ComConsult Research

Der Netzwerk Insider

Mai 2007

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

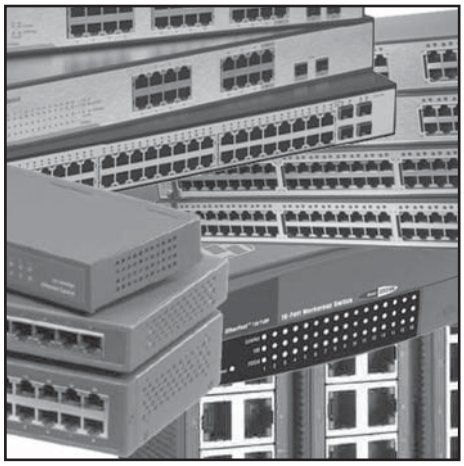
Dual-Vendor-Strategien im LAN

von Dr. Simon Hoff, Dr. Frank Imhoff

1. Vorbemerkungen

Monokulturen im Sinne der exklusiven Verwendung der Komponenten eines einzelnen Herstellers sind im LAN-Switching-Bereich noch die Regel. Dabei drängen Ausrüster auch bewusst durch herstellerspezifische Funktionen und Dienste bzw. deren herstellerspezifische Ergänzungen auf die ausschließliche Verwendung ihrer Komponenten.

Dem stehen wirtschaftliche Erwägungen entgegen. Warum sollte auf einer Netzebene (z.B. im Access-Bereich) nicht ein anderer Hersteller als auf einer anderen Netzebene (z.B. im Distribution-Bereich)



eingesetzt werden, sofern dies insgesamt wirtschaftlicher ist?

Die Schwierigkeiten liegen dabei nicht nur auf einer technischen Ebene (etwa in der Problematik der Freiheitsgrade in der Implementierung eines Protokolls, das zwischen den Geräten unterschiedlicher Hersteller genutzt wird). Kaufmännische und organisatorische Aspekte haben einen entscheidenden Anteil am Erfolg einer Dual-Vendor-Strategie.

Dieser Artikel analysiert Rahmenbedingungen, Konzepte, Szenarien und Vorgehensweisen für eine Dual-Vendor-Strategie.

weiter auf Seite 24

Zweitthema

Der schnelle Baum

von Markus Schaub

Mit dieser Ausgabe beginnen wir im Netzwerk-Insider eine Serie zu den elementaren Netzwerk-Grundlagen, die insbesondere die Neueinsteiger in den LAN-Markt unterstützen soll.

Den Anfang macht die Beschreibung des mittlerweile wichtigsten Layer-2-Redundanz-Verfahrens im LAN: der Rapid Spanning Tree, der seit einigen Jahren den ursprünglichen Spanning-Tree abgelöst hat. Allerdings gibt es im Low-End-Bereich immer noch Switche, die nur das alte Verfahren unterstützen.

Der seit Ende der 80er-Jahre existierende Spanning-Tree hat eine ganze Reihe von Mängeln aufzuweisen. Schnell lassen sich darunter zwei Hauptkritikpunkte ausmachen:

1. Die Umschaltzeiten des klassischen Spanning-Tree liegen jenseits dessen, was in modernen Netzen toleriert werden kann.

2. Durch das faktische Abschalten von Verbindungen wird jegliche Lastverteilung unterbunden und man hat jede Menge „totes Kapital“ in Form von ungenutzten Leitungen in seinen Kabelschächten liegen, die noch dazu an teuere Switch-Ports angeschlossen sind, aber keine Pakete transportieren.

weiter auf Seite 9

Kongress des Monats

ComConsult SIP-Forum 2007

auf Seite 6

Geleit

Unruhe im Wireless-Markt: IEEE 801.11n-Design mit Fragezeichen

auf Seite 2

Juni-Highlight

Sommerschule 2007

auf Seite 4

Zum Geleit

Unruhe im Wireless-Markt: IEEE 801.11n-Design mit Fragezeichen

Obwohl die offizielle Verabschiedung des IEEE 802.11n-Standards nicht vor August 2008 zu erwarten ist, sind seit der Verabschiedung des Draft 2.0 im März alle Signale auf Fahrt gesetzt. Der Draft wird allgemein so interpretiert, dass zukünftige Änderungen nur noch die Firmware betreffen, der Chip aber stabil ist. Das letzte Hindernis für eine großflächige Ausbreitung liegt im Nachweis der Interoperabilität der Produkte verschiedener Hersteller.

Die WiFi-Alliance wird dieses Hindernis in den nächsten Wochen mit einem offiziellen Interoperability-Test beseitigen. Im Konsumer-Markt rollen bereits die Produkte an, vorneweg Apple und D-Link. Verschiedene Leistungstests zeigen, dass die Probleme früherer Generationen scheinbar überwunden sind. Zumindest können eine Reihe von Produkten stabile Nutzdatenraten von 70 bis 80 Mbit/s auch über größere Distanzen nachweisen.

Nun mehren sich die Anzeichen, dass noch in diesem Jahr die ersten namhaften Enterprise-Anbieter mit Produkten auf der Draft 2.0-Basis auf den Markt kommen werden, der Name Cisco wird in diesem Zusammenhang häufiger genannt. Der Blick hinter die Kulissen zeigt, dass viele Hersteller in ihren Entwicklungen weit fortgeschritten sind. Der erste namhafte Anbieter, der diesen Markt betritt, wird eine sofortige Welle entsprechender Produkte aller führenden Anbieter auslösen. Im Moment spricht also einiges dafür, dass der Wechsel auf 11n im Enterprise-Markt bis Ende des Jahres erfolgt.

Damit wird es Zeit, sich mit dem Standard näher zu befassen. Für viele wird dies ein unangenehmes Erwachen bringen. Bisher war die Botschaft des Standards klar:

- zwischen 300 und 600 Mbit/s Rohdatenrate, Nutzendatenraten über 100 Mbit/s
- dies kombiniert mit einer höheren Reichweite (keine falschen Erwartungen, hier wird im Kern die Reichweite angesprochen, die stabil ohne große Schankungen abgedeckt werden kann. Diese wird weiterhin bei maximal 25 oder 30m im Inhaus-Bereich liegen, je nach Umfeld auch darunter). Auch ansonsten sollte mit der erhöhten Reichweite vorsichtig umgegangen werden, je größer eine Zelle wird, desto mehr Teilnehmer können in der Zelle sein, die Schwankungen im Bedarf nehmen mit größeren Reichweiten deutlich zu

Alles in Allem klingt das doch gut, oder? Parallel müssen die Hersteller eine neue Produkt-Generation einläuten, da die mit 11n zu realisierenden Datenraten mehr CPU-Leistung und mehr Pufferspeicher erfordern.

Doch dies ist bei näherer Betrachtung zu kurz gedacht. Geht man näher ins Detail, dann kann man den Standard in 3 Teile zerlegen:

- eine Konsumer 2,4 GHz-Version mit 20MHz-Kanälen
- eine Enterprise 5 GHz-Version mit 20 MHz-Kanälen
- eine Enterprise 5 GHz-Version mit 40 MHz-Kanälen

Parallel muss mit zunehmender Leistung die Zahl der Antennen zunehmen, was bei gleichzeitig vorgegebenen Mindestabständen zwischen Antennen große Auswirkungen auf das Produktdesign hat. Wie auch immer, die volle Leistung wird IEEE 802.11n nur im 5 GHz-Bereich erzielen. Dies ist einerseits erfreulich, da der Wechsel in den 5 GHz-Bereich mit einer Reihe von Vorteilen verbunden ist (und mit einer Reihe von unangenehmen Problemen), aber andererseits wirft dies sofort die Frage der Einbindung der bestehenden 11b/g-Geräte auf. Rückwärts-Kompatibilität ist eines der großen Fragezeichen des 11n-Standards. Nicht, dass diese nicht im Standard vorgesehen ist, doch irgendwie macht sie keinen Sinn im Design.

Hinzu kommt ein anderes sehr ernst zu nehmendes Problem. Eine Schlüsselfrage im Wireless-Design ist seit Jahren der Wechsel von Einzelzellen auf ein flächendeckendes Design. In einigen Märkten wie Krankenhäusern und Warenhäusern ist dies zwar üblich, in der breiten Masse bisher nicht. Das macht auch durchaus Sinn, konnte doch allgemein mit dem Wechsel auf 11n eine komplette neue Generation von Produkten erwartet werden.

Nun ist aber die “Killer-Applikation” für ein flächendeckendes Wireless-Netzwerk Voice-over-Wireless. Vielleicht sollte man hier auch besser SIP-over-Wireless sagen, um damit zu unterstreichen, dass es nicht nur um Voice geht sondern um eine umfassende Einbindung mobiler Teilnehmer in Realzeit- und Kollaborations-Dienste.

Und nun wird es unschön. Bisher ist in keiner Weise abzusehen, dass entsprechende Telefone im 5GHz-Bereich entwickelt werden, für die 40 MHz-Version ist es eigentlich auch fast undenkbar, allein schon wegen der Zahl dafür notwendiger Antennen und deren Mindestabstand. Auch ist das Stromversorgungsproblem bisher scheinbar nicht lösbar.

Im Rahmen des Geleitworts soll das nicht weiter vertieft werden, da es den Rahmen sprengt. Wir werden diese Dis-

kussion im Detail in der Sommerschule führen.

Aber was ist die Konsequenz aus dieser Diskussion? Bisher ganz einfach: IEEE 11n wird aus Gründen der Rückwärtskompatibilität und der Einbindung von Voice-over-Wireless eine parallele 11g-Struktur erfordern! Dies hat ohne Frage Riesen-Auswirkungen auf das Design.

Mach nichts, denken Sie wahrscheinlich, es gibt ja Dual-Radio-Access-Points. Dies ist einer der großen Fragen an die zukünftigen Produkt-Generationen. Aufgrund des Antennen-Designs ist das nicht selbstverständlich. Im schlimmsten Fall kann es passieren, dass 11n-Access-Points nicht unbedingt Dual-Radio sein werden. Vermutlich wird es Sonderprodukte für Wireless-Distribution-Systeme und MESH-Netzwerke geben, aber diese werden aus heutiger Sicht einen hohen Preis haben.

Überhaupt deutet sich an, dass die von Dr. Kauffels in den letzten Insider-Ausgaben gestartete Diskussion über MESH-Netzwerke eine hohe Aktualität hat. Mit dieser Diskussion war ja auch die Frage verbunden, ob der traditionelle Wireless-Weg, auf dem wir gerade gehen, nicht auf Dauer in eine Sackgasse führt. Betrachtet man die soeben ausgeführte 11n-Problematik, so wird klar, dass in der Tat der Charme einer MESH-Lösung zunimmt. Auch MESH-Netzwerke sind nicht frei von Fragezeichen. Der technische Schlüssel zum Erfolg liegt hier im intelligenten Routing und in der Lastadaption zwischen den Knoten, da MESH-Netzwerke die Gefahr von Engpass-Stellen beinhalten.

Wie auch immer, wer heute ein Wireless-Netzwerk zu designen hat, ist nicht zwingend zu beneiden. Auf jeden Fall sollte er mitten in der aktuellen Diskussion stehen.

Wir haben Wireless-Technologien zu einem der Schwerpunkte der Sommerschule gemacht. Im Rahmen einer umfassenden Design-Diskussion werden wir mit Ihnen auf der Sommerschule 2007 diskutieren, wie Sie im Moment sinnvoll mit diesen Technologien umgehen können.

Auf jeden Fall werden wir Sie in den nächsten Monaten hier auf dem Laufenden halten,

Ihr
Dr. Jürgen Suppan

Juni-Highlight

Sommerschule 2007

Die ComConsult Akademie veranstaltet vom 11.06. - 15.06.07 ihre „Sommerschuel 2007 - Intensiv-Update auf den letzten Stand der Netzwerktechnik“ in Aachen.

Die ComConsult-Sommerschule bietet den kompakten und intensiven Update auf den letzten Stand der Netzwerk-Technick. Damit wendet sich die Sommerschule speziell an erfahrene Teilnehmer/Innen, die neue Entwicklungen und Technologien kennen lernen und den Betrieb ihrer bestehenden Netzwerke weiter optimieren wollen.

Die Sommerschule 2007 bietet folgende Themen-Schwerpunkte über 5 Intensiv-Tage:

Netzwerk-Design

Viele bestehende Netzwerke kommen an das Ende der Lebensdauer wichtiger Komponenten. Parallel ändern sich Design-Prinzipien, um den Anforderungen moderner Anwendungen von SOA bis IP-Telefonie gerecht zu werden.

Der Design-Block der Sommerschule greift die aktuellsten Neuentwicklungen und Diskussionen auf:

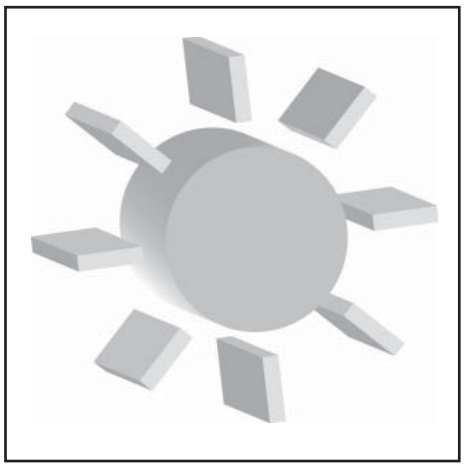
Sprache und Realzeitdienste im Netzwerk
- VLAN´s: pro und kontra
- Dynamische kontra statische VLANs
- Einsatz des Link Layer Discovery Protocols

Einfache und effiziente Netzwerk-Konfiguration
- Wie einfach darf ein Netzwerk-Design sein?
- Entscheidungen für Design-Alternativen

Die Rolle des VLAN im modernen Netzwerk-Design
- Typische Einsatzbereiche
- Statische VLANs

Dynamische VLANs: automatische Zuordnung von Endgeräten, wie geht das?

Quality of Service in der Kritik
- Motivation für Quality of Service
- Umsetzungs-Alternativen
- Wo QoS unverzichtbar ist?
- Flächendesign erforderlich?
- Nachteile
- Umsetzung eines partiellen QoS-Designs
- Was passiert an den Übergangen zum WAN?
- Was passiert zwischen WLAN und LAN?



Wie reagiert ein Switch auf MAC-Flooding, wie stabil ist dabei die bestehende VLAN-Zuordnung?

WAN: Planung und Redesign
- Auswirkung und Handhabung von Engpässen
- QoS im WAN
- WAN-Optimizer: Verzichtbarer Luxus oder auf Dauer unvermeidbar?
- Setzung automatischer Prioritäten nach Protokolltyp und Anwendung
- Wie kann dynamisches, adaptives und Session-bezogenes Bandbreiten-Management realisiert werden?
- Kann IP-Telefonie ohne WAN-Optimizer auf Dauer sicher und stabil betrieben werden?
- WAN-Ausschreibung

Ausgewählte Technologien

In diesem Themenblock werden ausgehend von der Vorgehensweise bei einem Netzwerk-Audit wichtige neue technologien bzw. Änderungen und Weiterentwicklungen bestehender Technologien diskutiert:

Netzwerk-Audit: Ihr Netzwerk kommt in die Jahre, nach welchen Kriterien kann es überprüft werden?
- Kriterienliste
- Projekterfahrungen
- Empfehlungen

10 Gigabit-Ethernet in der Analyse:
- Arbeitsweise und Varianten
- Twisted Pair: wo stehen wir?
- Design-Einflüsse von 10 Gigabit
- Auswirkungen auf Buchungsfaktoren?

Netzwerke im Rechenzentrum
- Spezielle Eigenschaften von RZ-LAN´s
- Server und Speicher: welcher Bedarf besteht
- Lösungsalternativen
- Einbindung in das Core-Netzwerk

Verkabelung: Update auf den Stand der Technik
- Standardisierung letzter Stand
- Kabel- und Stecker-Qualitäten
- Was erfordert 10 Gigabit
- Kupfer-Trends
- Glasfaser-Trends
- Wichtige Installations-Themen

IP-Redesign
- Adressbedarf
  - Wann sind die öffentlichen Adressen ausgeschöpft?
  - Wie viele Adressen benötigt ein Unternehmen in Zukunft?
  - NAT und seine Grenzen
- DNS/DHCP im Redesign
- Risikobereich Multicast-Routing
- Mobile Teilnehmer und ihre Integration in TCP/IP
- IPv6
- TCP/IP-Tuning
- Management und Monitoring

Netzwerk-Sicherheit

Wie viel Sicherheit im Netzwerk ist sinnvoll und notwendig? Die zur Verfügung stehenden Sicherheits-Lösungen bieten immer neue Varianten und Ansätze zur Erhöhung der Sicherheit, aber zum Teil sind die Ansätze sehr komplex, zum Teil muss auch an ihrem Sinn gezweifelt werden. Neu im Rennen um das sicherste Netzwerk ist Network Access Control NAC, in den USA bereits ein Hype, in Deutschland noch vor der Einführung. Aber speziell die Allianz zwischen Cisco und Microsoft puscht diese Technologie vorwärts. Geht es hier um Sicherheit oder um die Schaffung neuer Abhängigkeiten?

Dieser Themen-Block analysiert wichtige Sicherheits-Technologien, erklärt ihre Arbeitsweise und bewertet sie:

Basis-Konzepte für Netzwerk-Sicherheit

ACL: Vorteile und Grenzen des Konzepts

MAC-Adress-Authentifizierung und seine Grenzen

Sommerschule 2007 - Intensiv-Update auf den letzten Stand der Netzwerk-Technik

- Wann sind Tools wie QIP sinnvoll?

IEEE 802.1X in der Analyse:
- Arbeitsweise
- Notwendige Entscheidungen
- MD5, PEAP, TLC: wie kann eine überschaubare und einheitliche Lösung erreicht werden, müssen Telefone und PC´s identisch behandelt werden?
- Mobile Teilnehmer und ihre Integration
- Einsatz von Directory Services: Machbarkeit und Grenzen
- Machen Gruppenrichtlinien für Windows XP Sinn, wofür sind sie nutzbar, wo fehlen sie?
- Wie werden Endgeräte behandelt, die 1X nicht unterstützen?
- Mehrere Geräte pro Port: Arbeiten gegen den Standard?
- Geeignet für Kabelnetze oder beschränkt auf WLANs
- Schlüsselfrage Monitoring: sollen gehäufte Fehlversuche erkannt werden? Ist eine Alarmfunktion erforderlich? Wie geht das?

Network Access Control NAC: der Mega-Hype und seine Nutzbarkeit
- Arbeitsweise
- Frameworks im Vergleich
- Wie ist die NAC-Allianz aus Cisco und Microsoft zu bewerten?
- Wo steht TNC?
- Brauchen wir Sicherheitsbereiche, in denen nur geprüfte Clients ins Netzwerk dürfen?

Wireless LANs

Das Warten auf IEEE 802.11n blockiert den WLAN-Markt. Doch es gibt erhebliche Missverständnisse und Fehleinschätzungen zu dieser Technologie. Speziell der Bereich der Rückwärts-Kompatibilität und Einsatzsituationen mit Dual-Radios bedürfen der Analyse. Sie haben massive Auswirkungen auf das Design. Parallel ist der gesamte Enterprise-Markt auf Wireless-Switches gewechselt. Auch hier gibt es deutlichen Diskussions-Bedarf. Zum Teil fehlen den Produkten wichtige Eigenschaften, Projekte können ernsthaft gefährdet sein.

Ein besonderes Highlight dieses Themenblocks wird die Vorstellung einer neuen und innovativen Technologie sein, die das Potenzial hat, unsere gesamte Arbeit, unser Verständnis von Netzwerken zu ändern: MESH-Netzwerke. Bisher blockierten hier fehlenden Standards eine Weiterentwicklung, doch nun zeichnet sich ein klares und revolutionäres Bild dieser neuen Technologie ab.

Dieser Themenblock analysiert und diskutiert weiterhin mit Ihnen:

- Stand der Technik und Trends
- IEEE 802.11n: wie arbeitet es, was wird es bringen?
- High-End-Konsumer-Produkte: eine Alternative?
- Fat-Access-Points kontra Wireless-Switche
- Zentrales Management von Fat Access-Points
- Wireless-Switches: wohin geht der Weg?
- Einfluss von IEEE 802.11n auf das zukünftige Design von Netzwerk-Komponenten
- Sicherheit im WLAN: Aufwand und Ertrag
- IEEE 802.1k, 802.1r, 802.1v, 802.1p: wichtige Standarderweiterungen in der Diskussion

Session Initiation Protocol SIP

SIP wird zur wichtigsten Netzwerk-Protokoll-Welt der nächsten Jahre. Es ist nicht nur Basis aller zukünftigen IP-Telefonie-Lösungen, es ist auch der Kern für viele andere Kollaborations-Techniken und Realzeit-Anwendungen. Zu verstehen, wie SIP aufgebaut ist, wie typische Architekturen aussehen und was das im Netzwerk bedeutet ist ein Muss für jeden Netzwerk-Planer und Betreiber.

In diesem Themen-Block analysieren wir SIP, beschreiben typischen Architekturen und diskutieren mit Ihnen zugehörige Netzwerk-Design-Fragen.

- Arbeitsweise von SIP
- Typische Nutzungsformen
- Architekturen
- IP-Telefonie: Strategien der Hersteller
- Compliance-Regeln: wann liegt wirklich eine SIP-Lösung vor?

10% Frühbucherrabatt bis 20.05.07

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sommerschule 2007

☐ Ich buche die
Sommerschule 2007
11.06. - 15.06.07 in Aachen
zum Preis von € 2.015,-* zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

*gültig bis 20.05.07, dann regulär
€ 2.290,- zzgl. MwSt.

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Sonderveranstaltung

ComConsult SIP-Forum 2007

Die ComConsult Akademie veranstaltet vom 14. - 15.05.07 erstmalig ihr „ComConsult SIP-Forum 2007“ in Frankfurt.

