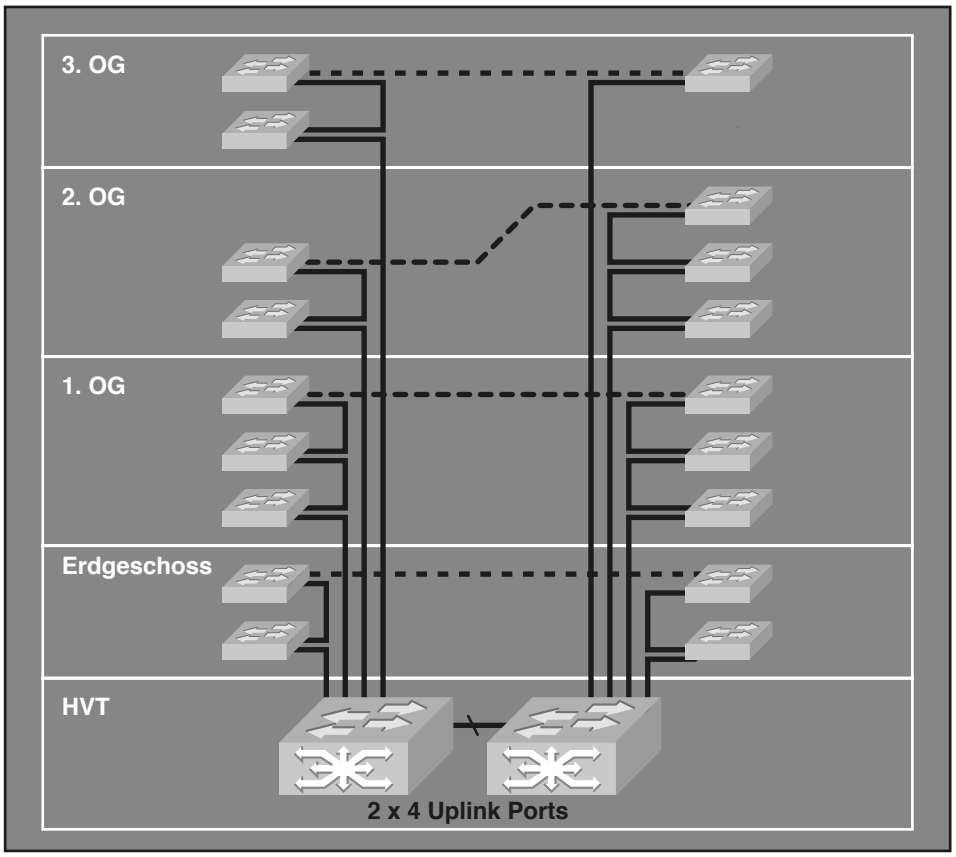
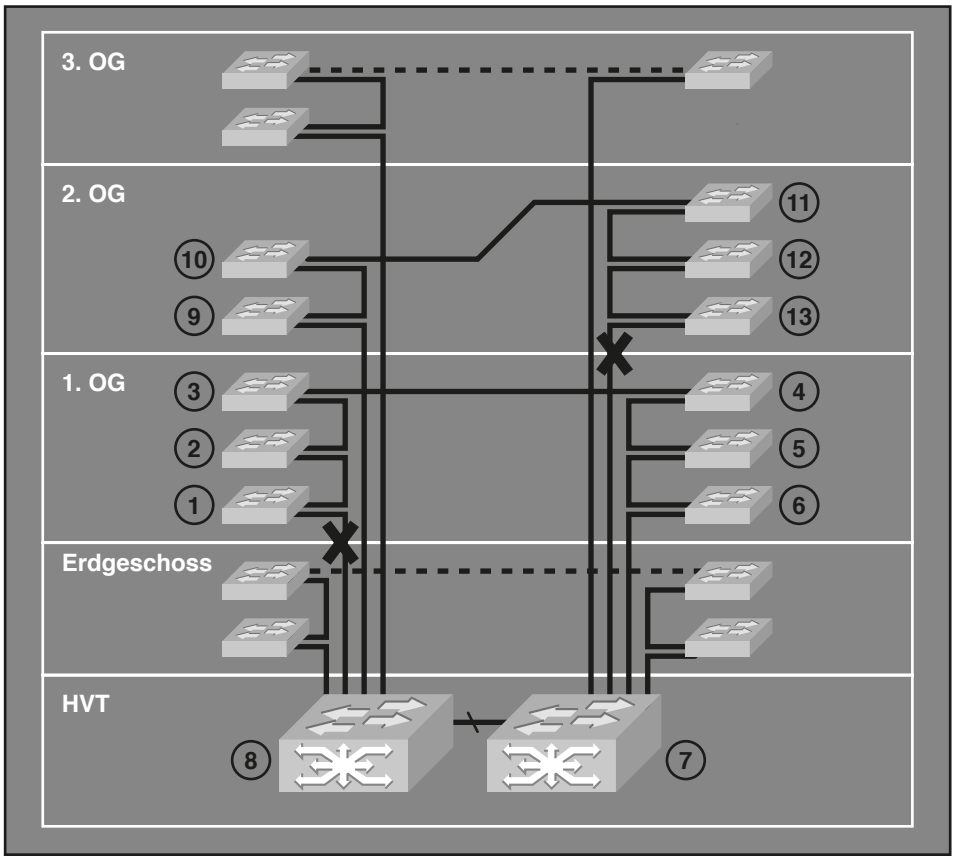


Bild 10 (o.): Kaskadenförmiges Netzwerkdesign, Bild 11 (u.): Ausfall beim Kaskadendesign



Der Spanning Tree ist tot! – Es lebe der Spanning Tree!

Wie bereits bei der Vorstellung der Messergebnisse erläutert, ist die Anzahl der hintereinander geschalteten Switches von entscheidender Bedeutung für die Umschaltzeit. Selbst bei guten Implementierungen des RSTP sollte man im vorgestellten Fall durchaus mit Umschaltzeiten von bis zu 5 Sekunden rechnen.

Die längere Umschaltzeit ist jedoch nicht das eigentliche Problem, vielmehr gibt es Implementierungen des RSTP, die bei einem Netzdurchmesser von mehr als sieben Switches nicht mehr stabil sind. Das äußert sich dadurch, dass nach einem Respanning zum Umschalten auf die redundanten Leitungen, Pakete nicht mehr von jedem beliebigen Punkt zu jedem beliebigen anderen Punkt durchkommen. Neben einen Totalverlust der Verbindung gibt es jedoch auch den Fall dass Pakete für einige Sekunden durchkommen, dann wieder nicht, und später wieder doch usw.

Wenn es aber so viele Schwierigkeiten gibt, die man vorher testen soll, was spricht dann für die Kaskade? Ist die Kosteneinsparung wirklich so immens?

Zunächst muss eines festgestellt werden: es gibt gute Implementierungen des RSTP, die sowohl schnell als auch stabil sind, man darf zum aktuellen Zeitpunkt jedoch nicht leichtfertig davon ausgehen, dass das auf alle zutrifft. Insbesondere sollte man aktuell noch nicht verschiedene Hersteller bei der RSTP-Kaskade mischen. Will man verschiedene Hersteller auf der Etage und im HVT einsetzten, sollte man zur Zeit lieber die klassische Dreiecklösung nutzen oder aber sehr ausführlich alle möglichen Ausfallsituationen testen beziehungsweise solche Test in Auftrag geben, bevor man im laufenden Betrieb böse Überraschungen erlebt.

Was die Kosteneinsparung angeht, so können diese erheblich sein. Bild 12 zeigt einen Kostenvergleich eines Netzes mit und ohne Kaskade. Die Klassen beschreiben Redundanzklassen, wobei die Klasse A ohne jede Redundanz arbeitet und die Klasse C eine vollredundante Lösung mit Layer 3 im Geländebackbone (siehe Bild 13a - c). Die Zahlen beziehen sich dabei auf ein Netz das aus drei unterschiedlich großen Gebäuden und zwei Rechenzentren zusammensetzt. Da die Kaskade im Backbone nicht eingesetzt werden kann, ist die prozentuale Einsparung bei einem Flächennetz geringer als bei einem einzelnen Gebäude.

Anhand der Abbildung kann man gut erkennen, dass die Einsparung durch den Einsatz der Kaskade leicht die Mehrausgaben für ein Backbone-weites Layer 3 Design aufwiegen kann.