- Siemens verstärkt SIP-Strategie
- Cisco steigt auf SIP um
- Avaya, Alcatel, Nortel kündigen verstärkten SIP-Support an
- Microsoft steigt mit SIP-Produkten in den Markt ein

Die Bedeutung von SIP für den TK-Markt nimmt lawinenartig zu. Keiner der Hersteller kann mehr auf SIP in Teilen seiner Lösung verzichten, die Ankündigungen für immer weitere SIP-Nutzungen stehen in den Roadmaps aller Hersteller. Dabei reicht deckt die Spannweite möglicher SIP-Nutzungen ein breites Band von Anwendungen ab:

- Signalisierungsprotokoll zur Realisierung von Anlagen-Verbunden (SIP-Trunks)
- Schnittstelle zur Anbindung von Applikationen (ACD, IVR, UM, …) und zur offenen Kommunikation zwischen Applikationen
- Anlagen-internes Signalisierungsprotokoll zur Anbindung der Endgeräte
- Anbindung von Gateways und Analog-Umsetzern

Nun setzt Siemens seine Konkurrenten weiter unter Druck. Siemens bekennt sich klar und umfassend zu SIP. Das entsprechende Statement zur HiPath 8000 lautet: Siemens realisiert immer basierend auf offenen SIP-Standards unter 100%er Einhaltung des Standards. Sobald ein Funktionsmerkmal auch nur als Draft vorliegt, wird dieser realisiert. Liegt ein Funktionsmerkmal momentan nicht im Standard und auch nicht als Draft vor, wird es proprietär, aber so nahe wie möglich am Standard implementiert und sofort durch eine Standard-konforme Lösung abgelöst, wenn ein neuer Draft existiert. Entsprechend dieser klaren strategischen Ausrichtung wird auch die gesamte TK-Produktlinie von den Anlagen über Gateways bis zu den Endgeräten immer mehr an SIP ausgerichtet. Dies gilt auch für die verschiedenen Applikationen im Siemens Portfolio. Dies bedeutet nicht, dass der Bereich der HiPath 4000 vernachlässigt wird, aber die Richtung für die Zukunft ist klar.

Wo steht die Konkurrenz?

- Microsoft lässt seine neue Lösung ebenfalls komplett auf SIP basieren, das Produkt wird aber erst Ende 2007 auf den Markt kommen
- Cisco hat mit dem Call Manager Version 6 klar und offensiv den Weg Richtung SIP eingeschlagen
- Alcatel, Avaya und Nortel bekennen sich ebenfalls zu SIP, sind aber in der Überführung ihrer Anlagen weiter zurück. Alcatel ist aufgrund seiner speziellen Anlagen-Architektur mit einem integrierten SIP-Registrar in einer Sonderrolle und hat nun auch die SIP-Fähigkeit seiner Telefone angekündigt

Wo sind die Vorteile dieser Entwicklung?

- ein offener TK-Standard erlaubt Kombinationen beliebiger Produkte unter voller Beibehaltung aller Leistungsmerkmale. Insbesondere im Bereich der Einbindung von Applikationen wird dies den Markt in relativ kurzer Zeit völlig verändern. In Summe wird die Leistungsfähigkeit von TK-Lösungen funktional stark ansteigen und gleichzeitig der Betriebsaufwand sinken
- Viele der TK-üblichen Applikationen werden immer mehr aus einem offenen Markt kommen und das bestehende Preisgefüge komplett verändern. Schon heute ist erkennbar, dass der bisherige Markt für Unified Messaging Lösung als eigenständiger Markt verschwinden wird und in umfassenderen Lösungen aufgehen wird (Beispiele: Mincrosoft Exchange 2007, Asterisk)
- durch die standardisierte Signalisierung entsteht ein breiter Markt für Gateways und Analog-Umsetzer. Schon heute setzen fast alle Hersteller hier OEM-Produkte ein, das Angebot wird sich hier deutlich verbessern, die Preise werden sinken
- Mit dem Wandel von Hersteller-spezifischer Hardware hin zu Standard-basierter Software werden alle Formen von TK-Lösungen zu reinrassigen IT-Applikationen. Dies ermöglicht eine funktionale Integration mit anderen Kommunikationsbereichen wie E-Mail, Instant-Messaging und Web-Konferenzen. Das Ergebnis wird in kurzer Zeit der Unified Client sein, der alle wichtigen Kommunikationsfunktionen in einem Client vereint. Nahezu alle Hersteller bekennen sich zum zu diesem Trend, Cisco, Microsoft und Siemens sind die Vorreiter, die den Markt hier treiben
- SIP bringt auch neue Funktionsbereiche, deren Potenzial sich erst noch in den nächsten Monaten erschließen muss. Vorrangig betrifft dies Präsenz-Kommunikation, die in einer vollständigen Umsetzung Kommunikation erheblich effizienter gestalten kann. Allerdings muss hier der gordische Knoten der Komplexität des damit verbundenen Regelwerks durch eine wirklich gute Bedienerführung noch durchschlagen werden.

Welche Nachteile hat SIP?

- SIP ist in vielen Bereichen anders als bisherige Lösungen. Anwender müssen sich in Teilen an ein etwas anderes Handling gewöhnen
- Die bestehenden SIP-Standards und Drafts decken nicht alle aus den traditionellen Produkten gewohnten Leistungsmerkmale ab. Der Funktionsumfang ist zwar viel größer als allgemein angenommen, aber es verbleiben einzelne und wichtige Funktionen, die im Moment nur Hersteller-spezifisch implementiert werden können. Ein typisches und gern genanntes Beispiel ist die Chef-Sekretärinnen Schaltung (die allerdings durch Team- und Präsenz-Funktionen in SIP-Lösungen nachgestellt werden kann, je nach Definition dieser Schaltung)
- Insbesondere die Hersteller, die SIP nur teilweise in ihren Architekturen nut-

ComConsult SIP-Forum 2007

zen, machen interoperable Lösungen schwer, da für den Anwender ein Aufwand in der Bewertung der Verfügbarkeit und Machbarkeit besteht

Unter dem Strich gilt, dass der Markt auf dem Wege zu SIP ist. Dies ist auch unbestritten. Unterschiede gibt es in der Erwartung des zeitlichen Verlaufs.

An dieser Stelle setzt unser herausragendes Forum des Jahres 2007 an.

Das ComConsult SIP-Forum 2007.

Wir analysieren für Sie und stellen auf dem Forum vor:

- Die große SIP-Studie von ComConsult-Research wird vorgestellt
- Was leistet SIP?
- Was bedeutet Offenheit?
- Wie offen sind die Lösungen der Hersteller?
- Wichtige Hersteller präsentieren ihre Strategie zu SIP:
- Siemens erläutert Hintergründe und Zukunft der HiPath 8000
- Cisco präsentiert wichtige Details zum Call Manager 6
- Alcatel geht auf die Perspektiven eines offenen Standards im Zusammenhang mit gehosteten Lösungen ein
- Unser Labor präsentiert die Ergebnisse einer Reihe aktueller Untersuchungen
- Wo steht Microsoft, wie tragfähig ist die Microsoft/Nortel-Lösung?
- Wie lassen sich offene SIP-Lösungen um Applikationen von Drittherstellern ergänzen, was leisten Asterisk und co?
- Wir analysieren und präsentieren die Frage der Gestaltbarkeit zukünftiger Lösungen
- Wie gestaltbar ist eine Linux-basierte TK-Installation?
- Wir berichten über laufende Projekte und die Sicht repräsentativer Anwender

Die Moderation übernimmt Dr. Jürgen Suppan.

Dr. Jürgen Suppan gilt als einer der führenden deutschen Berater für Kommunikationstechnik. Unter seiner Leitung wurden diverse Netzwerkprojekte aller Größenordnungen erfolgreich umgesetzt. Seine Seminare zählen durch ihren didaktischen und lebendigen Aufbau und ihre Praxisnähe und Herstellerneutralität zu unseren erfolgreichsten Veranstaltungen.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult SIP-Forum 2007

☐ Ich buche das
ComConsult SIP-Forum 2007
14.05. - 15.05.2007 in Frankfurt
zum Preis von € 1.590,- zzgl. MwSt.

☐ mit Reportneuerscheinung
„Session Initiation Protocol“

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

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

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

Programmübersicht ComConsult SIP-Forum 2007

Montag, den 14.05.2007

9:30 bis 10:30 Uhr

TK-Lösungen auf der Basis des SIP-Standards: was bedeutet das?

- Internationale Marktsituation heute
- Telefonie als IT-Applikation: was bedeutet das eigentlich?
- Traditionelle TK versus IP-Telefonie verus SIP: wo liegen die Vor- und Nachteile für den Anwender?
- Nutzungsbereiche von Offenheit und der Reifegrad:
  - Telefon
  - Telefon-Programmierung
  - Applikationen und Schnittstellen
  - Architektur
  - Betrieb
- Bewertung der Strategien ausgewählter Hersteller:
  - Wo steht Siemens und was ist das Ziel?
  - Cisco CallManager 6 und Unified Communication, was will Cisco wirklich?
  - Microsoft: warum Microsoft den Markt verändern wird?
  - welche Rolle spielt IBM?
- Bewertung der Gesamtsituation
  - Wie wird SIP den Herstellermarkt und die Positionen der Hersteller verändern?
  - Wo liegen Risiken und Fragezeichen?
  - Wo liegen Vor- und Nachteile für den Anwender
- Fazit: was sollte der Anwender heute tun?

Dr. Jürgen Suppan, ComConsult Research

10:30 bis 13:00 Uhr

Ergebnisse der SIP-Studie

- Die SIP-Grundidee
- SIP: Architektur und Protokoll im Überblick
- SIP in der Praxis: wie sehen typische Einsatz-Szenarien aus, wie sind sie redundant auslegbar
- Bedarf nach SIP-Compliance und Compliance-Kriterien

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

14:30 bis 15:30 Uhr

SIP: IP-basierende Echtzeitkommunikation bei DaimlerChrysler

Dipl.-Ing. Holger Lieb, DaimlerChrysler AG

16:00 bis 17:00 Uhr

Analyse: Telefonieren mit Microsoft: Wie weit wird Microsoft den Markt verändern?

- Microsofts Unified Communications Strategie
- Analyse: welche Auswirkung hat der Microsoft UC-Client auf die Branche?
- Übersicht über die Serverprodukte, d.h. Communications Server, Exchange Server und LiveMeeting
- Microsofts Office Communications Server 2007 als neue Kernkomponente
- Client-Software und ihre Integration mit anderen Produkten
- Standards, die von Microsoft unterstützt werden
- Strategische Allianzen und ihre Bedeutung
- Roadmap: wie sieht die Zeitachse aus, wann kommt Version 3?
- Kann MS eine traditionelle TK-Lösung ersetzen?

Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH

17:00 bis 17:45 Uhr

Asterisk: Applikations-Server oder vollständige PBX-Lösung?

- Geschichte und Hintergrund
- Übersicht der grundlegenden Leistungsmerkmale
- Architektur und Erweiterungsmöglichkeiten
- Asterisk vs. SIPPING
- Distributionen und kommerzielle Lösungen
- Das Lizenzmodell und seine Auswirkungen
- Bedeutende Referenzinstallationen
- Unified Communications Lösungen mit Asterisk
- DUNDI und andere Mechanismen zur Sicherstellung der Verfügbarkeit
- Kostenvergleich mit Lösungen konventioneller Hersteller

Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

11:30 - 12:00 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

Dienstag, den 15.05.2007

9:00 bis 10:00 Uhr

Cisco Unified Communications Manager 6.0: Protokollphilosophie, SIP und Unified Communications

- Historie und Abgrenzung: CM 4/5/6
- Was bedeutet SIP aus der Sicht von Cisco
- Leistungsumfang im Vergleich zu SIPPING19
- Stellenwert von Skinny im CM6
- Offenheit der Architektur
  - Einbindbarkeit der Telefone anderer Anbieter
  - Nutzung von CISCO-Telefonen an SIP-Produkten anderer Hersteller
  - Integration von Applikationen von Drittherstellern
  - Nutzung von CISCO-Gateways in offenen SIP-Lösungen
- Unified Communication: Bedeutung und zukünftige Entwicklung
- Ausblick auf die weitere Roadmap

Daniel Gluch, Cisco Systems Deutschland

10:00 bis 11:00 Uhr

Die Siemens-Kommunikations-Strategie im Rahmen offener Standards

- Bedeutung von Software-Lösungen für den Markt
- Siemens Statement zu SIP
- HiPath 8000: Positionierung in der Siemens-Strategie
- Applikations-Architekturen
- Wie offen kann eine Lösung sein

Rudolf Bitzinger, Siemens AG

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause

11:30 bis 12:30 Uhr

Sicherheit und SIP: was ist zu tun?

- Nutzung von SIP für die Signalisierung verschlüsselter Sprach-übertragung
- Verschlüsselung und Authentifizierung von SIP-Nachrichten
- Aufbau einer Vertrauenskette bei SIP-Signalisierung
- SIP und Firewalling
- Sicherheit bei externer SIP-Kommunikation ueber Trunks zu Provider-Netzen

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

14:00 bis 15:00 Uhr

Hosted-Services auf der Basis von SIP

- Bedeutung und Leistungsumfang von Hosted Services
- SIP als tragendes Element einer offenen Lösung
- Ausblick auf zukünftige Potenziale derartiger Lösungen

Dr. Jörg Fischer, Alcatel Deutschland GmbH

15:00 bis 16:00 Uhr

SIP: Brücke zwischen TK und TK-nahen Applikationen

- SIP als Voraussetzung für mehr Flexibilität und niedrigere Kosten
- Vorreiteranwendungen: Unified Messaging, CTI und Instant Messaging
- ACD, CRM, Voice Recording, Alarmserver, u.a. Applikationen
- Die Rolle von SIP bei der Fixed Mobile Konvergenz
- Telefone als generische Benutzerschnittstellen
- Hersteller und Lösungen

Dr. Frank Imhoff, Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

Der Veranstalter behält sich Änderungen im Programm vor!

Zweitthema

Der schnelle Baum

Fortsetzung von Seite 1

Markus Schaub ist als Consultant bei der Wachter & Karbon IT-Consulting GmbH & Co KG in den Bereichen Perfomance Quality Management und Service Level Management tätig. Zuvor bearbeitete er über 10 Jahre bei der ComConsult Technologie Information GmbH die Schwerpunkte Netzwerk-Design, IP-Infrastrukturen und VoIP, zu denen er viele erfolgreiche Vorträge und Seminare hielt und zahlreiche Veröffentlichungen schrieb.

mschaub@wachter-karbon.com

Wie die meisten Netzwerkbetreiber aus leidvoller Erfahrung wissen, gibt es noch mehr Probleme: den Spanning Tree selbst. Die Palette reicht von instabilen Spanning Trees, die gelegentlich unmotiviert ein Respanning durchführen über unerklärliche Loops bis hin zu Umschaltzeiten, die noch einmal über dem liegen, was eigentlich sein dürfte. Es klingt fast schon wie Hohn, wenn im Zuge der Standardisierung des RSTP ein langjähriges Mitglied der Arbeitsgruppen geäußert haben soll, dass mit dem RSTP der erste funktionstüchtige Spanning Tree auf den Markt kommt.

Im Prinzip lassen sich zwei Ursachen für diese Mängel ausmachen: zum einen die Zeit, die seit dem Ende der 80er nicht stehen geblieben ist und zum anderen der Standard selbst.

Als der Spanning Tree eingeführt wurde, ging man davon aus, dass viele Stationen an Netzwerk-Segmenten angeschlossen sind (vgl. Abbildung 1), und von VLANs hatte wohl noch nie jemand was gehört. Mit anderen Worten, an einem Bridge-Port waren mehr als eine Station angeschlossen und insbesondere konnte es sich dabei um mehr als eine weitere Bridge handeln.

Mit der Einführung von Switch-Systemen und der damit verbundenen Verbreitung von dedizierten Netzen ergaben sich andere Möglichkeiten. Um vorab nur schon mal ein Beispiel zu erwähnen: bereits bei der Erweiterung 802.1t des Spanning Tree wurde berücksichtigt, dass es Ports gibt, an denen keine weiteren Brücken, sondern nur noch Endsysteme angeschlossen sind, so genannte Edge-Ports. Diese Ports brauchen bei ihrer Aktivierung die klassischen Port-Stati Blocking, Listening, Lerning und Forwarding nicht mehr zu durchlaufen, da bei Zuschalten dieser Ports kein Loop geschlossen werden kann. Folglich können sie sofort vom Blocking in den Forwarding Status wechseln. Aber es gibt noch weitreichendere Konsequenzen, auf die im Folgenden genauer eingegangen wird.

Rapid Reconfiguration Spanning Tree

Bei der Entwicklung des Rapid Spanning Tree hat sich zwar das Verfahren geändert, das Endresultat, nämlich eine loopfreie (spanning) und vollständige (tree) Topologie, ist jedoch dasselbe wie beim klassischen Spanning Tree. Genau genommen geht die Übereinstimmung sogar so weit, dass die stabile Topologie beider Varianten identisch ist. Mit anderen Worten, würde man nur das Resultat nach „vollzogener“ Konvergenz betrachten, so könnte man nicht entscheiden, ob es durch das klassiche STP oder das moderne RSTP entstanden ist. Dies gilt unabhängig davon, ob es sich um die Konvergenz nach Inbetriebnahme eines geswitchten Netzes handelt oder um ein Respanning, sprich dem Umschalten auf Redundanz-Links.

Ziele

Ziel bei der Standardisierung des RST war es, einen Algorithmus zu entwickeln, der eine dramatisch kürzere Rekonfigurationszeit hat. Dazu wurden folgende Teilziele definiert und auch erreicht:

- **Eventgesteuerte Auslösung der Rekonfiguration**
  Bislang war der Spanning Tree ausschließlich timer-basiert. Um bei einem Switch eine Reaktion auf eine Topologieänderung auszulösen, musste er 10 BPDU-Pakete auf einem Port verpassen. Das ist in der heutigen Zeit nicht mehr angemessen. Vielmehr kann ein Switch sofort reagieren, wenn der Link auf down geht, schließlich ist es offensichtlich, dass er nach Wegfall des Links die nächsten BPDUs verpassen wird.

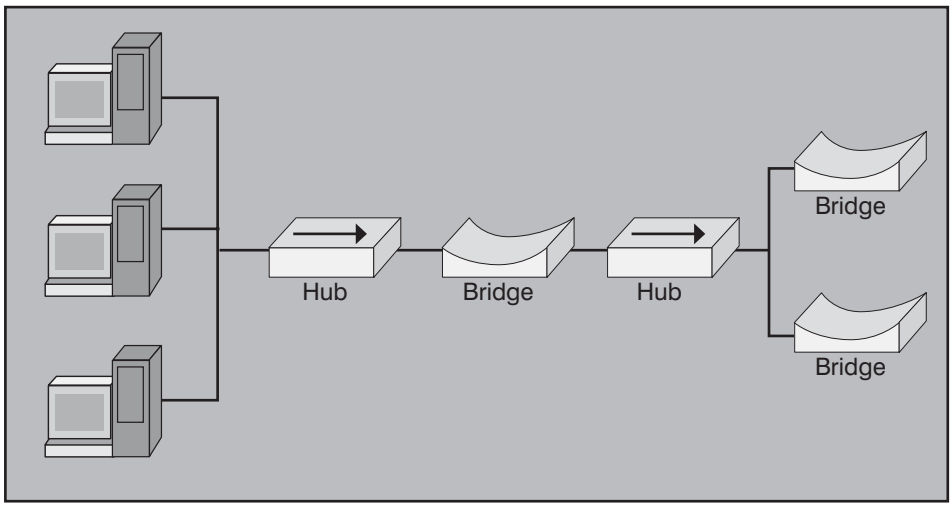


Abbildung 1

- **Angemessene Reaktion auf Änderungen**
  Viele Fehlerfälle können lokal behoben werden und müssen keine Auswirkungen auf die gesamte Topologie haben. Beispielsweise ist es häufig möglich die Änderungen auf zwei bis drei Switches zu beschränken, wenn ein Link ausgefallen ist.

- **Portbasierte Auswertung von Informationen**
  Zu Zeiten der Entwicklung des klassischen Spanning Tree ging man von Bridges aus, die nur wenige Ports haben, nicht von den heutigen Multiportsystemen. Damals hatte eine Bridge nur eine einzige Bridge-Table, die als Ganzes gepflegt wurde. Heute sind moderne Switches in der Lage, ihre Tabellen port-bezogen zu bearbeiten. Das hat, wie im Folgenden noch erläutert wird, insbesondere Konsequenzen auf die Verbreitung von Topologieänderungen.

Als letzten Punkt wäre noch die Abwärtskompatibilität anführen, die für den gemischten Betrieb von Switches, die RSTP und nicht RSTP fähig sind, notwendig ist.

Bevor nun auf den neuen Spanning Tree eingegangen werden kann, zunächst eine kurze Wiederholung dessen, was von seinem klassischen Vorfahren her bekannt ist und auch bei RSTP noch Gültigkeit hat.

Root Brigde

Um die Kompatibilität zum STP zu erhalten, wird auch beim RSTP zunächst eine Root gewählt (vgl. Abbildung 2). Das Verfahren ist dabei - ebenfalls aus Kompatibilitätsgründen - dasselbe wie schon beim STP:

Zunächst tauschen die Brücken BPDU-Frames aus und diejenige Brücke gewinnt die Wahl, die die kleinste Priorität besitzt. Die Priorität ist ein pro Bridge/Switch konfigurierbarer Parameter. Haben zwei Switches dieselbe Priorität, weil beispielsweise mit den Default-Werten gearbeitet wird, so werden die MAC-Adresse der Switches zu Tie-Breakern: der Switch mit der kleinsten MAC-Adresse wird Root.

Die Priorität sollte auf alle Fälle gesetzt werden, da ansonsten die Auswahl der Root dem Zufall überlassen wird und zu Topologien führen kann, die nicht gewollt sind.

Designated Bridge

Ist ein LAN-Segment an zwei oder mehr Switches angeschlossen, so handeln diese Switches untereinander aus, welche Bridge die Pakete in Richtung der Root

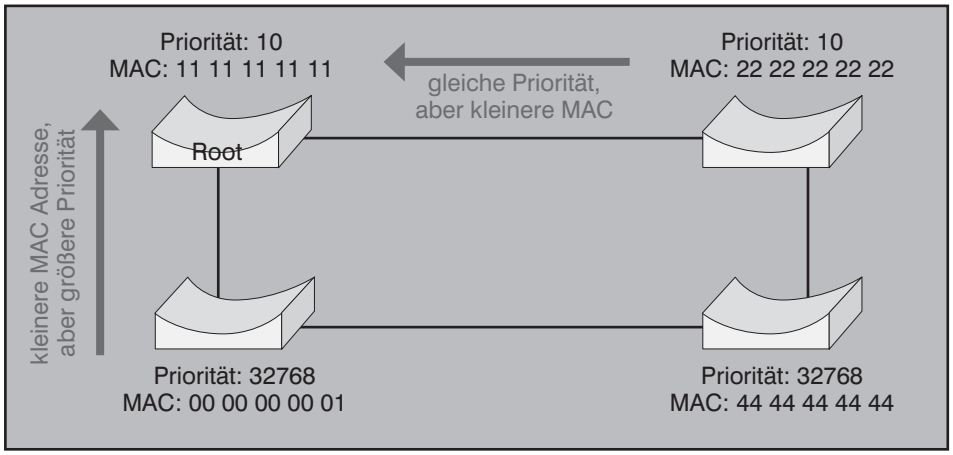


Abbildung 2

weiterleitet (vgl. Abbildung 3). Um Loops zu verhindern, kann das nur eine Bridge sein. Diese Bridge wird zur so genannten Designated Bridge. Entscheidend dafür, wer zur Designated Bridge wird, ist nicht mehr die Bridge Priorität, sondern in erster Linie die Pfadkosten, die sich von dieser Bridge bis zur Root hin ergeben. Die Bridge mit den niedrigsten Kosten wird Designated Bridge. Haben zwei Switches dieselben Pfadkosten, so wird die Portpriorität als zweites Kriterium herangezogen. Sollten auch die Prioritäten identisch sein, beispielsweise weil man sie bei den Default-Werten belassen hat, so kommt als nächstes Kriterium die Port-ID zum Zuge. Es mag den Leser verwundern, aber auch hier gilt, die niedrigste ID macht das Rennen. Sollten alle drei zuvor genannten Kriterien bei zumindest zwei Switches identisch sein, so wird als letztes anhand der kleinsten MAC-Adresse entschieden, welche Bridge Designated Bridge wird.