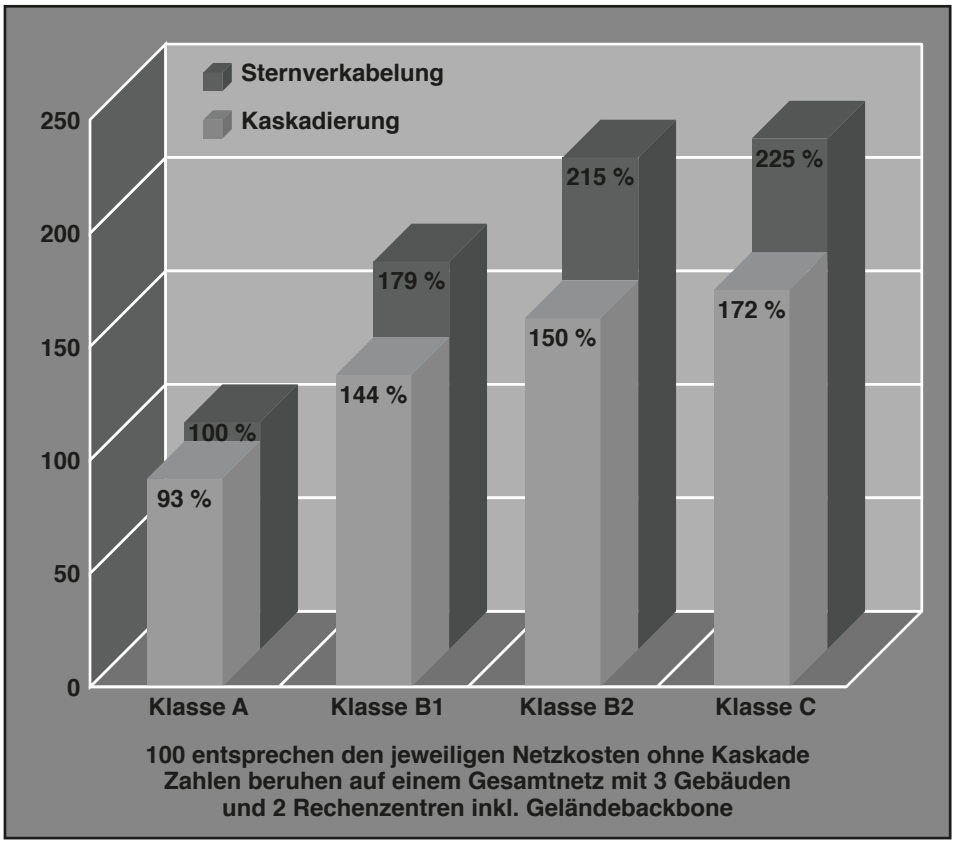
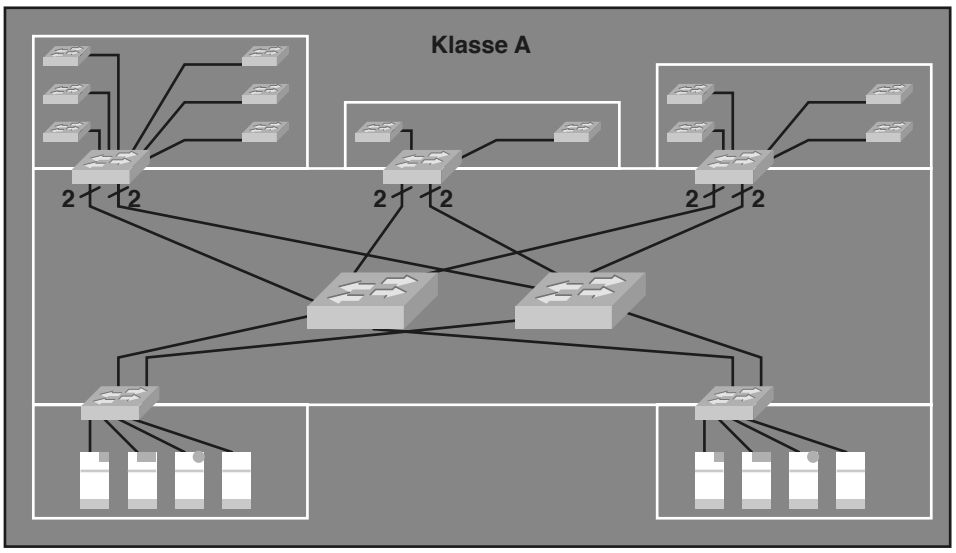


Bild 12: Kosteneinsparung durch Kaskadenmodell

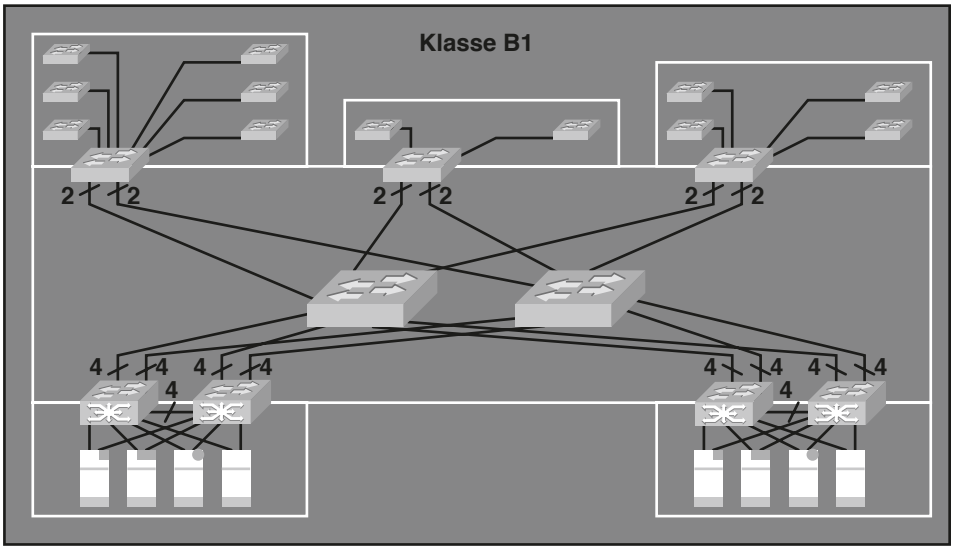
Eine vollständige Abhandlung zu den verschiedenen Netzklassen, den dazugehörigen Risikogruppen und unterschiedlichen Designlösungen für komplette Netze unterschiedlicher Größe gibt es im ComConsult Technologie Report „Design-Varianten Lokaler Netzwerke im Vergleich“.

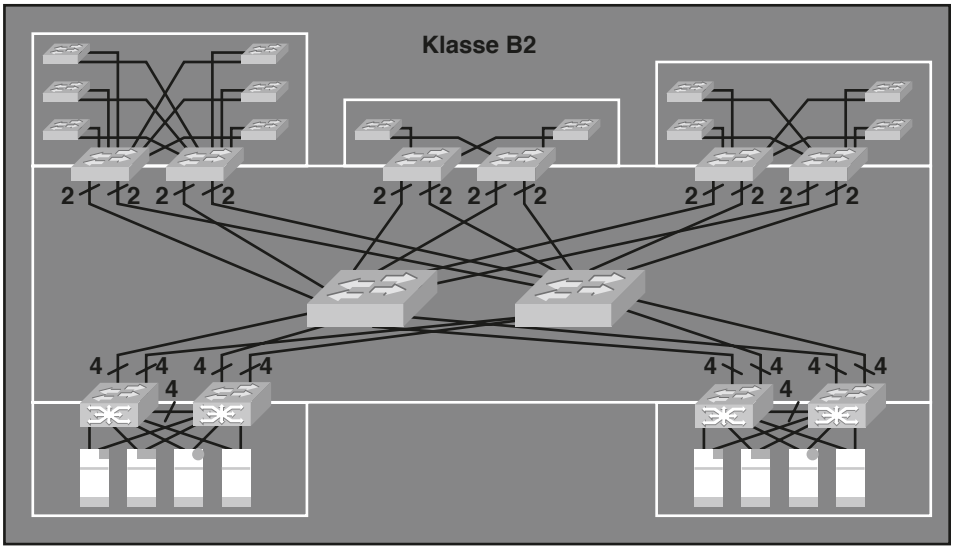
Bevor man jedoch nun freudig loszieht und die vorgestellte Kaskadenlösung umsetzt, sollte man einige weitere Überlegungen anstellen, denn es gibt natürlich auch Nachteile bei dieser Lösung:

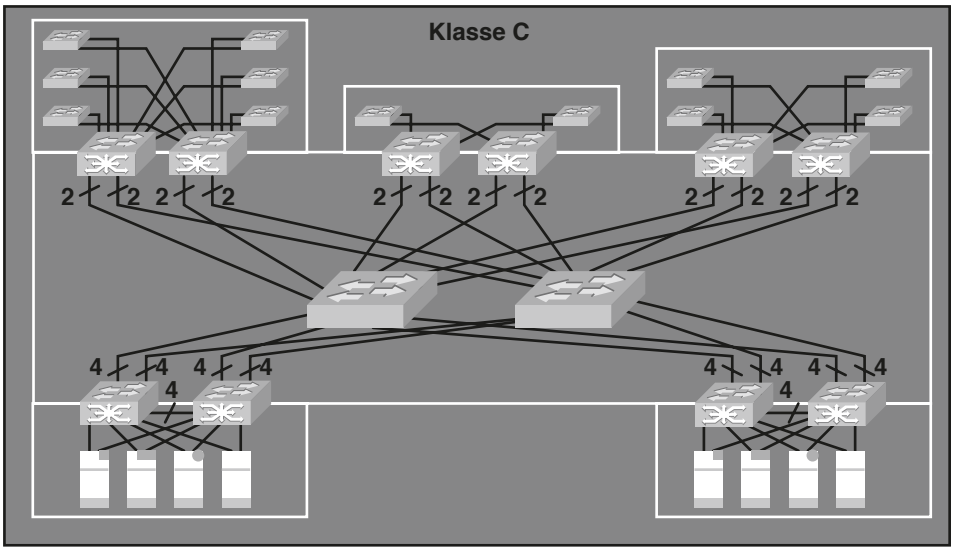
Bild 13a: Netzklasse A



Bilder 13b$_1$, b$_2$ und c: Netzklasse B1, B2 und C







Bandbreitenreserven und Skalierbarkeit

Eine einfache Überlegung: jeder der Etagenswitche verfügt über 48 100 Mbit/s Ports und zwei Gigabit Uplinks. In der Dreiecklösung ergibt sich daraus ein Überbuchungsfaktor von 4,8. Das ergibt sich zumindest in der Theorie, wenn alle 48 Clients gleichzeitig mit 100 Mbit/s senden, da der Switch die Daten nur mit 1000 Mbit/s zum HVT weiterleiten kann. Solange also nie mehr als circa ein Fünftel aller Clients mit Volllast senden, sollten sich keine Probleme ergeben.

Kaskardiert man nun, wie im Beispiel angenommen, drei dieser Etagenswitche ergibt sich ein Überbuchungsfaktor von 14,4. Jetzt darf nur noch etwa jeder 14. Client mit Volllast senden, ohne dass es auf dem Link zwischen HVT-Switch und dem 1. Etagenswitch zu Engpässen kommt.

Die Frage, die man sich stellen muss, ist somit: wie viel Überbuchung ist noch vertretbar.

Wohl dem, der die Auslastung seiner Uplinks kennt. Sollte ein Redesign des Netzes anstehen und man mit der Überlegung spielen, die Kaskade zum Einsatz zu bringen, muss man zuvor die Auslastung seiner Uplinks über einen längeren Zeitraum hinweg beobachten. Zwei Punkte sollte man jedoch bei der Untersuchung beachten:

1. Die Lastspitzen und nicht die Durchschnittslast ist entscheidend.

2. Die Entwicklung der Lastspitzen über den gemessenen Zeitraum.

Ersteres ergibt sich daraus, dass Netze nicht kontinuierlich unter Last stehen, sondern es in jedem Netz Zeiten gibt, in denen die Last größer ist, als normalerweise. Ein beliebtes Beispiel dafür sind die Zeiten zum Arbeitsanfang und zum Arbeitsende, wenn die Mitarbeiter quasi gleichzeitig ihre PCs einschalten und ihre Daten laden, bzw. wieder speichern. Den Rest des Tages, evtl. mit Ausnahme der Mittagspause, werden nur wenige Mitarbeiter gleichzeitig auf die Server zugreifen, so dass die Last auf den Uplinks während dieser Zeit eher zu einem Hintergrundrauschen als zu einem Problem wird. Ein Netz muss jedoch darauf ausgelegt sein auch in den kritischen Sekunden/Minuten noch fehlerfrei zu funktionieren.

Der zweite Punkt, die Entwicklung der Lastspitzen, ist deshalb von Interesse, da man bei einem Design nicht davon ausgehen darf, dass sich die Auslastung in einem Netz nicht verändert.

Im Gegenteil, man muss von vornherein davon ausgehen, dass sowohl die Auslastung, wie auch die Anzahl der am Netz angeschlossenen Systeme zunehmen wird. Darum sollte man eine Vorstellung davon haben, um wie viel Prozent die Netzlast pro Jahr anwächst – natürlich ist das eine Art von Orakeln, da man sich nie sicher sein kann, was in Zukunft passieren wird und ob nicht doch eines Tages noch eine Bandbreiten-intensive Applikation kurzfristig den Bedarf drastisch erhöhen wird. Aber umso wichtiger ist es, den aktuellen Bedarf und die vorhandenen Reserven zu kennen.

Bei einem Redesign mit und ohne RSTP-Kaskade müssen also ausreichend Bandbreitenreserven eingeplant werden. Als Faustregel kann man dabei davon ausgehen, dass ab einer Auslastung von 50% in Spitzenzeiten es zu ersten Problemen bei der Übertragung delay-kritischer Applikationen kommen kann. Es ist nicht zwingend notwendig, teuere Management-Tools zum Einsatz zu bringen, um die Auslastung der kritischen Uplinks im Auge zu behalten, gerade für solche, thematisch klar abgegrenzten Untersuchungen reicht ein freies Tools wie MRTG vollständig aus.

Neben ausreichenden Reserven gibt es noch einen anderen Punkt, den man bei der Planung berücksichtigen muss: Netze können wachsen. Auch bei Gebäuden, bei denen man sich nicht vorstellen kann, dass auch nur ein einziger weiterer Schreibtisch mehr hineinpasst, sollte man damit rechnen, dass in Zukunft trotzdem mehr Netzwerkanschlüsse benötigt werden. Es gibt viele Gründe, die zu einer Zunahme von Netzwerkanschlüssen in einem bereits voll besetzten Gebäude führen können, um nur einige zu nennen:

- Einführung einer VoIP Lösung
- Hinzukommen neuer Drucker
- Installation von Wireless LAN Access Points

Um dieser Anforderung begegnen zu können, sollte eine Lösung skalierbar sein. Das bedeutet, dass man ein Netz niemals so planen darf, dass das hinzukommen einiger weniger Clients dazu führt, dass die gesamte Architektur geändert werden muss. Um das zu verhindern, plant man von vornherein erstens freie Ports auf den Etagen und HVT-Switches ein, die bei Bedarf sofort genutzt werden können. Zweitens kauft man bei den modularen Geräten Chassis, die auch nach Bestückung und Inbetriebnahme noch freie Modulslots aufweisen. Auf diese Weise kann man später leicht Module nachrüsten und damit weitere Ports zur Verfügung stellen, ohne das ganz neue Geräte angeschafft werden müssen.

	Kaskade mit Nachrüstung	volle Dreieckschaltung
2002	Installation der Switches: 8 Port Modul inkl. 4 GBICs ca. 17.000 EUR	volle Dreieckschaltung: 3 Module mit 18 GBICs 56.000 EUR
2003	Umstellung auf Dreieckschaltung: 2 Module und 14 GBICs 24.000 EUR	
	ca. 41.000 EUR	56.000 EUR

Gerade was die Skalierbarkeit angeht, kann die Kaskaden-Lösung ihre Stärken ausspielen: stellt sich irgendwann heraus, dass mehr Bandbreite benötigt wird, kann man schrittweise von der Kaskadenlösung hin zur Dreieckschalung migirieren und somit den Überbuchungsfaktor verringern, was einer Bereitstellung weiterer Bandbreite gleichkommt. Dazu muss man den HVT-Switch jedoch so ausgelegt haben, dass er im Bedarfsfall ausreichend Uplinkports zur Verfügung stellen kann, um eine teuere Neuanschaffung zu vermeiden.