Die Kosten und Portprioritäten sind konfigurierbare Parameter und sollten ebenfalls beim Design bedacht werden.

Port-Rollen

Entsprechend der Bridge-Rollen werden

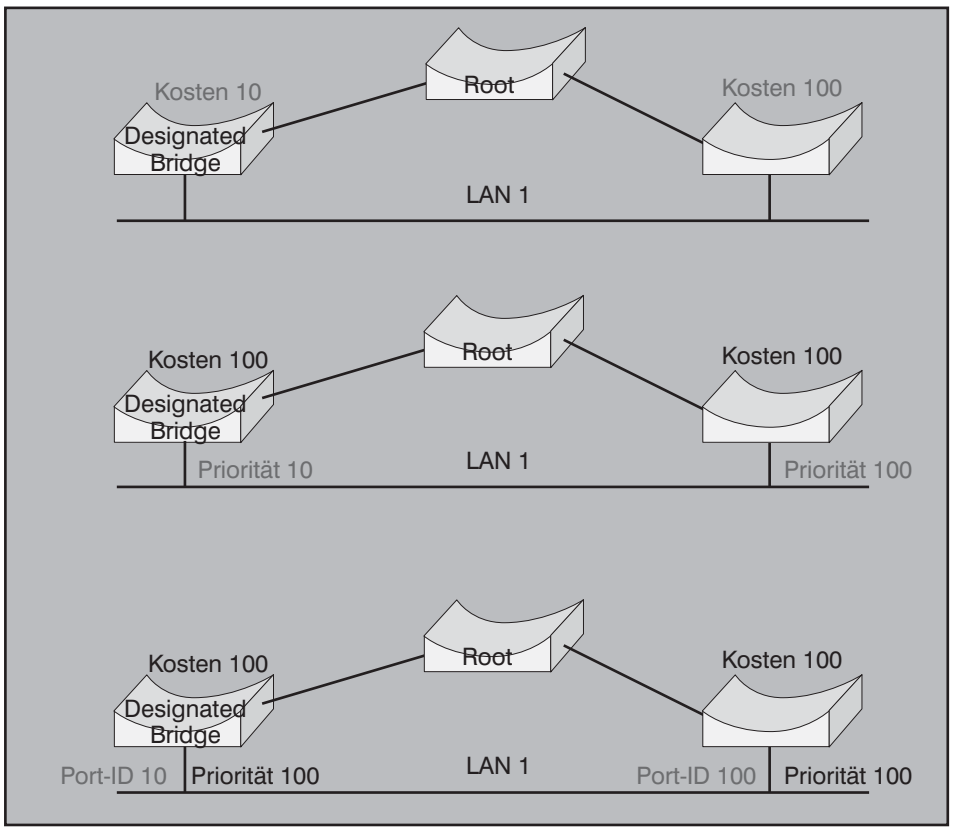


Abbildung 3

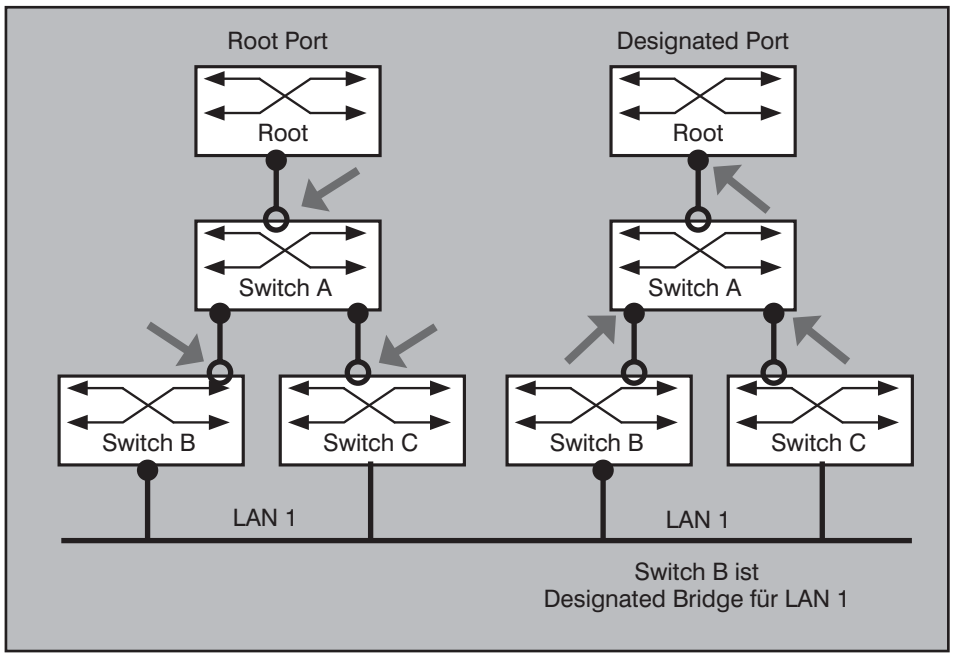


Abbildung 4

nun Port-Rollen für die einzelnen Ports der Bridge verteilt. Bereits im klassischen STP gab es diese Port-Rollen, die beschreiben, welche Funktion innerhalb der Topologie ein Port erfüllt. Diese Port-Rollendefinition war jedoch reine Nomenklatur, die keine Bedeutung für die Bridge hatte. Das ändert sich mit dem RSTP: neben den altbekannten Rollen des Root Port, des Designated Ports und des Edge Ports (seit dem STP-Update IEEE 802.1t) werden weitere eingeführt. Zum Verständnis des RST-Algorithmus ist es notwendig, zunächst auf die alten wie neuen Port-Rollen einzugehen, bevor das Verfahren beschrieben werden kann.

Die Definition des Root Port hat sich im Vergleich zum klassischen STP nicht geändert (vgl. Abbildung 4, links). Ein Root Port ist ein aktiver Port, der upstream zur Root hin zeigt. Also ein Port, der in einem stabilen Zustand des Spanning Trees Pakete in Richtung der Root weiterleitet. Ein Root Port ist stets im Forwarding Modus, sobald der Spanning Tree vollständig und stabil ist. Sollte ein LAN-Segment zwei Ports in Richtung der Root haben und für beide dieselben Kosten zur Root aufweisen, so gilt ein Auswahlverfahren analog dem zur Wahl der Designated Bridge:

Zunächst wird der Port gewählt, der die geringsten Kosten zur Root vorweisen kann. Sollten zwei Ports dieselben Kosten aufweisen, so wird der mit der niedrigsten Priorität zum Root Port gewählt. Als letztes Kriterium wird die Port-ID herangezogen, falls auch diese Prioritäten identisch sind. Da die Port-ID auf einem Gerät eindeutig ist, wird die MAC-Adresse nicht mehr herangezogen wie bei der Wahl zur Root.

Unmittelbare Folgerung daraus ist, dass jedes LAN-Segment maximal einen Root Port haben kann. Sollte ein Switch selbst zwei Ports zur Root haben, so wird der Root Port genauso ausgewählt wie im oben beschriebenen Fall.

Designated Port
Designated Ports werden im Gegensatz zu Root Ports downstream zur Root bestimmt (vgl. Abbildung 4, rechts). Der Designated Port ist dabei der Port, der zu der Designated Bridge eines LAN Segmentes gehört.

Edge Port
Bis hierher hat sich in Bezug auf Bridge und Port-Rollen seit Einführung des Spanning Trees noch nichts geändert (vgl. Abbildung 5). Die erste diesbezügliche Änderung ergab sich mit der Erweiterung des STP-Standards durch IEEE 802.1t. Dieser führte erstmalig den Edge Port ein.

Die Definition eines Edge Ports ist denkbar einfach: an einem Edge Port sind keine weiteren Brücken oder Switches mehr angeschlossen. Dabei ist es egal, ob es sich um ein Endsystem wie einen PC oder Server handelt oder um eine weitere LAN-Komponente wie einen Router, Hauptsache das Gerät hat keinerlei Bridging-Funktionalität.

Alternate Port
Die erste echte Neuerung des RSTP ist nun die Einführung zweier weiterer Port-

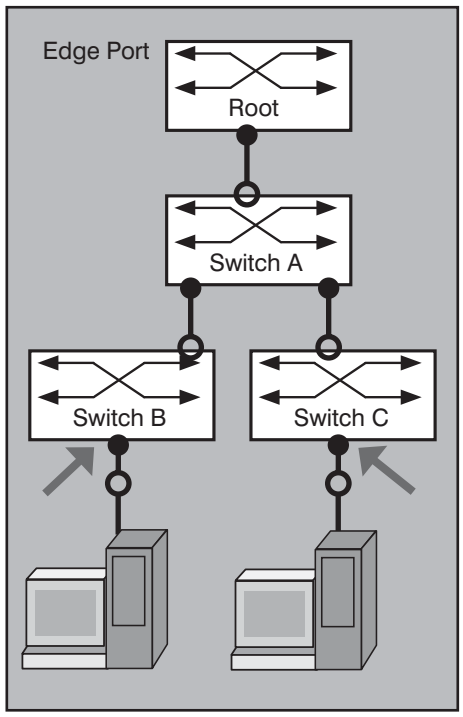


Abbildung 5

Rollen für die Ports, die an der aktiven Topologie nicht teilnehmen, d.h. keine Frames weiterleiten (vgl. Abbildung 6, links).

Die erste neue Rolle ist der Alternate Port. Zum Alternate Port wird ein Port, der zwar einerseits einen Weg zur Root darstellt, jedoch selbst nicht zum Root Port wurde.

Backup Port
So wie ein Alternate Port einen weiteren, jedoch schlechteren Weg zur Root für einen Switch darstellt, so ist ein Backup Port ein weiterer jedoch schlechterer Weg zur Root für ein LAN Segment (vgl. Abbildung 6, rechts).

Backup oderAlternate Port
Bleibt noch zu klären, was ist, wenn ein Port sowohl Backup wie auch Alternate Port sein könnte. In diesem Falle handelt der Switch getreu dem Motto: „jeder ist sich selbst der Nächste“ und erklärt den Port zum Alternate Port. Dies ist im Bild in der linken Konfiguration an Switch C dargestellt.

Port Modi
Neben der Einführung dieser beiden neuen Port-Rollen wurden auch Änderungen an den Port Modi vorgenommen. Im Grunde genommen kann man es auf eine inhaltliche Änderung reduzieren: der Listening Modus ist weggefallen. Existierte der Modus bei dem Klassiker noch, um eine Bridge nicht durch Lernen und Zuhören zu überfordern, so verzichtet man nun ganz darauf.

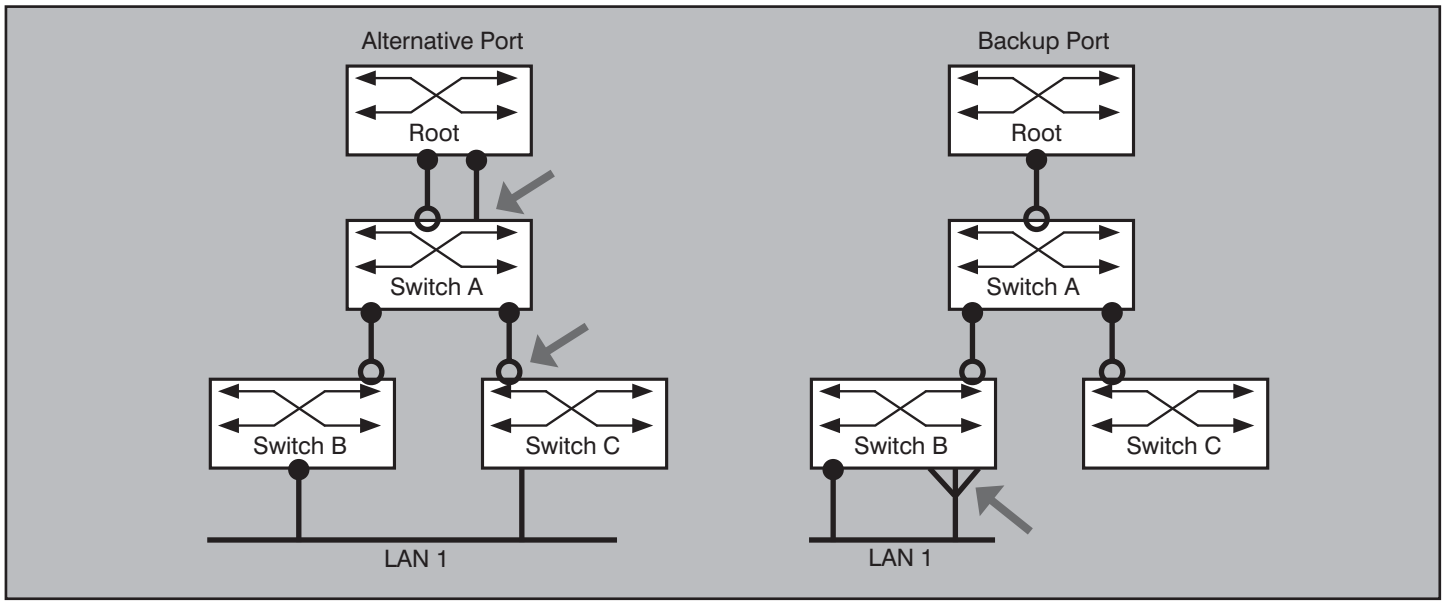


Abbildung 6

Des weiteren wurde noch der ehemalige Blocking Modus in Discarding umbenannt, was jedoch reine Nomenklatur ist.

Discarding Modus
Der ehemalige Blocking Modus heißt heute Discarding Modus. Ein Port in diesem Modus leitet keine Datenframes weiter. Somit handelt es sich also entweder um einen Alternate oder einen Backup Port. Weitere Konsequenz ist, dass für einen Port im Discarding Modus keine Bridge-Table angelegt wird, da er keine benötigt. Ein solcher Port ist jedoch nicht disabled, also nicht abgeschaltet. Er verarbeitet weiterhin BPDUs, die er empfängt, und versendet auch selbst welche. Schließlich müssen seine Nachbarn wissen, dass es ihn gibt, da er bei einem Respanning ggf. von Bedeutung wird.

Learning Modus
Hier hat sich noch nicht einmal der Name geändert, allerdings erfüllt er nun die Funktion des Listening Modus gleich mit. Ein Port im Learning Modus sendet, empfängt und verarbeitet BPDUs, allerdings sendet er keine Datenframes, auch verarbeitet er keine Frames mehr weiter, die er empfängt, außer dass er bereits aus den gesehenen Quelladressen die Bridge-Table aufbaut.

Im Grunde gibt es diesen Modus nur noch aus Kompatibilitätsgründen. In einem reinen RSTP-Netz kommt er zwar auch vor, ist jedoch - wie wir sehen werden - nicht mehr von Bedeutung.

Forwarding Modus
Hier haben sich keinerlei Änderungen ergeben: ein Port im Forwarding Modus sendet, empfängt und verarbeitet BPDUs und sendet und empfängt ebenso Frames zur Weiterleitung.

Stellt man die neuen Modi den alten gegenüber so ergibt sich Tabelle 1. Hier ist auch aufgeführt, wie sich ein Port in einem bestimmten Modus bezüglich der aktiven Topologie verhält. Damit ist gemeint, ob er an der Bildung des Spanning Trees beteiligt ist oder nicht. Zusätzlich stellt die Tabelle einen leicht erkennbaren Zusammenhang zwischen den Port-Rollen und den Port-Stati her.

Für die zeichnerische Darstellung schlägt der Standard IEEE 802.1w Konventionen vor, die in dem Bild (Abbildung 7) dargestellt werden.

So komplex die Zeichnung auf den ersten Blick auch erscheint, so ist sie im Grunde einfach: der Beginn einer Linie repräsentiert die Port-Rolle, ein ausgefüllter Punkt ist ein Designated Port, ein leerer Kreis ein Root Port usw. Die senkrechten Striche bezeichnen den Status: kein Strich heißt Forwarding, einer Learning und zwei Discarding. Allerdings gibt es Ausnahmen: warum die IEEE das Dreieck als Backup Port im Discarding Modus weglässt und stattdessen drei senkrechte Linien einzeichnet, bleibt dem Autor verschlossen.

Punkt-zu-Punkt-Verbindung
Bevor nun der Algorithmus, der zu den niedrigen Umschaltzeiten führt, erläutert werden kann, muss noch kurz auf eine letzte Voraussetzung eingegangen werden, die seit Einführung des Spanning Trees durch die Switchsysteme hinzugekommen ist: Punkt-zu-Punkt-Verbindungen. In der WAN-Welt sind diese bereits lange bekannt, typische Vertreter sind serielle X.25-Verbindungen oder auch ein B-Kanal einer ISDN-Einwahl (oder beide B-Kanäle, wenn Multilink gefahren wird).

Eine Punkt-zu-Punkt-Verbindung zeichnet sich dadurch aus, dass es genau eine Verbindung zwischen genau zwei Geräten gibt. Dabei ist es unerheblich, ob diese Leitung physikalischer Natur (beispielsweise ein Patchkabel) oder logischer ist (beispielsweise Link Aggregation oder Multilink). Auch wenn wir schon lange solche Punkt-zu-Punkt-Verbindungen in Ethernet betreiben, in einem vollgeswitch-

Port Status			
STP	RSTP	Active Topology	Port Role
Disabled	Discarding	Excluded	Disabled
Blocking	Discarding	Excluded	Alternate /Backup
Listening	Discarding	Included	Root, Designated, Edge
Learning	Learning	Included	Root, Designated
Forwarding	Forwarding	Included	Root, Designated, Edge

Tabelle 1

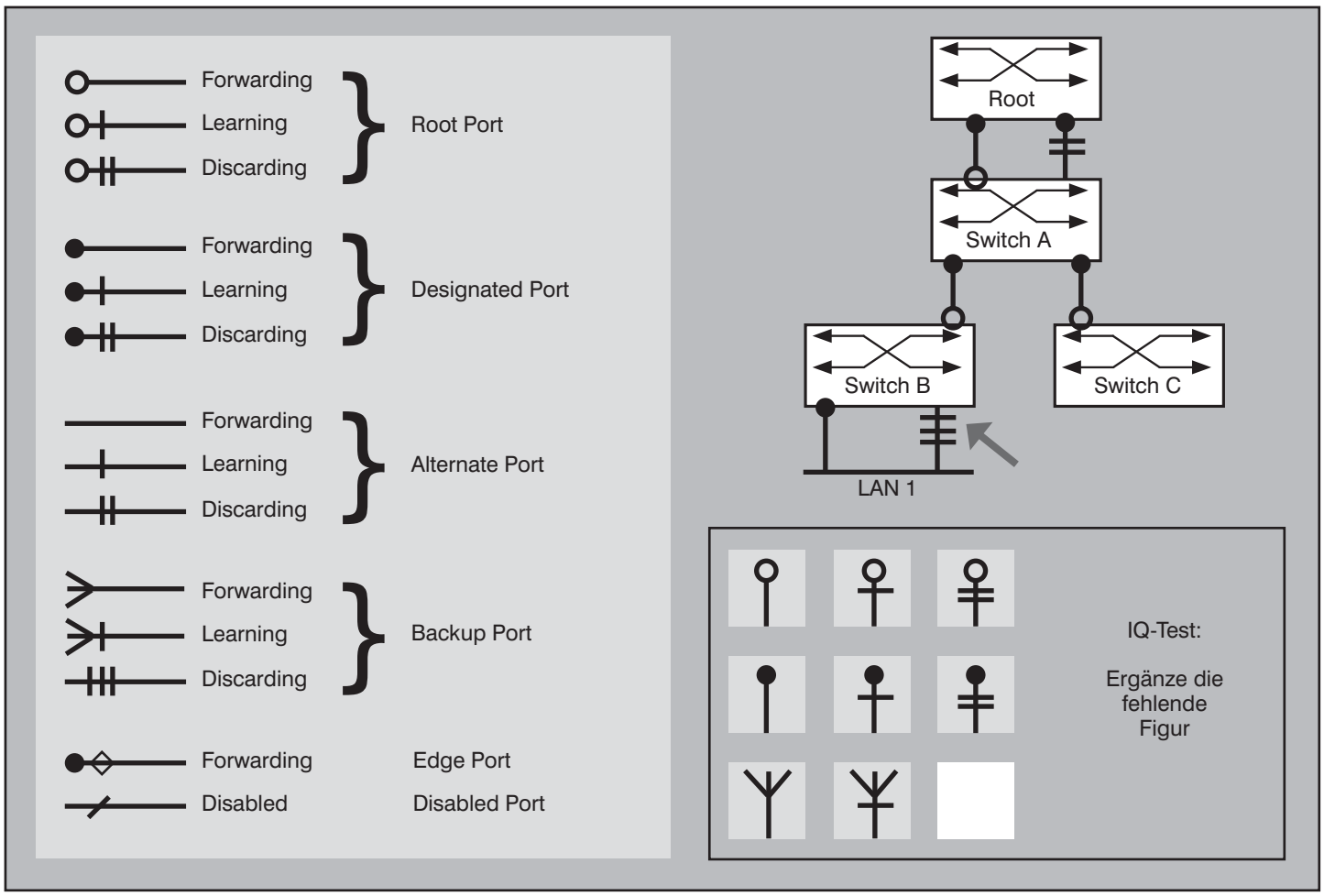


Abbildung 7

ten Netz gibt es im Grunde nichts anderes mehr, so ist die Idee doch neu. Das ganze CSMA/CD-Verfahren des Ethernets ist darauf ausgelegt, dass mehr als eine Station in einem Ethernetsegment existieren kann. Entsprechend war auch der klassische Spanning Tree darauf ausgelegt, dass er mehr als eine Bridge über ein shared Medium und mehr als eine weitere Bridge über einen eigenen Port erreichen kann.

Diesem veränderten Design, dem dedicated LAN, trägt der RSTP-Standard Rechnung, indem er Punkt-zu-Punkt-Verbindungen bei dem Algorithmus berücksichtigt. Dazu wird ein Parameter eingeführt, der angibt, ob ein Port im Punkt-zu-Punkt-Modus arbeitet oder nicht. Es gibt zwei Möglichkeiten, die einen Switch einen bestimmten Link als Punkt-zu-Punkt-Verbindung betrachten lassen:

1. Es handelt sich um einen aggregierten Link.

2. Ein Port arbeitet **full-duplex.**
   Für Punkt zwei ist es egal, ob full-duplex konfiguriert wurde oder mittels Autonegotiation ausgehandelt wurde.

Wechselkriterien

Das oberste Ziel des RST-Algorithmus ist es, eine Topologie zu gewährleisten, die immer loopfrei ist.

Schon aus dieser Hauptdirektive lassen sich zusammen mit den Port-Rollen einige Kriterien für den Wechsel des Port-Status ableiten:

RST-Regel 0

Ein Port kann sofort in den Discarding Modus versetzt werden

Die Regel ist so offensichtlich, dass sie fast keiner weiteren Erläuterung bedarf: ein Port, der keine Frames weiterleitet, kann logischer Weise auch keinen Loop schalten.

Es ist allerdings eben so offensichtlich, dass mit dieser Regel allein der Spanning Tree noch nicht schneller wird. Bei der Bildung des Spanning Trees kommt diese Regel jedoch häufig zur Anwendung, so dass man sie im Hinterkopf behalten sollte.

RST-Regel 1

Der einzige Port eines LAN-Segmentes kann unmittelbar nach Link-Aktivierung in den Forwarding Modus wechseln.

Auch das ist eine schlüssige Regel. Gibt es für ein Segment nur einen Port, so wird auch dieser keinen Loop schalten können, da Pakete, die aus dem Port hinausgehen, ja von keinem anderen Switch mehr in den Baum zurückgeleitet werden können. Voraussetzung ist allerdings, dass der Switch „weiß“, dass er der einzige Switch des Segmentes ist. Dafür muss der entsprechende Port die Port-Rolle Edge haben. Dies kann entweder administrativ gesetzt werden, oder aber der Switch hat es selbst herausgefunden, weil er keine BPDU-Pakete auf dem entsprechenden Port empfängt. Wegen dieses Auto-

sensing Mechanismus ist die Einstellung Edge Port bei einigen Herstellern der Default für alle Ports. Da auch ein Edge Port BPDUs versendet, würde ein später an einem Segment installierter Switch ihn bemerken. Ebenso wie er den „Neuling“ im Segment erkennen würde, da er BPDUs empfangen würde. In diesem Fall würden beide Switches in den RSTP- bzw. in den STP-Modus wechseln – auch entgegen der manuell vorgenommenen Konfiguration.

RST-Regel 2

Hat ein Root Port oder ein Designated Port diese Rolle ausreichend lange, so wechselt er in den Forwarding Modus.

Dass sowohl ein Root wie auch ein Designated Port sich in einer stabilen Topologie im Forwarding Modus befinden sollte, ist klar, schließlich ist es Aufgabe dieser Ports den Spanning Tree zu bilden. Der erste Teil der Regel ist da schon etwas schwerer zu verstehen, was ist mit „ausreichend lange“ gemeint? Im Grunde genommen nichts anderes, als dass das Forwarding Delay abgewartet werden muss, so wie es beim STP war, nur unter Verkürzung um das Listening Intervall.

Diese Regel hat zwei Funktionen. Erstens regelt sie das Verhalten eines Links, von dem der Switch nicht sicher weiß, ob es sich um eine Punkt-zu-Punkt-Verbindung oder um einen Edge Port handelt (siehe Regel 1). Zweitens stellt diese Regel die Abwärtskompatibilität sicher: ist ein Switch mit einem anderen Switch verbunden, der kein RSTP spricht, wechselt der RSTP-Switch in den STP-Kompatibilitätsmodus und arbeitet nach den klassischen Regeln.

RST-Regel 3

War der Spanning Tree zuvor lange genug stabil, darf ein Alternate Port sofort zum Root Port werden und in den Forwarding Modus wechseln, falls der eigentliche Root Port ausfällt.

Dies ist die erste wirklich neue Regelung. Anschaulich besagt sie folgendes:

Hat ein Switch einen Root Port und einen Alternate Port und der Root Port fällt aus, so kann der Switch den Alternate Port sofort zum Root Port erklären und unmittelbar in den Forwarding Modus wechseln. Diese Regel wird auch Rapid Transition genannt (vgl. Abbildung 8).

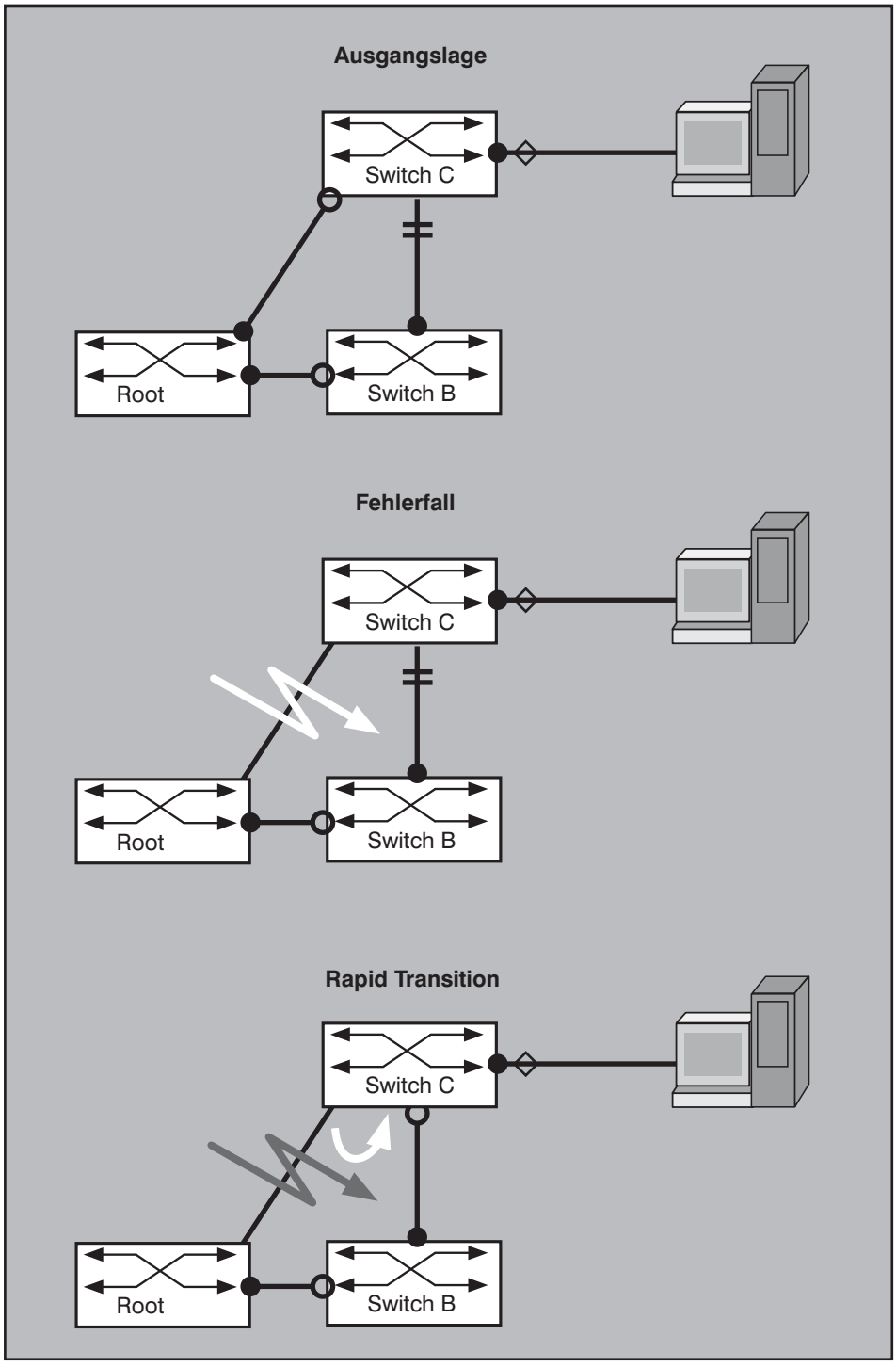


Abbildung 8

Betrachten wir ein einfaches, in der Praxis jedoch häufig vorkommendes Beispiel:

Die Skizze zeigt den Ausschnitt eines Gebäudenetzes. Die Root und Switch B sind die beiden redundanten Systeme im HVT eines Gebäudes. Der Switch C ist aus Redundanzgründen an beide angeschlossen. In der Ausgangslage ganz oben im Bild ist der Link zwischen Switch B und C nicht aktiv. Konkret sieht das so aus, dass Switch C seinen Port in Richtung B im Discarding Modus hat. Beim Rapid Spanning Tree weiß C jedoch, dass er einen alternativen Weg zur Root über einen Port besitzt, der derzeit nicht aktiv ist. Für diesen Port zu B merkt er sich die Port-Rolle (Alternate Port).

Wenn der direkte Link zwischen der Root und Switch C ausfällt, kann C sofort auf

den Alternate Port umschalten, indem er ihn zum Root Port macht und ohne Verzug vom Discarding in den Forwarding Modus wechselt.

Salopp kann man diese Regel 3 auch so formulieren: der Switch hält sich wenn möglich eine Hintertüre offen. In der Tat ist es so, dass ein Switch also nicht mehr nur den besten Weg zur Root berechnen muss, sondern auch den zweitbesten, um im Zweifelsfall auf diesen wechseln zu können.

RST-Regel 4

> Ein Designated Port einer Punkt-zu-Punkt-Verbindung darf in den Forwarding Modus wechseln, sobald der Nachbarswitch sein ok gegeben hat.

Waren die Regeln 0 bis 3 noch verständlich, so wird es bei dieser Regel schwierig, sie auf Anhieb greifen zu können. Hinzu kommt, dass dies nicht nur eine neue Regel ist, sondern diese Regel nur dann ausgeführt werden kann, wenn sich zwei Switche miteinander über einen Wechsel verständigen, was ebenfall neu ist. Dazu werden zwei Messages definiert, der Request des Switches, der wechseln möchte, und der Reply des Nachbarn.

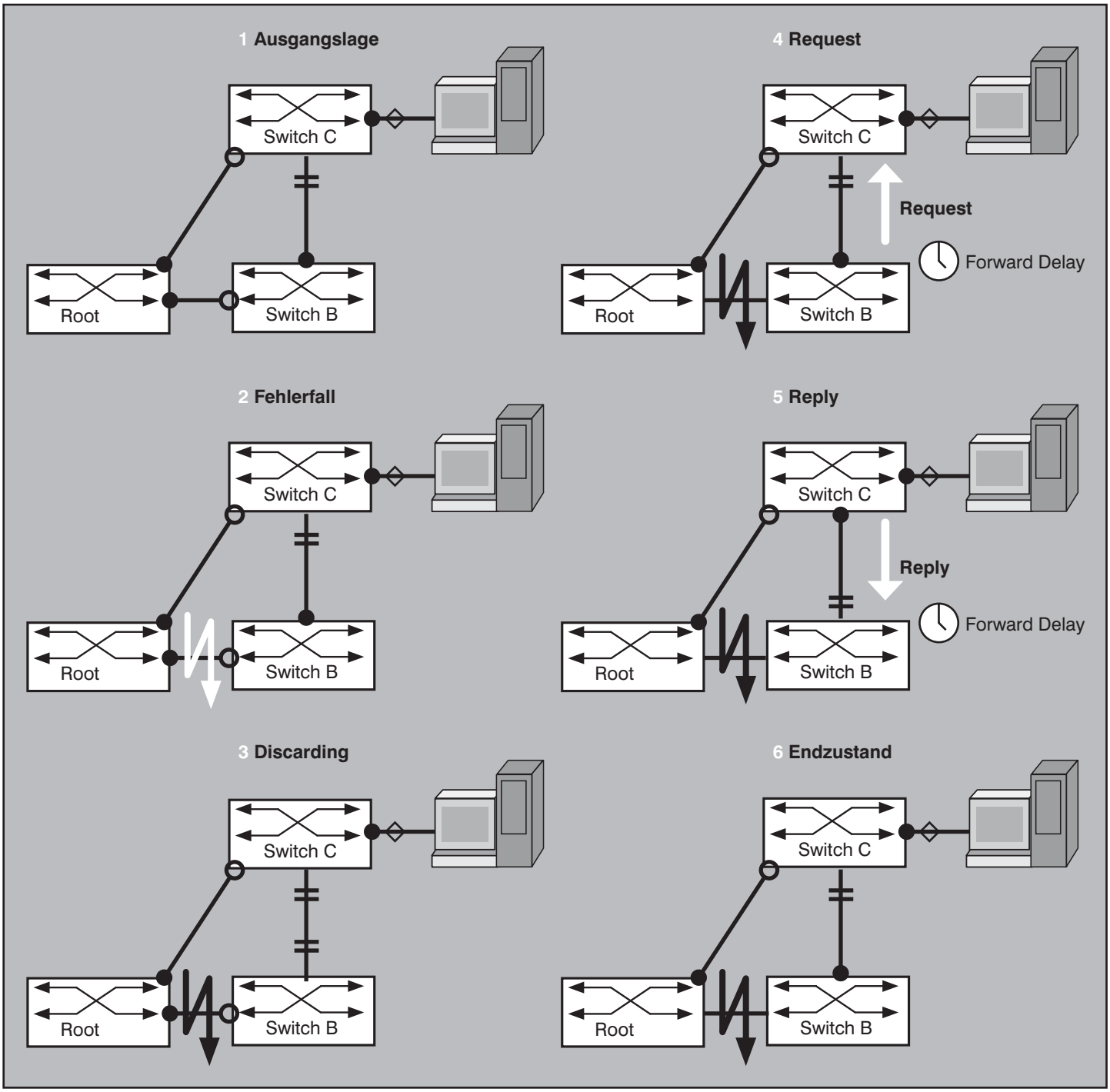


Abbildung 9

Der schnelle Baum

Betrachten wir ein erstes Beispiel, das die Regel inklusive der neuen Mechanismen veranschaulichen soll (vgl. Abbildung 9):

Als Ausgangslage dient das gleiche Beispiel wie bereits bei Rapid Transition.

Dieses Mal fällt jedoch nicht der Link zwischen der Root und dem Etagen Switch C aus, sondern stattdessen der Link zwischen den beiden Switches im HVT, also zwischen der Root und Switch B. Anders als im vorherigen Beispiel besitzt B keinen Alternate Port sondern „nur“ einen Designated Port, der grundsätzlich auch geeignet wäre, einen Weg zur Root über Switch C zu schalten. In diesem Fall kann er jedoch nicht sicher sein, dass es dabei zu keinem Loop kommt.

Aus diesem Grunde kommt zunächst Regel 0 zur Anwendung, der Designated Port zu Switch C wird auf discarding gesetzt.

Als nächsten Schritt sendet er einen Request an seinen Nachbarn C auf der Etage, um diesen zu informieren, dass sich etwas geändert hat. Dies muss er tun, denn ein einfaches offen Halten des ehemaligen Designated Ports hätte keinen Effekt, da die Verbindung zur Root nur dann wieder hergestellt werden kann, wenn auch C etwas ändert. Zeitgleich startet er

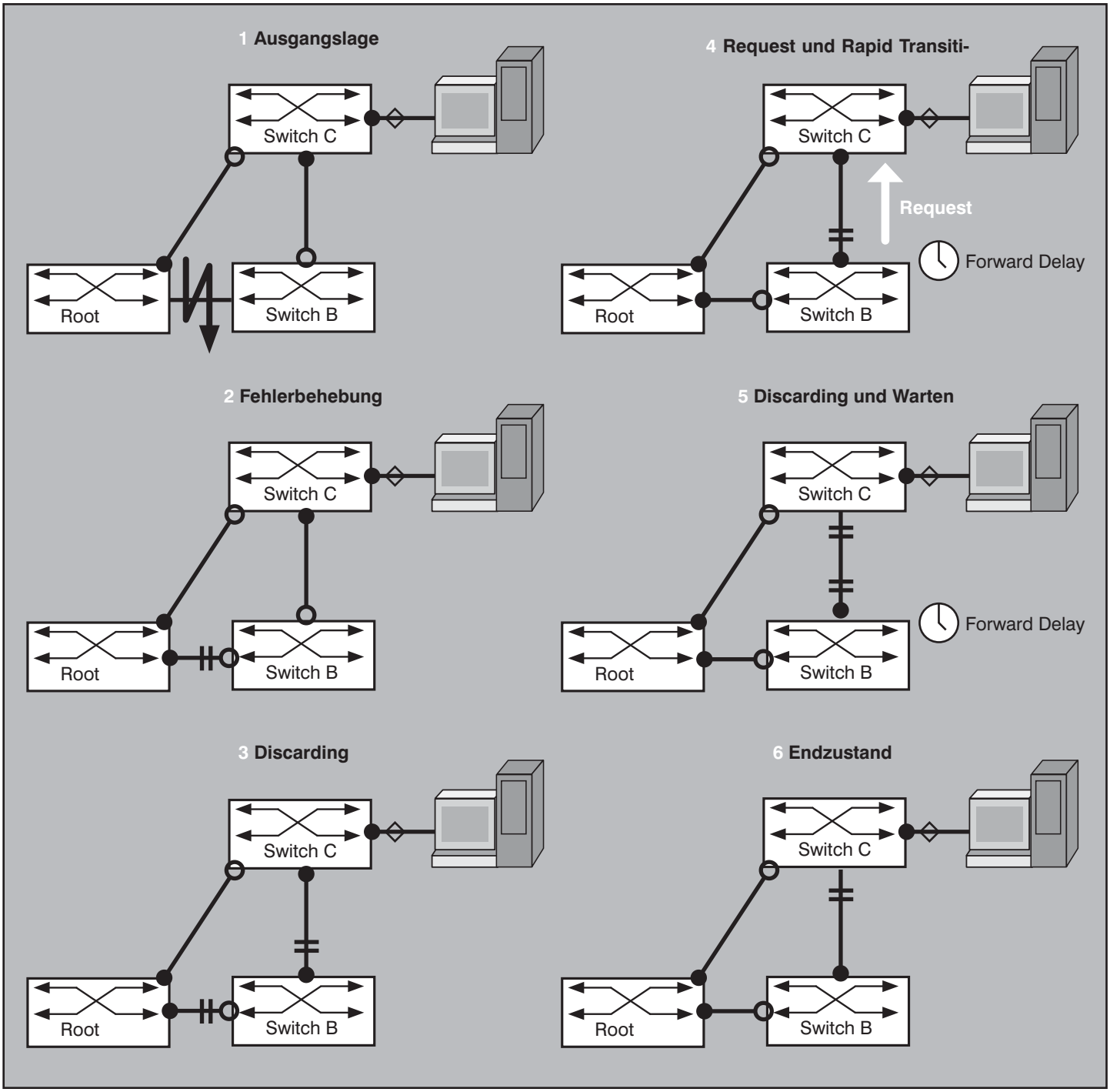


Abbildung 10

einen Timer. Dieser Timer dient der Abwärtskompabilität, denn wäre der Etagenswitch nicht RSTP-fähig, so würde der Request ungehört verhallen und der Etagenswitch würde erst nach Durchlaufen des klassischen STP in einen Zustand kommen, der den Aufbau eines Spanning Trees ermöglicht. Deshalb lässt ein RSTP-Switch den Timer laufen und nach Ablauf des Forward Delay des klassischen Spanning Trees, würde der Switch den Port auf Forwarding setzen.

Switch C empfängt nun den Request. Das hat für ihn zunächst einmal nur zwei Konsequenzen:

1. Der Weg über Switch B ist nicht länger ein alternativer Weg zur Root und somit ist der entsprechende Port auch kein Alternate Port mehr.

2. Sein Nachbar Switch B hat im Gegensatz zu ihm keinen Weg zur Root mehr.

Da er selbst noch einen Weg zur Root besitzt, wird sein Port zu Switch B nun zum Designated Port. Bislang hatte der Switch im HVT ja die günstigeren Pfadkosten für den Link, weswegen auch der Port auf Switch B der Designated Port des Uplinks auf die Etage war. Jetzt allerdings hat nur noch C bezüglich dieses Links überhaupt einen Weg zur Root, weswegen C auch zur Designated Bridge wird.

Switch C ändert daraufhin die Port-Rolle des Ports von Alternate auf Designated. Da sich ansonsten für ihn nichts geändert hat, kann er den Port auch gleich auf Forwarding schalten, da er jetzt der Root näher ist als zuvor Switch B, das hat er durch den Request erfahren. Zudem sendet er seinem Nachbarn ein positives Reply, genannt auch „go ahead“, in dem er ihm mitteilt, dass kein Loop geschlossen werden kann, wenn er (der Nachbar) in den Forwarding Modus wechselt.

Switch B empfängt den Request, und ändert nun die Port-Rolle von ehemals Designated auf Root und wechselt in den Forwarding Modus. Der Forwarding Timer hat keine Bedeutung mehr und wird nicht weiter beachtet, nachdem der Switch das Reply bekommen hat.

Zusammenfassung des ersten Beispiels:
So kompliziert der Mechanismus auch erscheint verglichen mit dem klassischen Spanning Tree, so effektiv ist er jedoch auch. Die Ziele des Verfahrens wurden alle erreicht:

1. Zu keiner Zeit hat es einen Loop im Netz gegeben.
2. Der Endzustand entspricht dem des klassischen Spanning Trees.
3. Es wurde nicht mehr Timer- sondern Event-basierend gearbeitet.

Gerade der letzte Punkt ist für die Umschaltzeit entscheidend. Versuche verschiedener Hersteller, die RSTP bereits implementiert haben, zeigen, dass Umschaltzeiten von unter einer Sekunde problemlos selbst über mehrere kaskadierte Switches hinweg erreicht werden können.

Doch schauen wir uns noch ein zweites Beispiel an:

So einfach die Beispieltopologie auch gewählt ist, so brauchbar ist sie auch, um die verschiedenen Auswirkungen der vierten RSTP Regel zu verdeutlichen. Nehmen wir an, der Linkausfall im HVT wurde vom Netzbetriebspersonal festgestellt und beispielsweise durch einen Kabeltausch behoben. Damit müsste sich auch der Spanning Tree wieder in seinen ursprünglichen Zustand zurück transformieren. Betrachten wir, was geschieht (vgl. Abbildung 10).

Der Link zwischen der Root und Switch B ist wieder hergestellt, der Fehler ist behoben. Bevor Switch B jetzt seinen direkten Link zur Root wieder auf Forwarding schalten darf, muss er zunächst seinen aktiven Root Port in den Discarding Modus versetzten, da ansonsten ein Loop geschaltet würde. Gemäß Regel 0 ist das jedoch kein Problem. Anschließend kann er den neuen Root Port aktivieren.

Jetzt möchte Switch B jedoch auch den Port in Richtung Etagenswitch zum Designated Port für das LAN-Segment zwischen sich und Switch B machen. Dies darf er jedoch nicht ohne Zustimmung des Etagenswitches, da es auch sonst wieder zu einem Loop kommen würde. Also sendet er wie im ersten Beispiel einen Request und startet ebenfalls wieder den Timer für das Forward Delay.