In diesem Zusammenhang kann man sich natürlich die Frage stellen, warum man nicht gleich die Dreieckschalung verwirklichen soll, wenn die HVT-Switches ohnehin über ausreichende Kapazitäten verfügen? Der Grund dafür liegt in dem Preisverfall der Module der HVT Switches. Betrachten wir das Beispiel erneut: reichen zunächst die 2x4 Ports aus, so kommt man mit einem 8 Port Modul pro Switch aus, damit hat man noch 4 Ports Reserve pro Switch, abzüglich der Ports die ggf. für die Standortbackbone-Verbindung benötigt werden. Die Anschaffungskosten belaufen sich somit zwei Mal auf die Kosten für das Chassis zzgl. je ein 8 Port Gigabit Modul. Die vollständige Dreieckschaltung benötigt 18 Ports pro Switch, was drei Gigabit-Modulen mit jeweils 8 Ports pro Switch beim Kauf bedeutet. Berücksichtigt man diese Skalierbarkeit bei der Anschaffung, so entscheidet man sich von vornherein für ein Chassis mit mindestens vier Modulslots, anstatt eines mit zweien, was zunächst ausreichen würde. Geht man davon aus, dass der Modulpreis bei der späteren Anschaffung um 30% gefallen ist, so spart man für dieses Geld gleich vier Mal: zweimal pro Switch (zwei Module werden erst später zum günstigeren Preis nachgekauft) und das für zwei Switches.

Noch zu theoretisch? Dann hier eine konkrete Rechnung, die Preise entstammen der Preisliste eines großen Distributors ohne jegliche Abzüge. Angenommen wird für die Berechnung folgendes: die Installation der Switches wurde im März 2002 vorgenommen und heute (November 2003), also ca. $1^1/_2$ Jahre später, müsste von der Kaskadenschaltung auf die Dreieckschaltung umgestellt werden. Vor $1^1/_2$ Jahren hätte das 8 Port Modul inkl. 4 GBICs ca. 17.000 EUR gekostet. Der Nachkauf heute kostet noch mal rund 24.000 EUR für zwei Module und 14 GBICs, macht zusammen ca. 41.000 EUR für die Kaskade mit Nachrüstung. Hätte man sich stattdessen direkt für die volle Dreieckschaltung entschieden, wären damals Kosten von 56.000 EUR angefallen, für 3 Module mit 18 GBICs. Macht eine Einsparung von 15.000 EUR pro Switch.

Es lohnt sich also, erst später nachzurüsten und nicht gleich voll aufzurüsten.

Design-Fazit

Durch den Rapid Spanning Tree lassen sich bei einem Redesign immens Kosten sparen, jedoch hat diese Einsparung, wie alles im Leben, seinen Preis: ohne Tests der Komponenten, die zum Einsatz kommen sollen und ohne das notwendige Wissen über die Auslastung des Netzwerkes bleibt alles beim Alten. Erst wenn man sein Netz kennt und bereit ist sich mit den Produkten auseinanderzusetzen, ist es möglich auch auf lange Sicht Kosten massiv einzusparen. Anders formuliert, es gibt keine allgemeingültige Lösung, kein Schema für ein Netzdesign mehr, sondern heute müssen individuelle Lösungen gefunden werden, und das ist nur möglich, wenn die notwendigen Kenntnisse vorhanden sind. Andernfalls muss man zur Maximallösung greifen, die jedoch auch maximal teuer ist.

Der Spanning Tree ist tot! – Es lebe der Spanning Tree!

Spezialfall Industrie: der HiPER-Ring

Neben den Tests zum RSTP wurde vom ComConsult Research Labor dieses Jahr auch eine ausführliche Untersuchen zu einem in der Industrie zum Einsatz kommenden alternativen Verfahren durchgeführt, dem High Performance Ring, kurz HiPER-Ring. Die gesamte Studie kann kostenfrei vom Web der ComConsult Technologie Information herunter geladen werden.

Im Folgenden werden die drei Verfahren kurz vorgestellt und nur auf einige der Ergebnisse kurz eingegangen. Diese werden zum Abschluss noch mit den bereits vorgestellten Ergebnissen der RSTP Tests verglichen.

HiPER-Ring

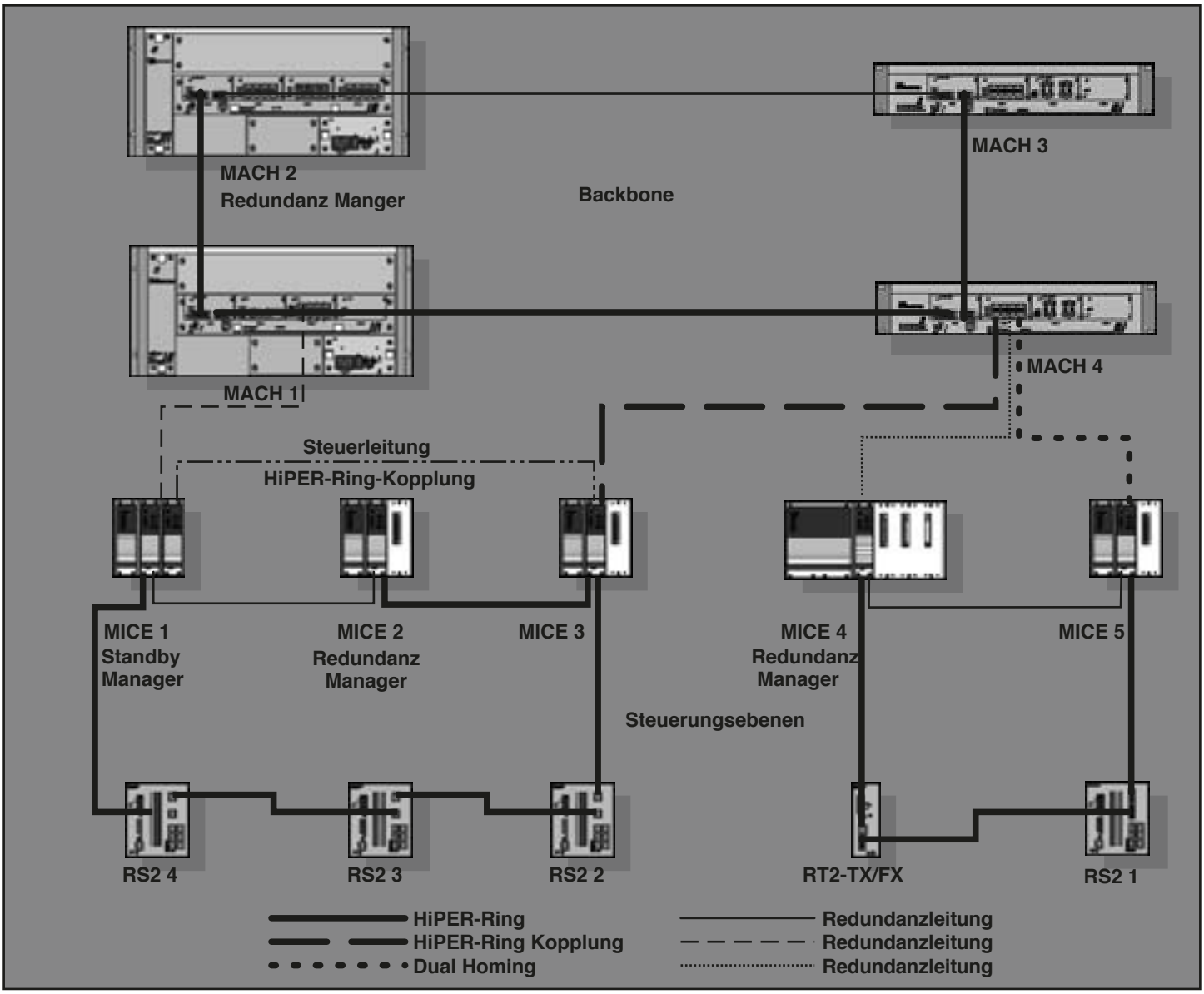
Herzstück der Hirschmann-eigenen Verfahren ist der HiPER-Ring. Die Idee ist, dass man ein gesamtes Netz in lauter Ringe zerlegen kann, die man wiederum redundant miteinander koppelt.