Der Etagenswitch erkennt nun, dass er in dieser neuen Situation zu Unrecht der Designierte Switch für die Strecke zwischen ihm und Switch B ist, weil er beispielsweise eine höhere Portpriorität als sein Nachbar hat. Er versetzt gemäß Regel 0 den Port also sofort in den Discarding Modus. Ferner erkennt er an dem Request, dass Switch B jetzt wieder einen Weg zur Root hat. Zwar nicht den besten aber den zweitbesten Weg. Also ändert er die Port-Rolle von Designated in Alternate.

Was er jetzt nicht tut, im Gegensatz zum ersten Bespiel, ist, er sendet kein „go ahead“ also keinen Reply. Switch B muss also den Ablauf des Timers abwarten, bevor er den Port zum Etagenswitch in den Forwarding Modus versetzen kann. Streng genommen durchläuft er sogar den Learning Modus zuvor, auch wenn er dabei nichts lernt.

Warum nun unterbleibt der Reply des Etagenswitches? Der Grund ist einfach: der Link zwischen Switch B und Switch C ist eine Punkt-zu-Punkt-Verbindung und beide Switches haben einen eigenen Root

Port, der mit dem Nachbarn nichts zu tun hat. Das Unterlassen des Replys hat somit zwar Auswirkungen auf die Vollständigkeit des Spanning Trees, der erst nach Ablauf des Timers und des Learning Modus wieder hergestellt ist, jedoch keinerlei Auswirkungen auf den Pakettransport, da das Segment, das für diese Zeitspanne keine Pakete erhält, das einzig betroffene Segment ist und selbst keine Endstationen enthalten kann (Punkt-zu-Punkt-Bedingung).

Zusammenfassung des zweiten Beispiels: Auch hier wurden die Ziele des Verfahrens alle erreicht:

1. Zu keiner Zeit hat es einen Loop im Netz gegeben.
2. Der Endzustand entspricht dem des klassischen Spanning Trees.
3. Es wurde nicht mehr Timer- sondern Event-basierend gearbeitet.
4. Der einzige Timer, der bis zum Ende durchläuft, hat keine Konsequenzen bei der Paketvermittlung.

Betrachtet man beide Beispiele zusammen, wird aber noch eine Bedingung des Rapid Spanning Trees klar, die zwar nur bei Regel 3 erwähnt wurde, jedoch anlog für alle anderen Regeln (außer der Nullten) gilt: „War der Spanning Tree zuvor lange genug stabil“. Was damit verhindert werden soll, ist ein kontinuierliches Respanning ausgelöst durch einen Flapping Port. Wäre in dem Beispiel der Link aufgrund eines Wackelkontaktes ausgefallen und wenige Sekunden später wieder aktiviert worden, so hätte das zu einer Verzögerung der zweiten Neuberechnung geführt. Damit versucht man den Spanning Tree vor solchen „Wacklern“ zu schützen, die ansonsten je nach Position des Wacklers zeitweise zu Komplettausfällen des Netzes führen würden.

Topologie Change

Beim Klassiker war es so, dass eine Änderung irgendwo im geswitchten Netz dazu führte, dass alle Switches ihre gesamten Bridging Tables vergaßen und neu lernten. Das war notwendig, damit Pakete nicht falsch zugestellt wurden, also in einen Zweig des Baumes weitergeleitet wurden, über den sie wegen des Respanning nicht mehr zugestellt werden konnten.

Nehmen wir das erste Beispiel von eben: Hat die Root ihre Bridge-Table nicht vergessen, so würde sie versuchen, Pakete zu Rechnern, die an Switch B angeschlossen sind, weiterhin durch einen nicht mehr funktionsfähigen Port zu versenden.

Grundsätzlich gilt das natürlich auch beim Rapid Spanning Tree. Allerdings sind die meisten Switches heute dazu in der Lage ihre Bridge-Table portbezogen zu verwalten und nicht wie die alten Bridges nur als Ganzes betrachten zu können. Aus diesem Grund hat man versucht auch diesen Effekt beim RSTP zu optimieren und das „Vergessen des Gelernten“ auf die notwenigen Porteinträge zu beschränken.

Diese Funktionen sind allerdings optional und jeder Switch kann für sich entscheiden, ob er nicht doch seine ganze Bridge-Table verwirft, anstatt nur auf Portebene zu löschen. Auch das ist notwendig um eine Abwärtskompatibilität zu gewährleisten.

Versand der TC-Meldung

Früher wurde die Meldung upstream in Richtung Root von allen Switchen nur durchgereicht, jedoch vorläufig nicht beachtet, erst wenn sie von der Root als TC-Meldung downstream zurück kam, wurde sie beachtet und anschließend der Erhalt bestätigt.

Das wurde beim Rapid Spanning Tree geändert:

1. Die TC-Meldung wird auch auf downstream Ports (also auf dem Weg zur Root) beachtet.
2. Der Empfang wird nicht bestätigt.
3. Um den Empfang sicherzustellen wird die Meldung beim RSTP zweimal verschickt.

Verarbeitung der TC-Meldung

Aber nicht nur der Versand sondern auch die Verarbeitung durch die Switches hat sich geändert. Das Regelwerk klingt kompliziert, ist jedoch im Grunde recht einfach. Betrachten wir die einzelnen Punkte:

1. Einträge, die sich auf wegfallende Ports (discarding oder disabled) beziehen, werden gelöscht.
2. Löschen der Einträge aller Ports eines Switches, bei dem ein Alternate Port zum Root oder Designated Port wurde.
3. Ein Switch löscht alle Einträge seiner Routing Table, es sei denn Regel 4 oder 5 findet Anwendung.
4. Für Edge Ports ändert sich niemals etwas, solange sie Edge Port bleiben. Einsichtig, sie bilden auch eine Ausnahme zu Regel 2 und 3.
5. Für einen Port, auf dem eine TC-Meldung empfangen wird, bleibt die Bridge-Table erhalten.
6. Wird ein Alternate Port zum Root Port, so kann der Alternate Port alle Adressen übernehmen, die zuvor dem Root Port zugeordnet waren.

Hinzu kommen noch zwei Punkte, die sich auf die Erzeugung und Weiterleitung von TC-Meldungen beziehen:

1. Systeme, auf denen sich etwas ändert, senden TC-Meldungen auf dem Root und auf allen Designated Ports.
2. Empfangene TC-Meldungen werden auf dem Root und auf allen Designated Ports weitergeleitet.

Der schnelle Baum

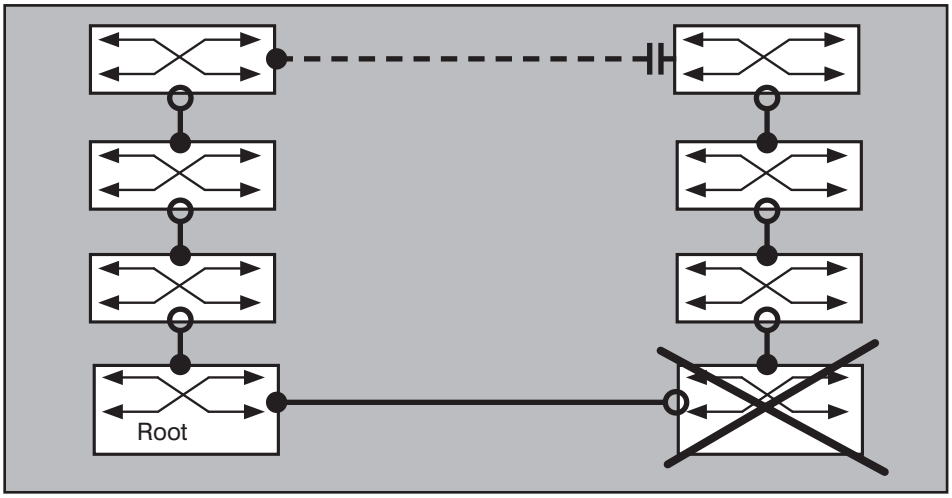


Abbildung 11

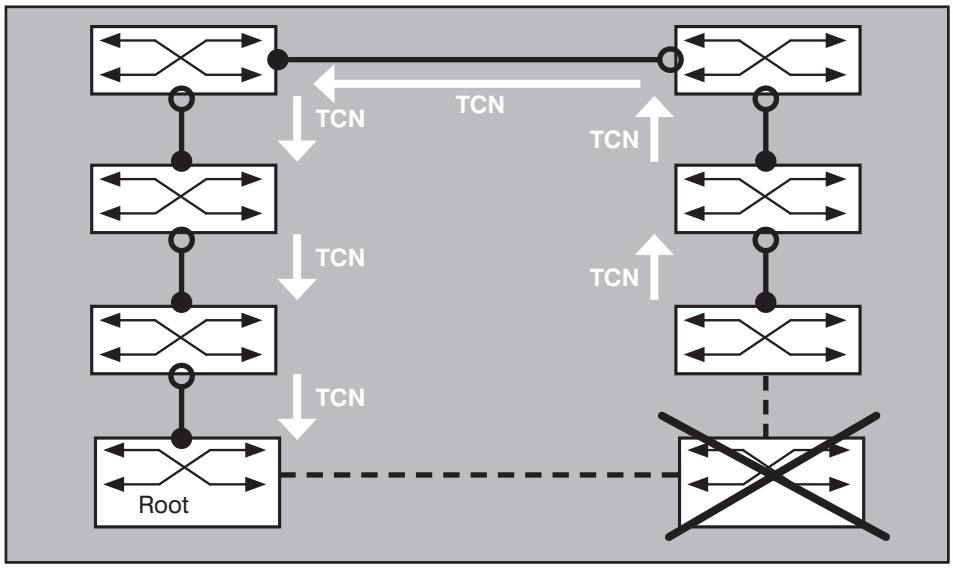


Abbildung 12

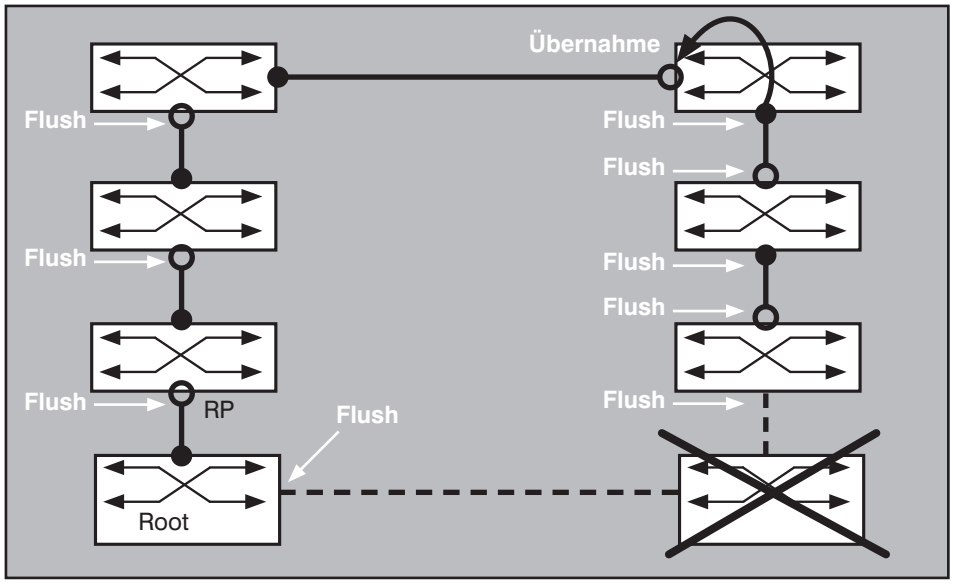


Abbildung 13

Auch hierfür ein Beispiel.

Ausgangslage (vgl. Abbildung 11) sei dieses Mal ein Gebäude mit einem HVT mit zwei Switches, auf der Etage werden sechs Etagenswitche betrieben. Da die Switches nicht stackable sind, jedoch RSTP beherrschen, werden sie kaskadiert betrieben. Zudem fehlen Uplink-Leitungen zwischen HVT und Etagenverteiler. Man verzichtet auf die Dreieckschaltung und verbindet die beiden „Stacks“ direkt miteinander.

In dieser Situation lassen wir nun einen der Hauptswitches ausfallen. Das Respanning läuft nun nach den zuvor schon beschriebenen Mechanismen ab. Was passiert jedoch mit den TC-Meldungen?

Im Bild außen vor gelassen sind die Endgeräte, die an den Etagenswitches angeschlossen sind. Es wird davon ausgegangen, dass es sich um Switches handelt, die Edge Ports bereits kennen und verwalten können, insofern ändert sich für die Bridge-Table in Bezug auf diese Ports auch nichts.

Der Switch, der den Ausfall bemerkt, sendet nun eine TC-Meldung (offizielle Bezeichnung: TCN für Topologie Change Notification) an alle seine Nachbarn (2x) (Abbildung 12). Diese reagieren bereits auf diese Meldung und warten nicht erst ab, dass sie eine TC-Meldung von der Root erhalten. Gemäß dem oben beschriebenen Regelwerk, werden nun die Tabellen port-bezogen gelöscht.

Man beachte, dass besonders die Ausnahmeregel 5 auf der linken Seite zum Zuge kommt, da nur noch für einen von zwei Ports die Tabelle gelöscht werden muss (Abbildung 12).

Das ist auf der rechten Seite anders. Das liegt daran, dass sich die Root und die Designated Ports vertauscht haben, weshalb die Bridge-Tables der gesamten Systeme gelöscht werden müssen.

Zusammenfassend lässt sich zur Änderung der TC-Verbreitung sagen, dass sie sicherlich „nice to have“ ist, man jedoch auch ohne leben kann, sollte es von dem ein oder anderen Hersteller nicht unterstützt werden. Die Einsparungen überflüssiger Löschungen halten sich in Grenzen und die Zeit, bis sich das Netz bezüglich ungewollter Weiterleitungen wieder stabilisiert hat, hält sich in Grenzen.

Probleme macht der Rapid Reconfiguration Spanning Tree nicht was die TC-Verbreitung angeht, Probleme kommen aus

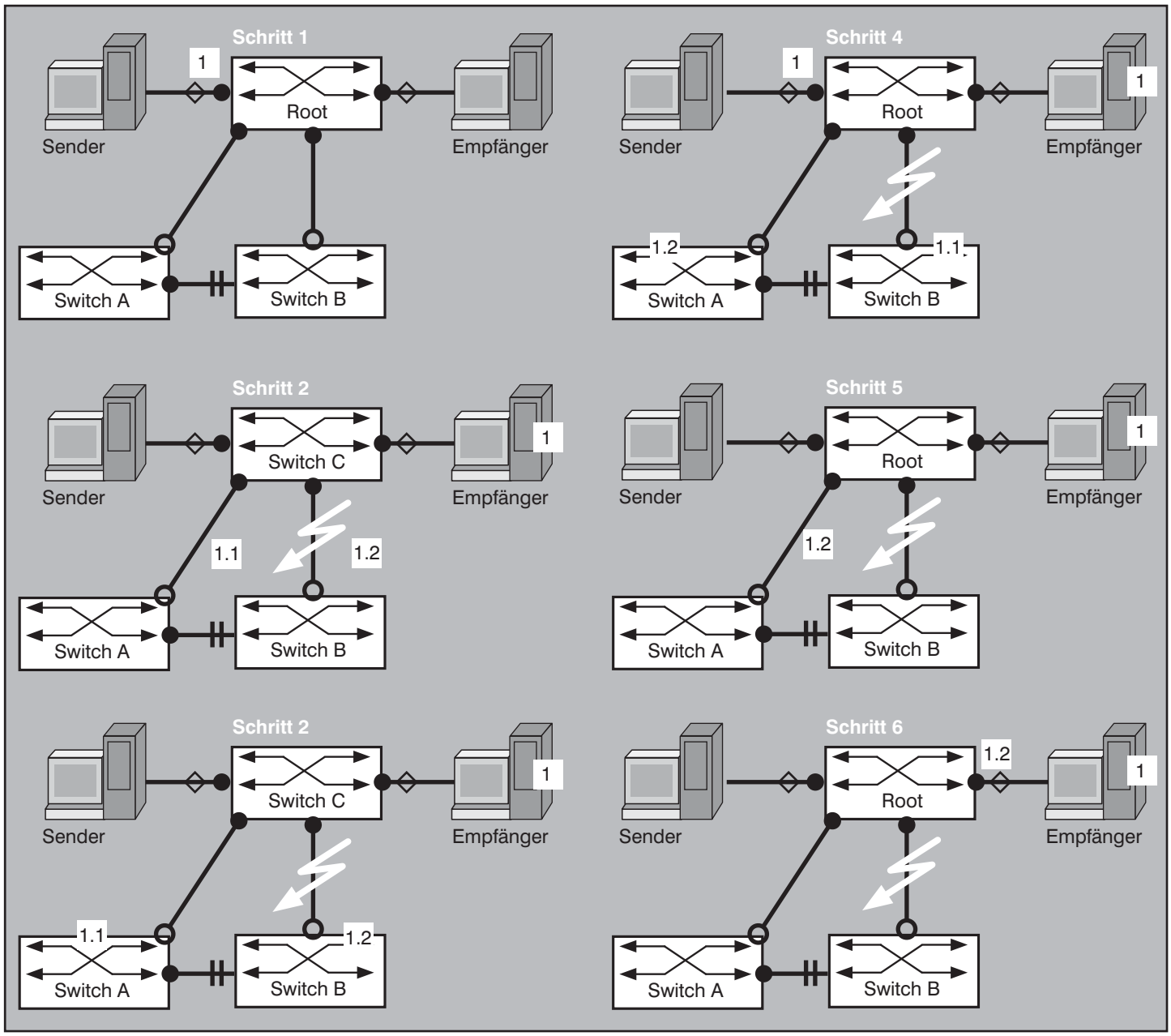


Abbildung 14

einer ganz anderen Richtung: er ist zu schnell.

Problemfälle

Frameverdopplung
Durch die schnelle Umschaltung kann es theoretisch zu Frameverdopplungen beim RSTP durch das Respanning kommen.

Zu einer Frameverdopplung kann es nur während eines Respanning-Prozesses kommen. Abbildung 14 zeigt ein Beispiel, wie es dazu kommen kann.

Im ersten Schritt sendet eine Station ein Paket an eine Station. In dem Beispiel hängt der Empfänger am selben Switch wie der Sender, so dass der Frame direkt zugestellt werden kann. Nehmen wir jedoch an, dass der Switch die Empfängeradresse noch nicht gelernt oder bereits wieder „vergessen“ hat oder dass es sich um einen Broadcast bzw. Multicast handelt. Der Switch, im Beispiel die Root, leitet den Frame also einerseits zum Empfänger, der ihn damit zum ersten Mal erhält, und andererseits an alle anderen Switche weiter (Schritt 2).

Noch bevor die anderen Switche A und B den Frame verarbeiten können, fällt der Link zwischen der Root und Switch B aus (Schritt 3) und es kommt zum Respanning. Währenddessen warten die Frames 1.1 und 1.2. noch in den Puffern der Switche auf ihre Abarbeitung. Nimmt man nun an, dass der Respanning-Prozess entweder wichtiger als die Paketverarbeitung ist oder das Respanning so schnell vonstatten geht, dass sich die Frames noch in den Speichern der Switche befinden, nachdem die neue Topologie berechnet wurde, so werden die Frames 1.1 und 1.2 von Switch A und Switch B wechselseitig weitergeleitet (Schritt 4).

Switch B wird den Frame anschließend verwerfen, da er keinen Partner mehr

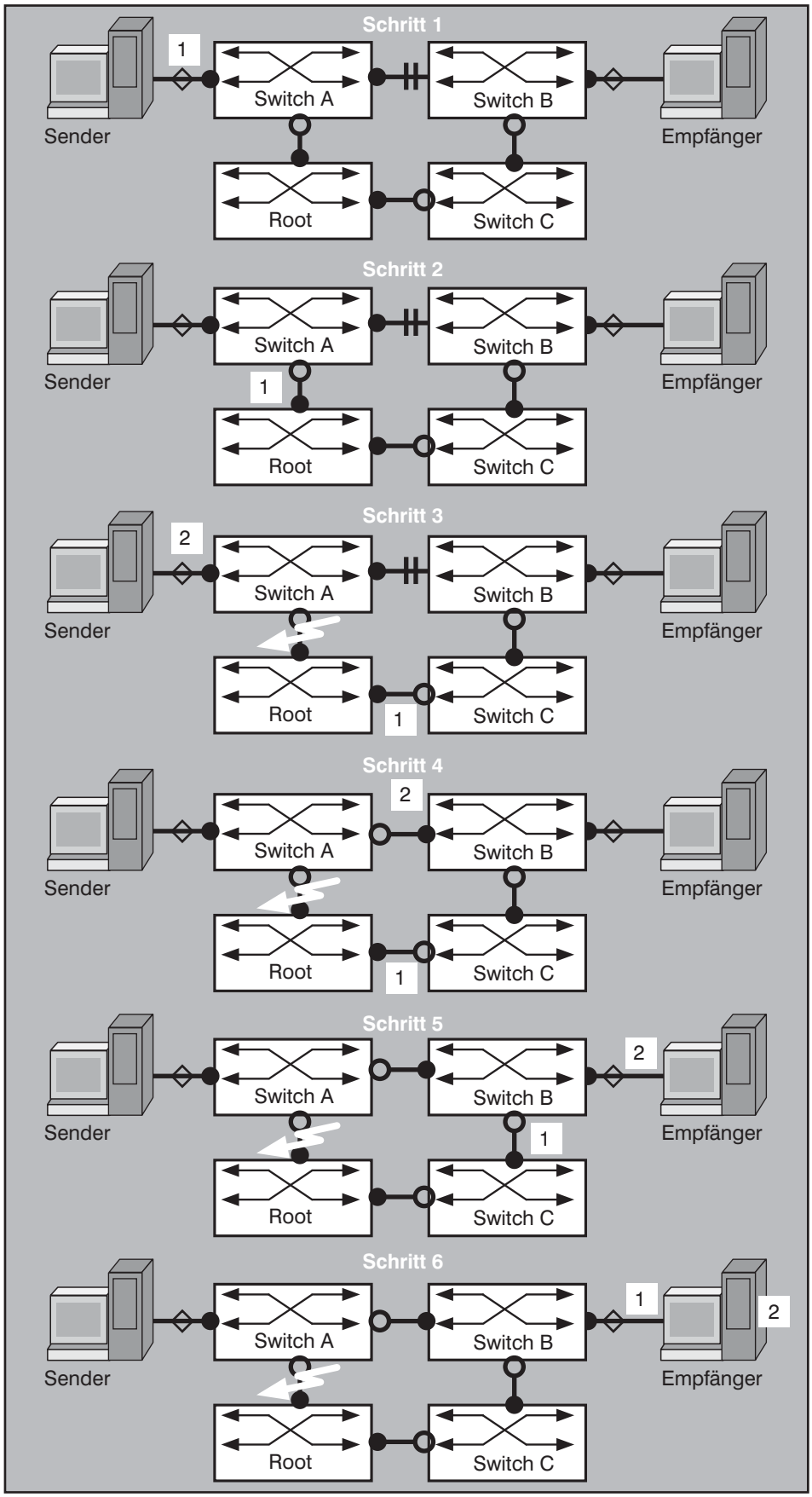


Abbildung 15

hat, an den er den Frame zustellen könnte, ohne ihn zurück zu A zu schicken. Anders aber Switch A: dieser hat den Frame 1.2 über den Port zu Switch B empfangen und leitet ihn nun zur Root weiter (Schritt 5). Die Root kann nicht erkennen, dass sie den Frame bereits schon einmal verarbeitet hat und leitet ihn an den Empfänger weiter, der in somit ein zweites Mal erhält. Beachtenswert bei der Frameverdopplung sind folgende Dinge:

1. Eine Verdoppelung von Frames ist natürlich auch in anderen Topologien als der dargestellten möglich.
2. Es ist durchaus möglich, dass sogar Unicasts dupliziert werden.
3. Eine „Vermehrung“ von Multicast und Broadcast ist sehr viel wahrscheinlicher als von Unicasts.