Bild 14 zeigt solch ein Design verschiedener gekoppelter Ringnetze: der Backbone und die einzelnen Steuerungsebenen werden mit dem HiPER-Ring verwirklicht, untereinander werden die Ringe entweder mit der neueren HiPER-Ring-Kopplung (grob gestrichelte Linien im Bild) oder dem älteren Verfahren, Dual Homing (fein gestrichtelte Linien im Bild), verbunden.

Durch die Kombination der Kopplungsverfahren und der Ringe entsteht typischerweise eine Topologie, die an einen Backbone-Ring sternförmig die Steuerungsringe anschließt. Da sowohl in jedem einzelnen Ring wie auch bei redundanter Ringkopplung jeweils eine Leitung deaktiviert ist, entsteht eine insgesamt loopfreie Topologie.

In jedem Ring gibt es eine ausgezeichnete Station, den Redundanz-Manager. Um einen Loop zu verhindern, unterbricht der Redundanz-Manager den Ring. Dazu werden auf einem passiven Ringport des Redundanz Managers keine dort empfangenen Datenframes verarbeitet und auch keine aus dem Port hinaus gesendet.

Bild 14: Übersicht der Hirschmann Verfahren



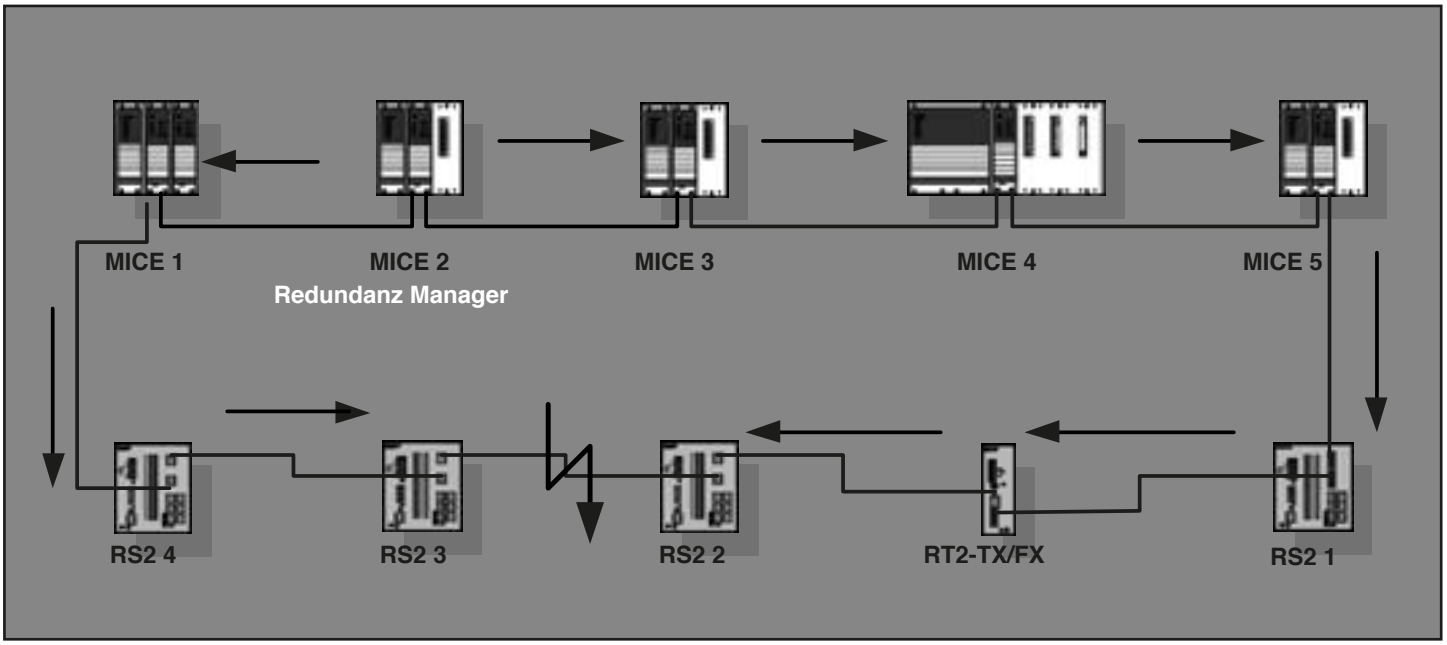


Bild 15: Fehlerbehebung im HiPER-Ring

Zur Überwachung des Ringes sendet der Redundanz-Manager alle 100 ms so genannte Watchdog-Pakete in beide Richtungen des Ringes, also auch aus dem Port, der keine Daten-Frames weiterverarbeitet. Gehen drei dieser Watchdog-Pakete in einer der beiden Richtungen verloren, so erkennt der Redundanz-Manager eine Unterbrechung des Ringes und aktiviert den bislang passiven Port. Für die Umschaltung bedeutet das, dass nach dem Ausbleiben des vierten Paketes, also nach 400ms der Switch erkennt, dass der Ring unterbrochen ist. Auf diese Weise entsteht, trotz Ausfall einer Leitung oder eines Gerätes, wieder eine vollständig verbundene Topologie.

Nach der Aktivierung des geblockten Ports durch den Redundanz-Manager, sendet dieser weiterhin Watchdog-Pakete, um auch die Wiederherstellung der Ausgangstopologie zu erkennen. Wird die defekte Leitung beispielsweise ausgetauscht und so wieder aktiv, so kommen die Watchdog-Pakete wieder durch und der Redundanz-Manager deaktiviert den Port, der auch vor dem Ausfalll deaktivert war. Um auch kurzfristige Loops im Ring zu verhindern, verwerfen die Systeme die Datenframes im Speicher, bis der Ring wieder hergestellt wurde. Im Gegensatz zum Rapid Spanning Tree kann es beim HiPER-Ring somit weder zu einer Vervielfachung von Frames noch zu einer Vertauschung der Reihenfolge kommen. Der Preis, den man dafür zahlen muss, ist jedoch, dass es bei der Umschaltung sowohl bei der Recovery wie auch bei der Wiederherstellung der ursprünglichen Topologie zu Paketverlusten kommt. Das gilt laut Aussage des Herstellers auch für alle anderen Redundanzverfahren von Hirschmann. Einen Tod, muss man halt sterben.

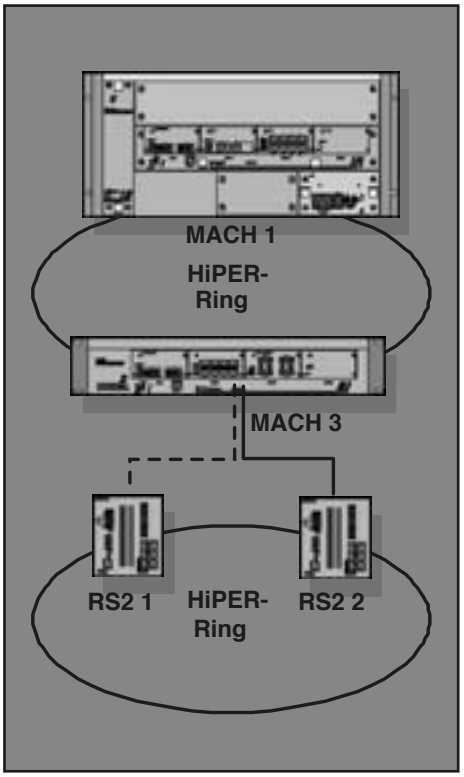
Anders als der Spanning Tree ist die Umschaltzeit des HiPER-Rings nicht von der Anzahl der eingesetzten Systeme abhängig. Die verzögernden Faktoren, die durch eine größere Anzahl von Switches hinzukommen, sind die Laufzeit der Watchdog-Pakete auf den Kabeln, die systembedingte Verzögerung pro Switch und maximal ein Paket, das von einem Switch gerade begonnen wurde zu senden, wenn ein Watchdog-Paket eintrifft, da die Systempakete mit höchster Priorität weitergeleitet werden. Diese Faktoren beeinflussen, wie auch die Messungen durch das ComConsult Research Labor gezeigt haben, die Umschaltzeit jedoch nur geringfügig, so dass Hirschmann eine Umschaltung unterhalb von 500 ms selbst bei 50 Switches und 3.000 km Leitungsweg garantiert.