Theoretisch kann es Anwendungen geben, die kritisch darauf reagieren, jedoch gerade Multicast-Anwendungen können sehr gut mit Frameverdopplungen umgehen. Auch bei TCP dürfte es zu keinen Problemen führen, da vom TCP-Stack die Verdopplung erkannt und das überflüssige Paket verworfen wird. Es wird nicht damit gerechnet, dass dieses Phänomen ein „echtes“ Problem darstellt.

Frame Misordering
Anders sieht das allerdings bei dem zweiten Problem aus:

Durch die schnelle Umschaltung kann es zu einer Vertauschung der Paketreihenfolge beim Empfang kommen. Betrachten wir auch dazu zunächst ein Beispiel (Abb. 15).

Als Beispiel dient die „verkleinerte“ Kaskade, die bereits aus dem Beispiel des Topologie Change bekannt ist (Abbildung 11 bis Abbildung 13).

Ein Sender sendet einen ersten Frame an seinen Switch A. Angenommen der Empfänger befindet sich auf dem benachbarten Switch B, der Topologie des Spanning Trees wegen wird der Frame jedoch über die Root geleitet, da der Link zwischen A und B nicht benutzt wird (Schritte 1 und 2). Nachdem der Frame bei der Root angekommen ist, fällt der Uplink zwischen der Root und Switch A aus. Währenddessen sendet der Sender einen zweiten Frame, der zur selben Kommunikation gehört wie der erste (Schritt 3). Durch das Respanning wird nun der Link zwischen den Switches A und B aktiv, was zur Folge hat, dass der direkt Weg zwischen Sender und Empfänger nun genutzt werden kann (Schritt 4). Dadurch kann der Frame, der als zweites verschickt wurde, vor dem eintreffen, der als erstes gesendet wurde (Schritte 5 und 6).

Zu beachten ist hierbei, dass es durchaus mehr als nur zwei Frames betreffen kann, man braucht sich zur eine Kaskadierung über mehr Geräte vorzustellen als im Beispiel; schon vom Standard sind bis zu sieben Brücken kaskadiert vorgesehen. In dem Fall könnten weitaus mehr Frames betroffen sein als „nur“ zwei.

Anders als das Problem der Frameverdopplung gibt es durchaus einige Protokolle, die eine Vertauschung von Frames nicht abfangen können. Beispiele sind LAT, LLC2 oder NetBEUI. Hat man solche Protokolle im Netz, sollte man den RSTP besser im compatible Mode betreiben, das heißt wie den klassischen STP, nur ohne Listening Phase.

Zusammenfassung

Der Rapid-Spanning-Tree hat trotz der beschriebenen Nachteile den Bedarf und die Notwendigkeit von Hersteller-spezifischen Layer2-Redundanz-Lösungen beseitigt. Er bildet eine solide Basis für die meisten Anwendungsfälle, Ausnahmen wird es sicher immer geben. Historisch gesehen bildete die Einführung des RSTP einen wichtigen Schritt in rein Standard-basierte und Hersteller-neutrale Netzwerk-Architekturen.

Abkürzungsverzeichnis

BPDU	Bridge Protocol Data Unit
CSMA/CD	Carrier Sense Multiple Access with Collision Detecion
HVT	Hauptverteiler
ID	Identifier
IEEE	International Electrical and Electronic Engineers
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LAT	Local Area Transport
LLC2	NetBIOS Extended User Interface
MAC	Media Access Control
MSTP	Multiple Spanning Tree Protocol
NetBEUI	Logical Link Control, type 2
NetBIOS	Network Basic Input/Output System
RST	Rapid Reconfiguration Spanning Tree
RSTP	Rapid Reconfiguration Spanning Tree Protocol
STP	Spanning Tree Protocol
TC	Topologie Change
TCN	Topologie Change Notification
TCP	Transmission Control Protocol
VLAN	Virtual LAN, Virtual Local Area Network
WAN	Wide Area Network

Aktuelles Seminar

Exchange 2007 - Upgrade lohnenswert oder sogar erforderlich?

Die ComConsult Akademie veranstaltet vom 18.06. - 20.06.07 ihr Seminar „Exchange 2007 - Upgrade lohnenswert oder sogar erforderlich?“ in Bonn.

E-Mail ist heute für die meisten Unternehmen ein missionskritisches Kommunikationsmittel, welches für die Mitarbeiter zu jeder Zeit und unabhängig vom Aufenthaltsort erreichbar und uneingeschränkt nutzbar sein muss. Exchange 2007 adressiert diese Anforderungen durch neue und, im Vergleich zu seinen Vorgängern, verbesserte Technologien, so dass sich für Betreiber vorhergehender Exchange-Versionen die Frage aufwirft, ob sich ein Upgrade lohnt oder gar als erforderlich herausstellt.

Das Seminar richtet sich sowohl an Betreiber mittelständischer sowie komplexer Exchange-Umgebungen. Da davon auszugehen ist, dass Exchange 2007 meist in vorhandene Exchange-Welten realisiert wird, liegt das Hauptaugenmerk für Deployment und operatives Geschäft auf diesen „gemischten Umgebungen“.

Das Seminar hilft dabei, zu entscheiden, welche Konsolidierungspotentiale durch ein Produktupgrade bestehen und welche neuen Anforderungen an das Messagingdesign zu stellen sind.

Die Verwendung der Exchange Shell wird das Seminar durchgehend begleiten, da die derzeitige GUI nur maximal 20 Prozent der Konfigurationsmöglichkeiten abdeckt.

Zielgruppe dieses Kurses sind IT-Mail-Administratoren und IT-Entscheider, Kenntnisse in Active Directory / IP Design unter Windows 200x und Kenntnisse im Messagingbereich werden vorausgesetzt.

Themschwerpunkte
- Überblick
- Verwaltung einer gemischten Exchangeumgebung
- Client Access
- Routing: Veränderte Messageflow-Architektur
- Hochverfügbarkeit mit Exchange 2007
- Deployment
- Security, Policies und Compliance
- Best Practices für die verschiedenen Rollen und Funktionalitäten
- Unified Messaging - Integration von VoiceMail und Fax
- Exchange 2007 in Zusammenarbeit mit
  - Office 2007
  - Sharepoint Server 2007
  - Office Communication Server
  - ISA-Server

Durch das Seminar führen Hans-Willi Kremer und Dipl.-Ing. Peter Kleynen.

Hans-Willi Kremer ist bei der ComConsult Beratung und Planung GmbH als Berater im Competence Center Backoffice tätig. Mitte der 90er Jahre qualifizierte er sich zum Microsoft Certified Systemengineer + Internet (MCSE + I), Microsoft Certified Database Administrator (MCDBA), Microsoft Certified Solution Developer (MCSD) und Microsoft Certified Trainer. Als Exchangeexperte hat Herr Kremer in internationalen Migrationsprojekten Messagingumgebungen vom Design bis hin zum Rollout verantwortet.

Dipl.-Ing. Peter Kleynen ist seit 2004 als freier Mitarbeiter bei der ComConsult Beratung und Planung GmbH als Berater im Competence Center BackOffice tätig. Zu seinen Kernkompetenzen zählen der Entwurf von Active Directory- und Exchange-Umgebungen sowie deren Implementierung und Migration. Herr Kleynen ist seit über 10 Jahren als MCSE und MCT zertifiziert und verfügt über langjährige Erfahrung in der Durchführung von Projekten und Seminaren.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Exchange 2007 - Upgrade lohnenswert oder sogar erforderlich?

☐ Ich buche das Seminar
Exchange 2007 - Upgrade lohnenswert oder sogar erforderlich?
18.06. - 20.06.07 in Bonn
zum Preis von € 1.690,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____07

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Schwerpunktthema

Dual-Vendor-Strategien im LAN

Fortsetzung von Seite 1

Dr. Simon Hoff ist technischer Direktor bei der ComConsult Beratung und Planung GmbH und unter anderem verantwortlich für den Bereich IT-Sicherheit. Dr. Hoff blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung und Betrieb in den Bereichen IT-Infrastrukturen, mobiler und drahtloser Kommunikationssysteme zurück.

Dr. Frank Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

2. Technische Ebene

Eine Dual-Vendor-Strategie bietet sich grundsätzlich auf zwei verschiedene Arten an. Zum einen ist es möglich, an verschiedenen Standorten eines Unternehmens Komponenten verschiedener Hersteller einzusetzen, aber innerhalb eines Standortes immer nur Komponenten eines Herstellers zu verwenden. Zum anderen ist der Einsatz von Komponenten verschiedener Hersteller an einem Standort eines Unternehmens denkbar, wenn pro Netzebene nur Komponenten eines Herstellers verwendet werden.

Ein wesentliches Argument für eine solche Dual-Vendor-Strategie ist zunächst darwinistischer Natur: Die Auswahl an Netzkomponenten vergrößert sich, und die jeweilig besseren Komponenten können für Aufbau, Umbau oder Erweiterung eines Netzes eingesetzt werden. Dies trägt zur Erhöhung der Qualität des Netzes bei. Mit der gestiegenen Konkurrenz gewinnt außerdem automatisch die Produkt-Evolution an Qualität und Tempo.

2.1 Standort-Modell: Hersteller-homogene Standorte

Bei dieser Variante werden innerhalb eines Standortes nur Komponenten eines einzigen Herstellers eingesetzt. Verschiedene Standorte können aber Komponenten verschiedener Hersteller einsetzen.

Um eine Interoperabilität sicherzustellen, müssen neben der standortübergreifenden Kommunikation insbesondere Aspekte betrachtet werden, die sich aus der Mobilität von Clients ergeben.

2.1.1 Standortübergreifende Kommunikation

Normalerweise sind hier keine Probleme zu erwarten, sofern zwischen den Standorten eine WAN-Technik mit standardisierter Routing/MPLS-Funktionalität eingesetzt wird und die verwendeten Produkte der verschiedenen Hersteller diese Funktionen unterstützen.

Probleme können unter Umständen bei dynamischem Routing auftreten. Hier müssen Standardprotokolle eingesetzt werden
.

2.1.2 Mobilität

Wird im LAN eine Netzzugangskontrolle eingesetzt, müssen Hersteller-spezifische Konzepte beachtet werden. Kritisch wird dieser Bereich, wenn ein Roaming von Clients zwischen Standorten unterstützt werden soll. Zu betrachten ist dabei der Wechsel eines mobilen Endgeräts von einem Standort mit Komponenten des einen Herstellers zu einem Standort mit Komponenten des zweiten Herstellers. (siehe Abbildung 1)

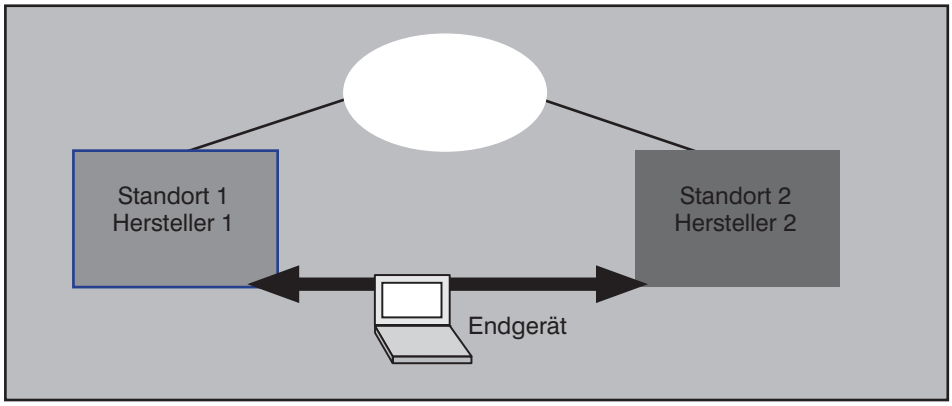


Abbildung 1: Roaming von Endgeräten zwischen Standorten

Die meisten Methoden zur Implementierung einer Netzzugangskontrolle basieren auf IEEE 802.1X. Dabei wird die Zugangskontrolle unmittelbar am Netzwerk-Port durchgeführt. Die Unterstützung von Roaming erfordert bei einer auf IEEE 802.1X basierte Netzzugangskontrolle die zwischen den Standorten abgestimmte und möglichst einheitliche Verwendung von EAP-Methoden (d.h. den verwendeten Authentifizierungsmethoden).

Weitergehende Sicherheitsmechanismen, die der Integritätsprüfung der Client-Konfiguration dienen und oft EAP als Träger verwenden, basieren oft auf herstellerspezifischen Funktionen im Netz (wie z.B. Cisco Network Admission Control, NAC). Dabei wird typischerweise eine dedizierte EAP-Methode zur Übertragung der Informationen der Client-Integrität verwendet (z.B. EAP-FAST bei NAC). Ein Roaming zwischen Standorten mit unterschiedlichen Herstellern erfordert dann auch eine Harmonisierung der verwendeten Sicherheitsfunktionen zur Integritätsprüfung der Client-Konfiguration.

2.2 Access-Modell: Dual-Vendor-Konzepte im LAN

Eine Dual-Vendor-Strategie kommt zunächst für große und mittlere Standorte in Frage, die im Allgemeinen über die Netzebenen Core-Bereich, ggf. Distribution-Bereich und Access-Bereich verfügen. Für die Integration des zweiten Herstellers bietet sich folgende Aufteilung an:

- Innerhalb des Core-Bereichs und, wenn vorhanden, im Distribution-Bereich sollten nur Komponenten eines Herstellers eingesetzt werden.

- Innerhalb des Access-Bereichs sollten möglichst nur Komponenten des zweiten Herstellers eingesetzt werden. Es erfolgt möglichst keine Mischung mit Komponenten des für die anderen Netzebenen eingesetzten Herstellers.

  Für eine Migration sollte zumindest sichergestellt werden, dass an einem Distribution Switch ausschließlich Access Switches eines Herstellers angebunden werden. Eine Migration für das Access-Modell kann schrittweise erfolgen, wobei einzelne Gebäude (im Sinne des Einzugsbereichs der entsprechenden Distribution Switches) in einem Schritt migriert werden sollten.

Die Schnittstelle zwischen Access-Bereich und der nächsthöheren Netzebene muss herstellerübergreifend harmonisiert werden. Für den Endgerätebereich ist für den Mischbetrieb beider Hersteller im Access-Bereich zu beachten, dass sich die herstellerspezifischen Funktionen unterscheiden und auch für standardisierte Funktionen spezifische Erweiterungen zu berücksichtigen sind. Generell gilt, dass die Interoperabilität der eingesetzten Protokolle im Einzelfall durch entsprechende Tests geprüft werden sollte, sofern die Hersteller hier nicht eine entsprechende Aussage machen. Abbildung 2 zeigt die kritischen Elemente im Überblick.

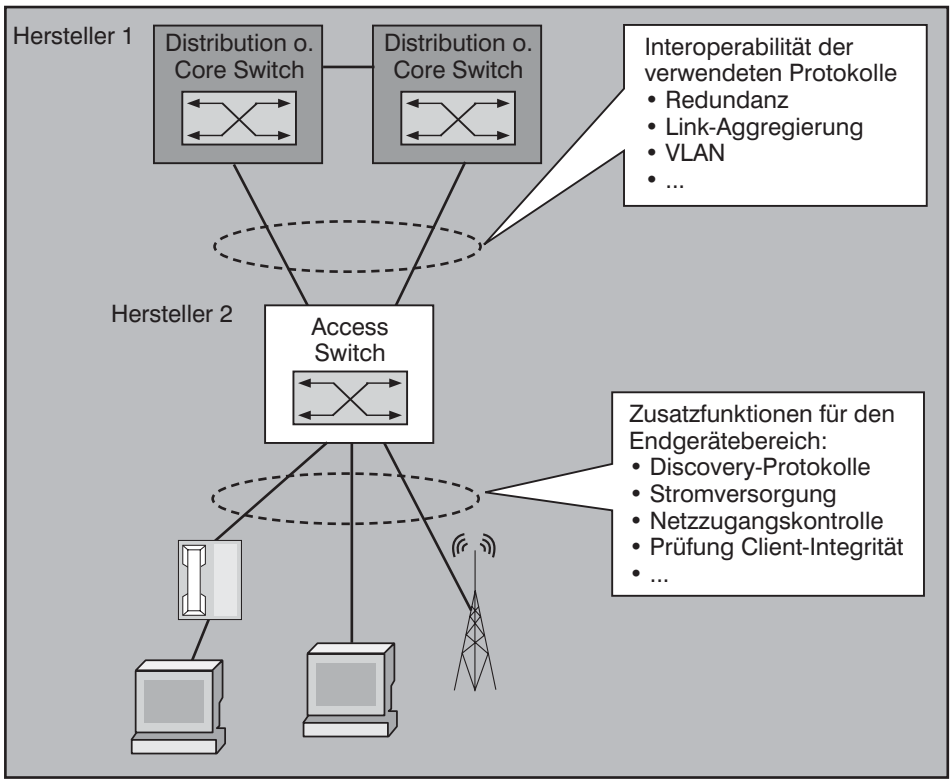


Abbildung 2: Kritische Schnittstellen

2.2.1 Anbindung der Access Switches

Für den Einsatz unterschiedlicher Hersteller im Access-Bereich und im Distribution- bzw. im Core-Bereich muss die Interoperabilität der Protokolle zwischen den Netzebenen zugesichert werden. Die folgenden Ausführungen zeigen, dass für die wesentlichen Bereiche auf standardisierte Mechanismen zurückgegriffen werden kann, was die Implementierung der hier betrachteten Dual-Vendor-Strategie erheblich erleichtert.

Redundanzmechanismen

STP (Spanning Tree Protocol, siehe IEEE 802.1D-1994) ist derzeit nur noch als Notfall-Variante vorzusehen, wenn alte Komponenten ohne RSTP (Rapid Spanning Tree Protocol, siehe IEEE 802.1D-2004) eingebunden werden müssen. STP wird seit langem von den Herstellern unterstützt und eine Interoperabilität kann weitgehend zugesichert werden.

Kritischer ist die Situation bei herstellerspezifischen Erweiterungen von STP. Beispielsweise können gewisse Cisco-spezifische Ergänzungen zum STP in einem Dual-Vendor-Szenario ggf. nicht mehr eingesetzt werden. Dies betrifft unter anderem Verfahren zur beschleunigten Umschaltung (z.B. BackboneFast). Dies kann aber auch durch RSTP erreicht werden. Die Abbildung von STP auf verschiedene VLAN ist ein weiterer Aspekt, der bei einer Interoperabilitätsbetrachtung bewertet werden muss. Das Cisco Per-VLAN-STP (PVST+) wird z.B. von HP ProCurve nicht unterstützt. In dieser Situation kommt das standardisierte MSTP (Multiple Spanning Tree Protocol gemäß IEEE 802.1s, jetzt integriert in IEEE 802.1Q) in Frage.

Link-Aggregierung

Eine Link-Aggregierung (IEEE 802.3ad) gestattet eine Zusammenfassung von mehreren physikalischen Leitungen zu einer logischen Leitung und ist nutzbar für Fast Ethernet und Gigabit Ethernet. Für herstellerspezifische Funktionen im Bereich der Link-Aggregierung ist oft keine Interoperabilität gegeben. Ein Beispiel ist Cisco EtherChannel (FEC, GEC), ein Vorläufer von IEEE 802.3ad.

VLAN

Die Aushandlung einer VLAN-Konfiguration zwischen Switches kann das Fehlerrisiko von VLAN-Konfigurationen reduzieren.

Eine Interoperabilität zwischen Herstellern kann dabei durch das standardisierte GVRP (GARP VLAN Registration Protocol) erreicht werden. Für herstellerspezifische Verfahren, wie Cisco VTP (VLAN Trunking Protocol) ist eine Interoperabilität mit anderen Herstellern meist nicht gegeben.

2.2.2 Endgeräteanschluss
Für den einen Mischbetrieb zweier Hersteller im Access-Bereich (der im Rahmen einer Migration nicht zu vermeiden ist) muss die Konfiguration so gestaltet sein, dass es für ein Endgerät möglichst keine Rolle spielt, wo es angeschlossen wird. Dabei ist wesentlich, dass der notwendige Funktionsumfang zur Erkennung angeschlossener Geräte, zur Stromversorgung über Ethernet und zur zeitgemäßen Absicherung des LAN-Zugangs unterstützt wird.

Discovery-Protokolle
Discovery-Protokolle zur Erkennung der Nachbar-Knoten (Identität und Eigenschaften) können der Abstimmung von Parametern dienen. Insbesondere für VoIP-Geräte ist ein offenes Discovery-Protokoll beispielsweise zur Zuweisung eines Voice VLAN wichtig. Mit LLDP bzw. LLDP-MED sind standardisierte Protokolle für diesen Bereich verfügbar.

Im Zusammenhang mit einer Dual-Vendor-Strategie sind oft Geräte zu berücksichtigen, die lediglich ein herstellerspezifisches Discovery-Protokoll unterstützen (zu nennen ist hier insbesondere das Cisco Discovery Protocol, CDP). Bei der Migration zu einem zweiten Hersteller im Access Bereich muss (sofern der zweite Hersteller CDP nicht unterstützt) in dieser Situation eine alternative Konfigurationen beispielsweise für die Anbindung eines IP-Telefons in Kauf genommen werden.

Stromversorgung
Für die Stromversorgung über Datenkabel zum Anschluss von beispielsweise VoIP-Telefonen oder WLAN Access Points hat sich der Standard IEEE 802.3af durchgesetzt. Herstellerspezifische Verfahren, wie Inline Power von Cisco sind in der Praxis nur noch zur Anbindung von Altlasten erforderlich. Dabei ist zu erwähnen, dass verschiedene Hersteller (z.B. manche HP ProCurve Switches) auch Cisco Inline Power unterstützen.

Zugangskontrolle
Für eine effektive Zugangskontrolle mit IEEE 802.1X an einem Switch Port sind über den Standard hinausgehende Funktionen wichtig:

- Default Policy und Kommunikation des Netzwerkports im unautorisierten Zustand: Manche Hersteller gestatten den Transport von Nachrichten spezieller Protokolle über einen noch nicht durch eine erfolgreiche Authentifizierung per IEEE 802.1X freigeschalteten Port (Beispiel CDP bei Cisco). Besser ist hier die Standard-konforme Verwendung einer Default Policy, die einen nicht autorisierten Port zunächst in einem VLAN mit eingeschränkten Rechten belässt und bei einer erfolgreichen Authentifizierung den Port in ein anderes VLAN hebt.

- Eine Multi-Client-Authentication gestattet den Anschluss mehrerer Geräte über einen Port (z.B. ein VoIP-Endgerät und darüber einen PC) und die separate Authentifizierung dieser Geräte sowie die damit verbundene Zugangskontrolle für jedes Gerät.

- Bei einer mehrstufigen Authentifizierung wird zunächst ein Authentifizierungsversuch per IEEE 802.1X gestartet. Antwortet das Endgerät nicht, kann in der zweiten Stufe geprüft werden, ob die MAC-Adresse des Endgeräts bekannt ist. Wenn dies der Fall ist, kann ein eingeschränkter Zugang über ein VLAN gewährt werden, über das nur spezielle Ziele und Dienste gestattet werden (z.B. nur Sprachkommunikation). Auf diese Weise kann für Geräte, die kein IEEE 802.1X unterstützen, eine Zugangskontrolle realisiert werden und so ein sanfter Migrationspfad geschaffen werden.

Das Angebot dieser Funktionen und deren Implementierung unterscheidet sich zum Teil erheblich zwischen den Herstellern und muss daher bei Planung und Migration für ein Dual-Vendor-Szenario entsprechend berücksichtigt werden.

Client-Integritätsprüfung
Die Integritätsprüfung von Clients muss (sofern gefordert) bei der Produktauswahl im Access-Bereich betrachtet werden, da hier meist herstellerspezifische Konzepte eingesetzt werden. In einem Dual-Vendor-Szenario ist hier bei einem Mischbetrieb im Access-Bereich natürlich mit erheblichen Problemen zu rechnen. Eine einheitliche Verwendung eines Produkts zur Integritätsprüfung kommt praktisch nur dann in Frage, wenn die Lösung keine herstellerspezifischen Funktionen in den LAN-Switches erfordert. Ein Beispiel hierzu ist die mit Microsoft Vista und Longhorn kommende Funktion Network Access Potection (NAP). NAP realisiert eine Client-Integritätsprüfung, die Switch-unabhängig ist und auf IEEE 802.1X aufsetzen kann. In diesem Zusammenhang sind auch die Arbeiten der Trusted Computing Group zu erwähnen, die mit dem Industriestandard Trusted Network Connect (TNC) eine Architektur geschaffen hat, welche die Client-Integritätsprüfung als zentralen Bestandteil einer Netzzugangskontrolle spezifiziert.

3. Dual-Vendor aus kaufmännischer Sicht

Auf kaufmännischer Ebene sind zweifelsohne die größten Vorteile einer Dual- oder sogar Multi-Vendor-Strategie zu erwarten.

Gründe dafür sind die erfahrungsgemäß deutlich größeren Preisnachlässe, die durch eine herstellerneutrale Ausschreibung zu erzielen sind sowie die teilweise erheblich günstigeren Einkaufspreise alternativer Hersteller.

Bei von ComConsult durchgeführten Hersteller-neutralen Ausschreibungen zeigt es sich immer wieder, dass je nach Produkt und Umfang zwischen fünf und 60 Prozent günstigere Preise zu erzielen sind als bei einer Hersteller-gebundenen Ausschreibung. Diese Unterschiede ergeben sich vor allem aus dem zum Teil hart umkämpften Markt sowie der vorherrschenden Strategie der Hersteller, sich bei einem Kunden in der Hoffnung zu etablieren, dass dieser künftig nur noch eine Single-Vendor-Strategie verfolgt. Zudem könnten weitere Kriterien eine Rolle spielen, wie etwa die lebenslange Bereitstellung von Updates und Patches für die angebotenen Komponenten oder aber die Bereitschaft der Hersteller, Rückkauf-Angebote zu machen. Es zeigt sich aber immer wieder, dass durchaus noch erhebliche Preisunterschiede zwischen den einzelnen Anbietern zu erwarten sind, so dass bei entsprechenden Nachverhandlungen auch mit derartigen Rabatten gerechnet werden kann. Voraussetzung dafür sind jedoch einige Grundregeln, die bei einer Ausschreibung zu beachten sind.

Ein besonderer Fall sind öffentliche Auftraggeber. Hier ist es in der Regel nicht möglich, so auszuschreiben, dass lediglich ein Hersteller zum Zug kommen kann. Zudem besteht häufig die Sorge, dass nach dem Ergebnis der Ausschreibung nicht mehr gegen den billigsten Anbieter entschieden werden kann, obwohl es möglicherweise organisatorische Vorteile hätte. Um dennoch über ein Angebot mit Technik vom gewünschten Hersteller bevorzugen zu können, werden die Anforderungskataloge häufig so eng gefasst, dass aufgrund nebensächlicher Kriterien doch noch ein Ausschluss erfolgen kann. Der Aufwand für diese Ausschreibungen ist immens, da für nahezu jede ausgeschriebene Position Kriterien gefunden werden müssen, die ein Alleinstellungsmerkmal darstellen. Diese Vorgehensweise ist zudem aus juristischer Sicht höchst fragwürdig und dürfte einer genaueren Untersuchung nicht standhalten.

Ein häufiger Grund, warum auch die Mitarbeiter eines Unternehmens sehr gerne an einem Hersteller „kleben“ und eine Multi-Vendor-Strategie ablehnen, sind Nebenabreden der Hersteller. Sowohl im öffentlichen als auch im gewerblichen Bereich binden die Hersteller ihre Kunden häufig mit Hilfe von Meistbegünstigungsklauseln, in Aussicht gestellter Rabatte oder Nebenangeboten, die z.B. die kostenlose Überlassung von Software, Updates oder höhere Service Level bei der Wartung versprechen. Diese Boni führen bei den verantwortlichen Mitarbeitern eines Kunden zu einer gewissen Gewöhnung an einen Hersteller, die nur schwer zu durchbrechen ist. Aufgrund dieser Gewöhnung werden dann nicht selten diverse Scheinargumente für eine herstellerspezifische Ausschreibung verwendet, die Angebote von anderen Herstellern von vornherein sinnlos erscheinen lassen.

Nichtöffentliche Auftraggeber sind im Gegensatz zu öffentlichen Auftraggebern nicht zu Hersteller-unabhängigen Ausschreibungen gezwungen. Hier werden erfahrungsgemäß nicht selten sowohl technische als auch kaufmännische Argumente gegen eine Hersteller-unabhängige Ausschreibung ins Feld geführt. Auf kaufmännischer Seite wird häufig argumentiert, dass der Mehraufwand einer Hersteller-unabhängigen Ausschreibung erheblich größer ist und die zu erzielenden Vorteile nicht aufwiegt. Dem ist aus der Erfahrung von ComConsult eindeutig zu widersprechen. Richtig ist zwar, dass der Aufwand für eine neutrale Ausschreibung im Vergleich zu häufig schon vorbereiteten Ausschreibungsunterlagen einzelner Hersteller größer ist, die zu erzielenden Preisvorteile überwiegenden diesen Aufwand erfahrungsgemäß aber bei Weitem.

Die Gestaltung der Leistungsverzeichnisse sollte die Gemeinsamkeiten der Produkte als Spezifikation enthalten. Dadurch ist gewährleistet, dass nicht ausgefallene Spezialitäten zum Ausschlusskriterium werden. Zudem sollte der Ausschreibung eine realistische Schätzung des Lieferumfangs zugrunde liegen. Auf Mindestabnahmeverpflichtung sollte verzichtet werden. Jedoch ist erfahrungsgemäß die Verpflichtung von Vorteil, innerhalb eines bestimmten Zeitraums nur von einem oder zwei Herstellern zu beziehen. Im Gegenzug sollte sich der Anbieter verpflichten, denselben Rabattsatz nicht nur für die konkret angebotenen LAN-Komponenten, sondern für die ganze Produktkategorie für einen festen Zeitraum zu gewährleisten.

3.1 Marktposition der Hersteller

Ein nicht unwesentlicher Aspekt bei der Entscheidung über eine Dual-Vendor-Strategie ist die Marktposition der einzelnen Hersteller. Es ist wenig erfreulich, wenn sich ein Hersteller kurz nach dem Kauf einer großen Menge seiner Produkte entschließt, den Geschäftsbereich zu verkaufen oder gar zu schließen. Zwar wird in der Regel noch über einige Jahre hinweg Support versprochen, jedoch zeigt die Erfahrung, dass LAN/WAN-Komponenten auch noch nach Jahren der Einführung z.T. erhebliche Fehler aufweisen, die nur durch das Aufspielen neuer Patches beseitigt werden können. Die Fortentwicklung der Software bleibt häufig jedoch aus oder wird sehr schnell zurückgefahren. Fehler können damit nicht mehr beseitigt, Performance-Engpässe nicht mehr ausgeglichen werden.

Diese Argumente sprechen zweifelsohne für die unumstrittenen Marktführer. Cisco Systems hat aber nicht nur im Bereich „Managed Switch Ports“ eine Marktbeherrschende Stellung erreicht, sondern erzielt den größten Teil des Umsatzes mit Netzkomponenten (Switches und Router). Somit ist der Hersteller ganz entscheidend auf Erhalt der eigenen Marktstellung in den beiden Märkten für Router und LAN-Switches angewiesen. Hinzu kommt, dass auf dem Markt für Dienstleistungen und auf dem Stellenmarkt Know-how zu Cisco-Komponenten im Vergleich zur Expertise im Umgang mit anderen Produkten sehr weit verbreitet ist, so dass mit dem Einsatz von Cisco-Komponenten nur eine geringe Abhängigkeit von einzelnen Dienstleistungsunternehmen oder einzelnen Mitarbeitern verbunden ist.

Um den zweiten Platz hinter Cisco war lange Zeit ein heftiger Kampf entbrannt. Beispielsweise hat HP ProCurve in den letzten Monaten jedoch deutlich aufgeholt und belegt auf dem Europäischen Markt nun gleich bei mehreren Kriterien und nach Meinung namhafter Analysten Platz zwei. Die langjährige Schwäche von HP – das Produktportfolio für das High-End-Segment – wurde inzwischen beseitigt. Anders als früher ist neben dem Marktführer damit nicht nur ein preislich günstigerer Anbieter auf dem Markt, sondern auch ein technologisch mindestens gleichwertiger Mitbewerber verfügbar. Mit einer Reihe von neu entwickelten Tools, die dem Administrator bzw. dem Helpdesk die Arbeit erheblich erleichtern sollen, begegnet HP zudem der Furcht vieler Anwender, die zunehmende Komplexität neuer Netzwerkkomponenten nicht mehr im Griff zu haben. Damit hat sich HP von der ursprünglich verfolgte Strategie, nur als eine preiswerte Alternative zu Cisco-Produkten auf den Markt zu kommen, verabschiedet. Inzwischen reicht das Angebot von einfachen Access Switches bis hin zu High-End-Komponenten im Core-Bereich. Die Support-Strukturen sind mit denen von Cisco mindestens vergleichbar.

Im Vergleich zu Cisco und HP ProCurve hat Nortel Networks im LAN-Switch-Bereich keine so breite Produktpalette, aber ein für die meisten Unternehmen ausreichendes Portfolio anzubieten. Die Beschaffungskosten für Nortel-Komponenten sind nach den Erfahrungen von ComConsult mit denen für Cisco-Komponenten vergleichbar. Nortel gewinnt in erster Linie keine Projekte mit dem Vorteil der günstigeren Beschaffung, sondern durch Vorteile hinsichtlich der installierten Basis (einige Automobilhersteller setzen beispielsweise seit Jahren Nortel-Komponenten ein). Ein eventueller Wechsel von Cisco zu Nortel könnte nach Erfahrungen von ComConsult nicht allein durch die günstigere Beschaffung begründet werden.

Foundry sieht den eigenen Schwerpunkt im Wesentlichen im Bereich von High-End-Produkten wie BigIron oder ServerIron. Günstigere Access-Komponenten als Cisco Systems oder HP bietet Foundry in der Regel nicht an. Der Einsatz von Komponenten des Herstellers Foundry ist aus Sicht von ComConsult mit dem Nachteil verbunden, dass Know-how und technische Unterstützung für diese Produkte auf dem Markt nicht sehr verbreitet sind. Extreme ist hinsichtlich des Verbreitungsgrades der Produkte sowie Know-how und Erfahrungen zu den Produkten mit Foundry vergleichbar.

3Com hat vor wenigen Jahren die Unterstützung für ihre damaligen High-End-Produkte beendet und damit viele eigene Kunden gezwungen, zu anderen Herstellern wie Cisco und Extreme zu wechseln. Jetzt versucht 3Com, im High-End-Markt wieder Boden zu gewinnen, wobei die Produktpalette noch Lücken aufweist.

Die Firma Enterasys gewinnt ähnlich wie Nortel kaum Projekte mit dem Vorteil der günstigeren Beschaffung, sondern entweder auf der Basis der langjährigen Kundenbeziehungen oder in Bereichen, in denen Sonderfunktionen insbesondere bei der Absicherung des Netzzugangs erforderlich sind. Auch bei Enterasys muss man den geringen Verbreitungsgrad der Produkte und somit des Know-hows über die Produkte berücksichtigen.

In letzter Zeit werden Huawei-Produkte in Deutschland sehr offensiv vermarktet, zum Beispiel durch die Siemens AG. Dabei wird stark auf das Argument der günstigeren Beschaffung gesetzt. Um die Defizite bezüglich des Know-hows über Huawei-Produkte zu beheben, werden zurzeit Siemens-Mitarbeiter für den Umgang mit Huawei-Komponenten geschult. In der jetzigen Situation werden jedoch für die Lösung komplexer Probleme häufig Entwickler und Spezialisten aus dem Stammland des Herstellers (Volksrepublik China) eingesetzt. Nach wie vor sind die Vertriebs- und Supportstrukturen in Deutschland und Europa kaum ausgebaut, so dass diese Produkte derzeit weniger empfohlen werden können.

Andere Hersteller kommen aufgrund ihres Produktportfolios höchstens für Access-Bereich in Frage, da Core-Komponenten oder modulare Router nur höchst unzureichend zur Verfügung stehen. Auch fehlt es in diesem Segment an entsprechenden Support-Strukturen, Erfahrungswerten und Testergebnissen. Vor allem ist aber jederzeit damit zu rechnen, dass Billiganbieter ihre Produktstrategien wechseln, sehr viel später erst Innovationsschritte und neue Standards umsetzen, sich nur schwer in Management-Konzepte einpassen lassen oder gänzlich vom Markt verschwinden.

3.2 Wartungs- und Betriebskosten

Ein oft gegen eine Dual-Vendor-Strategie ins Feld geführtes Argument sind die Wartungskosten. Hierbei wird in der Regel davon ausgegangen, dass bei größerer Stückzahl geringere Wartungskosten pro Gerät anfallen. Das ist in der Regel richtig, jedoch zeigt die Erfahrung, dass die Hersteller auch hier zu erheblichen Abschlägen bereit sind, sofern sich die Hoffnung auf größere Stückzahlen ergibt. Insbesondere dann, wenn zwar firmenweit eine Dual- oder Multi-Vendor-Strategie genutzt wird, pro Standort jedoch nur ein Hersteller zum Zug kommt (Standort-Modell), bleiben die Wartungskosten in der Regel auf demselben Niveau wie bei einer reinen Single-Vendor-Strategie. Zudem sind die Hersteller auch hier nicht selten zu sehr unterschiedlichen Zugeständnissen bereit. Beispielsweise könnte die lebenslange kostenlose Belieferung mit Patches und Updates ausschlaggebend sein.

Kritischer ist hier schon die Frage zu bewerten, welcher Mehraufwand beim eigenen Personal und den eigenen Kosten zu erwarten ist. Es hat sich in der Vergangenheit gezeigt, dass sich beim Wartungspersonal sehr schnell Präferenzen herausbilden, die nicht zuletzt auf menschliche, emotionale Aspekte zurückzuführen sind. Sind beispielsweise mal mit einem Produkt größere Schwierigkeiten entstanden, hat das z.T. erhebliche Langzeitwirkungen und beschränkte sich im Lauf der Zeit subjektiv auch nicht mehr auf dieses eine Produkt, sondern auf die gesamte Produktpalette eines Herstellers. Um dies zu vermeiden, sind entsprechende Schulungsmaßnahmen für die Mitarbeiter eines Unternehmens erforderlich. Diese Schulungsmaßnahmen stellen naturgemäß einen Mehraufwand gegenüber einer Single-Vendor-Lösung dar, wobei der tatsächliche Aufwand eher vom Know-how und der Güte der Mitarbeiter abhängt. Einige Hersteller unterstützen diese Maßnahmen u.a. mithilfe von Tools, z.B. zur Steuerung von Zugriffspolicies auf Basis der Identität oder zur Unterstützung des Helpdesks. Aber auch hier reduziert die Treue zu etablierten Standards diesen initialen Mehraufwand jedoch deutlich.

3.3 Aufwandsoptimierung für den Betrieb von Produkten unterschiedlicher Hersteller

Aus technischen Gründen spricht vieles für die Beschränkung einer Dual-Vendor-Strategie auf den Access-Bereich eines LANs (Access Modell). In diesem Bereich sind inzwischen umfangreiche Standards seit Jahren etabliert und nur wenige (proprietäre) Neuerungen zu erwarten. Eine andere Strategie ist der Ausbau eines gesamten Standorts mit nur einem Hersteller (Standort-Modell), andere Standorte aber möglicherweise mit anderen Herstellern. Letztere Strategie ist zwar nur für große Unternehmen sinnvoll, erlaubt aber die Nutzung von Einsparmöglichkeiten bei gleichzeitig minimiertem Risiko von Inkompatibilitäten. Zudem müssen nur zentrale Stellen mit unterschiedlichen Herstellern zurechtkommen. Die lokal verantwortlichen Mitarbeiter bleiben bei einem Hersteller.

Welche der Strategien für das jeweilige Unternehmen besser geeignet ist, entscheidet sich beispielsweise am Anteil der Beschaffungskosten für den Access-Bereich, an der erforderlichen Stückzahl und der damit verbundenen Ausfallwahrscheinlichkeit. Liegt ein Großteil der Kosten im Access-Bereich, ist eine Dual-Vendor-Strategie dringend zu empfehlen. Neben den Einsparungen bei der Beschaffung entstehen in diesem Bereich kaum Schulungsaufwand für Mitarbeiter oder besondere Schwierigkeiten bei der Integration. Defekte Access-Switches können in der Regel ohne komplexe Konfiguration oder sonstige aufwändige Management-Eingriffe ausgetauscht werden.

Beim Standort-Modell wirft die Neu-Ausstattung eines gesamten Standorts hingegen größere Probleme auf. Neben der Umstellung der Mitarbeiter bei einem Wechsel des Herstellers muss möglicherweise nicht nur der Access Bereich, sondern auch der Core- und Distribution-Bereich ausgewechselt werden. Grund dafür sind die oft proprietären Möglichkeiten eines Herstellers (z.B. Port-Trunking, VLAN-Trunking, Management etc.). Das zentral mit dem Management des Netzes befasste Personal muss sich naturgemäß mit allen Herstellern auskennen und entsprechende Fault- oder Change-Prozesse beherrschen. Die Betriebskosten einer solchen Lösung können erfahrungsgemäß kurzfristig bis zu 20 Prozent höher liegen als bei einem homogenen Umfeld, sind auf lange Sicht jedoch kaum höher als bei einer Single-Vendor-Strategie. Hinzu kommen unter Umständen einige technische Gesichtspunkte im WAN- und Management-Bereich sowie bei Fragen der Quality of Service und bei Sicherheitsfunktionen. Zweifelsohne sind im Fall einer Dual-Vendor-Strategie auch andere Verfahren und Prozesse erforderlich als bei einem einzigen Hersteller, jedoch sind die Kosten dafür in der Regel zu vernachlässigen. Auf diese Fragen soll im folgenden Abschnitt eingegangen werden.

4. Organisatorische Ebene

Netzwerk-Betrieb ist heutzutage nicht einfach eine Techniker-Leistung, die aus der Aufstellung, Konfiguration und Wartung von Netzwerk-Technik besteht. Vielmehr ist das Netzwerk Teil einer Gesamtleistung, in deren Rahmen den Anwendern Informationstechnik (IT) in einer Form und Weise zur Verfügung gestellt wird, dass diese überhaupt mit anforderungsgerechtem Produktivitätsgrad ihre fachlichen Aufgaben wahrnehmen können. Daher erfolgt keine isolierte Betrachtung einzelner technischer Beiträge mehr (nur Netzwerk, nur Server, ...), sondern es wird ein funktionierender technischer Verbund zur Bereitstellung eines bestimmten Service-Angebotes betrachtet und bewertet. Im Rahmen dieser Gesamt-Dienstleistung ist „Netzwerk-Bereitstellung“ für Anwender Teil eines komplexen Gebildes von Prozessen und Management-Aufgaben: die Technik-Spezialisten müssen sich organisieren, um effiziente Arbeitsteiligkeit (Aufbauorganisation, Aufgabenverteilung) und Abläufe (IT-Service-Prozesse) erreichen zu können.

Die Aufgabenstellung des effizienten Organisierens des Netzwerk-Betriebs lässt sich nur im Rahmen einer systematischen Betrachtung und Gestaltung der Gesamtdienstleistung lösen. Dabei müssen Netzwerk-nahe Aufgaben und Prozesse zunächst in übergeordnete (für alle Technikbausteine Hersteller-unabhängig und einheitlich zu gestaltende) Management-Funktionen eingeordnet werden (z.B. Problem Management). Ein Hersteller-gebundenes, gleichzeitig aber umfassendes Netzmanagement würde schon alleine daran scheitern, dass kein Hersteller alle Komponenten eines Netzes, also z.B. auch die Server anbietet.

Der Netzwerk-Betreiber ist also gezwungen, maßgebliche Management-Elemente möglichst unabhängig von Hersteller-spezifischen Eigenschaften der Geräte im LAN zu gestalten. Gleichzeitig sind aufgrund der spezifischen Eigenschaften einzelner Komponenten keine Management-Lösungen verfügbar, die wirklich alle Möglichkeiten jeder beliebigen Komponente ausschöpfen. Solche so genannten Umbrella-Management-Systeme beschränken sich in der Regel auf die Nutzung von standardisierten SNMP-Objekten. Sollen aber beispielsweise Patches auf viele hundert verteilt installierte Switches aufgespielt werden, kann dies häufig nur mit Hersteller-spezifischer Software erledigt werden. Diese für einzelne Elemente eines Netzes spezifische Software wird als Element-Management-System (EMS) bezeichnet. Jeder große Hersteller von managebaren Netzwerk-Komponenten stellt inzwischen entsprechende Tools und Management-Werkzeuge zur Verfügung.