Dual Homing

Ursprünglich wurde ein HiPER-Ring aus Hub-Systemen mittels Dual Homing an das Backbone gekoppelt. Dazu werden zwei Geräte des Ringes an ein Gerät, einen modularen Switch der MACH-Serie, angeschlossen wie in Bild 16 gezeigt.

Auf dem MACH 3 wird das Dual Homing konfiguriert, und dieser setzt einen der beiden Ports in den Discarding Modus. Fällt die primäre Verbindung aus, kann der MACH die sekundäre nahezu sofort in Betrieb nehmen.

Bild 16: Dual Homing



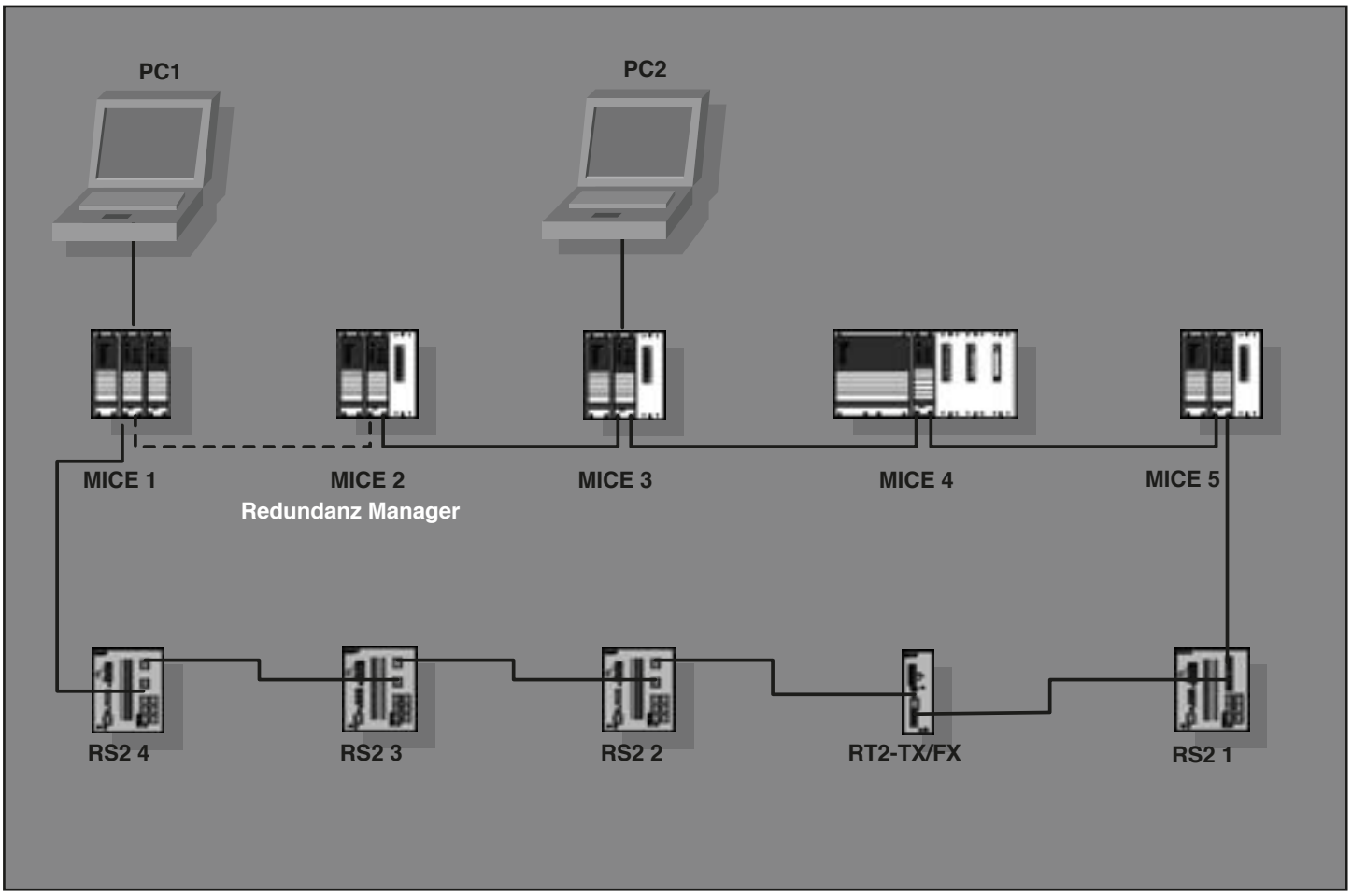


Bild 17: Testaufbau HiPER-Ring

Vorteil des Dual Homings sind sehr geringe Umschaltzeiten. Gravierender Nachteil ist jedoch, dass der Backbone-Switch einen Single-Point-of-Failure darstellt. Um diesen Nachteil abzumildern ist es möglich, für Dual-Homing-Ports verschiedener Basisbords desselben MACH-Gerätes zu nutzen. Es bleibt bei diesem Verfahren jedoch die Möglichkeit eines Ausfalls des gesamten modularen Systems als nicht auszugleichender Fehler. Ein weiterer Nachteil ist, dass Dual Homing nicht geeignet ist um zwei Steuerungsringe miteinander zu koppeln, da die Funktion nur für die MACH-Serie verfügbar ist.

HiPER-Ring-Kopplung

Die modernere HiPER-Ring-Kopplung hat diese Nachteile nicht mehr. Bei diesem Verfahren wird die Redundanz durch die Switches im Steuerungsbereich hergestellt. Dazu wird ein Switch als Standby-Manager konfiguriert. Dieser und ein zweiter Switch des Ringes werden dann an einen oder zwei verschiedene Geräte eines anderen Ringes angeschlossen. Zudem werden beide über einen speziellen „Standby Port“ miteinander verbunden. Einer dieser beiden Switches wird nun der Master und aktiviert die Kopplungsleitung zum anderen Ring, der andere wird zum Slave und setzt seinen Port in den Discarding Modus.

Fällt die Verbindung des Masters zum anderen Ring aus, so informiert er daraufhin sofort den Slave, und dieser aktiviert seine Verbindung.

Da theoretisch auch die Verbindung im anderen Ring unterbrochen werden kann, im Beispiel zwischen dem MACH 1 und MACH 3, oder die Standby-Leitung zwischen RS2 1 und RS2 2 ausfallen kann, senden sich Master und Slave wie beim HiPER-Ring Testpakete zu. Kommen diese Testpakete nicht mehr durch, so aktiviert RS2 2 ebenfalls seine Verbindung zum MACH 3 unabhängig davon, dass der Befehl über die ausgefallene Steuerleitung ausblieb; allerdings ist diese Art der Umschaltung, wie der Test gezeigt hat, signifikant langsamer.

Ende 2003, also jetzt, soll es für die MICE-Switches eine Lösung geben, die auf die zusätzliche Steuerleitung verzichten kann, indem sie durch Steuerpakete ersetzt wird.

Testaufbau HiPER-Ring

Bei den Tests wurden insgesamt fünf MICE-Systeme und vier RAIL-Switches der Firma Hirschmann eingesetzt. Besonderes Augenmerk wurde bei den Tests darauf gelegt, ob die Aussagen von Hirschmann, dass keine Umschaltung länger als 500ms braucht und das die Anzahl der Switches die Recoveryzeit kaum beeinflusse. Der Testaufbau ergibt sich aus Bild 17.

Es wurden analog zur RSTP Messung sowohl die Zeiten für die Unterbrechung des Ringes wie auch für seine Wiederherstellung gemessen. Das Testverfahren war mit dem Testverfahren zum RSTP identisch.

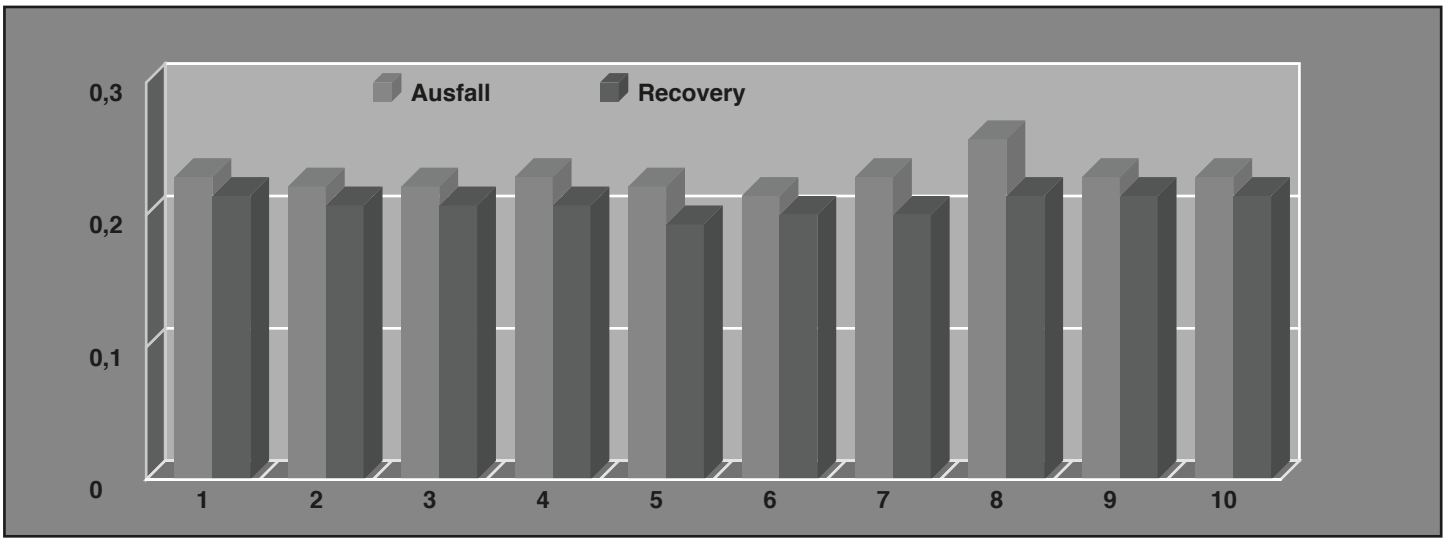


Bild 18: Umschaltzeit über 9 Switches beim HiPER-Ring

Schwankung der Umschaltzeit beim HiPER-Ring

Wie beim RSTP Versuch wurde auch bei den Test zum HiPER-Ring der Test zunächst 10 Mal hintereinander ausgeführt und der Mittelwert gebildet. Abbildung 18 zeigt die Einzelergebnisse sowohl für die Ausfall des Links wie auch für die Wiederherstellung des Ringes.

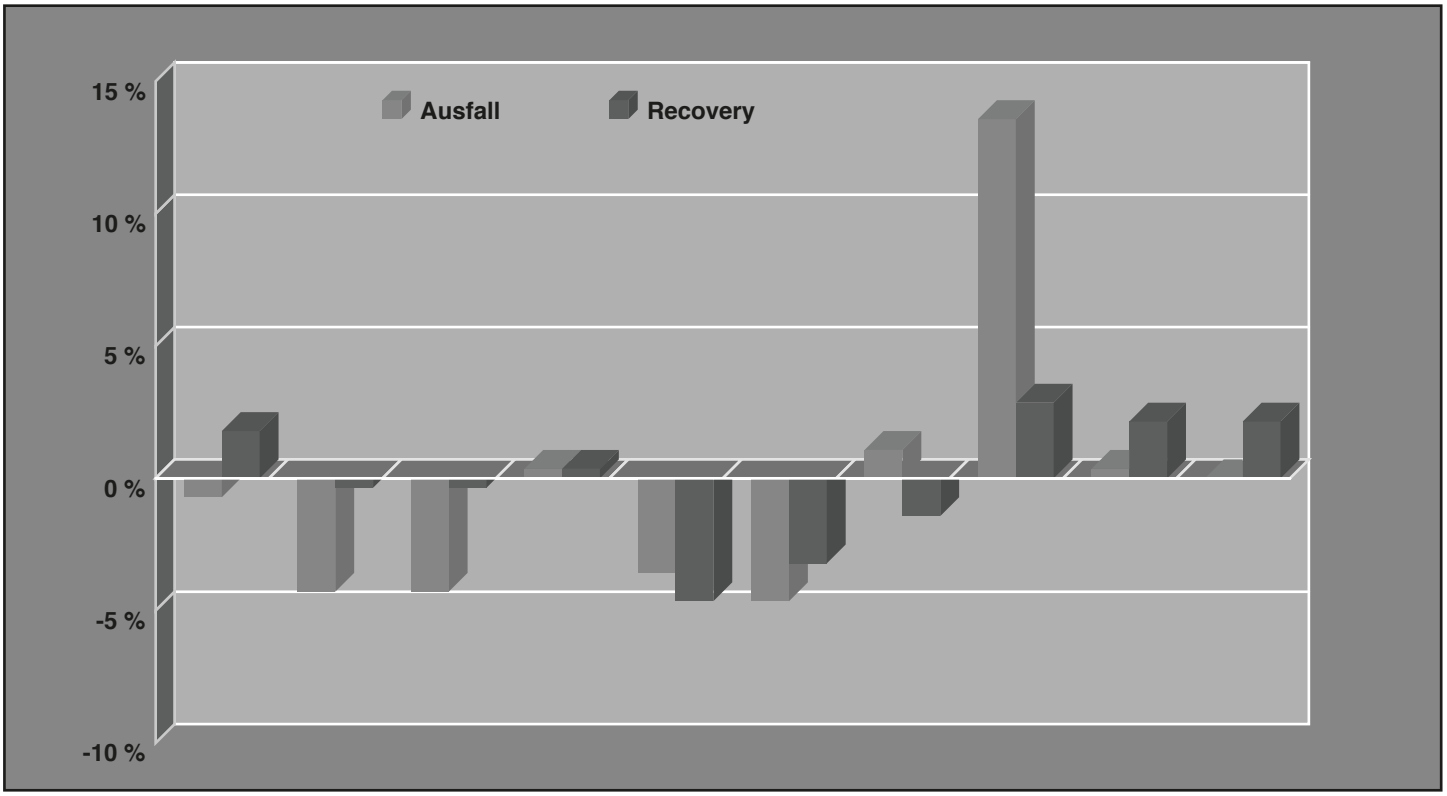
Es fallen zwei Punkte sofort ins Auge:

3. Die Umschaltzeit für den Ausfall und die Recovery ist - anders als beim RSTP - nahezu identisch.

4. Die Schwankung zwischen den einzelnen Messungen ist offensichtlich geringer, als sie es beim RSTP Verfahren war.

In der Tat ist die größte Abweichung vom Mittelwert ca. 13% und bei den 20 Messungen war das die einzige, die mehr als 5% vom Durchschnittwert abwich. Damit ist die Schwankung beim HiPER-Ring entschieden geringer als die beim RSTP, oder anders formuliert, sie sind vorhersagbar, also deterministisch.

Bild 19: Prozentuale Schankung der Umschaltzeit beim HiPER-Ring



Ansteigen der Umschaltzeit in Relation zur Anzahl der Switches

Wie bereits für den Rapid Spanning Tree wurde auch für den HiPER-Ring die Abhängigkeit der Umschaltzeit von der Anzahl der eingesetzten Switches untersucht.

Wie Abbildung 20 zeigt, besteht anders als beim RSTP keine messbare Abhängigkeit. Die leichten Schwankungen zwischen den einzelnen Messergebnissen resultieren aus den protokollbedingten Abständen zwischen den Watchdog-Pakten. Da anders als beim Rapid Spanning Tree beim HiPER-Ring keine Kommunikation zwischen benachbarten Switches notwendig ist, sondern allein der Ring-Manager die Entscheidung trifft, hängt die Umschaltzeit nur von der Laufzeit der Pakete ab, was erklärt, warum die Anzahl der Switches nahezu keinen Unterschied macht.

Bei den dargestellten Testergebnissen handelt es sich um die Ergebnisse der Messungen des Worst-Case: die Umschaltung wurde durch das ziehen einer einzelnen Glasfaserverbindung (Erzeugen einer Unilink-Situation) ausgelöst. Zwar wird auch in diesem Fall eine eventgesteuerte Meldung an den Ring-Manager geschickt, die eine schnellere Umschaltung auslösen kann, jedoch wurde der Link so gezogen, dass die Meldung an den passiven Port des Ring-Managers geschickt wurde. Der Ring-Manager des dargestellten Tests war nicht in der Lage solche Messages auf dem passiven Port zu verarbeiten, weshalb die Ring-Recovery durch das Ausbleiben der Watchdog-Pakete ausgelöst wurde. Gegentests, sowohl mit Komponenten, die auch auf dem passiven Port Änderungsmeldungen verarbeiten, als auch Messungen bei denen beide Glasfasern gleichzeitig gezogen wurden, zeigen, dass die Umschaltzeit dadurch noch einmal erheblich minimiert wird.

Tests bezüglich der Umschaltzeiten in Lastsituationen und bei bidirektionalen Datenströmen zeigen wie auch beim RSTP, dass keine Abhängigkeiten vorliegen. Auch die anderen vorgestellten Verfahren liegen bei Recovery-Zeiten unter 500 ms.

Zusammenfassung der Ergebnisse des HiPER-Rings

Sämtliche Verfahren rund um den HiPER-Ring glänzen mit Umschaltzeiten von unter 500 ms, nicht bei einer einzigen Labormessung dauerte es länger. Gerade der HiPER-Ring eignet sich gut für Projekte mit großen Ausdehnungen, in denen lange Leitungen und viele hintereinander geschaltete Switches benötigt werden. Ebenso ist er einsetzbar, wenn es wichtig ist, dass es zu keiner Paketwiederholung oder Paketvertauschung kommt.

Fazit

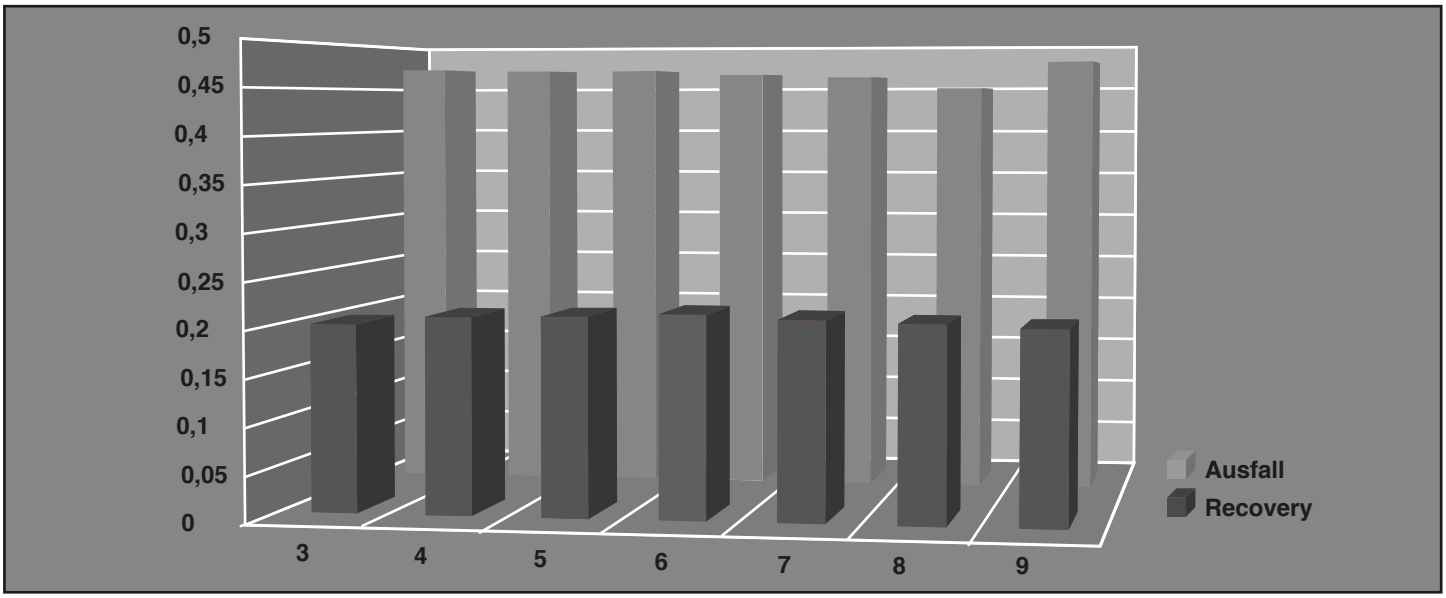
Vergleicht man abschließend den neuen Spanning Tree mit einem propietären Verfahren wie dem HiPER-Ring, so ergibt sich folgendes Bild:

Für die meisten Anwendungen dürfte der Rapid Spanning Tree mit seinen Umschaltzeiten im Sekundenbereich durchaus ausreichen. Unter der bereits angesprochenen Einschränkung, dass es Implementierungen gibt, die deutlich länger für die Recovery brauchen. Auch ist in den meisten Fällen nicht entscheidend, dass die genaue Zeit für die Wiederherstellung einer aktiven Topologie vorhersagbar ist. Hinzu kommt, dass sich der RSTP ausgezeichnet eignet, um sowohl Mehrfachredundanzen wie auch komplexe Topologien mit einem einzigen Protokoll zu verwirklichen. Ausreichende Tests der Komponenten vorausgesetzt, kann bei einem Neu- oder Redesign eines Netzes durch den Einsatz von RSTP eine Menge Geld gespart werden, ohne auf Redundanzen oder eine schnelle Recovery verzichten zu müssen. Ungeklärt ist jedoch zum aktuellen Zeitpunkt die Verträglichkeit von Implementierungen verschiedener Hersteller.

Die HiPER-Ring Verfahren auf der anderen Seite erfordert ein strenges Design, bei dem mit zumindest zwei Techniken gearbeitet werden muss, dem HiPER-Ring als Basistechnologie und der HiPER-Ring-Kopplung, um die einzelnen Ringe miteinander zu verbinden. Mehrfachredundanzen sind zunächst nicht vorgesehen, sondern müssen durch mehre Ringe, die parallel laufen, unter Einbeziehung der angeschlossenen Endsysteme verwirklicht werden (Stichwort: doppelter Netzanschluss).

Seine Vorteile kann der HiPER-Ringes in Umgebungen ausspielen, bei denen schnelle, vorhersagbare Umschaltzeiten gefordert sind, ebenso wenn Paketwiederholungen bzw. Verdopplungen um jeden Preis ausgeschlossen werden müssen. Auch bei großflächigen Projekten mit weitläufigen Ausdehnungen, bei denen viele Switches benötigt werden, sollte man diese Alternative zum Standardverfahren in Betracht ziehen.

Bild 20: Abhängigkeit der Umschaltzeit von der Anzahl der Switches beim HiPER-Ring



CCNE

ComConsult Certified Network Engineer

Lokale Netze
- 02.02.-06.02.04 Aachen
- 19.04.-23.04.04 Aachen

TCP/IP und SNMP
- 02.02.-06.02.04 Bonn
- 03.05.-07.05.04 Berlin

Internetworking
- 02.02.-06.02.04 Aachen
- 19.04.-23.04.04 Aachen

Ethernet Technologien – neuester Stand
- 08.03.-12.03.04 Aachen
- 28.06.-02.07.04 Aachen

Paketpreis für alle vier Seminare: € 7.780 ,-- zzgl. MwSt.
(Einzelpreise: je € 2.290,--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
- 02.02.-06.02.04 Aachen
- 26.04.-30.04.04 Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
- 01.03.-05.03.04 Aachen
- 10.05.-14.05.04 Aachen

Trouble Shooting für TCP/IP-und Windows-Umgebungen
- 19.01.-23.01.04 Aachen
- 29.03.-02.04.04 Aachen

Paketpreis für alle 3 Seminare mit Sniffer-Lizenz:
€ 7.500,-- zzgl. MwSt. (Seminar-Einzelpreise: je € 2.490,--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
- 01.03.-05.03.04 Köln
- 24.05.-28.05.04 Köln

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
- 22.03.-24.03.04 Bonn
- 28.06.-30.06.04 Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
- 19.04.-23.04.04 Aachen
- 19.07.-23.07.04 Aachen

Paketpreis: € 5.330,-- zzgl. MwSt.
(Einzelpreise: € 2.290,-- / € 1.690,-- / € 2.290,--)

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

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