Als eines der am weitesten verbreiteten Umbrella-Management-Systeme ist hier neben Tivoli und Spectrum sicherlich HP OpenView zu nennen, das aufgrund seiner umfassenden Funktionalität und seiner absichtlich möglichst geringen Hersteller- oder System-Bindung beste Voraussetzungen für ein umfassendes LAN-Management mit sich bringt. Um auch Komponenten anderer Hersteller nicht nur durch standardisierte SNMP-Objekte managen zu können, erlaubt HP OpenView beispielsweise die Integration von Cisco Works, um auch Komponenten von Cisco möglichst komfortabel und ohne Verzicht auf Hersteller-spezifische Eigenschaften managen zu können.

Der Betreiber eines Netzwerks muss bestrebt sein, ein Höchstmaß an Hersteller-Unabhängigkeit zu erhalten, ohne gleichzeitig auf spezifische Vorteile und Möglichkeiten einzelner Komponenten zu verzichten. In der Praxis sieht das in der Regel so aus, dass neben einem umfassenden Management-System ohnehin schon diverse spezifische Management-Systeme im Einsatz sind. Eine Dual-Vendor-Strategie wird daran kaum etwas ändern.

Gleiches gilt für die Bereitstellung von Personalkapazitäten. Denn Release- und Configuration-Management-Aufgaben können beispielsweise nur bis zu einer bestimmten Größenordnung sinnvoll von Generalisten wahrgenommen werden. Danach ist eine Spezialisierung je nach Netzwerk, Systemen, Herstellern usw. notwendig. Die evtl. vorhandene ITIL-Konformität bleibt dabei gewahrt, indem eine optimierte Ausgestaltung der Management-Prozesse im Sinne der Empfehlungen und Ratschläge von ITIL vorausgesetzt wird. Eine Dual-Vendor-Strategie verursacht hier also keinen zusätzlichen Aufwand im Vergleich zu einer Single-Vendor-Strategie.

Trotz aller Hersteller-Unabhängigkeit bleiben aber insbesondere das Change-Management, das Configuration-Management und das Fault-Management (Incident- und Problem-Management) von

Dual-Vendor-Strategien betroffen, da diese im Wesentlichen von Hardware-Eigenschaften der Geräte abhängig sind. Auf diese Prozesse soll im Folgenden eingegangen werden.

4.1 Change-Management-Prozesse

Bei einer Dual-Vendor-Strategie sind herstellerübergreifende Seiteneffekte und Kompatibilitätsprobleme z.B. bei Release-Wechseln und beim Einspielen von Patches unter Umständen problematisch. Gründe dafür sind proprietäre Erweiterungen von Protokollen und Mechanismen, Anpassungen von Schwellenwerten und anderen Parametern sowie Modifikation der Hardware und der etablierten Standards. Aus diesem Grund sollte eine Dual-Vendor-Strategie möglichst in den technischen Bereichen stattfinden, die über wohl definierte Schnittstellen vom Rest des Netzes abgegrenzt werden können und die Verwendung von Standards mit höchster Priorität durchgehalten werden. Dabei sollte eine Standardisierung weitestgehend abgeschlossen sein und einen stabilen Zustand erreicht haben (z.B. bei Ethernet im Access-Bereich). Leider halten sich nicht alle Hersteller an solche Standards, sondern modifizieren diese „aus technischen“ Gründen nicht selten in erheblichem Umfang.

Dort, wo Geräte unterschiedlicher Hersteller zusammenarbeiten müssen, sind umfangreiche Tests vor einem Rollout unumgänglich. Diese Tests sind jedoch nicht auf Dual-Vendor-Umfelder beschränkt, sondern auch bei der Einführung neuer Geräte oder Patches eines Herstellers zu empfehlen. Zahlreiche Beispiele zeigen, dass ein einziger Hersteller keineswegs die Garantie für eine tadellose Zusammenarbeit aller eigenen Geräte übernimmt sowie die Funktionsfähigkeit aller Patches garantiert. Daher ergibt sich durch eine Dual-Vendor-Strategie zunächst kein zusätzlicher Aufwand. Jedoch müssen die mit den Tests befassten Mitarbeiter über vertiefte Kenntnisse beider Produktlinien verfügen.

Häufig stellt sich das Problem, dass Hersteller bestimmte „Verbesserungen“ ihrer Produkte, also beispielsweise effizientere, aber nicht Standard-konforme Übertragungsprotokolle als Default-Wert einstellen, obwohl die Komponente durchaus auch zur Nutzung des Standards in der Lage ist. Dies könnte bei einer Dual-Vendor-Strategie und selbst bei vor dem Einsatz stattfindenden Tests durchaus zu erheblichen Problemen führen, wenn dazu kein Fachwissen vorhanden ist. Diesen Schwierigkeiten ist kaum durch eigenes Personal eines Netzbetreibers zu begegnen, da naturgemäß bei Neubeschaffungen noch jegliche Erfahrung mit diesen Produkten fehlt. Daher sollte hier bei einer Dual-Vendor-Strategie von vornherein durch entsprechende Ausschreibungen und Verpflichtungen der Hersteller gewährleistet sein, dass eine Zusammenarbeit unterschiedlicher Komponenten funktioniert. Wichtiger noch ist aber, dass der Hersteller sich möglichst präzise und dauerhaft an etablierte Standards hält. Dies hat sich HP ProCurve beispielsweise als Teil der Adaptive-Networking-Strategie auf die Fahnen geschrieben.

Zusätzliche EMS sind ebenfalls keine großen Investitionen, da die Hersteller in der Regel solche Systeme bei entsprechender Stückzahl der Komponenten preisgünstig zur Verfügung stellen. Zudem handelt es sich um einmalige Investitionen und ggf. entsprechende Schulungen der betroffenen Mitarbeiter, so dass hier keine großen Kosten zu erwarten sind.

In einem Umfeld, das jedoch keine besonderen Ansprüche stellt (z.B. der Access-Bereich ohne Voice, ohne besondere Management- oder Sicherheitsfunktionen etc.), sind die durch eine Dual-Vendor-Strategie zu erwartenden Aufwandssteigerungen gering. Das Change-Management besteht hier praktisch nur aus dem Nachziehen des Asset-Managements und ggf. noch des jeweiligen EMS. Überwachungs- und Managementfunktionen bleiben von einem Austausch unberührt. Ebenso ist nicht davon auszugehen, dass Release-Wechsel oder Patches in diesem Bereich zu Problemen führen.

4.2 Configuration Management

Für das Configuration Management gilt ähnliches wie für das Change-Management. Unterschiedliche Hersteller, aber selbst unterschiedliche Geräte eines Herstellers erfordern unterschiedliche Konfigurationen. Prozesse, welche die Vorgaben hinsichtlich der Konfiguration einzelner LAN-Komponenten betreffen, sind daher unmittelbar mit den spezifischen Eigenschaften der Komponenten verbunden.

Auch hier gilt wiederum, dass Seiteneffekte beispielsweise aufgrund unterschiedlicher Release-Stände oder Eigenschaften bei der Einführung neuer Komponenten nicht ausgeschlossen werden können. Auch mit Hilfe umfangreicher Tests und entsprechender Anforderungen an den Hersteller bzw. den Lieferanten lassen erfahrungsgemäß solche Probleme nicht vollständig vermeiden. Eine Dual-Vendor-Strategie führt hier also zu keiner wirklichen Steigerung von Aufwand und Kosten.

Innerhalb eines Standorts lassen sich die vom Hersteller empfohlenen Release-Stände zu einem Zeitpunkt einhalten. Entsprechende Herstellergarantien für Updates und Patches können dann in vollem Umfang greifen. Die Kommunikation über den Standort hinaus erfolgt schon allein aufgrund der dazwischen liegenden WAN-Provider in der Regel auf der Basis festgelegter und etablierter Standards, so dass hierüber keine Seiteneffekte auftreten können. Diese WAN-Provider-Grenze spricht auch gegen „intelligentere“ Netze wie sie beispielsweise von Cisco mit der Service Oriented Network Architecture (SONA) angeboten werden. Viele Eigenschaften eines solchen Frameworks scheitern schon allein an den Möglichkeiten der Standort-übergreifenden WANs. Die Umsetzung einer Dual-Vendor-Strategie im Sinne des Standort-Modells wird so auf eine natürliche Art und Weise erleichtert.

4.3 Incident- und Problem-Management

Im Bereich des Fault- bzw. Incident- und Problem-Managements sind sämtliche Beiträge der Netzwerk-Spezialisten zur akuten Störungsbehandlung sowie zur anschließenden Nachbehandlung nach Störungsbeseitigung zu sehen. Dazu gehört die Störungsannahme, also die Annahme von Tickets für den Netzwerk-Bereich und die unmittelbare Reaktion auf Alarme durch die überwachende Netzwerk-Management-Lösung. Dazu gehört aber auch die Diagnose und Problembehebung bzw. Nachsorge z.B. bei Instandsetzungsmaßnahmen, ebenso die Konfigurationsänderung zur Fehlerbehebung.

Hinsichtlich Monitoring und Fehlerbehandlung sind einige Anpassungen bestehender Support-Prozesse bei einer Dual-Vendor-Strategie notwendig. Beispielsweise müssen den Technikern vor Ort entsprechende Ersatzgeräte zur Verfügung stehen, um im Rahmen der bestehenden SLAs hinreichend schnell für Ersatz sorgen zu können. Je nach Zentralisierung solcher Ersatz-Komponenten-Lager entstehen mit einer Dual-Vendor-Strategie zusätzlicher Bedarf an Lagerplatz und Lager-Verwaltung. Geht man jedoch davon aus, dass die Lager möglichst dezentral aufgestellt sind, sind keine zusätzlichen Kosten zu erwarten, wenn wiederum von einer Standort-bezogenen Dual-Vendor-Strategie ausgegangen wird. Werden derartige Dienstleistungen, wie heute weit verbreitet, von externen Dienstleistern übernommen, stellen sich derartige Kosten- und Aufwandsfragen erst gar nicht. Es ist kaum anzunehmen, dass ein Deutschland- oder Europaweit operierender Dienstleister über nur eine Hersteller-Linie verfügt und daher entsprechende Reserven auch von anderen Herstellern vorhält.

Die Erweiterung der Kompetenz im eigenen Haus, z.B. im zentralen Network Operation Center ist bei einer Dual-Vendor-Strategie hingegen nicht zu vermeiden. Im Fehlerfall sind dann die Mitarbeiter im Second- oder Third-Level mit dem Problem befasst, die mit dem jeweiligen Hersteller am besten vertraut sind. Eine entsprechende Größe des LANs vorausgesetzt, könnte ein einziger Mitarbeiter ohnehin nicht die Kompetenz für den gesamten Second-Level-Bereich aufbringen, so dass eine sinnvolle Aufteilung hier so oder so geboten ist. Die Nutzung von entsprechenden Tools und das Festhalten an Standards erleichtert die Fortbildung der Mitarbeiter in diesem Bereich erheblich. Hier ist zu hoffen, dass die anderen Hersteller dem Beispiel von HP ProCurve folgen und ebenfalls die zunehmende Komplexität der Thematik durch das Festhalten an etablierten Standards und die Entwicklung von Werkzeugen vorantreiben.

5. Fazit

Eine Dual-Vendor-Strategie basierend auf Hersteller-homogenen Standorten ist von einem technischen Blickwinkel mit geringen Risiken und einem vergleichsweise überschaubaren technischen Aufwand verbunden. Das Roaming von Geräten zwischen Standorten erfordert allerdings eine Harmonisierung der eingesetzten Mechanismen. Für das Access Modell ist zunächst die Interoperabilität der Protokolle zwischen Access- und Distribution-Bereich (bzw. zwischen Access- und Core-Bereich, falls die Distibution-Ebene entfällt) entscheidend. Dies kann ohne funktionale Einschränkungen durch den Einsatz von Standardprotokollen erreicht werden. Für den Endgeräteanschluss ist insbesondere die herstellerunabhängige Erkennung von Geräten, die Authentifizierung am Netzwerk-Port und die Zusicherung der Integrität der Client-Konfiguration wichtig.

Aufgrund einer Dual-Vendor-Strategie im LAN sind bei der Beschaffung der erforderlichen Komponenten durchaus erhebliche finanzielle Vorteile zu erzielen. Es zeigt sich immer wieder, dass die Hersteller bereit sind, besonders dann hohe Rabatte einzuräumen, wenn eine Ausschreibung Hersteller-neutral erfolgt oder entsprechende Nachverhandlungen geführt werden. Demgegenüber steht zwar zum Teil ein technischer und betrieblicher Mehraufwand, der erfahrungsgemäß aber nur kurzfristig bzw. einmalig anfallen und auf lange Sicht kaum die Einsparungen aus einem Herstellerneutralen Einkauf kompensieren wird, sofern sich der Netzbetreiber an bestimmte Regeln hält. Dazu gehören vor allem ein Hersteller-neutrales Netzmanagement und ein möglichst Standard-konformer Netzbetrieb. Letztlich muss aber jeder Einzelfall betrachtet werden, um eine sinnvolle Entscheidung im Hinblick auf eine bestimmte Dual-Vendor-Strategie zu treffen.

Die Erfahrung zeigt, dass es nur zwei denkbare Varianten einer Dual-Vendor-Strategie gibt:

1) Im Access-Bereich eines LAN (Access-Modell) oder
2) einzelne Standorte werden komplett von einem Hersteller bestückt (Standort-Modell)

Bei der ersten Variante entstehen kaum Nachteile durch eine Dual-Vendor-Strategie, sofern keine komplexen Management- oder Monitoring-Prozesse bis hinunter auf die Port-Ebene stattfinden. Der Austausch dieser Produkte erfolgt im Fehlerfall unabhängig vom Hersteller. Dazu müssen lediglich geringe Eingriffe im Management-System des Netzbetreibers vorgenommen werden. Zudem sind in diesem Bereich schon entsprechende Standards etabliert.

Die zweite Variante ist typischerweise für große Unternehmen sinnvoll, welche ohnehin eine Größenordnung erreicht haben, die eine zunehmende Spezialisierung des mit dem Support befassten Personals mit sich bringt. In diesem Fall entstehen je Standort keine Kosten bei einer Dual-Vendor-Strategie. Lediglich bei der Einführung eines neuen Herstellers müssen initiale Kosten z.B. aufgrund von Schulungen und der Einführung eines zusätzlichen EMS berücksichtigt werden. Diese Kosten bleiben aber weit hinter den z.T. erheblichen Einsparungen zurück, die sich aus der Konzern-weiten Hersteller-Unabhängigkeit ergibt.

6. Abkürzungen

CDP	Cisco Discovery Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EMS	Element Management System
FAST	Flexible Authentication via Secure Tunneling
FEC	Fast EtherChannel
GEC	Gigabit EtherChannel
GARP	Generic Attribute Registration Protocol
GVRP	GARP VLAN Registration Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ITIL	IT Infrastructure Library
LAN	Local Area Network
MAC	Medium Access Control
MPLS	Multiprotocol Label Switching
MSTP	Multiple Spanning Tree Protocol
NAC	Network Admission Control
NAP	Network Access Protection
PVST+	Per-VLAN-STP
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
SONA	Service Oriented Network Architecture
STP	Spanning Tree Protocol
TNC	Trusted Network Connect
VLAN	Virtual LAN
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WLAN	Wireless LAN

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Sommerschule 2007, 11.06. - 15.06.07 in Aachen
Dieses Seminar vermittelt, welche Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind, wie man mit diesen Fehlersituationen analysiert und wie dabei methodisch vorgegangen wird, um in kürzester Zeit zu einem Ergebnis zu kommen. Preis: € 2.290,- zzgl. MwSt.

Troubleshooting Windows Server 2003 Active Directory, 11.06. - 14.06.07 in Aachen
Dieses 4-tägige Seminar besteht aus einem Mix aus Know-How-Auffrischungen, Aufgaben, Live-Demonstrationen und Troubleshooting durch die Teilnehmer selber, so dass ein hoher Praxisgrad erreicht wird. Die Referenten kommen vom bekannten Competence Center Backoffice der ComConsult Beratung und Planung, das auf zahlreiche erfolgreiche nationale und internationale AD-Projekte im Bereich von ca. 300 bis zu 80.000 Benutzer/Computer zurück blicken kann. Preis: € 1.990,- zzgl. MwSt.

Grundlagen des Trouble Shooting in Lokalen Netzwerken, 11.06. - 15.06.07 in Aachen
Dieses Seminar vermittelt, welche Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind, wie man mit diesen Fehlersituationen analysiert und wie dabei methodisch vorgegangen wird, um in kürzester Zeit zu einem Ergebnis zu kommen. Preis: € 2.490,- zzgl. MwSt.

Kommunikationssysteme, Kollaborationssysteme und Anwendungsintegration vor dem Hintergrund der Netz-Konvergenz, 11.06. - 13.06.07 in Bonn
In diesem 3-tägigen Seminar werden sowohl die Einflüsse der Konvergenzfelder und Technologien auf das Design der Unternehmensnetze diskutiert, als auch die Potentiale, die sich daraus ergeben. Preis: € 1.690,- zzgl. MwSt.

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Projektteams leiten, 11.06. - 13.06.07 in Bonn
In diesem 5-tägigen Intensiv-Seminar steht das Führungsverhalten des Projektleiters eindeutig im Mittelpunkt. Professionelles Moderieren, Präsentieren, Verhandeln und Teamleiten ist eine Kunst, die trainierbar ist. Anhand begleitender Rollenspiele und Praxisübungen werden die führungsrelevanten Eigenschaften klar verbessert. Preis: € 2.290,- zzgl. MwSt.

EMV-gerechte Planung der Elektroinstallation für Rechnerräume und Rechenzentren, 14.06. - 15.06.07 in Bonn
Dieses Seminar zeigt, wie eine EMV-gerechte, hochverfügbare und störungsarme Elektroinstallation mit gleichzeitig hoher Betriebssicherheit geschaffen werden kann. Es vermittelt mit engem Bezug zur Praxis wie ausgehend von Analyse und Messtechnik bestehende Mängel beseitigt werden und ein wartungsoptimierter Betrieb aufgebaut wird. Preis: € 1.390,- zzgl. MwSt.

Exchange 2007 - Upgrade lohnenswert oder sogar erforderlich?, 18.06. - 20.06.07 in Bonn
E-Mail ist heute für die meisten Unternehmen ein missionskritisches Kommunikationsmittel, welches für die Mitarbeiter zu jeder Zeit und unabhängig vom Aufenthaltsort erreichbar und uneingeschränkt nutzbar sein muss. Exchange 2007 adressiert diese Anforderungen durch neue und, im Vergleich zu seinen Vorgängern, verbesserte Technologien, so dass sich für Betreiber vorhergehender Exchange-Versionen die Frage aufwirft, ob sich ein Upgrade lohnt oder gar als erforderlich herausstellt. Preis: € 1.690,- zzgl. MwSt.

Trouble Shooting in konvergenten Netzwerken, 18.06. - 22.06.07 in Aachen
Dieses Seminar vermittelt das notwendige Hintergrundwissen über die typischen Fehler, erklärt ihre Erscheinungsformen im laufenden Betrieb und trainiert systematisch ihre Diagnose und Beseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainingsnetzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Preis: € 2.490,- zzgl. MwSt.

IP-Wissen für Voice-over-IP, 18.06. - 19.06.07 in Düsseldorf
Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das Sie zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen. Preis: € 1.390,- zzgl. MwSt.

IP-Telefonie: Vorbereitung, Migration, Management, 18.06. - 20.06.07 in Bonn
Der Referent dieses 3-tägigen Seminars vermittelt seine jahrelange Projekt-Erfahrung bei der Nutzung und des Betriebs von IP-Telefonie sowie bei der Durchführung hochkomplexer Projekte in diesem Umfeld. Preis: € 1.690,- zzgl. MwSt.

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit, 18.06. - 22.06.07 in Bonn
Bedrohungen der IT-Sicherheit bestehen für praktisch alle Elemente einer vernetzten IT-Infrastruktur. Die Quelle der Bedrohung kann sowohl von außen auf das Netz wirken als auch von innen stammen. Sicherheit entsteht erst, wenn alle signifikanten Gefahrenbereiche systematisch verriegelt werden. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Dabei wird jeder einzelne Baustein detailliert erklärt und anhand typischer Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt. Preis: € 2.290,- zzgl. MwSt.

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten, 25.06. - 29.06.07 in Berlin
Sicherheitskonzepte müssen mehr sein als Papier. Ihre erfolgreiche Umsetzung erfordert: eine umsichtige Planung und Beschaffung der Sicherheitsinfrastruktur, eine effektive Integration in Prozesse und Organisation, konzeptkonforme Einbindung externer Leistungen (Lieferung, Implementierung, Wartung und Betriebsleistungen). Bei der notwendigen Erfolgskontrolle helfen Standards wie BS7799, ISO 27001 und die IT-Grundschutz-Standards und -Kataloge des BSI. Eine entsprechende Zertifizierung des erreichten Sicherheitsniveaus ist möglich, aber auch eine Verwendung solcher Standards als internes Hilfsmittel. Preis: € 2.290,- zzgl. MwSt.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
25.06. - 29.06.07 in Aachen
15.10. - 19.10.07 in Aachen
03.12. - 07.12.07 in Aachen

Internetworking
17.09. - 21.09.07 in Aachen
10.12. - 14.12.07 in Aachen

TCP/IP und SNMP
15.10. - 19.10.07 in Berlin

Ethernet Netzwerke
10.09. - 12.09.07 in Aachen
26.11. - 28.11.07 in Aachen

Paketpreis für alle vier Seminare € 7.704.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--, Ethernet Netzwerke: € 1.690.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
11.06. - 15.06.07 in Aachen
03.09. - 07.09.07 in Aachen
12.11. - 16.11.07 in Aachen

Trouble Shooting in konvergenten Netzwerken
18.06. - 22.06.07 in Aachen
17.09. - 21.09.07 in Aachen
19.11. - 23.11.07 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
22.10. - 26.10.07 in Aachen

Paketpreis für alle drei Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 6.990.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
18.06. - 22.06.07 in Bonn
10.09. - 14.09.07 in Berlin

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheits-konzepten
25.06. - 29.06.07 in Berlin
15.10. - 19.10.07 in Aachen

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolg-reichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs
27.08. - 31.08.07 in Aachen
03.12. - 07.12.07 in Aachen

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolg-reichen Lösung“ und und „Sicherheit in Wireless LANs“.
€ 6.183.-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

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

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 3234415

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie