ComConsult Research

Der Netzwerk Insider

Juni 2009

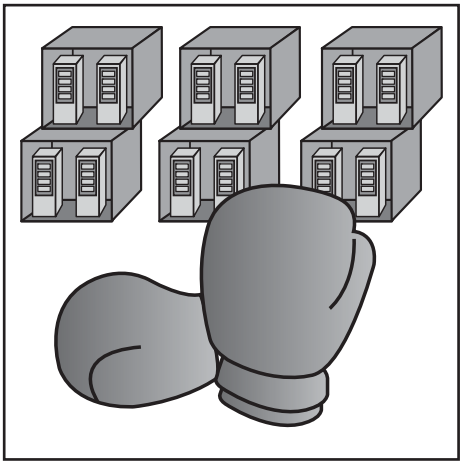
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Der Kampf ums RZ:
die nächste Runde - Teil 1

von Dr. Franz-Joachim Kauffels

I/O-Konsolidierung ist ein wesentliches Element bei der Restrukturierung von RZ-Netzen. Mittlerweile ist aber auch ins Bewusstsein gerückt, dass der Umgang mit Speichern ein wesentliches Element einer jeden Virtualisierungsstrategie ist. In 2008 gab es eigentlich nur einen Hersteller, der diesen Problembereich angesprochen hat. Auf dem Markt ist aber jetzt der Kampf ums Rechenzentrum entbrannt. Dabei spielen I/O-Konsolidierung und passende Netzkomponenten eine zentrale Rolle. FCoE erfährt eine breitere Unterstützung von den Herstellern, die IEEE DCB-Standardisierung ist vorangekommen und es gibt zu all dem tatsächlich noch weitere Alternativen. Noch nie war ein Bereich so extrem spannend.



Wegen der Komplexität der Thematik benötigen wir zwei Artikel. Im heutigen ersten Teil fassen wir die zugrundeliegende Motivation und das heftige bunte Treiben der Hersteller zusammen. Dann kommen wir zu einer Einführung in das DCB-Projekt von IEEE und erste wichtige Erweiterungen: DCBX und ETS. Im zweiten Teil geht es dann um die aktuellen Vorstellungen der Hersteller. Besonders die von HP angekündigte Blade System Matrix ist hier ein Meilenstein. Verblüffend und technologisch attraktiv ist aber auch die I/O-Konsolidierung mittels EoFC.

weiter auf Seite 18

Zweitthema

„Cloud Computing“
Dunkle Wolken über der IT-Sicherheit?

von Dr. Michael Wallbaum und Dr. Simon Hoff

Das Modewort „Cloud Computing“ wird derzeit inflationär eingesetzt - kaum ein Hersteller, der nicht vorgibt seine Lösungen seien in irgendeiner Weise „cloud-fähig“. Dennoch müssen Produkte und Dienstleistungen, die unter diesen Begriff fallen, spätestens seit der Ankündigung der Microsoft Online Services ernst genommen werden. Microsoft bietet seit etwa zwei Monaten verschiedene gehostete Varianten seiner Produkte Exchange, Sharepoint, Live Meeting und Office Communications Server an.

Microsoft selbst verwendet in diesem Zusammenhang nicht den „Cloud“-Begriff, obwohl er vermutlich angebracht wäre. Hier stellt sich die Frage was „Cloud Computing“ eigentlich bedeutet bzw. auszeichnet. Bevor der Versuch einer Begriffsbestimmung vorgenommen wird, soll eine Marktübersicht zeigen, welche Produkte die Anbieter unter dem Schlagwort „Cloud Computing“ anpreisen. Hierbei wird deutlich, dass der Markt ein äußerst breites Spektrum an Produkten bietet.

weiter auf Seite 11

Sommer-Highlights

IT-Sicherheits-Forum 2009

Sommerschule 2009

ab Seite 5

Geleit

Mythos Cloud-Computing

ab Seite 2

Early-Bird-Rabatt

Rechenzentrum Infrastruktur-Redesign Forum 2009

ab Seite 17

Zum Geleit

Mythos Cloud-Computing

Betrachtet man die amerikanische Presse und Anbieter wie Amazon, IBM, Google, Microsoft, Salesforce, SUN, Yahoo und Zoho, dann sind „Clouds“ die Zukunft der IT-Welt. Zitat aus dem Economist Oktober 2008: „It will undoubtedly transform the IT industry, but it it will also profoundly change the way people work and companies operate“.

Für die Befürworter der Technologie bilden die Mischung aus Grids und Virtualisierung in Kombination mit weiteren Webtechnologien und hoher Bandbreite im Zugang zur Cloud die Zutaten für ein Preis-Leistungs-Verhältnis, dem sich kein Kunde entziehen kann. Dies soll im folgenden in Kurzform analysiert und zum Teil auch in Frage gestellt werden.

Allgemein versteht man unter Cloud-Computing für ein Unternehmen die Nutzung der Leistungen externer Anbieter für sehr unterschiedliche Dienste, die alle unter diesen Begriff fallen:

- Reine Rechenleistung, zum Beispiel durch Verlagerung von lokalen virtuellen Maschinen oder durch Einbindung externer Grids, oder auch Bereitstellung virtueller Maschinen als „Platform as a Service“ PaaS, Beispiel XEN image oder „Elastic Compute Cloud“ EC2 von Amazon Web Services (siehe aws.amazon.com)

- Bereitstellung von Applikationen von „Software as a Service“ SaaS, Zum-Beispiel-Bereiche sind Email oder Kollaboration, typisch dafür sind Google Apps, Salesforce, WebEx Connect oder Zoho. Auch Microsoft Windows Live und LiveMeeting gehen in diese Richtung

- Bereitstellung einer Entwicklungsumgebung für Cloud-Applikationen, Beispiel ist Microsoft Azure

- Bereitstellung von Speicher oder Netzwerk-Ressourcen („Storage as a Service“, „Infrastructure as a Service“ IaaS), Beispiele sind „Simple Storage Service“ S3 von Amazon Web-Services oder Nirvanix Storage Delivery Network SDN

Schon diese Spannbreite macht klar, dass es keine allgemeingültige Aussage zur Nutzbarkeit von Cloud-Computing geben kann. In Bereichen wie der Kollaboration mit externen Partnern oder Kunden werden vermutlich die meisten Kunden zu einer SaaS-Lösung wie WebEx oder Mi-

crosoft LiveMeeting (oder Adobe, IBM, ...) tendieren. Umstritten ist der Bereich Email-as-a-Service, da hier auch Themen wie die Einbindung in weitergehende Workgroup-Anwendungen ins Spiel kommen. Trotzdem gehen durchaus wichtige Anbieter wie WebEx/Cisco in die Richtung, Exchange-kompatible Email-Dienste als SaaS anzubieten. Anbieter wie Zoho haben belegt, dass es auch Akzeptanz für derartige Dienste gibt.

Die Vorteile, die man sich davon verspricht, sind ebenfalls sehr verschieden:

- Senkung von Kapitaleinsatz im Unternehmen entweder durch Auslagerung kompletter Hardware-Bereiche oder durch externe Abdeckung von Überlastsituationen, allgemein Vermeidung von Überversorgung im Unternehmen

- Senkung der Kosten durch gemeinsame Nutzung von Hardware mit anderen Unternehmen und der damit verbundenen besseren Auslastung

- Senkung der Betriebskosten durch Ausnutzung eines höheren Grads an Automatisierung in der Cloud

- Umstieg auf eine Abrechnung nach Verbrauch anstatt der üblichen pauschalen Abrechnung (Übernahme der Grundidee des Utility Computing, einige Anbieter sprechen auch von der nächsten Generation des Utility Computing) . Da dies in vielen Unternehmen bisher intern nur schwer durchsetzbar war, kann der Umstieg auf einen externen Diensterbringer dies nun möglich machen

- Flexibilität in der Entwicklungsphase von insbesondere Web-basierten IT-Produkten

- Flexible Lastanpassung

- Umsetzung einer örtlich verteilten und hochgradig verfügbaren Desaster Recovery-Lösung

Möglich wird diese gesamte Entwicklung

Kongress

IT-Sicherheits-Forum 2009
22. - 25.06.09 in Königswinter

Das IT-Sicherheits-Forum wird auch in diesem Jahr wieder einen umfassenden Überblick zu aktuellen Themen der IT-Sicherheit in Theorie und Praxis anbieten. An insgesamt vier Tagen wird mit einführenden Tutorien, technischen Workshops und neutralen Fachvorträgen für jeden Interessierten etwas geboten. Dabei wird äußerst hoher Wert auf sofort verwendbare Informationen gelegt, die Teilnehmer sollen die gewonnenen Erkenntnisse möglichst sofort in der eigenen Umgebung anwenden können.

Moderation: Dr. Simon Hoff
Preis: € 2.290,- zzgl. MwSt.

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

erst durch die Verfügbarkeit einer Reihe von Technologien:

- Weitverkehrsnetze mit einer sehr hohen Bandbreite (bis in den Gigabit-Bereich hinein), so dass Delay-Zeiten deutlich verbessert werden können. Damit wird erst die Verbindung zwischen Unternehmen und externen Rechenzentren möglich. Auch für die Anbieter ist das wichtig, da diese auf dieser Basis verteilte Rechenzentren zur flächigen Abdeckung aufbauen können. Dies erklärt auch, warum Anbieter wie Cisco so begeistert von Cloud-Computing sind

- Grid-Computing auf der Seite der Anbieter, so dass diese die geforderte Leistung mit verteilten Systemen erbringen können, die kostengünstiger an den Lastbedarf adaptiert werden können

- Virtualisierung zum einen als Technologie der besseren Ressourcen-Auslastung, zum anderen als technische Basis zur Verlagerung von Applikationen zwischen Unternehmen und externen Anbietern. Speziell VMware und Cisco haben diese Zukunftsperspektive in den letzten Wochen betont (siehe auch vCloud von VMware)

- Applikationsentwicklung auf der Basis von Webtechnologien (Beispiel: Apache, MySQL, PHP, Perl, CSS, AJAX, Java)

- Geeignete Client-Technologien zur Umsetzung eines Browser-basierten Zugangs zu zentralen Applikationen unabhängig vom Standort

- Weiterentwicklung von Browser-Technologien in einer Form, dass Browser mehr als Laufzeitumgebung für Applikationen als zum einfachen Browsen genutzt werden können (stark verbesserte Leistung für JavaScript und AJAX), siehe Internet Explorer 8, Chrome 2.0, Safari 4.0

Genau diese Technologien zeigen sofort auch den Weg in die lange Liste der Probleme des Cloud-Computings auf:

- Viele Unternehmen sind gar nicht in der Situation, dass ihre bestehenden Applikationen in eine Cloud integriert werden können. Hier steht erst einmal ein Redesign der Applikationen und der bestehenden IT-Infrastruktur an

- Bei jedem Redesign ist erst einmal zu klären, was denn die beste technologische Basis für eine neue Applikations-Architektur ist. So einfach das auf den ersten Blick ist (hin zu Webbasierten n-tier-Architekturen), so kompliziert ist das im Detail (was ist denn die Zukunftssichere Applikations-Technologie, lighttpd, Hadoop, MogileFS? Zum Teil hoher Zusatzaufwand in der Entwicklung von Java-Anwendungen, Sicherheitsprobleme in Browsern beim Einsatz von Scripting und AJAX)

- Mit jedem Redesign wird man eigentlich auch den Anspruch der Senkung der Abhängigkeit von Herstellern und eine stark verbesserte Plattform-Neutralität verbinden. Dies ist aber genau bei den führenden Cloud-Anbietern gar nicht immer der Fall, die in der Regel sehr spezielle API´s oder auch spezielle Programmiersprachen erfordern

- Spätestens bei der externen Speicherung sensitiver Unternehmensdaten oder von Benutzer- und Kundendaten entstehen erhebliche Fragen zur Sicherheit dieser Daten und auch der rechtlichen Zulässigkeit. Je nach einzuhaltender Regulierung hat das Unternehmen den aktiven Nachweis zu erbringen, dass ein nichtautorisierter Zugang zu diesen Daten nicht möglich ist

- Management in gemischten Infrastrukturen, bei denen ein Teil der Leistung intern und ein Teil extern erbracht wird (so genannte hybride Clouds), wie sind da die Schnittstellen?

- Durch die Bindung an den externen Anbieter und insbesondere, wenn Spezialentwicklungen notwendig sind, kann der Kostenvorteil verloren gehen. Ein Beispiel ist die aktuelle Entwicklung im Bereich Prozessor-Technik und Virtualisierung. Die Kombination aus Intel Nehalem und VMware vSphere als Beispiel in Verbindung mit einer hohen Integration von Netzwerk und Speicher so wie sie Cisco, HP und IBM gerade angekündigt haben, kann die Kosten auf einen Schlag gegenüber einer 4 oder 5 Jahre alten Installation mehr als halbieren (gleiches gilt für die neuen Produkte von Citrix und Microsoft). Häufig wird die Einsparung gegenüber dem Invest von 2005 noch deutlich höher sein. Würde ein externer Cloud-Anbieter diese Einsparung wirklich in diesem Umfang weiter geben oder fährt hier das Unternehmen nicht besser, wenn es selber die Flexibilität in der Nutzung solcher neuen Technologien behält?

- Die Freiheit in der Technologiewahl wird begrenzt. Wer Microsoft Azure als Basis für seine Cloud wählt, der wird nun mal an die Microsoft-Technologie gebunden. Auch bei der Nutzung von Amazon, Google und anderen bestehen ähnliche Einschränkungen. Wer Cloud generell mit der Nutzung offener Standards gleichsetzt, der liegt falsch

- VMware und Cisco haben speziell den Aspekt der dynamischen Verlagerung von virtuellen Maschinen zu externen Anbietern von Rechenleistung betont. Tatsächlich scheint dies sehr weit hergeholt, wenn nicht völlig unrealistisch. Zum einen setzt das Wandern von VM´s bestimmte Eigenschaften (bestimmte Chipsätze) in der Basis-Hardware voraus (noch), zum anderen geht der Trend in der Virtualisierung hin zu Diskless VM´s. Dies bedeutet, dass im Extremfall der gesamte Speicher in einem SAN liegt und von dort auch gebootet wird. Dies erleichtert das interne Wandern von VM´s, bedeutet aber für ein Wandern hin zu externen Rechenzentren, dass ja dann von dort der SAN-Zugang erfolgen muss. Das ist ein wenig realistisches Szenario. Auch wenn Cisco Boss John Chambers sicher davon träumt, die dafür notwendigen Weitverkehrsverbindungen mit Cisco-Komponenten umzusetzen, wird der externe Zugang, selbst wenn er technisch in einigen Jahren machbar ist, immer auch ein höheres Delay mit sich bringen, das gerade für Datenbank-Anwendungen wenig hilfreich wäre

Tatsächlich ist gerade das Argument der mittel- und langfristigen Fragwürdigkeit der Kosteneinsparung je nach Anwendungsbereich sehr ernst zu nehmen. Zwar gibt es Ausnahmen wie den Bereich des Web-based Storage mit Produkten wie Amazon S3 oder Nirvanix SDN, aber diese Produkte sind auf einen bestimmten Typ von Anwendungen optimiert, bei dem zum Beispiel umfangreiche Multimedia-Informationen über das Internet zugänglich gemacht werden. So stellt sich die Frage, ob der Weg in Richtung Cloud-Computing wirklich so ein Hype ist, wie er allgemein gesehen wird.

Tatsache ist, dass Unternehmen gefordert sind, bestehende Software- und IT-Architekturen in Frage zu stellen und zu überdenken. Wer heute eine durchschnittliche Auslastung seiner Server von unter 20% hat, der sollte auch das Potenzial für Optimierungen sehen.

Was sind dann in diesem Zusammenhang die Alternativen zu Cloud-Computing?

- Zuerst einmal bleibt, wie schon einleitend angemerkt, festzuhalten, dass bestimmte Angebote von SaaS oder

Web-basierter Storage immer eine zu prüfende Option sind. Externe Kollaborations-Plattformen sind ein gutes Beispiel für zukunftsorientierte SaaS-Dienste

- Darüber hinaus gibt es eine Reihe von Sonder-Szenarien, in denen Cloud-Computing Sinn macht, seien es umfangreiche Video-Konvertierungen oder die Nutzung externer Server für Entwicklungsprojekte, ebenfalls ein Thema ist die Vermeidung von Lizenzkosten in einer Evaluierungsphase

- Dann bleibt für jedes Unternehmen ja auch die Option, ein internes Cloud-Computing umzusetzen. Da viele der Vorteile der externen Anbieter heute auch intern durch die neuen Virtualisierungs-Architekturen umgesetzt werden können, liegt hier ggf. der Mittelweg, viele der Vorteile zu erreichen und gleichzeitig die Nachteile zu vermeiden

Internes Cloud-Computing ist häufig ein irreführender Begriff. Tatsächlich ist er ein Synonym für die Weiterentwicklung der eigenen Architekturen durch Nutzung der neuesten Technologien. Im Kern steht dabei eine Server-Virtualisierung in Verbindung mit einer Konsolidierung von I/O- und Speicherzugang. Dies in Kombination mit der Integration des Managements von Server, Virtueller Infrastruktur und Speicher, so wie es gerade Cisco, HP und IBM angekündigt haben, führt zu einer völlig neuen Situation. Wir erreichen extrem hohe Packungsdichten von Blade-Servern in Verbindung mit einer hohen Zahl von VM´s pro Blade. VMware geht mit seinen neuen vSphere-Ankündigungen so weit, von 40 VM´s pro Blade zu sprechen. Möglich wird dies u.a. auch, weil die neuen Blade-Generationen neben mehr CPU-Leistung und mehr Threads auch deutlich mehr Hauptspeicher unterstützen. Gerade diese Intensivierung der Packungsdichte macht aber auch deutlich, dass eine Integration des I/O- und Speichersystems erforderlich ist. Zu hoch sind die Lasten, die hier zukünftig entstehen. Auch die Abhängigkeiten zwischen diesen Technologien werden so hoch, dass die Gesamtleistung aus einer Hand kommen muss. Wir haben in der Vergangenheit mehrfach unsere Zweifel an der Nutzbarkeit traditioneller I/O- und Netzwerklösungen an dieser Stelle geäußert. Cisco hat den Weg zu einer integrierten Architektur mit Unified Computing im April eingeläutet. HP und IBM haben umgehend nachgezogen.

Die neuen Technologie-Ansätze bieten für die Unternehmen so viel Potenzial, dass man wirklich die Frage stellen muss, welchen Mehrwert die externe Cloud realistisch noch erreichen kann. Verbrauchsabhängige Abrechnung wäre ein Vorteil und ist auch eine Voraussetzung für wirklich Service-orientierte Organisationen. Aber es ist nicht einzusehen, warum das nicht auch intern durchsetzbar sein sollte, wenn sich der Vorstand dahinter stellt.

Es gibt andere sehr ernst zu nehmende Gründe für eine interne Lösung. Viele Unternehmen werden zunehmend in den Zwiespalt der Frage kommen, mit welcher Technologie Applikationen standort-neutral zu mobilen Clients gebracht werden können. Bisher waren hier Webbasierte-Architekturen mit Browser-Frontends das Maß der Dinge. Die aktuellen Entwicklungen im Bereich Desktop- und Applikations-Virtualisierung stellen das klar in Frage (siehe Citrix Dazzle als Beispiel). Der Aufwand der Umstellung auf eine reine Webapplikation kann sehr hoch sein. Im Vergleich dazu kann der Aufwand des Umstiegs auf virtuelle Applikationen deutlich niedriger sein. Ohne hier eine allgemeingültige Antwort geben zu können, zeigt allein schon diese Diskussion, dass die Freiheit der Wahl der geeigneten Technologie für ein Unternehmen die höchste Priorität haben sollte. Der Einstieg in eine externe Cloud beschränkt diese Freiheit erheblich.

Damit kommen wir zum offensichtlichen Fazit. Cloud-Computing beinhaltet einige interessante Einzelaspekte speziell aus dem SaaS und PaaS-Bereich. Doch als generelle Basis-Architektur für die Zukunft der IT-Architektur von Unternehmen spricht auch einiges dagegen. Der Kunde muss für seinen Bedarf entscheiden, was der beste Weg ist.

Demgegenüber sind die internen Potenziale der neuen Technologien mehr als spannend. In den letzten 30 Jahren hat es keine Situation gegeben, in der Unternehmen so viel Ansatzpunkte für so umfassende Verbesserungen in ihrer IT-Architektur hatten.

In diesem Sinne
ein sehr optimistischer
Dr. Jürgen Suppan

ComConsult Research Ltd.
Christchurch

ComConsult IT-Sicherheits-Forum 2009

ComConsult IT-Sicherheits-Forum 2009

Die ComConsult Akademie veranstaltet vom 22.06. - 25.06.09 ihren Kongress „IT-Sicherheits-Forum 2009“ in Königswinter.

Das ComConsult Sicherheitsforum 2009 gibt einen umfassenden Überblick über den Stand moderner und erprobter Sicherheitstechnologien. Basierend auf den ermittelten Kernbereichen führen Top-Experten der Sicherheitstechnik von der Bedrohungslage zur praxiserprobten Umsetzung geeigneter Sicherheitslösungen.

Die Umsetzung von Sicherheits-Lösungen steht immer wieder und immer mehr vor folgenden Herausforderungen:

- Zunahme der Zentralisierung und Integration von Technologien
- Immer mehr verschiedene Technologien als Nutzer einer gemeinsamen Infrastruktur
- Zunahme der Abhängigkeiten und Wechselwirkungen zwischen Technologien

ComConsult Research hat deshalb exklusiv zum ComConsult Sicherheitsforum 2009 aktuelle Sicherheitsprojekte analysiert und die Schlüsseltechnologien herausgearbeitet, die angepackt werden müssen, um Sicherheit auch Technologieübergreifend realisieren zu können.

Dabei hat ComConsult Research die folgenden Bereiche als aktuell prägend für die erfolgreiche Umsetzung von Sicherheitsprojekten identifiziert:

- Virtualisierung und RZ-Redesign
- Netzwerk-Technologien
- Integration mobiler Geräte
- Voice und Unified Communications
- Webanwendungen
- Email
- Netzintegrierte Produktionsanlagen

Das ComConsult Sicherheitsforum 2009 geht intensiv auf diese Bereiche und deren zukünftige Entwicklung ein, analysiert die technischen Probleme und vergleicht die bestehenden Lösungsmöglichkeiten. Das Ganze wird in den Rahmen einer umfassenden Gesamtkonzeption gestellt, wobei auch die Frage der Prüffähigkeit der Lösung nach IT-Grundschutzhandbuch und ISO 27001 diskutiert wird.

Durch dieses Forum führt Sie Dr. Simon Hoff. Er ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
IT-Sicherheits-Forum 2009

Ich buche den Kongress
ComConsult IT-Sicherheits-Forum 2009

☐ **ohne Workshop**
22.06. - 24.06.09 in Königswinter
zum Preis von € 1.890,- zzgl. MwSt.

☐ **mit Workshop (bitte auswählen)**
22.06. - 25.06.09 in Königswinter
zum Preis von € 2.290,- zzgl. MwSt.

Workshopauswahl

vormittag	**nachmittag**
☐ 1	☐ 1a
☐ 2	☐ 2a
☐ 3	☐ 3a

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Programmübersicht ComConsult IT-Sicherheits-Forum 2009

Montag, 22.06.09

9:30 Uhr - 10:30 Uhr
Keynote: IT-Sicherheitsarchitektur unter Berücksichtigung aktueller Trends
- Aktuelle IT Trends und ihre Auswirkung auf die Informationssicherheit
  - Virtualisierung, Voice over IP und Unified Communications, Mobilität
- Bedrohungslage 2009: Unsichere Browser, unerwünschte Kommunikation, schadensstiftende Software
- Sichere Netze als Megatrend der nächsten Jahre: Authentisierung, Integrität und Verschlüsselung als Service im Netz

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

11:00 Uhr - 11:45 Uhr
Erfahrungen bei der Anwendung von IT-Grundschutz und ISO 27001
- Projektbeispiele zu folgenden Punkten: BSI-Grundschutz-Zertifizierung, BS27001-Zertifizierung, Sicherheitsanalysen und Konzepterarbeitungen auf Basis BSI-Standards 100-1 bis 100-3
- Wie eine Zertifizierung effizient vorzubereiten ist
- Was die Haupt-Knackpunkte sind
- Worauf Prüfer besonderen Wert legen
- Nicht nur saure Pflicht: die Vorbereitung hilft, sich gezielt zu verbessern
- Das Rad mehrfach erfinden oder Synergieeffekte - Sicherheitsaudits, Revision, branchenspezifische Auflagen, S-OX u.ä.
- Auch ohne Zertifizierung: die Grundschutz-Systematik als nützliches Hilfsmittel

Oliver Flüs, ComConsult Beratung und Planung GmbH

11:45 Uhr - 12:45 Uhr
Sicherheit in virtualisierten Umgebungen
- Herausforderung Virtualisierung: Betriebssystemsicherheit, Datenintegrität und Vertraulichkeit in virtualisierten Umgebungen
- Sicherheitskonzepte von Virtualisierungslösungen: die führenden Anbieter zur Servervirtualisierung im Vergleich
- „Virtuelle Sicherheit"? Was leisten Schnittstellen zum Virenschutz als Teil des Hypervisors?
- Vom einfachen Paketfilter bis zum Unified Threat Management: virtuelle Sicherheits-komponenten als virtuelle Maschine auf dem Host-System
- Virtuelle Sicherheitskomponenten: Integration in virtualisierte Umgebungen, Chancen und Risiken dieses Architekturwandels

Matthias Egerland, Comconsult Beratung und Planung GmbH

14:15 Uhr - 16:15 Uhr
Sicherheit der Virtualisierungslösungen im Vergleich
Referenten von den Herstellern von Virtualisierungslösungen mit anschließender Podiumsdiskussion

16:45 Uhr - 17:30 Uhr
Windows 7: Sicherheitsneuerungen
- Was ändert sich mit Windows 7?
- Gemeinsamkeiten mit Vista
- Werden die Probleme von Vista tatsächlich behoben?
- Breiterer 64-bit Support – auch von Drittherstellern (z.B. biometrische Authentisierung)
- BitLocker im neuen Gewand und BitLocker „To Go" für Wechseldatenträger
- Windows denkt mit: Action Center und automatische Erinnerung zur Sicherung von EFS Zertifikaten

Michael van Laak, Comconsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause
12:45 - 14:15 Uhr Mittagspause
16:15 - 16:45 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

Dienstag, 23.06.09

9:00 Uhr - 9:45 Uhr
IT-Sicherheit für netzintegrierte Produktionsanlagen
- Gefährdungen durch die Netzintegration von Produktionsanlagen
- Einsatz von Firewalltechniken und zugehörige Netzarchitekturen
- Absicherung auf Ebene der Endgeräte und der Netzelemente
- Sonderrolle von WLAN und anderen drahtlosen Kommunikationstechniken
- Einsatz und Grenzen von Security Scannern
- Verfügbarkeit kontra Sicherheit

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

9:45 Uhr - 10:30 Uhr
Sichere Netzarchitektur
- Was bedeutet die Virtualisierung für die Netzarchitektur?
- Wo gehören die Sicherheitsmechanismen hin: in die Applikationen, auf die Betriebssysteme oder ins Netz?
- Virtualisierte Netzarchitektur
- Folgen der Netzkonvergenz in Rechenzentren für die IT-Sicherheit
- Netztrennung kontra Policy-based Access Control: Was ist das bessere Konzept?
- Sind die Netze sicher genug für VoIP und Unified Communications?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 Uhr - 12:00 Uhr
Von der Geräteauthentisierung bis zu sicheren Netzen
- Tücken der dynamischen Zuordnung von Endgeräten in mandantenfähigen Netzen
- Grenzen der reinen Geräteauthentisierung
- MAC Security gemäß IEEE 802.1AE
- Ausblick auf die neue Version von IEEE 802.1X
- Pre-Standard-Lösungen und was gibt es neben Cisco TrustSec?
- Konsequenzen für den Aufbau von Sicherheitszonen

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

12:00 - 12:45 Uhr
Sicherheit in drahtlosen Kommunikationssystemen
- Das Ende von WPA und TKIP
- Wie man WLAN ordentlich absichert
- Bluetooth-Sicherheit
- Kompromittierung von DECT und die Konsequenzen
- Sicherheitsaspekte bei RFID und Lokalisierungssystemen
- Blick über den Tellerrand: ZigBee, NFC und Konsorten

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

14:00 Uhr - 14:45 Uhr
Herausforderung Mobilität und wie ihr zu begegnen ist
- Gefahren durch immer mehr Daten auf immer intelligenteren mobilen Geräten
- Sicherheitskonzepte im Vergleich: Blackberry, Windows Mobile, Symbian, ...
- Wie lassen sich mobile Geräte sicher managen?
- Neue Leitlinien des BSI im Mobilfunkbereich

Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH

14:45 Uhr - 15:30 Uhr
Gesetz über die Vorratsdatenspeicherung: Was müssen Unternehmen tun?
- Voice over IP Speicherpflichten- Bestandsdaten oder Verkehrsdaten?
- Speicherpflichten bei E-Mail-Postfächern
- Speicherpflichten bei WLAN-Zugängen
- Kostentragung der Speicherung

Ulrich Emmert, e/s/b Rechtsanwälte

16:00 Uhr - 17:00 Uhr
Sicherheit bei Voice und Unified Communications
- Muss Voice over IP verschlüsselt werden?
- Session Border Controller: warum eine neue Klasse von Systemen erforderlich ist
- Ist SPIT eine ernste Gefahr? Schutzkonzepte dagegen
- Gefahren durch Unified Communications
- Tauglichkeit von Skype für den Unternehmenseinsatz
- Neue Leitlinien des BSI im TK-Bereich

Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause
12:45 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause

Mittwoch, 24.06.09 - vormittag

9:00 Uhr - 9:45 Uhr
Unified Communications: Überwinden von Grenzen
- Firewall-Techniken und Unified Communications
- Beispiel Video-Konferenz: Lässt sich eine Kommunikation auch über Unternehmensgrenzen hinaus sicher gestalten?
- Sichere Einbindung von Heimarbeitsplätzen und externen Kommunikationspartnern

Michael Thissen, Tandberg

9:45 Uhr - 10:45 Uhr
Sicherheit bei Kommunikations- und Kollaborationslösungen von Microsoft
- Sicherheit beim Microsoft Office Communications Server 2007 R2
- Sicherheit beim Microsoft Office Sharepoint Server:
- Sicherheit und Zugriffsschutz bei der SharePoint Suche
- Benutzer-Berechtigungen im Portal und in Bibliotheken
- Überwachungsmöglichkeiten im SharePoint-Portal
- Sicherheit bei Microsofts Online Services

Markus Holländer, Lars Kuhl, ComConsult Beratung und Planung GmbH

11:15 Uhr - 12:00 Uhr
Fortschrittliche SQL Injection in Webanwendungen
- Bedrohungen durch SQL Injection
- Unterschiede Oracle & MySQL & SQLServer
- Grundlagen Oracle SQL Injection
- Neue Möglichkeiten (XML, Tabelleninhalte in Fehlermeldungen)
- Suche nach Daten (z.B. Kreditkarten) via reguläre Ausdrücke in SQL Injection
- Lesen von Dateien via SQL Injection
- Ausführen von Betriebssystemkommandos

Alexander Kornbrust, Red-Database-Security GmbH

10:45 - 11:15 Uhr Kaffeepause

Der Veranstalter behält sich Änderungen im Programm vor!

Programmübersicht ComConsult IT-Sicherheits-Forum 2009

Mittwoch, 24.06.09 - nachmittag

12:00 Uhr - 12:45 Uhr
Sicherheitsaspekte Dienst-orientierter Architekturen
- Von SOA über SaaS bis Cloud Computing: Konkurriende Konzepte oder Begriffsverwirrung?
- Unscheinbar und gefährlich im Hintergrund: XML, SOAP und AJAX
- Marktübersicht: Dienste im Netz
- Technische und rechtliche Grundlagen des Dienst-Outsourcings
- Sicherheit in Unternehmen zwischen Anspruch und Wirklichkeit
- Auswahlkriterien für sicheres Outsourcing

Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

14:00 Uhr - 14:45 Uhr
E-Mail-Sicherheit in großen heterogenen Umgebungen
- Problematik E-Mail-Sicherheit
- Zentrale Lösung: Gateway-Verschlüsselung
- Projekterfahrungen bei der Umsetzung von Praxis-Anforderungen
- Berücksichtigung heterogener IT-Umgebungen
- Unsichere WAN-Transferstrecken
- Einbeziehung der vorhandenen Betriebs-Ressourcen
- Testszenarien und Integration in den laufenden Betrieb
- Skizzierung der Lösungen, Realisierung

Dr. Torsten Johr, GAI NetConsult Gmb

14:45 Uhr - 15:30 Uhr
Zentralisierte E-Mail-Sicherheit durch Virtuelle Poststellen
- Anforderungen an sichere E-Mail und Probleme clientbasierter Lösungen
- Virtuelle Poststellen: Prinzip und Eigenschaften
- Integration Virtueller Poststellen in E-Mail-Architekturen
- Wesentliche Aspekte der Migration vorhandener Lösungen

Dipl.-Inform. Andreas Meder, ComConsult Beratung und Planung GmbH

12:45 - 14:00 Uhr Mittagspause
15:30 Uhr Kaffeepause

Donnerstag, den 25.06.09 - Praxis-Workshoptag (Optional) - Bitte kreuzen bei Wunsch jeweils einen Workshop an

vormittags 9:00 - 11:15 Uhr

1 Workshop 1: Sichere Netze

- Rogue device insertion, Identitätsübernahme, DHCP- und TCP-Angriffe: Welche Gefährdungen im LAN wirklich revant snd
- Unterschiede der Implementierung von IEEE 802.1X zwischen den Herstellern: Von Po-licy-based NAC bis zur simultanen Authentisierung mehrer Endgeräte an einem Port
- CDP/LLDP & Co.: ja oder nein?
- Sicherheitsmechanismen auf Ebene der Switches und Router: Dynamic ARP inspection, IP source guard, Unicast Reverse Path Forwarding und Routing Authentication
- Management-VRF: ja oder nein? Oder Outband Management?
- Mit Live-Beiträgen der Hersteller

Dr. Simon Hoff, Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

2 Workshop 2: Mehr Sicherheit durch virtuelle Firewalls?

Nahezu alle führenden Firewall-Hersteller bieten heutzutage eine virtualisierbare bzw. eine virtuelle Sicherheitskomponente an. Dabei unterscheiden sich die technischen Realisierungsansätze genauso stark wie das etablierbare Sicherheitsniveau. Gemeinsam mit den Herstellern wird in diesem Workshop diskutiert:

- Wie unterscheiden sich die Architekturmodelle zur Virtualisierung von Sicherheitskomponenten?
- Was leistet eine virtualisierte/virtuelle Sicherheitskomponente?
- Welche Vorteile ergeben sich aus der Virtualisierung?
- An welche Grenzen stößt die virtualisierte/virtuelle Sicherheitskomponente?
- Welche organisatorischen Abläufe müssen durch die Virtualisierung neu gestaltet wer-den?

Matthias Egerland, ComConsult Beratung und Planung GmbH

3 Workshop 3: Notfallmanagement im IT-Bereich

Mit kleinen Praxis- und Diskussionsbeispielen zu Notbetriebsformen, Notfall-relevanten Dokumenten und Rückführung auf Tagesgeschäft-Erfahrung; kommender BSI-Standard 100-4

- Flexibler Notfallprozess statt statischer Szenarienbewältigung
- IT ist komplex geworden - Prioritäten setzen und Notbetriebsformen planen
- Wichtige Notfall-relevante Dokumente - was müssen sie leisten
- Das Unerwartete erwarten - und vorbereitet sein
- Im Notfall ist alles anders - das kann nicht sein: Bewährtes aus dem Tagesgeschäft nutzen
- Ausblick und Diskussion: der neue BSI-Standard 100-4

Oliver Flüs, ComConsult Beratung und Planung GmbH

nachmittags 11:45 - 15:30 Uhr

1a Workshop 1a: Wireless Security

- WLAN-Absicherung mit IEEE 802.1X und EAP: Konfigurationsbeispiele und Traces
- Wie sicher ist WPA Personal?
- Das Ende von TKIP, wie gelingt die Migration nach AES reibungslos?
- Hotspot-Security
- WLAN Guest Access, die Hintertür ins Corporate LAN?
- Alte und neue Angriffe auf Bluetooth und wie man sich davor schützt
- Bluetooth und Windows 7: Was gibt es hier neues?

Dr. Joachim Wetzlar, Björn Korall, ComConsult Beratung und Planung GmbH

2a Workshop 2a: Sichere Oracle-Architekturen und sichere Anwendungsentwicklung

- Typische Architekturen (RAC, HA-Lösungen, Streams, Data Guard, ...) und deren Security Probleme
- Typische Anwendungsarchitektur und typische Security Probleme
- Test-, Staging und Produktionssysteme (Cloning, Verschlüsselung, ...)
- Verschlüsselung - Auf welcher Ebene soll/muss wie verschlüsselt werden (Applikation, Datenbank, Netzwerk, Betriebssystem)
- Typische Probleme bei der Software-Entwicklung mit Oracle
- Source-Code Review

Alexander Kornbrust, Red-Database-Security GmbH

3a Workshop 3a: Telekommunikationsüberwachung und Datenschutz

- Welche Mitarbeiterdaten dürfen aufgezeichnet werden?
- Wie dürfen Telekommunikations- und Mitarbeiterdaten genutzt und ausgewertet werden?
- Wie können oder müssen Handy- und Voice-over-IP-Daten aufgezeichnet und geschützt werden?
- Was ist bei Telekom und Bahn falsch gelaufen?

Ulrich Emmert, esb Rechtsanwälte

11:15 - 11:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 Uhr Ende der Veranstaltung

Sommer-Highlight 2009

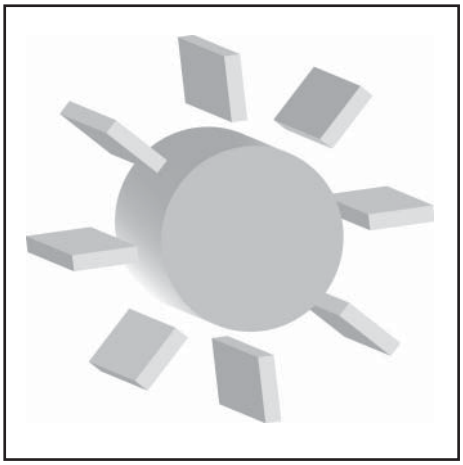
Sommerschule 2009

Intensiv-Update auf den letzten Stand der Netzwerktechnik

Die ComConsult Akademie veranstaltet vom 29.06. - 03.07.09 ihr diesjähriges Intensiv-Seminar „Sommerschule 2009“ in Köln.

Die Sommerschule gibt den kompakten und intensiven Überblick über die neuesten Entwicklungen im Umfeld der Netzwerk-Technologien und verteilter IT-Architekturen:

- Anforderungen an zukunftssichere Netzwerke: was ändert sich, wo gibt es neuen Bedarf? Was passiert speziell im Rechenzentrum; im Umfeld virtualisierter Server?
- Neue Technologien und Standards: welche neuen Netzwerk-Technologien gibt es? Wie werden bestehende Netzwerke durch neue Standards im Bereich Redundanz und Verfügbarkeit weiter entwickelt?
- Design-Verfahren im Vergleich: trotz zunehmender Standardisierung verfolgen die führenden Hersteller sehr unterschiedliche Design-Ansätze. Wie unterscheiden sich diese und für wen ist welches Design besser?
- IT-Sicherheit und Netzwerk-Sicherheit: wie sind die Grenzen? Was können Netzwerke leisten, um moderne IT-Lösungen besser zu machen?
- Ausgewählte Technologien in der Analyse: welche neuen Anwendungs-Technologien haben einen besonders großen Einfluss auf das zukünftige Design von Netzwerken und wie ist damit umzugehen?



Um diese Themenbereich zu bearbeiten, geht die Sommerschule in 5-Intensiv-Tagen unter anderem auf folgende Themen ein:

- Neue Ethernet-Technologien: 10/40/100 Gigabit Ethernet und was kommt danach?
- Neue Backbone und Corporate Network-Technologie: Carrier Ethernet in der Analyse, wie weit geht die Nutzbarkeit in normale Unternehmens-Netzwerke hinein?
- Virtualisierung im Rechenzentrum und die Auswirkung auf Netzwerke: wie hoch wird der Leistungsbedarf? Welche Bandbreite wird benötigt? Welche Redundanz-Verfahren kommen zum Einsatz? Wie weit müssen Netzwerke und Server aufeinander abgestimmt sein? Was bringen die neuen Produkte von 3Com, Brocade, Cisco, HP und den anderen Anbietern?
- Aktueller Stand der Verkabelungs-Technologie: welches Kabel und welcher Stecker nach welchem Standard? Was ist die passende Messtechnik?
- Wireless LANs: neueste Entwicklungen und Technologien: wie viel Bandbreite ist noch zu erwarten?
- Netzwerk-Design und ComConsult Design-Wettbewerb: führende Netzwerk-Hersteller haben sich dem direkten Vergleich auf der Basis eines Musterprojekts gestellt, die Ergebisse zeigen die unterschiedlichen Schwerpunkte der Anbieter
- Neue IEEE-Verfahren und ihre Relevanz
- Redundanz-Lösungen im Kern eines zukunftsorientierten Designs
- Sicherheits-Lösungen für Netzwerke und virtualisierte Umgebungen
- Verbesserungen von IEEE 802.1X: reicht das jetzt oder gibt es immer noch Mängel?
- Unified Communications: was muss das Netzwerk können? Welchen Stellenwert spielt Quality of Service? Wie weit muss der Planer die Eigenschaften von Codecs kennen? Cisco kontra Micorsoft: wer hat Recht mit seiner Sichtweise zur erforderlichen Netzwerk-Leistung?

Die Sommerschule wendet sich an Teilnehmer mit bestehenden Grundlagen-Kenntnissen und ist als Weiterbildung für berufserfahrene Netzwerker konzipiert.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Sommerschule 2009

Ich buche das Seminar
Sommerschule 2009

☐ 29.06. - 03.07.09 in Köln
zum Preis von € 2.290,- zzgl. MwSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 09
im NH Köln-City

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

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

Programmübersicht Sommerschule 2009

Montag, der 29.06.2009

09:30 - 13:00 Uhr
Neue Anforderungen und Technologien
- Anforderungs-Analyse: wo geht es hin?

Virtualisierung und I/O-Konsolidierung: Motivation, Konzepte, Konsequenzen
Dr. Franz-Jochaim Kauffels, unabhängiger Unternehmensberater

14:00 - 15:30 Uhr
Virtualisierung im Rechenzentrum und die Auswirkung auf Netzwerke
- Anbindung von Blade-Systemen mit und ohne I/O-Virtualisierung
- virtuelle Switches und virtuelle Koppelelemente: wieviele Netzwerkports werden wofür gebraucht?
- wie zeigt sich die Netztopologie in der Managementlösung?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

15:45 - 16:30 Uhr
10/40/100 Gigabit Ethernet
- Neue Ethernet-Technologien: 10/40/100 und ihre Nutzbarkeit

Dr. Franz-Jochaim Kauffels, unabhängiger Unternehmensberater

16:30 - 17:30 Uhr
Carrier Ethernet
- Carrier Ethernet: eine neue Technologie für Corporate Networks

Dr. Franz-Jochaim Kauffels, unabhängiger Unternehmensberater

Kaffeepause 10:45 - 11:00 Uhr | **Mittagspause 13:00 - 14:00 Uhr** | **Kaffeepause 15:30 - 15:45 Uhr** | **Happy Hour ab 18:00 Uhr**

Dienstag, der 30.06.2009 - Vom Kabel zum Wireless-Netzwerk

09:00 - 09:45 Uhr
Verkabelungstechnologie aktuell
Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

09:45 - 10:30 Uhr weiter 11:00 - 12:30 Uhr
Wireless-Technologien: Trends
Dr. Franz-Jochaim Kauffels, unabhängiger Unternehmensberater

13:30 - 14:15 Uhr
Neue Standards und Produkte in der Analyse
Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:15 - 15:00 Uhr
MESH in der Analyse und in der praktischen Messung
Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 - 17:00 Uhr
Planung und Überwachung von WLANs
Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Kaffeepause 10:30 - 11:00 Uhr | **Mittagspause 12:30 - 13:30 Uhr** | **Kaffeepause 15:00 - 15:30 Uhr**

Mittwoch, der 01.07.2009 - Netzwerk-Design

Beginn 09:00 Uhr
- Neue IEEE-Verfahren in der Analyse
- Redundanz-Lösungen im zukunftsorientierten Design
- Design-Aufgabe und Musterlösung aus der Sicht verschiedener Hersteller
- Ergebnisse des ComConsult Design-Wettbewerbs 2009

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

Kaffeepause 10:45 - 11:00 Uhr | **Mittagspause 12:30 - 13:30 Uhr** | **Kaffeepause 15:00 - 15:15 Uhr**

Donnerstag, der 02.07.2009

09:00 - 10:30 Uhr
Sicherheitskonzepte für Virtualisierungs-Lösungen
- die virtuelle DMZ: welcher Grad an Virtualisierung ist unter welchen Umständen vertretbar?
- die virtuelle Firewall: ihre Leistung, ihre Grenzen
- wie kann die Virtualisierungslösung selber gegen Angriffe geschützt werden?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

ab 10:45 Uhr
Sicherheit in Netzwerken
- SOA, Cloud-Computing und Sicherheit
- Absicherung von Unified Communications
- Aufbauprinzipien sicherer Netzwerke
- Grenzen von Firewalls und IPS-Systemen
- Authentifizierung am Netzzugang; wie reif ist 802.1X wirklich?
- Was bringen IEEE 802.1X-REV, IEEE 802.1AE und was gibt es außer TrustSec?
- Zertifikate und ihre Nutzung

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Kaffeepause 10:30 - 10:45 Uhr | **Mittagspause 12:45 - 13:45 Uhr** | **Kaffeepause 15:15 - 15:30 Uhr**

Freitag, der 03.07.2009

09:00 - 10:00 Uhr
Die Rolle der Standards: SIP und SIPConnect in der Analyse
- Leistungsumfang SIP: Pro und Kontra
- Marktbedeutung: wer nutzt es, wie wichtig ist es?
- SIP Trunking / Leistungsumfang SIPConnect
- Marktsituation: direkte Kommunikation zwischen Unternehmen in greifbarer Nähe?
- Microsoft OCS und SIP/SIPConnect: hält Microsoft den Standard ein? Wo sind Unterschiede zu Wettbewerbern?
- Trend-Analyse: Bedeutung der Signalisierung für zukunftssichere Entscheidungen

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

10:00 - 11:00 Uhr
Wo steht Cisco UC?
Wie groß ist die Bedrohung durch Microsoft?
- Strategische Grundsatz-Entscheidungen
- Leistungsumfang
- Cisco UC besser als TK plus OCS?
- Architekturen und Szenarien im Vergleich
- Investitions-Sicherheit: wer bietet mehr für die Zukunft?

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

ab 11:15 Uhr
Unified Communications im Netzwerk, Videokonferenztechnik
- Unified Communications und Kollaboration: was muss das Netzwerk können?
- Cisco kontra Microsoft: worin unterscheiden sich die Netzwerk-Anforderungen?
- Microsoft OCS und die Bedeutung für den UC-Markt
- Neuerungen der UC-Hersteller in der Übersicht
- Kosten unterschiedlicher Lösungen
- UC und Mobility-Lösungen: wo geht es hin?
- Videokonferenztechnik 2009: wohin geht der Weg?
- Videokonferenztechnik: Anforderungen an Bandbreiten und Qualität

Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH

Kaffeepause 11:00 - 11:15 Uhr | **Mittagspause 12:30 - 13:30 Uhr** | **Ende der Veranstaltung 14:30 Uhr**

Änderungen im Programm behält sich der Veranstalter vor!

Sonderveranstaltung

Ausschreibungen im Informations- und Kommunikationsbereich

Leitfaden für öffentliche Auftraggeber

Die ComConsult Akademie veranstaltet am 18.06.09 ihre Sonderveranstaltung „Ausschreibungen im Informations- und Kommunikationsbereich“ in Bonn.

Die laufenden Konjunkturprogramme beinhalten auch Investitionen der öffentlichen Hand im Bereich Informations- und Kommunikationstechnik (ITK). Viele öffentliche Auftraggeber müssen in der nächsten Zeit mehr als in der Vergangenheit Aufwand in Ausschreibungen im Bereich ITK investieren. Dabei haben die im April 2009 verabschiedeten Neuerungen des Vergaberechts die Komplexität von Ausschreibungen und den Aufwand dafür erhöht. Diese Neuerungen stellen öffentliche Auftraggeber, die Leistungen im Informations- und Kommunikationsbereich ausschreiben, vor neue Herausforderungen, zum Beispiel durch die nun verschärften Vorgaben hinsichtlich der Einteilung in Lose.

Die öffentliche Hand muss nun im hochkomplexen Bereich der Informations- und Kommunikationstechnologie oft unter großem Zeitdruck Vergabeverfahren durchführen. Hier ist interdisziplinäre Kompetenz dringend von Nöten. Um Risiken im Vergabeverfahren zu vermeiden, sind die öffentlichen Auftraggeber auf juristische Expertise angewiesen. Um die technischen Ziele

im IT- und Kommunikationsbereich (ITK) zu erreichen, brauchen die ausschreibenden Stellen erfahrene Planer, die jahrelange Ausschreibungspraxis mitbringen.

Unsere Sonderveranstaltung bietet genau diese kombinierte Expertise. Diese Veranstaltung ist als Leitfaden für öffentliche Auftraggeber gedacht, die in ihren ITK-Vergabeverfahren unter Einhaltung aller gesetzlichen Auflagen und Vermeidung aller rechtlichen Risiken für ihre Verwaltung das optimale Ausschreibungsergebnis erreichen wollen. Planer mit jahrzehntelanger Erfahrung bei Ausschreibungen der öffentlichen Hand vermitteln auf dieser Veranstaltung ihren Erfahrungsschatz. Das juristische Wissen wird von einem renommierten Rechtsanwalt mit dem Spezialgebiet Vergaberecht präsentiert. Somit richtet sich die Veranstaltung nicht ausschließlich an die Teilnehmer aus der öffentlichen Verwaltung, sondern auch an die Unternehmen, die gemäß dem öffentlichen Vergaberecht ihre Leistungen anbieten müssen. Auch die Unternehmen müssen wissen, mit welchen Verfahren sie bei ITK-Ausschreibungen der nächsten Zeit zu rechnen haben.

Diese Veranstaltung ist als Leitfaden für öffentliche Auftraggeber gedacht, die in ihren ITK-Vergabeverfahren unter Einhaltung aller gesetzlichen Auflagen und Vermeidung aller rechtlichen Risiken für ihre Verwaltung das optimale Ausschreibungsergebnis erreichen wollen. Planer mit jahrzehntelanger Erfahrung bei Ausschreibungen der öffentlichen Hand vermitteln auf dieser Veranstaltung ihren Erfahrungsschatz. Das juristische Wissen wird von einem renommierten Rechtsanwalt mit dem Spezialgebiet Vergaberecht präsentiert. Insofern ist der Besuch der Veranstaltung auch für Unternehmen vom Vorteil, die gemäß dem öffentlichen Vergaberecht ihre Leistungen anbieten müssen.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ausschreibungen im Informations- und Kommunikationsbereich

Ich buche das Seminar
Ausschreibungen im Informations- und Kommunikationsbereich
☐ 18.06.09 in Bonn
zum Preis von 790,- € zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer im Hilton Bonn

vom_____ bis_____09

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

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

Zweitthema

„Cloud Computing“

Dunkle Wolken über der IT-Sicherheit?

Fortsetzung von Seite 1

Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Wirtschaftlich betrachtet geht es in der Regel um ein Outsourcing von Diensten - technisch betrachtet findet meist ein Outsourcing von Rechenleistung und von Daten statt. Gerade die externe Datenhaltung ist dabei aus Unternehmenssicht überaus kritisch zu sehen. Der Schwerpunkt dieses Artikels ist daher die IT-Sicherheit im Kontext des Cloud Computing.

Marktübersicht - Wolkige Produkte

Im Folgenden wird ein Überblick über die verschiedenen Herstelleransätze bzw. deren neueste Entwicklungen gegeben und gezeigt, welche Produkte im Umfeld von Cloud Computing positioniert werden.

- Salesforce

  Das Customer Relationship Management (CRM) System Salesforce von force.com wird oft als der Urahn aller Software-as-a-Service (SaaS) Applikationen betrachtet. Salesforce ist ein gehostetes CRM-System, das über eine Web-Schnittstelle bedient wird. Dabei wurde als eines der ersten Web-basierten Enterprise-Produkte auf Web-Technologien gesetzt, die sonst nur bei Consumer-Produkten von Google, Yahoo, etc. zu finden waren. Die hieraus resultierende Benutzerfreundlichkeit, sowie das attraktive Preismodell haben zum Erfolg von Salesforce beigetragen. In der Enterprise Edition kostet ein Benutzer 125$ pro Monat.

- Microsoft Business Productivity Online Suite (BPOS)

  Microsoft verwendet für die im März in Deutschland gestarteten Online Services mit den Produkten Exchange, Sharepoint, Live Meeting und Office Communications Server sechs weltweit verteilte eigene Rechenzentren. Die europäischen Rechenzentren befinden sich in Dublin und Amsterdam (Backup). Alle Produkte zusammen kosten als BPOS Standard 12,78 EUR netto pro User und Monat bei einem Jahr Mindestlaufzeit und einem Monat Kündigungsfrist nach dem ersten Jahr. Neben BPOS positioniert Microsoft im Kontext von Cloud Computing auch die Windows Azure Plattform. Azure bietet im Prinzip eine von Microsoft gehostete Laufzeitumgebung für kundenseitig bereitgestellten .NET-Code.

- Zimbra

  Der Anbieter der Email- und Groupware-Lösung Zimbra stellt mit seiner Collaboration Suite eine SaaS-Lösung zur Verfügung, die nicht auf Zimbra-eigenen Servern gehostet wird, sondern auf Servern von Hosting-Partnern. Hier gibt also eine große Vielfalt, was die Speicherung und den Betriebsstandort der Daten betrifft. Je nach Anbieter werden dementsprechend auch unterschiedliche Preise verlangt und andere Features (Virenschutz, Speicherplatz, Verfügbarkeitsgarantie, etc.) angeboten. Der Kunde hat also die freie Auswahl, wem er seine Daten anvertraut und ist nicht auf die Server des Softwareherstellers angewiesen.

- Google

  Google will mit „Google Apps“ dem Konkurrenten Microsoft zumindest ein paar seiner Office Kunden abspenstig machen. Bei Apps handelt sich hierbei um eine Paket von gängiger Bürosoftware (Textverarbeitung, Email, Tabellenkalkulation, Präsentation, etc.) das der Kunde bei Google zusammen mit Speicherplatz auf den Servern des Suchriesen erwirbt. Noch ist der Funktionsumfang der angebotenen Produkte sehr überschaubar. Texte im Buchformat oder komplexe Tabellen mit Makros u.ä. sind mit Google Apps derzeit undenkbar. Es ist jedoch zu erwarten, dass sukzessive weitere Funktionen integriert werden und neue Anwendungen hinzukommen.

  Der Zugriff auf die Anwendungen und damit die Daten erfolgt mit einem beliebigen Webbrowser. Um das Gefühl einer nativen Applikation zu vermitteln, wird vorzugsweise mit Ajax-Konzepten

gearbeitet. Der Nutzer kann von überall auf der Welt auf seine Daten auf den Servern von Google zugreifen.

Die Preisstruktur ist hier denkbar einfach: Mit 40 EUR pro Benutzer und Jahr ist man dabei inkl. aller Applikationen und mehrerer Gigabyte Speicherplatz; Mengenrabatte gibt es nicht.

- WebEx

Eine weitere Lösung bietet WebEx. Hierbei handelt es sich um einen Dienst bzw. ein Netz, das es dem Kunden ermöglichen soll, Web-Konferenzen und Präsentationen professionell auszurichten. Das zum Cisco-Konzern gehörende Unternehmen liefert mit ihrem sogenannten MediaTone-Netzwerk die Infrastruktur für diese Zwecke. Der Kunde erwirbt lediglich eine Zugangsberechtigung und kann entsprechend seiner virtuell gebuchten Konferenzräume beispielsweise Präsentationen abhalten oder Schulungen durchführen ohne dabei in eigene Netzinfrastruktur investieren zu müssen. Es existieren unterschiedliche Preismodelle mit Minutenpaketen, an namentliche genannte Nutzer gebundene Pakete, Floating Lizenzen und Unternehmens-Flatrates. So zahlt ein Unternehmen mit 100 Mitarbeitern beispielsweise weniger als 20 EUR pro Nutzer und Monat.

- VMware

VMware hat mir vSphere (alias ESX 4.0 und vCenter 4) laut Eigenwerbung das erste Cloud-Betriebssystem veröffentlicht. (Vor wenigen Monaten nannte man das noch Virtualisierung.) Laut VMware ermöglicht vSphere ein dynamisches Management und dynamische Zuordnung von Ressourcen zu Anwendungen. So könne ein Konsolidierungsverhältnis von bis zu 15:1 erreicht werden.

Die Software besteht aus zwei zentralen Komponenten: Den Infrastruktur- und den Anwendungs-sServices. Alte und neue VMware-Funktionen sind entsprechend aufgeteilt worden. So beinhalten die Infrastruktur-Services beispielsweise die Basis der Virtualisierungslösung (ESX, ESXi, VMFS etc.), während erweiterte Funktionen, z.B. zur Erhöhung der Verfügbarkeit (vMotion, HA, Fault Tolerance) zu den Anwendungs-Services gezählt werden. Mit der InfrastrukturkomponenteDie zugrundeliegende Servervirtualisierung ermöglicht werden es, bisher getrennte Hardware-Ressourcen zu einer Gesamtstruktur zusammengefasstzusammenzufassen und diese als Plattform zu nutzen. DieseDie Leistungsreserven Ressourcen (Rechenleistung, Arbeitsspeicher) werden in logischen Pools zusammengefasst und Speicherplatz zentral verwaltet, um das Gesamtpotential möglichst effektiv zu verteilen. Anstelle einer statischen Zuweisung tritt eine dynamische Zuordnung von Ressourcen.Beim Plattenspeicherbedarf sollen so Einsparungen von bis zu 50% möglich sein.

Die Anwendungs-Sservices regeln die Service-Level (Verfügbarkeit, Sicherheit, Skalierbarkeit) für jede Anwendung einheitlich und an zentraler Stelle für die gesamte Cloud. Die Verfügbarkeitskontrolle soll beispielsweise bei Hardware-Ausfällen für eine Aufrechterhaltung des Betriebs sorgen. Neu ist an dieser Stelle beispielsweise die Funktion „Fault Tolerance“, wobei eine zweite virtuelle Maschine als Hot-Standby bereitsteht und ohne Unterbrechung die Aufgaben der ersten virtuellen Maschine übernehmen kann.

- Amazon

Nicht zuletzt wegen der „Amazon Elastic Compute Cloud (EC2)“ ist Cloud Computing zurzeit noch ein dehnbarer Begriff. Der Internet-Versandhändler trat als einer der Ersten auf den Plan und präsentierte unter dem Cloud-Begriff eine dynamisch anpassbare Server-Hosting-Lösung. Es wird der tatsächliche „Server-Verbrauch“ auf Stundenbasis abgerechnet, wobei keinerlei Mindestumsatz vorgeschrieben ist. Sollten beispielsweise für unbestimmte Zeit keine Ressourcen verbraucht werden, so fallen keinerlei Kosten an. Bei der Frage, ob eine Server-Instanz genutzt wird, spielt die tatsächliche Auslastung keine Rolle. Lediglich die Uptime wird als Berechnungsgrundlage herangezogen. Zu beachten wäre noch, dass ein- und ausgehender Datenverkehr nach Volumen (in Schritten von 1 GB) als weiterer Kostenfaktor zu Buche schlägt.

Der Kunde betreibt seine virtuellen Maschinen und kann diese entsprechend seinen Bedürfnissen hoch und herunterfahren und eigene Software installieren. Als vordefinierte Betriebssystemumgebungen stehen derzeit mehrere Linux-Distributionen sowie Windows 2003 Server zur Verfügung. Verschiedene Datenbanken und Anwendungsentwicklungsumgebungen sind ebenfalls nutzbar.

Man kann zwischen drei verschiedenen Server-Leistungsklassen wählen. Um eine einfachere Unterscheidbarkeit und Klassifizierung zu ermöglichen, hat Amazon die Einheit „EC2“ ins Leben gerufen. Ein „EC2 Unit“ besitzt ungefähr die Leistung eines 1.0-1.2GHz Opteron/Xeon Prozessors. So hat beispielsweise die Klasse „Small“ eine EC2 Compute Unit und „Large“ vier EC2 Compute Units. Für besonders rechenintensive Serveranforderungen bzw. Kundensoftware werden spezielle Pakete mit überproportional höherer CPU-Leistung angeboten.

„Cloud Computing“ - Dunkle Wolken über der IT-Sicherheit?

Versuch einer Begriffsbestimmung

Welches der genannten Produkte und Dienste verfolgt nun wirklich den Cloud Computing Gedanken? Was macht Cloud Computing aus? Und welche Zusammenhänge gibt es mit anderen Schlagwörtern wie Application Service Provider (ASP), Enterprise Application Integration (EAI), Software as a Service (SaaS), Utility Computing, Service-Oriented Architecture (SOA) usw.? Offensichtlich herrscht auch unter selbsternannten und anerkannten Fachleuten Konfusion. Eine Google-Suche mit den Stichwörtern „Cloud Computing“ und „SOA“ liefert unter den ersten Treffern sowohl einen Artikel mit dem Titel „SOA ist tot, es lebe Cloud Computing“ als auch Artikel die das Zusammenspiel zwischen SOA und Cloud Computing beschreiben. Was denn nun?

Im Folgenden werden die wesentlichen Begriffe kurz definiert und die vorgestellten Produkte entsprechend ihrer Ausrichtung eingeordnet:

- **Enterprise Application Integration (EAI):** Unter EAI wird die Integration von monolithischen Enterprise-Applikationen über einen sogenannten Business Bus, d.h. eine Integrationsplattform verstanden. Die funktionalen Schnittstellen der Applikationen werden dabei über entsprechende Adapter and den Business Bus angebunden, der im Gegensatz zu einer reinen Middleware eine Abstraktion auch auf Ebene einer Geschäftsprozesslogik gestattet. EAI kann daher durchaus als Vorläufer einer Service-Oriented Architecture (SOA) verstanden werden.

- **Application Service Provider (ASP):** Ein ASP übernimmt Hosting und Management von Enterprise-Applikationen in seinen Rechenzentren. Die Applikationen werden typischerweise für jeden Kunden einzeln in dedizierten Umgebungen aufgesetzt.

- **Service-Oriented Architecture (SOA):** Unter SOA wird ein Konzept für die Zerlegung von monolithischen Enterprise-Applikationen in kleine Dienste verstanden. In der Theorie können diese kleinen Dienstbausteine konsolidiert, neu verschaltet (auch über Unternehmensgrenzen hinweg) und outgesourced werden. In Reinform ist dieses Konzept aufgrund fehlender Standards derzeit schwer umsetzbar. Pakete mit grundlegenden Diensten werden u.a. von IBM, SAP, Siemens und Oracle angeboten.

- **Utility Computing:** Die Idee von Utility Computing ist die Bereitstellung von Rechenleistung und Speicherkapazitäten im Internet und ähnlich flexibel nutzbar zu machen, wie Strom und Gas. VmWare und andere Virtualisierungstechnologien stellen die Infrastruktur bereit. Der Kunde stellt seine virtuelle Maschine zusammen und lässt sie in der Cloud ablaufen. Ein Beispiel hierzu ist Amazon EC2.

- **Software as a Service (SaaS):** Der SaaS-Gedanke ähnelt dem ASP-Konzept. Während bei ASP der Kunde zumindest in der Theorie beliebige Applikationen beim Provider hosten kann, setzten SaaS-Provider tendenziell auf einzelne oft mandantenfähige Produkte. SaaS wird zudem eher mit Port-Preis-Modellen in Verbindung gesetzt, d.h. Dienste werden pro User bezahlt und Verträge haben eine deutlich kürzere Laufzeit bzw. Kündigungsfrist als ASP-Verträge. Schließlich werden mit SaaS häufig Web-Applikationen in Verbindung gesetzt. Beispiele sind Salesforce und Microsoft BPOS.

- **Cloud Computing:** Dies ist ein Oberbegriff für IT-Ressourcen (Rechenleistung, Speicherplatz und Software), die über das Internet bereitgestellt und abgerufen werden. Dieses Konzept umfasst somit auch SaaS, Utility Computing und ASP. Ein Beispiel ist das Angebot von Amazon.

Diese Darstellung stellt zunächst keinen offensichtlichen Zusammenhang zwischen den Begriffen EAI und SOA her. Jedoch spielen diese Konzepte auch im Kontext von Cloud Computing eine Rolle. SaaS-Anwendungen wie z.B. Salesforce können und müssen durch EAI-Verfahren mit selbst betriebenen Applikationen integriert werden. Langfristig könnte nach einer feingranularen Aufteilung der Dienste auch der (reine) SOA-Gedanke durch eine Verteilung der Software-Dienste auf die Internet-Wolke implementiert werden.

Wirtschaftlicher Druck

Es kann festgehalten werden, dass unter dem Begriff Cloud Computing eine Vielzahl von bekannten (aber nicht zwangsläufig erfolgreichen) Konzepten zusammengefasst werden. Einige Hersteller nutzen die Gunst der Stunde, um bereits vorhandene Produkte neu zu positionieren, andere bringen komplette Neuentwicklungen. Die immer weiter fortschreitende Ausstattung mit breitbandigen Internetzugangsmöglichkeiten (auch mobiler Endgeräte) könnte bei Anbietern und Nutzern von Software das Interesse und den Bedarf an ausgelagerten Servern und damit einhergehender flexibler Nutzung von Rechenleistung geweckt haben. Die technischen Bausteine für Cloud-Lösungen sind jedenfalls vorhanden. Es bleibt jedoch abzuwarten, welche Anwendungen wirklich Vorteile durch ein Outsourcing erfahren und bei welchen es sich eher hinderlich auf die Nutzbarkeit, Sicherheit und Verfügbarkeit auswirkt.

Die stattfindende Entwicklung kann von den IT-Abteilungen nicht länger ignoriert werden. Bislang werden Email und andere grundlegende Dienste vor allem im Mittelstand als notwendige und nahezu fixe Infrastruktur-Kosten betrachtet. Gas, Wasser, Strom, Email – aus Sicht des Managements sind das notwendige Übel.

Nun wächst der Druck auf die IT-Leiter Cent-genau nachzuweisen was den Unternehmen die Bereitstellung von zentralen Diensten kostet. Zudem wird erwartet, dass die Betriebskosten sich dynamisch an die Mitarbeiterzahlen anpassen. Im Zweifel bieten sich Microsoft, Google, 1&1 und andere Anbieter als kostengünstige und vor allem flexible Alternative. Mit wirtschaftlichen Argumenten hat man gegen eine jährlich kündbare Google-Apps-Flatrate für 40 EUR im Jahr inkl. Email und Office-Applikationen zunächst kaum eine Chance.

Sicherheitslücken

Vor allem unter dem Aspekt der Sicherheit wirft diese Variante des Outsourcings jedoch einige heikle Fragen auf. Ein fundamentales Problem des Cloud Computings liegt auf der Hand: Daten verlassen das Unternehmen. Dieser Schritt erfordert ein großes Vertrauen in den Dienstleister, selbst wenn davon ausgegangen werden kann, dass die Mitarbeiter des Dienstleisters darauf verzichten in den Kundendaten zu stöbern. Immer wieder kommt es zu Betriebsunfällen, wie z.B. im März diesen Jahres als unbefugte Nutzer auf Google Apps Dokumente eines holländischen Unternehmens zugreifen konnten und dies auch massenhaft ausgenutzt haben. Der Sicherheitslücke wurde übrigens durch den Kunden entdeckt und nicht durch Google.

Dies ist natürlich kein Einzelfall, auch wenn es derzeit eines der wenigen Beispiele im direkten Kontext von Cloud Computing darstellt. Grundsätzlich ist die Herausgabe von eigenen Daten an externe Unternehmen immer kritisch, auch wenn es sich oft nicht vermeiden lässt. Die folgende Liste ist ein wörtlicher Auszug einer vom MDR zusammengestellten Liste von „Datenskandalen“ der letzten Monate:

„Cloud Computing“ - Dunkle Wolken über der IT-Sicherheit?

- 2. April 2009 - Deutsche Telekom

  Die Deutsche Telekom hat dem Bundeskriminalamt (BKA) ohne Rechtsgrundlage Millionen von Kundendaten zur Verfügung gestellt. Einem Bericht der „Frankfurter Rundschau“ zufolge erfolgte die Datenweitergabe nach den Terroranschlägen vom 11. September 2001. Mit den Daten wollte das BKA nach sogenannten Schläfern suchen.

- 13. Dezember 2008 - Landesbank Berlin

  Bei der Landesbank Berlin (LBB) sind Kreditkartendaten von Zehntausenden Kunden verloren gegangen. Der „Frankfurter Rundschau“ wurden die Informationen anonym zugespielt. Die Mikrofilme listen genaue Kreditkartenabrechnungen mit Name, Adresse und Kontonummer auf. Außerdem hat die anonyme Post Briefe mit Geheimnummern (PIN) von Kreditkarten enthalten. Der Bank zufolge waren diese aber den Kunden noch nicht zugeschickt worden.

- 11. Oktober 2008 - Telekom

  „Spiegel“-Redakteure veröffentlichen, dass sie sich ohne großen Aufwand in das aktuelle Kundensystem von T-Mobile einloggen konnten. Es waren nur wenige Angaben zum Benutzer und ein einfaches Passwort notwendig. Besonders pikant: Die Daten konnten nicht nur gelesen, sondern auch geändert werden.

- 04. Oktober 2008 - Telekom

  Die deutsche Telekom bestätigt, dass ihrer Mobilfunk-Sparte T-Mobile vor gut zwei Jahren mehr als 17 Millionen Daten gestohlen worden waren, d.h. von nahezu jedem zweiten Kunden. Neben Telefonnummern wurden auch alle Adressen kopiert. Die Telekom wird auch deshalb scharf kritisiert, weil sie von dem Datendiebstahl gewusst hatte, ihre Kunden aber nicht informierte.

- 28. August 2008 - kommunale Melderegister

  Die „tageszeitung“ berichtet, dass acht Unternehmen illegal mit Angaben aus kommunalen Melderegistern aus Schleswig-Holstein gehandelt haben sollen.

- 18. August 2008 - Handel mit Millionen Datensätzen

  Dem Bundesverband der Verbraucherzentralen werden sechs Millionen Datensätze angeboten, davon vier Millionen mit Kontonummern.

  In Kiel taucht eine CD mit 130.000 Kundendaten auf, von denen 70.000 Bankverbindungen enthalten.

  Ein Callcenter in Bremerhaven gerät unter Verdacht, illegal Kundendaten der Telekom zu verkaufen.

- 23. Juni 2008 - Meldeämter

  Daten von einer halben Million Einwohner aus verschiedenen Bundesländern konnten über Jahre hinweg im Internet eingesehen werden. Das berichtete das ARD-Magazin „Report München“. Eine Softwarefirma bestätigt die „Panne“, korrigiert aber das Ausmaß. Es seien nur 15, nicht 200 Kommunen betroffen.

Diese Beispiele enthalten Fälle von eindeutigem Datenmissbrauch. Kundendaten zu verkaufen oder weiterzugeben ist ein schwerer Vertrauensbruch. Dennoch gilt es in gewisser Weise als paranoid diese Möglichkeit offen in Erwägung zu ziehen. Aber man muss nicht gleich an das Schlechte im Menschen glauben - Dummheit und Fahrlässigkeit sind menschliche Eigenschaften, die seltener bestritten werden. Mit Fahrlässigkeit beim Dienstleister sollte man daher jederzeit rechnen. Dies zeigt ein aktuelles Beispiel aus Großbritannien.

Die Air Force hat hohe Offiziere Befragungen unterzogen, die der Untersuchung einer möglichen Erpressbarkeit der mit Sicherheitsfragen betrauten Militärs dienen sollten. In den Interviews wurden Fragen nach außerehelichen Beziehungen, Kontakt zu Prostituierten, Spielsucht, Schulden, Drogenmissbrauch und anderen intimen Themen gestellt. Die digitalisierten Mitschnitte der Interviews wurden auf drei nicht verschlüsselten Festplatten gespeichert und dem IT-Dienstleister der Air Force, der Firma EDS, einer Tochter von HP, übergeben. Diese drei Festplatten sind laut einem Bericht der BBC vom 25.05.2009 nun nicht mehr aufzufinden.

Solche Risiken sind gegenüber den erwähnten wirtschaftlichen Vorteilen des Cloud Computings abzuwägen. Immerhin kann man sich auf den Standpunkt stellen, das fahrlässiges Verhalten auch den eigenen Mitarbeitern unterlaufen kann. Unabhängig von der Motivation: Wer grundsätzlich bereit ist dieses Risiko einzugehen, muss sich u.a. folgende Fragen stellen:

- Wer hat Zugriff auf die Daten?
- Wo werden die Daten tatsächlich gespeichert? Wo liegen Backups?
- Welche Möglichkeiten werden zur Absicherung der Daten vor unberechtigtem Zugriff angeboten?
- Werden alle rechtlichen Vorgaben denen der Kunde in seinem Heimatland unterliegt erfüllt?
- Verfügt der Anbieter über Prozesse, die bei der Entdeckung und Aufklärung illegaler Aktivitäten unterstützen?

- Verfügt der Anbieter über Zertifizierungen? Werden regelmäßig Audits durchgeführt?

- Welche Service Level werden geboten? Wie lange dauert es z.B. im Notfall Daten wieder herzustellen und verfügbar zu machen?

- Welche Prozesse existieren für den Fall, dass der Vertrag aufgelöst wird? In welcher Form werden z.B. die Daten ausgehändigt?

Beispielsweise ist das Thema der Standorte der Rechenzentren durchaus nicht unkritisch. schon allein weil sich manche Regierung unter dem Deckmantel der Terrorbekämpfung weitgehende Zugriffsrechte auf Daten aller Art sichern möchte. Die britische Regierung ist hierbei tonangebend. Zwar ist der letzte Versuch gescheitert eine zentrale Datenbank aufzubauen, in der alle Informationen, die von den Telefon- und Internetprovidern im Rahmen der Telekommunikations-Vorratsdatenspeicherung für 12 Monate gesammelt werden müssen, zusammengeführt werden. Statt der zentralen Datenbank soll nun aber gewissermaßen die dezentrale Vorratsdatenspeicherung durch die Provider ausgebaut werden. Hierbei handelt es sich zunächst nur um Verbindungsdaten, aber man kann vermuten, dass die französische Regierung sich etwas dabei gedacht, als sie den Einsatz von Blackberrys in französischen Ministerien untersagte. Emails und andere Daten mit einem Blackberry als Ziel laufen durchweg über wenige Rechenzentren von Research in Motion. Eines davon steht in Großbritannien.

Technische Umsetzung

Wer seine Daten einem Dienstleister in der Cloud anvertraut, der sollte auch bei der Kommunikation mit dessen Servern stets auf höchste Sicherheit und Vertraulichkeit achten. Doch wann findet Datenaustausch mit den Servern in der Cloud überhaupt statt? Zudem muss auch die technische Umsetzung unter dem Aspekt der IT-Sicherheit kritisch betrachtet werden, da mit „Cloud Computing“ eine Reihe von Technologien vermarktet werden (z.B. Ajax), die nicht über jeden Zweifel erhaben sind.

Bei Ajax handelt es sich um ein Konzept, das es Web-Seiten ermöglicht im Hintergrund Daten nachzuladen und so dem Benutzer den Eindruck vermittelt, er arbeite (im Falle von Web-Anwendungen) mit einer lokalen Anwendung. Zum Beispiel präsentiert Google die meisten seiner Dienste mit Ajax Features – eine Webbasierte Textanwendung wäre ohne Ajax undenkbar, da sonst nach jedem Tastendruck die komplette Seite nachgeladen werden müsste. (Einzig Adobe Flash bietet sich als Alternative.)

Um Anfragen an fremde Server zu unterbinden, implementieren die Webbrowser die sogenannte Same Origin Policy (SOP). Mit dieser Sicherheitsrichtlinie wird verhindert, dass eine Webseite von einer bestimmten Domain Zugriffe auf einen Server aus einer völlig anderen Domain startet oder ein anderes Protokoll benutzt wird. Da es für den Anwender auf den ersten Blick nicht ersichtlich ist, welche Inhalte im Hintergrund dynamisch nachgeladen werden ist eine solche Einschränkung zwingend notwendig. Sollte der Inhalt auf dem Web-Server, dem der Anwender vertraut, allerdings mit Schadcode bereits kompromittiert sein, schützt auch die beste SOP nicht. Dann fließen ungewollt Informationen unbemerkt hin und her.

Verfälschte Inhalte auf Webservern sind seit einigen Jahren zunehmend ein Problem. Mit dem sogenannten „Cross Site Scripting“ (XSS) injizieren Angreifer Schadcode in eine Webseite die dann von den nachfolgenden, ahnungslosen Besuchern heruntergeladen wird. So sieht der normale Anwender wie gewohnt die Seite mit den vertrauten/erwarteten Inhalten, nur wird diesmal im Hintergrund der Angreifer aktiv. Sollte es gelingen dem User verfälschte Seiten unterzuschieben, steht dem Datenspionage Tür und Tor offen. Dann werden mal eben Tastatureingaben protokolliert oder Cookies von der Festplatte eingesammelt.

Natürlich ist dies kein typisches Cloud-Computing-Problem. Aber im Zweifel sind die Unternehmensdaten, die ein Manager in „seine“ vertraute Cloud-Applikation eingibt bzw. auf seinem Firmenrechner bearbeitet, um ein vielfaches interessanter als die Urlaubsfotos auf dem Heim-PC.

Wie wahrscheinlich ist es, dass Schadcode auf den Cloud-Server gelangt? Diese Frage ist nicht ganz leicht zu beantworten. Je nach Sicherheitsstandard des Serverbetreibers ist die eine Antwort. Je nach Einfallsreichtum der Angreifer die andere. Sollte eine Sicherheitslücke in einer auf dem Server laufenden Software auftauchen, wird diese mit großer Wahrscheinlichkeit früher oder später ausgenutzt (sofern sie denn bekannt wird). Aber auch vermeintlich sichere Server werden immer wieder durch den Einfallsreichtum von Angreifern überlistet.

Die Sicherheit ist also ein Thema sowohl auf den Servern als auch in den Browsern (siehe Abbildung 1). In beiden Fällen sollten die verantwortlichen Administratoren stets aktuelle Sicherheits-Patches einspielen und die Benutzer entsprechend sensibilisieren. Eventuell darf auch nur ein bestimmter Browser eingesetzt werden, weil für die Alternative noch keine Sicherheits-Updates vorliegen.

Bei einem Angriff auf einen Server der nicht in der eigenen Sicherheitsdomäne liegt, dürfte es dagegen schwerfal-

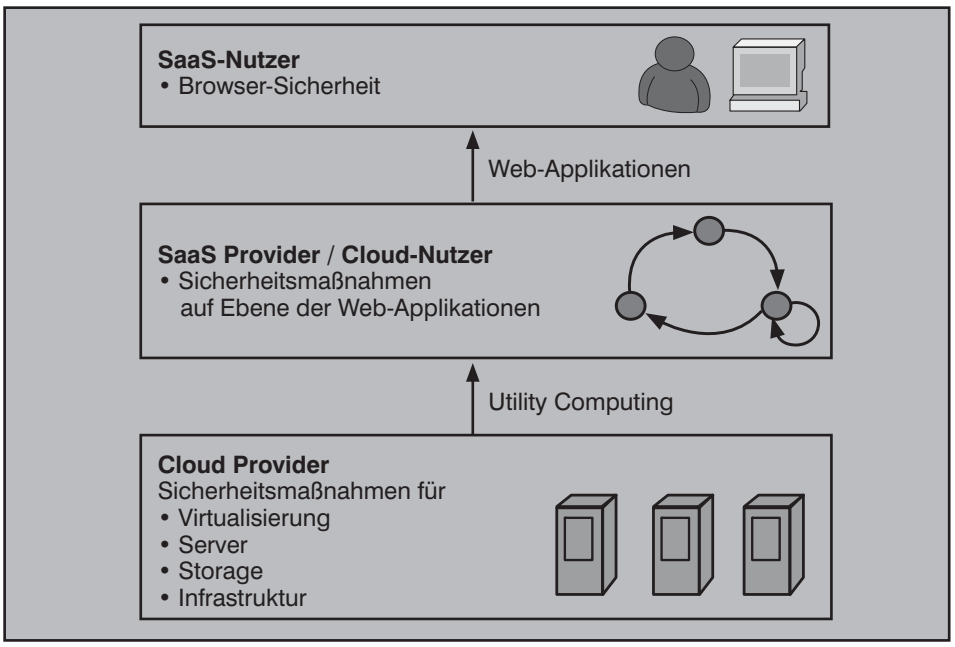


Abbildung 1: Elemente der Absicherung von Cloud Computing

len Gegenmaßnahmen zu ergreifen. Die Schwierigkeit wird schon darin liegen, einen Angriff auf den Service Provider überhaupt zu entdecken. Die Beispiele der „Datenskandale“ zeigen, dass solche geschäftsschädigenden Vorfälle gerne unter der Decke gehalten werden.

Fazit: Konsequenzen des Outsourcing-Trends

Mit dem Trend zu Cloud Computing und anderen Formen des Outsourcings verliert IT-Sicherheit ihren physischen Bezug. Wenn Datei-Server, Email-Server und andere vormals essentielle Hardware-Komponenten nun bei Dienstleistern stehen, was bleibt dann noch übrig? Konsequent zu Ende gedacht bleiben den Unternehmen lediglich ihre Daten und diese Einsicht stellt gängige Konzepte der IT-Sicherheit grundlegend in Frage.

Nun könnte argumentiert werden, dass es doch genügend technische Möglichkeiten gäbe, die Daten in der Cloud durch eine Verschlüsselung zu schützen. Für den Transport der Daten über das Internet in die Cloud hinein trifft dies beispielsweise mit TLS grundsätzlich zu (sofern die Tücken der zertifikatsbasierten Authentisierung berücksichtigt werden). Wenn die Daten jedoch z.B. per Ajax von einer Web-Applikation verarbeitet werden, sind die Grenzen der Verschlüsselung schnell erreicht. Aus einer Endnutzerperspektive ist also zunächst die Frage an den Dienstanbieter zu stellen, welche Elemente einer Anwendung überhaupt innerhalb der Cloud verschlüsselt werden können und welche Verschlüsselungsendpunkte bei der Verarbeitung der Daten in der Cloud bestehen. Hier ist durchaus auch zu klären, an welchen Stellen der Nutzer überhaupt die Kontrolle über das verwendete Schlüsselmaterial hat. Wenn Unternehmensdaten - auch nur temporär - in der Cloud unverschlüsselt vorliegen, muss im Einzelfall das bestehende Restrisiko betrachtet werden. Dabei geht es nicht nur um die technische Sicherheit beispielsweise der zugrundeliegenden Virtualisierungsplattform sondern auch um die Sorgfalt der beteiligten Anbieter.

Damit liegt automatisch der eigentliche Knackpunkt weniger in der Technik, sondern in Überprüfbarkeit und Auditierbarkeit von vertraglich vereinbarten Sicherheitsmechanismen und Sorgfaltspflichten. Dies ist oft schon in bewährten Bereichen des Outsourcings schwierig. Cloud Computing fügt jedoch noch eine Abstraktionsschicht hinzu und an einer in der Cloud ablaufenden Web-basierten Anwendung können mehrere Parteien beteiligt sein, was die Gefahr von Vertragslücken und juristischen Grauzonen nach sich ziehen kann.

Abkürzungen

Ajax	Asynchronous JavaScript and XML
ASP	Application Service Provider
BPOS	Business Productivity Online Suite
CRM	Customer Relationship Management
EAI	Enterprise Application Integration
SaaS	Software as a Service
SOA	Service-Oriented Architecture
SOP	Same Origin Policy
TLS	Transport Layer Security
XSS	Cross Site Scripting

Top-Kongress im Herbst

Early-Bird-Phase bis zum 30.06.2009

Rechenzentrum Infrastruktur-Redesign Forum 2009 16.11. - 18.11.09 in Königswinter

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Bereich bieten wir in diesem Jahr exklusiv eine Early-Bird-Phase für das „Rechenzentrum Infrastruktur-Redesign Forum 2009“ bis zum 30.06.2009 für eine rabattierte Teilnahmegebühr an.

Rechenzentrum Infrastruktur-Redesign Forum 2009
zum Early-Bird-Preis bei Buchung bis 30.06.09 von € 1.590,-
statt regulär € 1.890,- zzg. MwSt.

Rechenzentrum Infrastruktur-Redesign Forum 2009
zum Frühbucher-Preis bei Buchung bis 31.07.09 von € 1.690,-
statt regulär € 1.890,- zzg. MwSt.

Die Buchung innerhalb der rabattierten Phasen ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Rechenzentrum Infrastruktur-Redesign Forum 2009

Ich buche den Kongress
Rechenzentrum Infrastruktur-Redesign Forum 2009

☐ 16.11. - 18.11.09 in Königswinter
Early-Bird-Preis € 1.590,-* zzgl. MwSt.
*gültig bis 30.06.09

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis _____ 09
im Maritim Hotel

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

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

Schwerpunktthema

Der Kampf ums RZ: die nächste Runde -

Teil 1

Fortsetzung von Seite 1

Dr. Franz-Joachim Kauffels ist einer der erfahrensten und bekanntesten Referenten der gesamten Netzwerkszene (über 20 Fachbücher und unzählige Artikel) und bekannt für lebendige und mitreißende Seminare.

1. Einführung und Motivation

Corporate Networks stehen immer wieder vor neuen Herausforderungen. Ein wesentlicher Bereich ist die in Rechenzentren stattfindende Virtualisierung, die zum einen de facto die gewohnte Abteilungsrechnerebene völlig verschwinden lässt und zum anderen dabei natürlich die gewohnten Datenströme massiv ändert. In der Virtualisierung liegen aber derart massive Chancen und Optimierungspotenziale, dass sie neben der schon seit längerem statt findenden Rezentralisierung in jedem Falle schon jetzt ein nicht umkehrbarer Trend ist.

Auf verschiedene dieser Entwicklungen hat der durchschnittliche Netzbetreiber keinen Einfluss. Es wird vielmehr erwartet, dass das Netz immer stabil und performant zur Verfügung steht und letztlich die Leistung der virtualisierten Maschinen an jeden gewünschten festen oder mobilen Arbeitsplatz bringt. Natürlich unter Gewährleistung höchstmöglicher Sicherheit und Reaktionsgeschwindigkeit.

Angesichts all dieser Anforderungen stellt sich natürlich die bohrende Frage, ob die heute aufgebauten Netze auch in Zukunft in der Lage sind, diese Aufgaben zu bewältigen. Die Ethernet-Technologie geht in immer höhere Geschwindigkeitsbereiche, nach 10 GbE werden jetzt auch 40 und 100 GbE erschlossen. Über einen Server-Anschluss mit weniger als 10 GbE brauchen wir nicht mehr zu diskutieren.

Aber: ist es damit wirklich getan ? Auch ein 10, 40 oder 100 GbE Standard ändert nichts an den allseits bekannten strukturellen Schwächen des Ethernet.

Die letzten 12 – 15 Monate haben sowohl von der Seite der Standardisierung als auch im Rahmen von Herstellerinitiativen eine fast unüberschaubare Reihe von neuen Technologien und Verfahren hervorgebracht, deren Ziel letztlich eine völlige oder teilweise Renovierung der bisherigen Netzwerkstrukturierung ist. Optimierungen für das RZ unter den Stichworten CEE, DCE oder DCB haben durchaus das Potenzial zu einer erheblichen Komplexitäts- und Kostensenkung.

Im Jahr 2008 kam das Thema, vor allem konkretisiert an der Problematik der Abbildung des Fibre Channel-orientierten Speicherverkehrs vermöge des Verfahrens FCoE zum ersten Mal auf. Es gab dazu in dieser Publikation eine Reihe von technisch tiefgreifenden Darstellungen:

- Diskussion im Speichermarkt: Fibre Channel over Ethernet vs. iSCSI (Ausgabe Juni 2008, Dr. Moayeri)
- Lossless Ethernet mit 10GbE als Basis für FCoE und RZ-Optimierung (Ausgabe Juni 2008, Dr. Kauffels)
- Die neuen Gigabit Ethernet Standards: 10 GBASE-LRM und 40/100 GbE (Ausgabe Oktober 2008, Dr. Kauffels)
- DCE, CEE, FcoE, iSCSI: zum Dritten (Ausgabe Dezember 2008, Dr. Kauffels)

Den Stand im März 2009 kann man wie folgt zusammenfassen:

- Im Zusammenhang mit den Virtualisierungskonzepten ist die Integration von RZ-LAN und SAN an und für sich eine gute Idee
- Zwischen den Konzepten iSCSI und FCoE gibt es keine wirkliche Substitutionskonkurrenz, weil grob iSCSI den unteren und FCoE den oberen Leistungsbereich abdeckt.
- Die CEE/DCE/DCB-Konzepte benötigen wenigstens 10 GbE
- Ob nun mit oder ohne Koordinierung durch IEEE-DCB: selbst sorgfältig aufeinandergestapelt, haben die Verfahren KEIN DETERMINISTISCHES VERHALTEN. Es kann also nach wie vor zu Paketverlusten kommen. Das ist Gift für FCoE. Das zugrundeliegende Problem wurde NICHT richtig gelöst.
- Vor allem die Priotity-based Flow Control ist hochgradiger Kokolores.
- Dennoch kann man in kleinen übersichtlichen Umgebungen (z.B. ein Host, ein Switch, ein Speichersystem) damit arbeiten, und zwar, wenn man massiv Überkapazität spendiert, also z.B. eine 4 Gbps FC-Verbindung auf 10 GbE abbildet. Verwendet man statt der relationalen Bandbreitereservierung, wie sie in 802.1p/Q definiert ist, eine tatsächliche Bandbreitereservierung, wie sie durchaus realisierbar und auch in anderen Standards zu finden ist, kann man sogar noch ein wenig anderen Verkehr draufmischen.
- Der einzige Hersteller, der sich bisher ernsthaft in diesem Bereich engagiert, ist Cisco. Alle anderen befragten Hersteller lehnen sich erstmal zurück und warten ab, was passiert. Das drücken sie natürlich in anderen Worten aus.

Nur drei Monate später hat sich diese Situation dramatisch geändert. Was ist passiert ? Mit seiner Ankündigung, demnächst auch Server anbieten zu wollen, hat Cisco den gesamten Markt aufgemischt.

Es geht dabei weniger um Netze, als vielmehr um Gesamtlösungen für das RZ. Hersteller bemühen sich, Kunden dadurch zu binden, dass sie ihnen das kom-

plette Spektrum aus Servern, Netzen und Speicherlösungen, die man für eine virtualisierte Umgebung benötigt, aus einer Hand anbieten. Das hat für einen Kunden den entscheidenden Vorteil, dass er auch einheitliche Instrumente für das Management dieses neu entstandenen Gebildes bekommt.

Das ist nur logisch. Der Marktführer für Virtualisierungssoftware, VMware, hat mit vSphere das Modell einer lokalen Cloud geschaffen. Das besteht eben aus Servern, Speichern und Netzen und wird dann grob gesagt wie ein einzelner großer Rechner verwaltet. Anwendungen laufen auf den im Rahmen des Systems bereitgestellten virtuellen Maschinen und kommunizieren vornehmlich nicht mit IPC, sondern über virtuelle Switches. Und damit passiert eines:

Das Netz wird zum Systembus!

Das zieht natürlich unmittelbar nach sich, dass sich seine Aufgaben ändern, vor allem hinsichtlich des Speicherverkehrs. Bislang hat man oft den Speicherverkehr aufgrund seiner hohen Anforderungen auf ein eigenes Netz gelegt (das FC-SAN) und das „normale“ RZ-Kernnetz hatte die Aufgabe, die I/O zu implementieren, was vergleichsweise harmlos war. (siehe Abbildung 1)

IBM hat als erster reagiert. Nach vielen Jahren gibt es wieder Netzwerkkomponenten von IBM. Sie sehen zwar auf den ersten Blick harmlos aus, werden aber von Brocade geliefert. Brocade hat wesentlich mehr Möglichkeiten, darauf kommen wir später zu sprechen. IBM kann also eher im Zeitraum von Tagen als Wochen auf neue Anforderungen reagieren. So kann der Kunde also jetzt bei IBM Server, Speicher, Netzwerkkomponenten und Steuerungssoftware dafür aus einer Hand kaufen. Wir können die Qualität dieser Lösung hier nicht bewerten, darauf kommt es ja auch gar nicht so sehr an, es gibt bestimmt Kunden, die mit IBM gut gefahren sind und das auch weiter vorhaben. Außerdem kommt es ja immer darauf an, was ein Kunde am Ende mit seinem RZ machen möchte, und da sind reine Leistungsdaten eher zweitrangig.

Die nächste Reaktion kam von HP mit der Blade System Matrix. Hier kann man eigentlich zum ersten Male wirklich bildlich sehen, wie die Systeme im RZ der Zukunft aussehen könnten. HP sieht auf der Rack-Ebene zwei Arten von Netzen vor, ein klassisches SAN und ein angereichertes Ethernet. HP hat mit ProCurve bereits ein sehr großes Angebot an Netzkomponenten, arbeitet aber teilweise auch mit Brocade zusammen. Wir kommen auf die Blade System Matrix noch zurück. HP hat heute über 50% Marktanteil im Blade Server Segment. Auch HP bietet also dem Interessenten eine zusammenhängende Lösung aus Servern, Speichern und Netzkomponenten an.

IBM und HP haben zusammen ca. 75 bis 80% Marktanteil. Es wird problematisch sein, das zu ändern. Cisco steht hier auf dünnem Eis, eine Schlüsselposition wird die Haltung der Speicherhersteller haben. Die kann sich sozusagen täglich ändern. So war es bis zum 21. Mai 2009 so, dass man davon ausgehen konnte, dass Cisco und EMC sehr eng zusammenarbeiten. An diesem Termin aber haben HP und EMC eine enge Kooperation angekündigt, die vor allem die Herausforderungen durch die Virtualisierung betreffen. Bleibt jetzt nur noch NetApp als Speicher-Partner für Cisco?

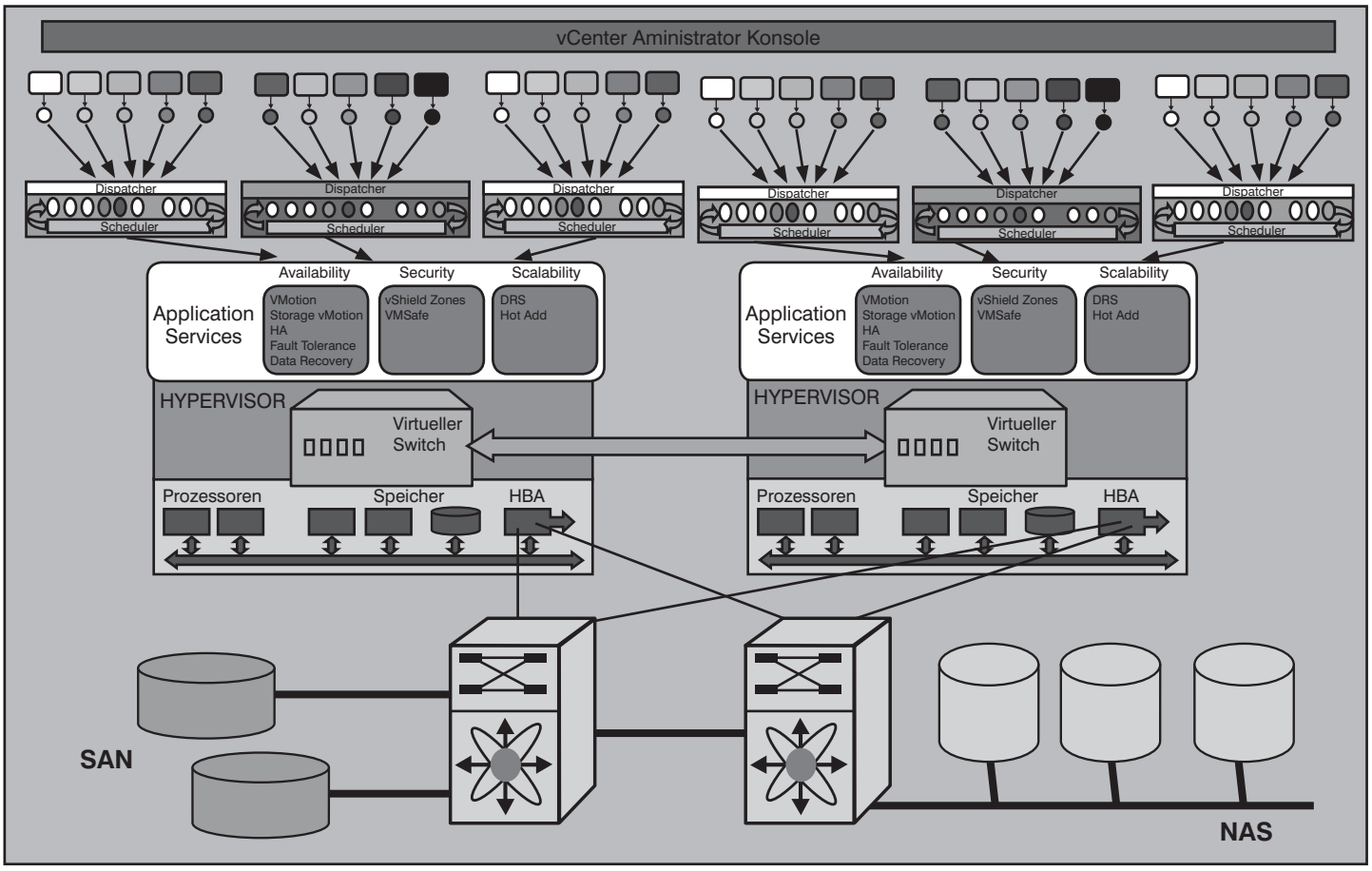


Abbildung 1: vSphere

Der Kampf ums RZ: die nächste Runde - Teil 1

Das werden wir hier nicht klären können, ich rechne aber weiterhin mit erheblichen Verwerfungen. Konzentrieren wir uns also auf die technische Perspektive.

Hier bewegen uns eine Reihe von Fragen, in deren Zentrum FCoE steht.

- IEEE 802.1 hat mit dem Projekt Data Center Bridging DCB einen Versuch gestartet, die veschiedenen funktionalen Standards, die in diesem Umfeld eine Rolle spielen, zusammenzufassen. Als erstes Ergebnis kam man denn darauf, dass die auch von uns geäußerten Bedenken, vor allem hinsichtlich der Realisierung eines verlustfreien Verkehrs („Lossless“ Ethernet), mehr als berechtigt waren. Was bedeutet also DCB für uns?

- Mitte 2009 gibt es eine Reihe von Vorschlägen, die DCB in die gewünschte Richtung bewegen sollen. Was hat es damit auf sich und wie können diese Vorschläge zur Lösung beitragen?

- SNIA und FCIA (Storage Networking Industry Association und Fibre Channel Industry Association) treiben FCoE im Rahmen von Interoperabilitätstests weiter voran. An diesen Tests beteiligen sich viele wichtige Hersteller. SNIA und FCIA haben in diesem Fall eine ähnliche Rolle wie WiFi für WLANs: Systeme nach Standard würden nicht zusammenarbeiten, wenn die Standards nicht durch Interoperabilitätsspezifikationen ergänzt würden.

- Brocade hat als erster Hersteller eine durchgängige FCoE-Lösung mit HBAs und entsprechenden Switches vorgestellt, es sieht also aus, als könne man es zum Laufen bringen. Folgen jetzt weitere Hersteller?

- HP hat mit Flex-10 ein System auf Blade-Switch-Ebene vorgestellt, welches eine echte Bandbreitenverteilung auf 10 GbE-Links implementiert. Zum Verständnis: die bisher von IEEE verfolgte Bandbreitenverteilung durch Priorisierung ist immer relativ, garantiert aber eigentlich nichts wirklich. Eine echte Bandbreitenverteilung sorgt dafür, dass Datenströme immer ein Fenster aus garantierter minimaler und normalerweise möglicher Bandbreite bekommen. Das ist in Provider-Netzen längst Standard, im normalen Ethernet-Universum nicht. Ist die HP-Lösung wegweisend?

- Als sei dies alles nicht genug, setzt Brocade noch einen oben drauf: EoFC !! Der Fibre Channel hat sich in den letzten Jahren ebenfalls erheblich fortentwickelt. Diese Entwicklung steht in engem Zusammenhang mit den Fortschritten bei der Integration Optischer Transceiverkomponenten, wenngleich es auch FC-Varianten über Kupfer gibt. Brocade hat mit dem DCX-Backbone eine neue Dimension des FC erreicht. Nun packt man das Ganze anders herum an: nicht Ethernet, sondern FC soll zum Kern eines konvergierten Netzes werden. Ethernet-Datenströme werden via EoFC (Ethernet over Fibre Channel) auf FC abgebildet, was übrigens recht einfach ist, weil FC rein abstrakt gesehen das wesentlich überlegene Netz ist und durch die Brocade 8000-Systeme am „Rand“ eines FC-Kernnetzes erledigt werden kann. Wir kennen die Preise noch nicht, aber wenn Brocade sich mit dem 10 GbFC dem 10 GbE annähert, ist das für bestimmte Umgebungen eine außerordentlich attraktive Alternative. Brocade ist ja Partner von HP und IBM. Beide Hersteller könnten das aufgreifen. Wie ist das insgesamt zu bewerten?

Diesen Fragen möchte ich in den zwei Artikeln nachgehen. Es gibt natürlich noch viele weitere Fragen, diese betreffen das Verhalten der anderen Hersteller. Da gibt es nämlich auch noch genügend mögliche Stifter erneuter Unruhe, wenngleich sie mangels eigener Server und Speicher nicht unmittelbar in den Hauptkampf um das RZ eingreifen können:

- BLADE ist ein Hersteller im Besitz einer Investorengruppe. Es gibt unabhängige Tests, in denen Switches der Firma BLADE (übrigens: das sind keine Blade-Switches) bestimmte vergleichbare Geräte von Cisco in jedem Belang schlagen.

- 3COM hat sich zurückgemeldet und leidet im Markt immer noch daran, dass viele sich an den unrühmlichen Rückzug dieses Herstellers vom Switch-Geschäft vor einigen Jahren erinnern. Dumm war eigentlich nur, dass sie den Namen behalten haben, das 3COM von 2009 hat mit der alten Firma nichts mehr gemein. Durch Fertigung in China könnten sie zum „ACER“ der Netzwerkwelt werden. Sie haben Mitte 2009 schon Nortel vom dritten Platz bei den Portauslieferungen verdängt. Gleichzeitig wurde eine neue umfassende Strategie für Corporate Networks vorgelegt, die auch FCoE umfasst. Sie werden vor allem im Preis punkten können.

- VOLTAIRE ist ein uns zunächst unbekannterer Hersteller, der aber für andere wie HP Blade-Switch Module herstellt. Sie sind mit einem 10 GbE-Switch neu in den Markt eingetreten. Interessant ist vor allem, dass sie sich als einer der wenigen, wenn nicht einziger Hersteller um die Integration von Infiniband kümmern.

- NORTEL NETWORKS bereitet ungeachtet seines Konkursverfahrens eine neue Strategie für Corporate- und RZ-Netze vor, in deren Mittelpunkt vor allem eine Vereinfachung und Reduktion der Menge der einzusetzenden Protokolle steht. Man kann schon ein bisschen davon sehen, wenn man auf die Carrier Ethernet-

Der Kampf ums RZ: die nächste Runde - Teil 1

Strategie dieses Herstellers blickt. Ggf. werden wir diese Produkte unter dem Namen eines neuen Besitzers des betreffenden Nortel-Bereiches sehen.

In dieser Liste nicht genannte Hersteller wie JUNIPER oder ENTERASYS sind momentan noch nicht aufgefallen, was aber nichts heißt. Vermissen Sie FOUNDRY? Die wurden von BROADE übernommen.

2. IEEE 802 Data Center Bridges DCB

In Darstellungen von Herstellern oder anderen Dritten zur Konsolidierungsproblematik werden teilweise unsystematisch verschiedene Standardisierungsaktivitäten referenziert. IEEE 802 hat die Problematik relativ spät erkannt. Es wurde klar, dass man für die Erzielung einer Lösung, besonders für „Lossles Ethernet“ eine Reihe von Standards gemeinsam anwenden muss.

Das hat aber wiederum einen Haken. Ein Standard auf der hier interessierenden Ebene enthält normalerweise einen endlichen Automaten. Dieser Automat ist eine Art abstrakte universelle und über Jahrzehnte bewährte Übergangssprache für die Implementierung. Der Automat besteht i.W. aus Zuständen. Dann kann man genau festlegen, unter welcher Eingabe er einen Zustand wechselt und welche Ausgabe dabei vorgenommen wird. Es gibt praktisch keine Möglichkeit, das bei einer Implementierung falsch auszulegen. Jede programmiersprachliche oder gar objekt-orientierte Beschreibung ist schwammiger.

Etwas schwierig wird es aber dann, wenn man sozusagen die Funktion mehrerer Standards gleichermaßen ausführen muss. Normalerweise muss man die entsprechenden Automaten dann zusammenlegen. Das ist aber nicht so einfach, weil dadurch viele Abhängigkeiten entstehen, die man alle berücksichtigen muss. Vergisst man eine oder mehrere dieser Abhängigkeiten, funktioniert das Endresultat nicht so wie es soll.

IEEE 802.1 Data Center Bridging DCB ist ein Projekt, welches verschiedene zur Thematik passende Standards unter einen Hut bringen soll:

→ 802.1 p/Q Traffic Forwarding
→ 802.3 x PAUSE
→ 802.1 Qau Congestion Notification
→ 802.1 Qaz Enhanced Transmission Selection
→ 802.1 ar Priority-based Flow Control

Die Arbeitsweise der verschiedenen Verfahren muss in einem gemeinsamen Modell koordiniert werden, denn sonst behindern sie sich gegenseitig. In diesen Zusammenhang gehören auch noch andere Standards, wie z.B. 802.1 Qay Provider Backbone Bridging - Trafic Engineering.

Die Sichtweise des IEEE 802.1 für die Topologie eines Data Centers kommt uns recht bekannt vor, siehe dazu ohne weitere Erläuterungen Abbildung 2.

IEEE 802.1 DCB formuliert die Herausforderungen an eine Lösung wie folgt:

Die Standard-Systeme Ethernet und Infiniband (IB) ersetzen proprietäre Lösungen. Dazu werden Verbesserungen benötigt:

→ Geringe Latenz
→ Differenzierung nach Verkehrsarten in der SW-Fabric
  → LAN-Traffic
  → SAN-Traffic
  → IPC-Traffic
→ Deterministisches Verhalten für IPC
→ Lossless für SAN
→ Multi-Path

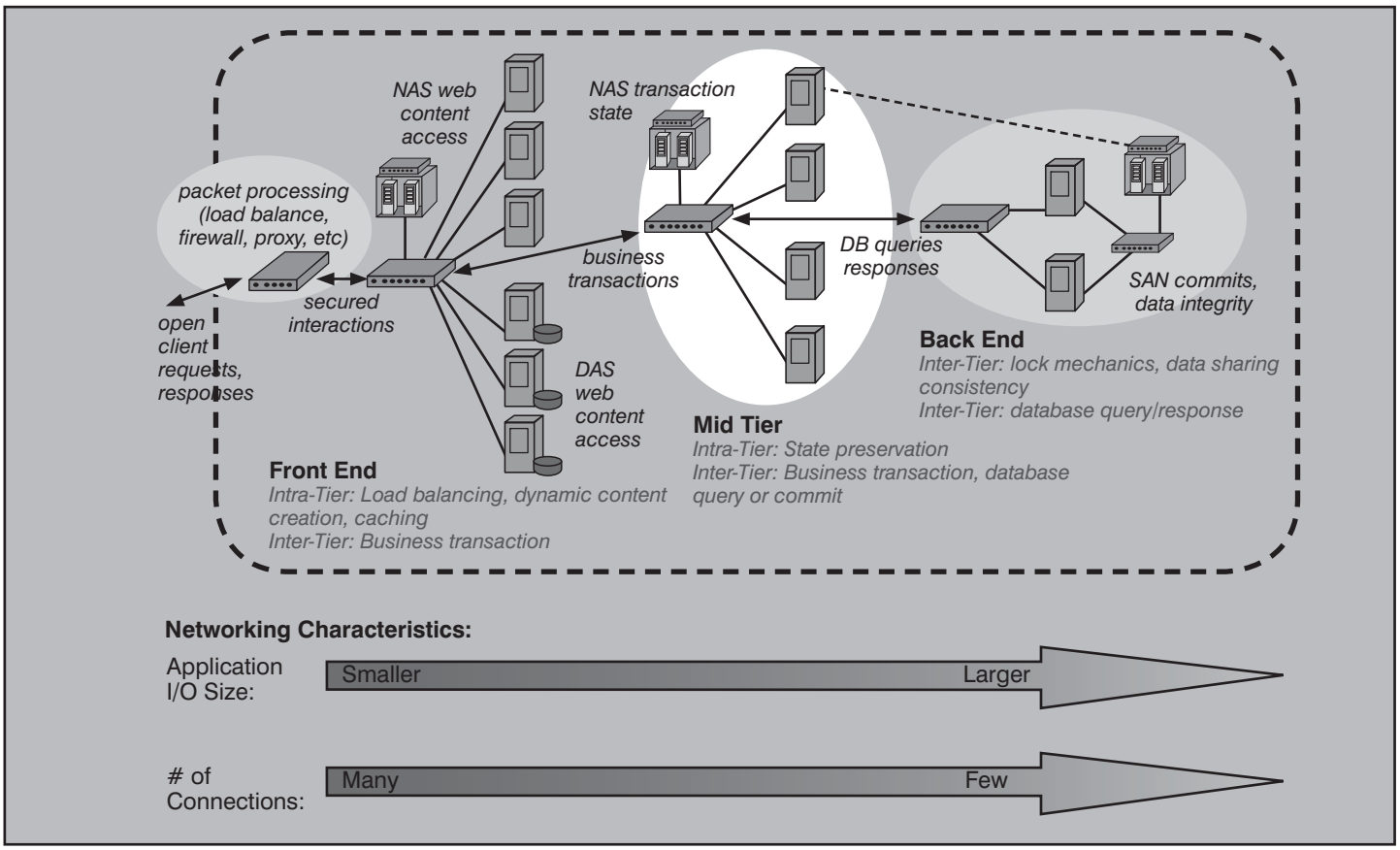


Abbildung 2: Data Center Topologie Sichtweise IEEE

Quelle: IEEE

Der Kampf ums RZ: die nächste Runde - Teil 1

Alternativen für Storage sind FCoE und iSCSI. FCoE benötigt lossless, iSCSI freut sich über bessere Leistung, lossless nicht notwendig, aber sehr hilfreich.

Data Center Bridging liefert Erweiterungen für die Bedarfe des Rechenzentrums

→ Storage
→ IPC
→ Blade Server usw.

Die Erweiterungen sind anwendbar auf Brücken (jeder Switch ist eine Multiport-Brücke :-)) oder Endgeräte. Der Markt verlangt eine konvergierte Fabric, deshalb erweitert DCB Ethernet so, dass es eine konvergierte Fabric realisieren kann. Der Sichtbereich von DCB ist auf das RZ beschränkt. Die erweiterte Perspektive liegt z.B. bei PBB / Carrier Ethernet.

Besonders interessant ist, dass IEEE 802.1 DCB im Vorfeld klare Aussagen zu Mängeln der bisherigen Standards macht, die unsere eigenen bisherigen Untersuchungen bestätigen, aber teilweise noch erheblich übertreffen. Das sehen wir uns einmal genauer an.

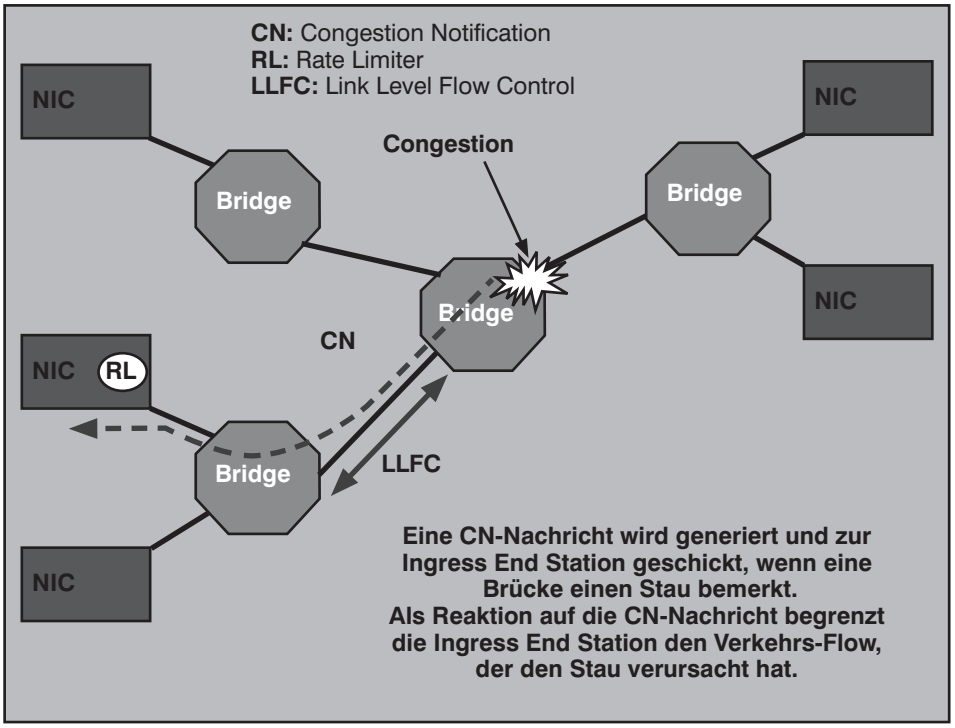


Abbildung 3: Lossless Transport mit 802.1 Qau und 802.3x Quelle:IEEE

So geht es zunächst um die Mängel von IEEE 802.1 p/Q. Strikte Priorisierung ist inadäquat für die Lösung der anstehenden Probleme. Stationen niedrigerer Priorität verhungern, es gibt keine minimale BW Garantie und keine obere BW Grenze. Ein Operator kann die Bandbreite nicht steuern (z.B. 1/3 IPC..). Die Verwaltung von Congestions ist schwierig, die Auflösung einer Congestion darf nicht dazu führen, dass sich der Verkehr höchster Priorität die gesamte Bandbreite nimmt. Ideal wäre eine virtuelle Pipe für jede Verkehrsklasse.

IEEE 802.1 p/Q ist nach Aussagen von IEEE 802.1 DCB nur gut für die Regulierung des normalen LAN-Verkehrs. Für weitergehende Ansprüche benötigt der Standard eine Einbettung in ein Gesamtkonzept.

Man hat dann versucht, den „Lossless"-Transport mit IEEE 802.3Qau und 802.3x zu analysieren, weil das ja die Kombination ist, die von manchem Hersteller favorisiert wird.

Es freut mich außerordentlich, dass die durch Simulation erhaltenen Ergebnisse von IEEE 802.1 DCB mit denen, die ich durch Anwendung der Warteschlangentheorie im Rahmen der weiter oben angeführten Argumentation erhalten habe, übereinstimmen:

Abbildung 3 fasst die Vorgehensweise beim Auftreten einer Staustelle im Rahmen von Congestion Notification nochmals anschaulich zusammen.

Die Simulationen durch IEEE 802.1 DCB haben gezeigt, dass IEEE 802.1 Qau effektiv arbeitet, wenn es darum geht, den Paketverlust zu reduzieren. Ein Paketverlust ist aber immer noch möglich !!! Link Level Flow Control LLFC ist die einzige Möglichkeit, Zero Loss zu garantieren.

Aber, es kommt noch dicker: der IEEE 802.3x PAUSE-Mechanismus hat durchaus seine Tücken. 802.3x ist ein on/off Mechanismus. Alle Verkehrsströme werden ausgeschaltet. 802.3x tut nichts für einen bestimmten Verkehr, sondern behandelt alle Verkehrsarten gleichartig: er schaltet sie ab. Verluste sind dabei durchaus möglich. 802.3x vergrößert die Latenz für interaktiven Verkehr und Kontrollnachrichten und deshalb schalten die meisten 802.3x aus. 802.3x bildet nur dann eine Lösung, wenn er mit PBC Link Level Flow Control kombiniert wird. Das ist aber noch nicht alles, wie wir gleich sehen werden.

IEEE 802.1 DCB geht davon aus, dass die DCB-Funktionen nicht überall benötigt werden, sondern nur innerhalb einer „DCB-Wolke", siehe dazu Abbildung 4.

Man geht für die Betrachtungen harmloserweise davon aus, dass es einen Congestion Point gibt und eine Reihe äquivalenter Geräte, die angemessen auf eine Congestion reagieren können, siehe Abbildung 5.

Congestion Management ist eine Ende-zu-Ende-Funktion. Daten aus verschiedenen Quellen treffen auf einen Punkt, an dem sie abgewürgt werden (Choke Point). Eine Congestion wird dann erkannt, die Ingress-Rate in der Konsequenz gesenkt. Eine Kontrollschleife senkt die Datenrate auf das, was der Choke Point noch wegbringen kann. Ein einfacher Fall: 2 oder mehr (N) ähnliche Ingress-Geräte, 1 Choke Point CP. Dann bekommt jedes Endgerät 1/N CP-Bandbreite. Man möchte eine minimale Benutzung von Puffern am CP erreichen. Es gibt aber auch komplexe Fälle wie unterschiedliche Ingress-Geräte und Verkehrsflüsse, komplexe CPs. Hier sagt man, dass dann die Situation mit CM immer noch besser ist als ohne. Probleme sind insgesamt ein möglicher Pufferüberlauf, bevor CM eingreifen kann und die Notwendigkeit von Zusatzlösungen für ein wirklich sicheres Netz.

In manchen Fällen ist Congestion Management einfach nicht schnell genug, um den Pufferüberlauf zu verhindern: ===> LOSS !!!

Das betrifft besonders „wichtige" Verkehrsflüsse. Wenn diese mittels 802.1 p/Q eine höhere Priorität haben, werden die betreffenden Ausgangswarteschlangen

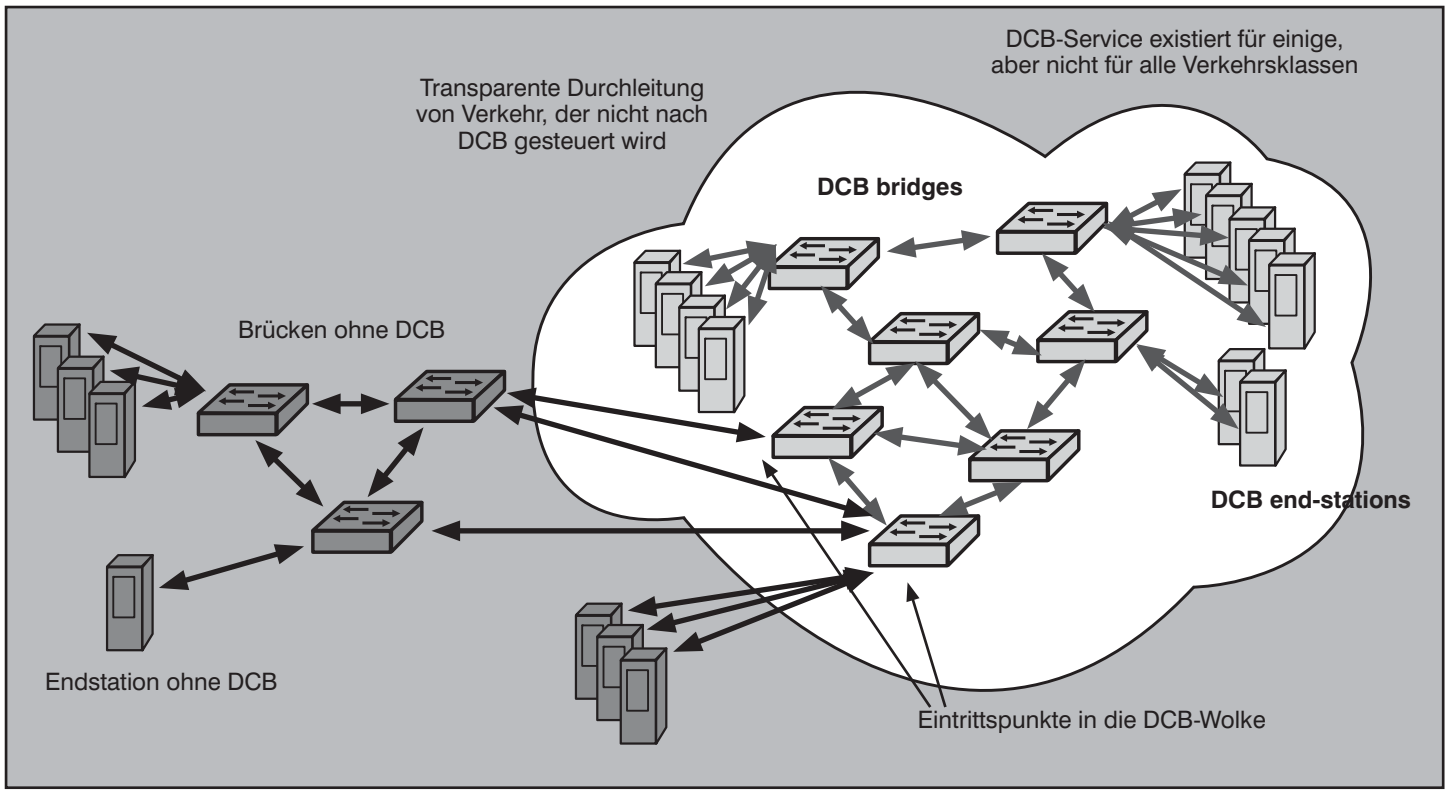


Abbildung 4: DCB Netzwerk Wolke

Quelle: IEEE

bevorzugt entleert, also sind auch diese Pakete eher als andere an Staustellen und werden dann zurückgewiesen. Bei einer priorisiert gesteuerten „Bremsung“ laufen natürlich in dem Switch, der vor der Staustelle liegt, die Puffer für die Pakete höherer Priorität schneller voll. Und so wie das Congestion Management momentan gestaltet ist, hat es in etwa die Reaktionszeit von Spanning Tree, der Weinbergschnecke unter den Algorithmen.

In diesem Zusammenhang werden dann nochmals die Grenzen von 802.1p deutlich. Der aktuelle Standard definiert nur simples Verhalten, weil nur strikte Priorisierung möglich ist. Die Welt hat intelligentere Modelle entwickelt, diese sind aber im Zusammenhang mit 802.1 nicht standardisiert. Es werden Erweiterungen für die Definition komplexerer, konvergenter Strukturen benötigt. Nötig ist, innerhalb der definierten 8 Code-Points Grouping und BW-Sharing zu definieren. Außerdem muss man „Abflussalgorithmen“ definieren, die min. und max BW sowie gewichtete Prioritäten unterstützen. Für stabile Interoperabilität wird ein gemeinschaftliches Modell für die Definition und das Management benötigt.

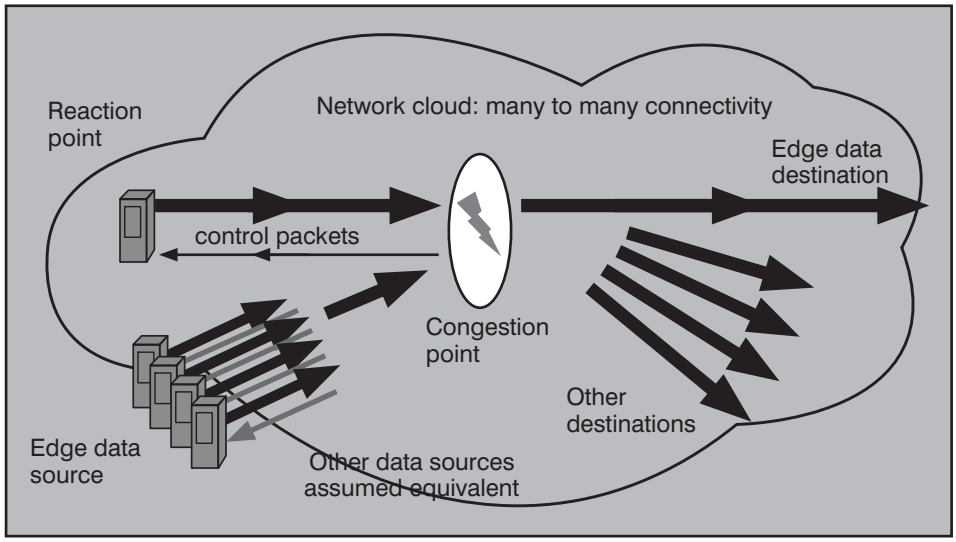


Abbildung 5: 1 Congestion Point, 1 Reaction Point

Nun, das ist nicht völlig aussichtslos, weil es derartige Lösungen im Bereich der Providernetze und auch von engagierten Herstellern schon länger gibt.

DCB hat insgesamt zwei erhebliche Problembereiche

→ Congestion Spreading: Priority Based Flow Control führt zu Congestion Speading, daraufhin schmilzt der Durchsatz zusammen

→ Deadlocks: Link Level Flow Control kann zu Deadlocks führen !!!!!!!

DCB ist nicht für alle Anwendungen und Produkte geeignet, in vielen Fällen ist es einfach eine zu große zusätzliche Last. Eine Schwierigkeit ist auch die Kompatibilität mit existierenden Geräten.

Multiple Hops in einem Netz mit PB Flow Control können Congestion erzeugen, die sich über das ganze Netz ausbreitet. Das habe ich ja schon weiter oben detailliert ausgeführt, so dass hier nochmal ein zusammenfassendes Abbildung 6 reicht.

Das Schärfste sind aber die Deadlocks. Also, ich habe persönlich die letzten Deadlocks innerhalb meines Informatikstudiums kennengelernt, also vor über 30 Jahren. Da waren sie ein beliebtes Thema im Rahmen der Betriebssysteme. Netze sind üblicherweise so konstruiert, dass es alles, aber bestimmt keine Deadlocks geben kann. Und jetzt haben wir endlich eine funktionale Konstellation, die uns auch einen Deadlock ins Netz bringen kann!

Priority Based Flow Control kann in Verbindung mit MSTP einen Deadlock erzeugen!

Damit das geschieht, muss folgendes zusammen passieren:

→ Es existiert eine zyklische Abhängigkeit in der Flow Control
→ Der Verkehr geht durch alle Ecken des Zyklus
→ In allen Verbindungen des Zyklus geschieht gleichzeitig Congestion

In Folge bleibt wirklich alles stehen, das dauert so ungefähr eine Sekunde. Danach geht das Congestion Spreading richtig los. Wirklich toll. Das hat uns wirklich noch gefehlt. Da nützt es auch nichts, dass IEEE die Wahrscheinlichkeit des Auftretens eines solchen Deadlocks als „sehr gering“ einstuft und das entsprechend mathematisch belegt. Alleine die Möglichkeit eines Deadlocks ist sehr bedrohlich, denn es gibt ja auch noch Murphy´s Law.

Hier sagt ein Bild mehr als 1000 Worte (siehe Abbildung 7).

Also, solange dieses Problem nicht wirklich zufriedenstellend gelöst wird, sind alle weiteren Diskussionen relativ substanzlos. Es gibt ja noch die ganzen Problemfelder, die sich daraus ergeben, wie die Endgeräte auf eine Congestion Notification reagieren sollen, wie die Adapter dann organisiert werden können usf, die ich ja schon weiter oben angesprochen habe.

Wenn der diesbezügliche Standardisierungsprozess überhaupt jemals terminieren sollte, dann dauert das noch eine ganze Zeit.

Hier an dieser Stelle kam es mir ja vornehmlich darauf an, die schöne neue RZ-Netz-Welt, wie sie von manchen, durchaus nicht allen Herstellern propagiert wird, erheblich in Frage zu stellen. Grade Einzelheiten, die in einer entsprechenden Präsentation harmlos erscheinen, wie „Lossless“ oder PBC, entpuppen sich bei näherem Hinsehen als außerordentlich heimtückisch und komplex.

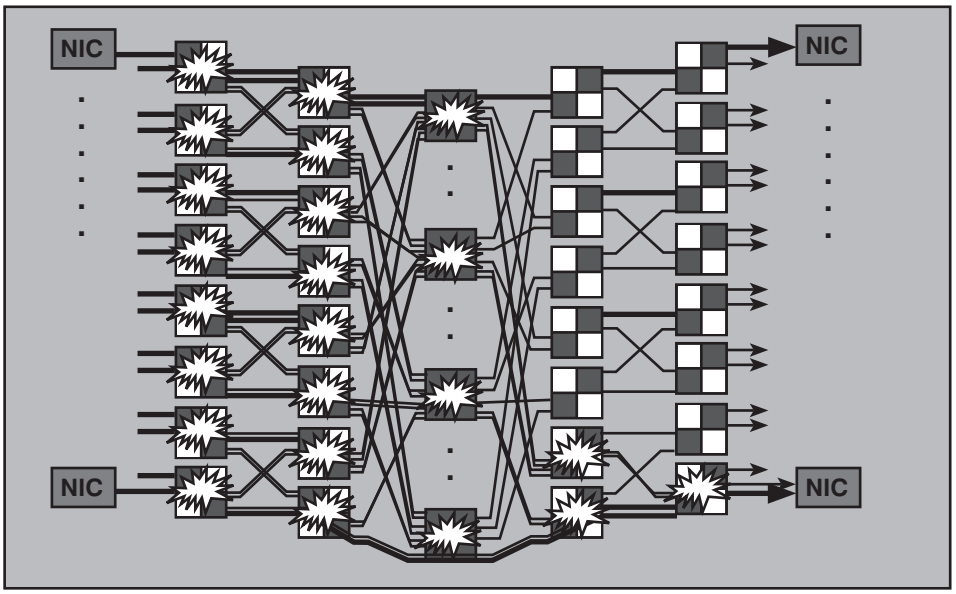


Abbildung 6: Congestion Spreading Quelle: IEEE

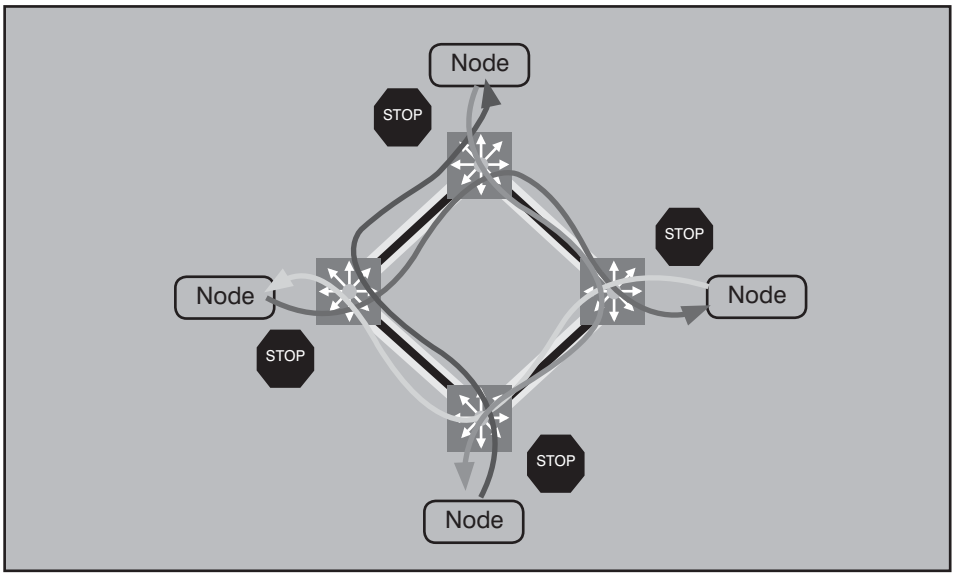


Abbildung 7: Deadlock

3. DCBX: DCB Capability Exchange Protocol

Stellen wir uns vor, dass es Geräte geben würde, die nach den DCB-Spezifikationen arbeiten. Das wären sicherlich nicht alle im RZ und seinem Umfeld. Außerdem könnten Geräte verschiedener Hersteller DCB-Spezifikationen in unterschiedlichem Maße implementieren.

Es muss einen Mechanismus geben, der das automatisch feststellt, so wie die Datenrate zwischen zwei Geräten durch die Autonegotiation festgelegt wird.

Überdies wäre es nützlich, wenn dieser Mechanismus Administratoren weitere Informationen für die Konfiguration gibt.

Eine diesbezügliche Erweiterung zu den bisherigen DCB-Spezifikationen wurde von Mitarbeitern der Hersteller Brocade, Broadcom, Cisco, Juniper, Fujitsu, Marvell, Qlogic, IBM, Mellanox, Intel, Dell, Emulex und PLX erarbeitet. Die Spezifikation das Data Center Discovery and Capability Exchange Protokoll, welches von DCB-Einheiten dazu benutzt wird, Daten über ihre jeweiligen Möglichkeiten unmittelbar auszutauschen. Das Protokoll kann ebenso zu Konfigurationszwecken und zur Entdeckung von falschen Konfigurationen benutzt werden.

In der Spezifikation wird das Basis-Protokoll durch endliche Automaten spezifiziert.

Der Kampf ums RZ: die nächste Runde - Teil 1

Die ist eine bewährte und recht deutungsfreie Methode.

Die Möglichkeiten von DCB-Einheiten wie HBAs und Switches werden durch sog. Features beschrieben. Für jedes Feature, das unterstützt wird, müssen die folgenden Informationen bereit gestellt werden:

- Die auszutauschenden Parameter
- Die Art der Benutzung der Parameter für die Entdeckung von Fehlkonfigurationen
- Eine Festlegung der Reaktion auf einen entdeckten Fehlerfall

In der Version 1.0 der DCBX-Spezifikation wird das für Priority Groups PG und Priority-based Flow Control (PFC) gemacht.

Die Ziele der DCBX-Spezifikation sind:

- Discovery von DCB-Fähigkeiten eines Peers. DCBX soll dazu benutzt werden, die DCB-Fähigkeiten eines Peers festzustellen. Der Peer eines HBAs ist normalerweise ein Switchport. Der Peer eines Switchports kann ein HBA oder ein anderer Switchport sein. In jedem Fall sind Peers technisch unmittelbar miteinander verbunden. Es geht darum festzustellen, welche DCB-Fähigkeiten wie PG oder PFC von einem Peer unterstützt werden. Man kann so bestimmen, welche Fähigkeiten im Rahmen der bidirektionalen Verbindung von zwei Peers unterstützt werden.
- Entdeckung einer Fehlkonfiguration des DCB-Features. DCBX kann dazu benutzt werden, Fehlkonfigurationen auf Peer-Links festzustellen. Die Feststellung einer Fehlkonfiguration ist jedoch Feature-spezifisch, da es Features geben kann, die auch eine asymmetrische Konfiguration zulassen.
- Peer Configuration von DCB-Features. DCBX kann von einem Gerät dazu benutzt werden, die Konfiguration von DCB-Features in seinem Peer-Kommunikationspartner vorzunehmen. Das Ziel ist es, eine Basis-Peer-to-Peer-Konfiguration in der Initial-Version von DCBX zu realisieren. Spätere Versionen von DCBX oder andere Anwendungen der höheren Schichten können darauf zurückgreifen, um komplexere Methoden zur Konfigurations-Verteilung zu etablieren.

Abbildung 8 zeigt ein Szenario für ein Netz, welches DCBX benutzt. DCBX-fähige Links tauschen Informationen über DCB-Fähigkeiten und Konfiguration aus und Warnungen über mögliche Konflikte werden an die Management-Station geschickt. Zum Beispiel kann man eine Grenze zwischen Geräten, die DCB unterstützen, und solchen, die das nicht tun, aufzeigen.

Jedes DC-Feature besitzt eine Menge von Parametern. DCB-Parameter können in zwei Kategorien eingeteilt werden: auszutauschende Parameter und lokale Parameter.

Die auszutauschenden Parameter werden an den Peer geschickt. Innerhalb dieser Parameter gibt es zwei Untergruppen: administrierte und operationelle Parameter. Erstere werden durch die Konfiguration festgelegt. Ein operationeller Parameter ist der betriebliche Status der betreffenden administrierten Parameter. Der betriebliche Status kann sich vom administrativen oder konfigurierten Status unterscheiden, hauptsächlich als Ergebnis der DCBX-Kommunikation zwischen den Peers. Operationelle Parameter gibt es nur für diejenigen administrierten Parameter, bei denen eine Wahrscheinlichkeit dafür besteht, dass der operationelle Status von dem, was der Administrator ursprünglich konfiguriert hat, abweicht. In eine LLDP-Nachricht werden operationelle Parameter nur zu informativen Zwecken eingefügt. Das kann z.B. ein Gerät darüber in Kenntnis setzen, wie der aktuelle operationelle Status eines Peers aussieht. Abbildung 9 fasst das nochmal zusammen.

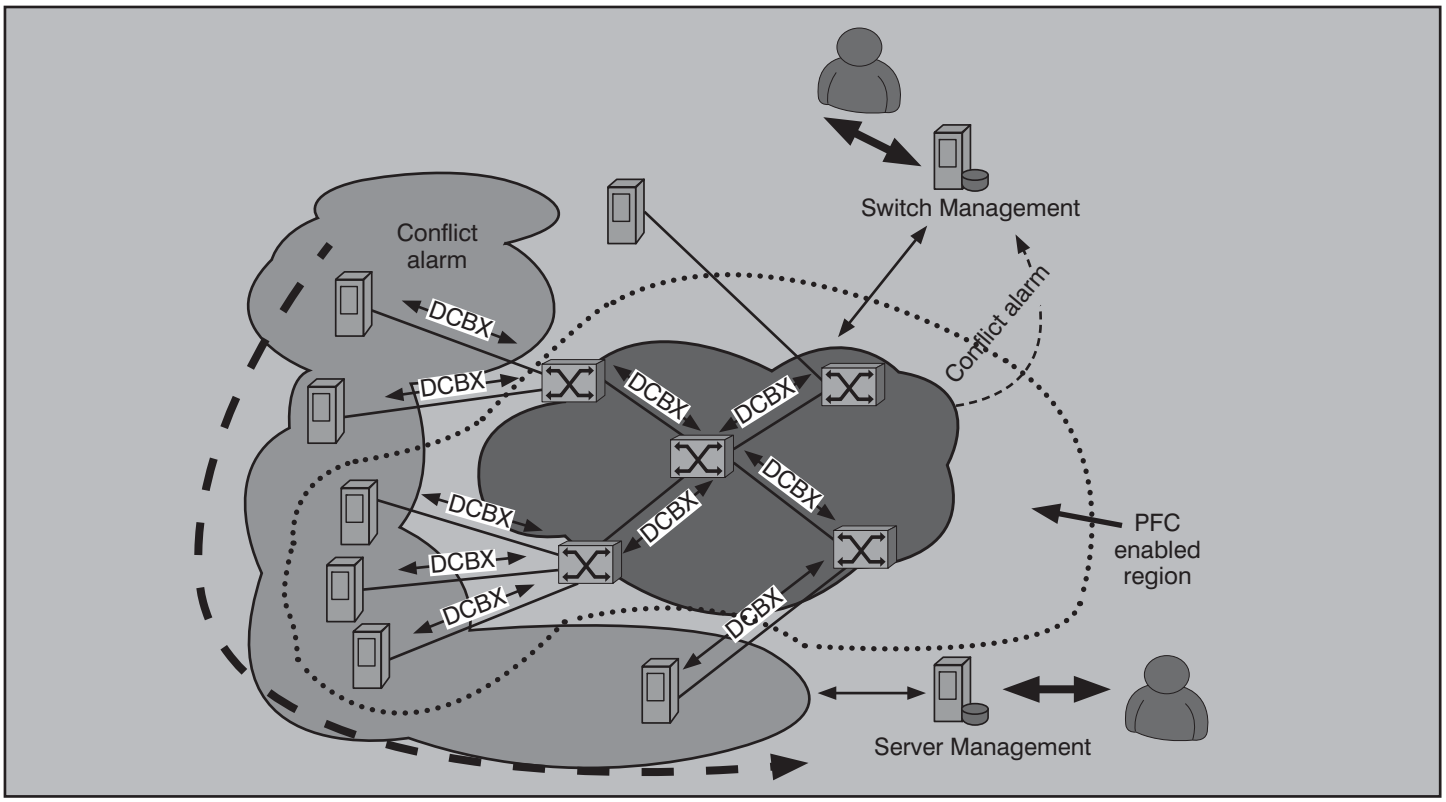


Abbildung 8: DCBX-Szenario

Quelle: IEEE

Der Kampf ums RZ: die nächste Runde - Teil 1

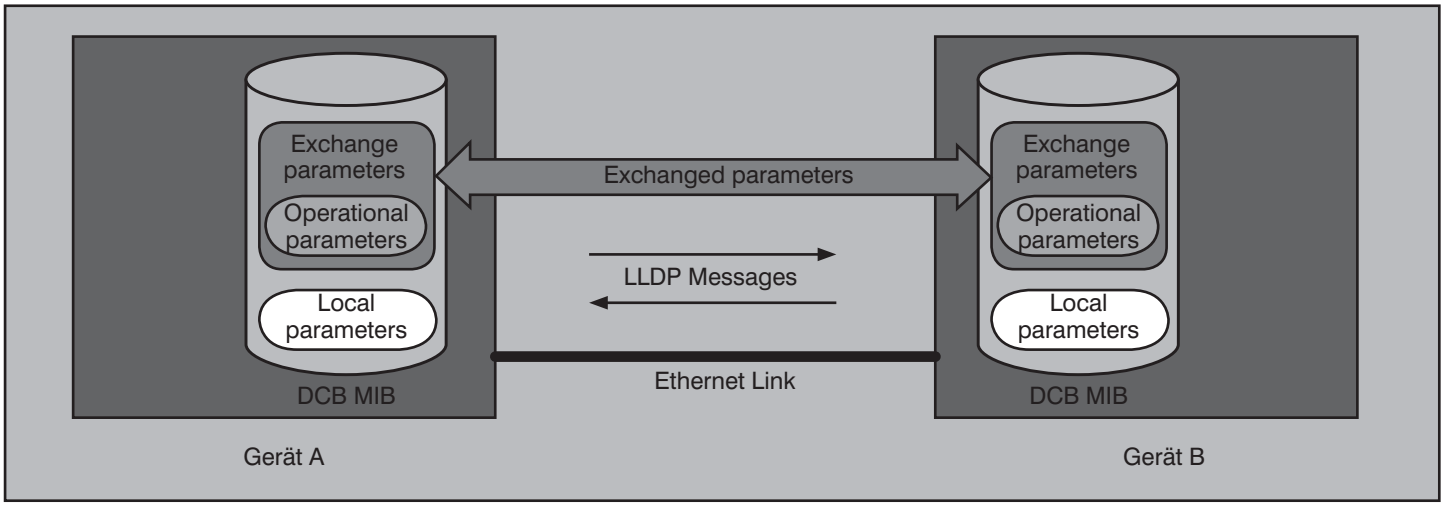


Abbildung 9: Arten von DCB-Parametern

Quelle: IEEE

DCBX benutzt das IEEE 802.1 AB Link Layer Discovery Protocol LLDP für den Austausch von Parametern zwischen zwei Link Peers. LLDP ist ein unidirektionales Protokoll. Es informiert die vermöge eines IEEE 802 LANs an eine lokale Station angeschlossenen anderen Stationen über die Konnektivitäts- und Management-Eigenschaften der lokalen Station. LLDP PDUs beinhalten zwingend notwendige und optionale Type Length Values TLVs. Zwingend notwendig sind z.B. Chassis ID, Port ID, TTL Time to Live, End of LLDPDU. Optional sind Informationen über das grundsätzliche Management und organisationsspezifische Informationen zu 802.1- oder 802.3-Protokollen.

Parameter, die über DCBX ausgetauscht werden, gehören zu den organisationsspezifischen TLVs. Abhängig von der Menge der auszutauschenden Information für alle Features werden für DCBX ein oder mehrere TLVs mit entsprechenden Sub-Typen definiert. Die Sub-Typen für ein TLV werden für jedes Feature, das von diesem TLV unterstützt wird, definiert.

Abbildung 10 zeigt das LLDP Frame Format

DCBX ist dazu gedacht, über eine Punkt-zu-Punkt-Verbindung zu arbeiten. Werden multiple LLDP-Nachbarn entdeckt, verhält sich DCBX solange so, als seien sie gar nicht da, bis die multiple Nachbarschaft nicht mehr vorhanden ist. Ein LLDP-Nachbar wird durch seinen logischen MAC Service Access Identifier MSAP identifiziert. Der MSAP ist eine Konkatenation aus Chassis-ID und Port-ID-Werten, die in der LLPDU transportiert werden.

Das hört sich zunächst einmal unnötig komplex an. Tatsache ist aber, dass nach heutigen Stand der Technik Protokolle wie FCoE mit der gewünschten „Lossless“-Eigenschaft nur über Punkt-zu-Punkt-Strecken sinnvoll realisiert werden können, weil sie eine geschützte resrevierte Bandbreite benötigen.

Ein Administrator kann LLDP sowohl an der Sende- als auch an der Empfangsseite aktivieren oder deaktivieren. DCBX ist aber ein Protokoll, welches Acknowledgements verwendet. Um sinnvoll arbeiten zu können, muss also LLDP sowohl an der Sende- als auch an der Empfangsseite des Interfaces, auf dem DCBX läuft, aktiviert sein. Ist eine der Seiten ausgeschaltet, wird auch DCBX deaktiviert. Ist DCBX aktiv und die LLDP-Sendeseite wird deaktiviert, wird gemäß der LLDP-Spezifikation eine Shutdown-LLDPDU ausgesendet. Erhält der Peer diese Nachricht, wird dadurch bei ihm auch DCBX deaktiviert. Das ist äquivalent zu dem Fall, dass ein Timeout oder ein Frame-Verlust passiert. Vergleichbares passiert, wenn die LLDP-Empfangsseite ausgeschaltet wird.

In der Initialphase kann es bei LLDP zu einem größeren Delay führen, bevor DCB-Parameter ausgetauscht und initialisiert werden können. Dieses Problem kann relativ einfach abgestellt werden und die Gruppe IEEE 802.1 AB-REV arbeitet daran. Sobald es aus der Welt geschafft ist, wird DCBX auf die neuen Bedingungen eingestellt.

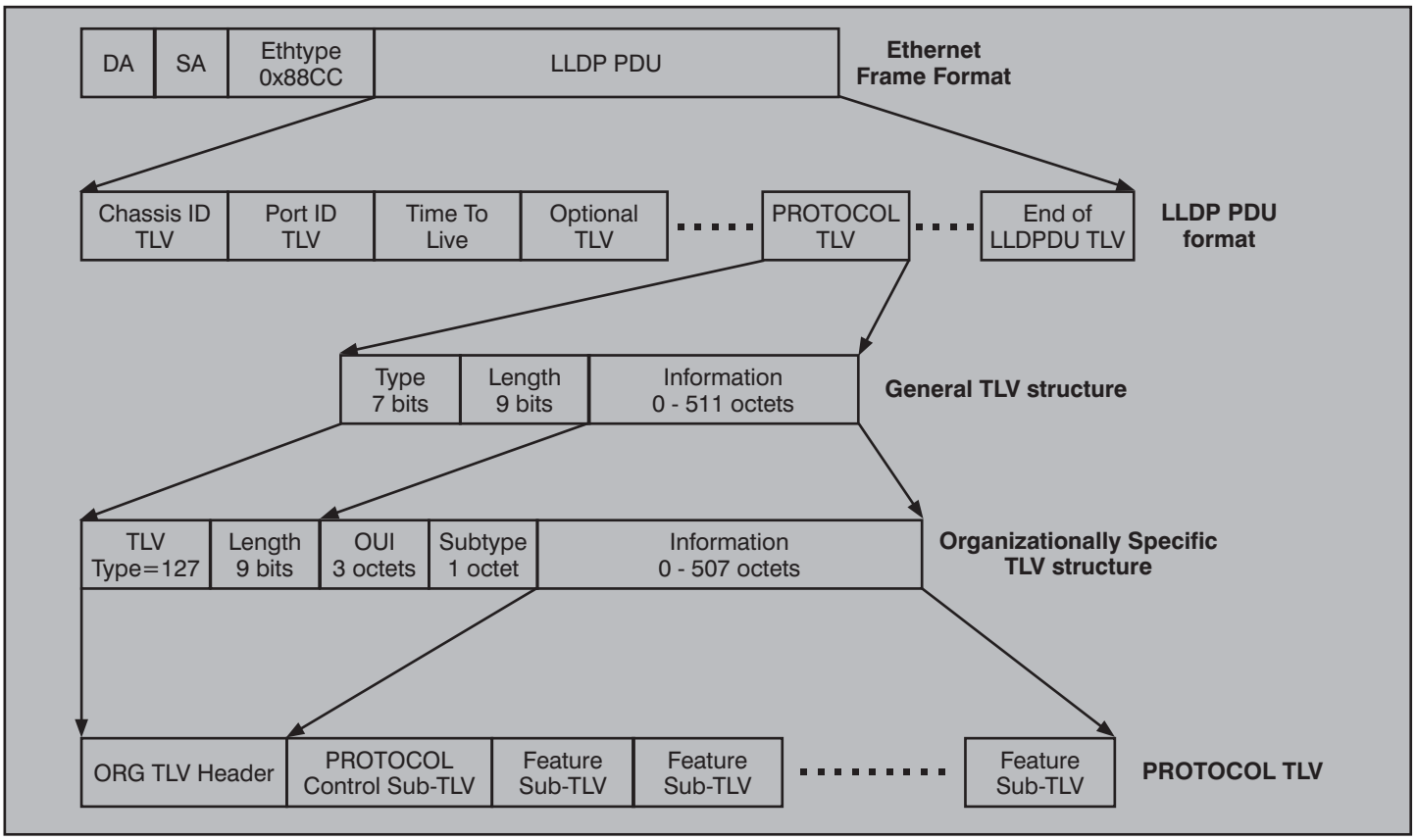


Abbildung 10: LLDP Frame Format

Quelle: IEEE

DCBX ist als endlicher DCBX Kontrollautomat mit einer Menge von endlichen Automaten für die DCB Features definiert. Die Aufgabe des DCBX-Automaten ist die Sicherstellung der Tatsache, dass die zwei DCBX-Peers nach dem Hochfahren der Verbindung oder nach einer Änderung der Konfiguration durch den Austausch von LLDPDUs synchronisiert werden. Die Automaten für die DCB Features handeln die lokale operationelle Konfiguration für jedes Feature. Die Informationen über den DCBX-Kontrollzustand und die Konfiguration der DCB-Features werden mit dem Peer mittels DCBX TLVs ausgetauscht, die vermöge von LLDP PDUs übertragen werden. Das DCBX TLV-Format zeigt Abbildung 11.

Die DCBX Control Sub-TLV und die Menge der Feature Sub-TLVs können innerhalb der DCBX TLV beliebig angeordnet sein, es darf jedoch keine Doppelten geben. Sie würden als Konfigurationsfehler gewertet. Weitere Einzelheiten zu den Bits in den Feldern oder zum Aufbau des endlichen Automaten ersparen wir uns hier. Im Gegensatz zu vielen anderen Protokollen ist jedoch hervorzuheben, dass DCBX aufgrund seiner Konstruktion vollständig und ausnahmslos deterministisch arbeitet.

Blicken wir noch auf die DCB Features, zunächst auf das Priority Group Feature. Die Priority Groups Specification liefert Konfigurationstabellen und ein Scheduling-Verfahren für die Verwaltung von Bandbreite verschiedener Verkehrsklassen auf einer konvergierten Verbindung. Auch wenn man für die Zukunft erwartet, dass DCB-Geräte eine Scheduling-Funktionalität , wie sie in der Priority Group Spezifikation festgelegt ist, oder sogar eine bessere haben, muss man auch berücksichtigen, dass es bereits „legacy“ Implementierungen gibt. Um eine hinreichend weite Akzeptanz für DCBX zu schaffen, werden auch Implementierungen unterstützt, die die Qualität der Priority Group Spezifikationen nicht ganz, aber so weit wie möglich, erreichen.

Das Priority Based Flow Control Feature ist wichtig, um einen möglichst verlustfreien Datentransport für diejenigen Verkehrsarten, bei denen das notwendig ist, zu gewährleisten. DCBX sieht vor, dass in einem Fall, bei dem nicht beide Peers PBFC unterstützen, die Verbindung auf den PAUSE-Mechanismus nach 802.3x zurückgeschaltet wird.

Auch wenn PBFC selbst zu einer nichtdeterministischen Reaktion eines Netzes führen kann, wird es dennoch im Rahmen von DCBX durch einen endlichen Automaten repräsentiert, der deterministisch ist. DCBX fügt also PBFC keine weitere nichtdeterministische Komponente hinzu.

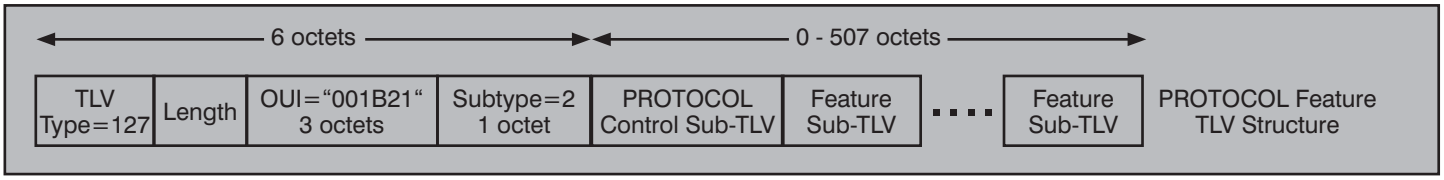


Abbildung 11: DCBX TLV-Format

Quelle: IEEE

4. Priority Grouping for DCB-Networks: Enhanced Transmission Selection ETS

Ein seit langem bekanntes Problem bei der Priorisierung in IEEE 802-Netzen ist, dass der definierte Mechanismus relative Prioritäten festlegt. Ein Verkehrsstrom mit einer höheren Priorität wird, im einfachsten Fall durch die Manipulation einer Warteschlange, schneller durchgeleitet als ein Verkehrsstrom niedrigerer Priorität. Von der Warteschlangentheorie weiß man, dass insgesamt bei einer solchen Mechanik nur ein einziger Verkehrsstrom gewinnt, nämlich der mit der höchsten Priorität. Der Verkehrsstrom mit der zweithöchsten Prio hat in etwa das gleiche Leben wie in einer ungesteuerten Variante. Alle Verkehrsströme mit niedrigerer Priorität werden beachteiligt und stehen schlechter da als bei einer ungesteuerten Lösung. Der Gewinn für einen Verkehrsstrom bezieht sich aber lediglich auf die mittlere Verzögerung und das Delay einer Verzögerung. Keineswegs aber auf eine für diesen Verkehrsstrom zur Verfügung stehenden Datenrate.

Das hat bei IEEE eine lange Tradition und es gibt ja auch viele Anwendungen, bei denen das gut funktioniert. Ein Voice-Datenstrom braucht vergleichsweise so gut wie keine Bandbreite, ist aber extrem pingelig hinsichtlich einer Varianz in der Verzögerung. Wendet man in einem System, wo Sprache und Daten gemischt auftreten eine Priorisierung für den Voice Verkehr nach oben beschriebenem Muster an, wird das sehr gut arbeiten, weil das Problem, was der Voice Verkehr sonst hätte, wirkungsvoll abgestellt wurde. Ähnliches gilt z.B. im Wireless-Bereich. Ein Video-Datenstrom ist an und für sich gegen nichts wirklich empfindlich, benötigt aber recht viel Bandbreite. Wird die nun wie im Fall von Wireless-Netzen knapp, kann man ihn erfolgreich priorisieren. Er grabscht sich dann soviel Bandbreite wie es geht, alle anderen Verkehrsströme werden übel untergebuttert. Dennoch ist das z.B. für den Home-Bereich eine sinnvolle Lösung.

Insgesamt kann man sagen, dass die Priorisierung solange gut funktioniert, wie ein Datenstrom, der einen prozentual auf die insgesamt zur Verfügung stehende Bandbreite nur relativ geringe Teil belegt, bevorzugt werden muss, so wie beim Voice-Beispiel. Die Priorisierung von Video im Heimbereich ist dagegen ein Beispiel dafür, wie man es eigentlich nicht machen sollte: die Auswirkung auf die anderen Datenströme ist fürchterlich.

Ziel der DCB/FCoE-Bemühungen ist es aber grade, einen fetten Datenstrom, der auch noch hohe Ansprüche stellt („lossless“), heil zusammen mit anderen Datenströmen über eine Leitung zu bringen. Und da versagt IEEE 802.1 p/Q auch in Verbindung mit 802.1ar Congestion Control sowohl in der Warteschlangentheorie, als auch bei Simulationen kläglich. Es gibt Hersteller, die behaupten, in der Praxis würde es funktionieren. Ich nehme stark an, sie haben es noch nicht belastet.

Dabei gibt es im Bereich der Carrier Netze, verankert in der Tradiiton der Optischen Netze, hierfür durchaus standardisierte Lösungen.

Das Ziel des Projektes IEEE 802.1 Priority Grouping for DCB-Networks Enhanced Transmission Selection ETS ist es, dies auch endlich in das normale IEEE 802.1-Universum zu tragen. Das Projekt wird von folgenden Herstellern unterstützt: Juniper, Brocade, Cisco, Fujitsu, Marvell, Qlogic, Broadcom, IBM, Mellanox, Nuova, Intel, Dell, HP, Emulex und PLX. Viel mehr geht nicht. (siehe Abbildung 12)

Das Dokument zu ETS beinhaltet Definitionen und ein Betriebsmodell für Prioritätsbearbeitung und Bandbreitezuordnung auf konvergierten Links für Endsysteme und Switches in einer DCB-Umgebung. Durch prioritätsbasierte Verarbeitung und Bandbreitezuordnung können unterschiedliche Verkehrstypen wie LAN, SAN, IPC und Management so konfiguriert werden, dass sie mit einer Bandbreitezuordnung, geringer Latenz oder anderen Charakteristiken wie Best Effort übertragen werden können.

Die Ziele für ETC in 802.1Q-Brücken sind wie folgt. Mit DCB und anderen neuen Benutzungsmodellen müssen 802.1Q-Brücken (zum Verständnis: damit meinen sie immer Switches, denn ein Switch ist nach IEEE 802 nichts weiter als eine Multiport-Brücke) verschiedene Verkehrstypen mit anderen Anforderungen, als es sie bisher beim Einsatz von 802.1Q-Brücken gab, bedienen können. Ein konvergiertes Ethernet wird Verkehrsströme behandeln müssen, die in verschiedener Weise empfindlich sind. So mag Speicherverkehr keinen Paketverlust, während IPC kritisch hinsichtlich der Latenz ist. Auf einer einzelnen konvergierten Verbindung müssen diese Verkehrsströme koexistieren können, ohne sich gegenseitig ernsthaft negativ in der Leistung zu beeinflussen. Um das zu erreichen, müssen DCB-Brücken folgendes unterstützen:

- Zuordnung von Prioritäten zu Prioritäten-Gruppen und zwar so, dass jede Gruppe Verkehr, der ein bestimmtes Verhalten der Verbindung verlangt, von einer solchen Gruppe repräsentiert wird, z.B. LAN, SAN, IPC
- Möglichkeit von unterschiedlichen Prioritäten in einer Prio-Gruppe
- Konfiguration von Bandbreite-Zuordnung für jede Prio-Gruppe:

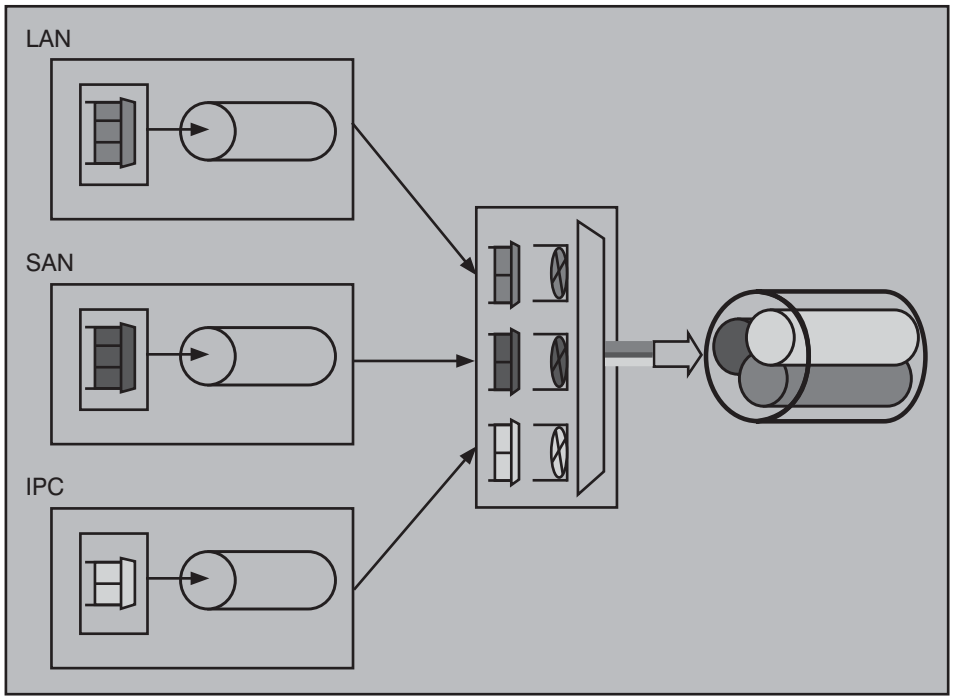


Abbildung 12: Konvergenz über Ethernet Quelle: IEEE

  - Die Zuordnung wird in Prozent der insgesamt zur Verfügung stehenden Bandbreite ausgedrückt, die Auflösung ist dabei 1%
  - Beispiel: 40% LAN, 40% SAN, 20% IPC
  - Die weitere Unterverteilung dieser Bandbreite im Rahmen der innerhalb einer Prio-Gruppe möglichen Prioritäten ist außerhalb des Betrachtungsbereiches von ETS
- Unterstützung von Minimalanforderungen an den Scheduler zur Minimierung des Einflusses der Abbildung unterschiedlicher Verkehrsströme auf eine Verbindung
  - Möglichkeit der Koexistenz von Verkehrstypen, die geringe Latenz verlangen, mit solchen, die bandbreiteintensiv, aber weniger empfindlich gegenüber der Latenz sind
  - Möglichkeit der Bewahrung relativer Priorisierung für manche Verkehrsarten bei gleichzeitiger Möglichkeit, die Bandbreite unter anderen Strömen aufzuteilen
- Bereitstellung eines konsistenten Management-Frameworks, um das alles via MIB-Objekten konfigurieren zu können

Also, dabei kann schonmal etwas durcheinander geraten. Nochmal die Definitionen:

- Priorität, Priority (Pri): es gibt acht mögliche Prioritäten für einen Verkehr, die durch das 3-bit 802.1Q-Tag festgelegt werden
- Prioritäten-Gruppe, Priority Group: eine Gruppe von Prioritäten, die durch eine Systemverwaltung zum Zwecke der Bandbreiten-Zuordnung zusammengebunden wird. Es wird erwartet, dass alle Prioritäten in einer einzelnen Gruppe gleichartige oder verwandte Anforderungen an die Behandlung des zu ihnen gehörigen Verkehrs hinsichtlich Latenz oder Paketverlust haben
- Priority Goup Identifier (PGID): ein 4-bit Identifier, der einer Prio-Gruppe zugeordnet wird. Dabei ist PGID = 15 ein spezieller Wert, der die Konfiguration von Prioritäten mit „No Bandwidth Limit“ erlaubt. PGID-Werte von 8 bis 14 sind reserviert
- Priority Group Bandwidth (PG%): der einer bestimmten PGID zugeordnete prozentuale Anteil einer verfügbaren Verbindung

Auf dieser Grundlage lassen sich dann Tabellen für die Abbildung von Prios in Prio-Gruppen und die Abbildung dieser Gruppen auf prozentuale Bandbreitenanteile erstellen. Die Summe der prozentualen Bandbreiteanteile muss immer 100% sein, sonst ist das Verhalten unspezifiziert. Abbildung 13 macht nochmals klar, wie die Begriffe zusammenhängen.

Damit kann man jetzt nun die Verhaltensweisen bei bisher üblichen Konfigurationen beschreiben. Ist eine IEEE 802.1Q-Brücke so spezifiziert, dass sie eine strikte Abarbeitung nach Prioritäten als Grundverfahren vornimmt, so kann man das dadurch nachbilden, dass man nur eine einzige Prio-Gruppe bildet, die alle Prios umfasst und mit PGID=15 die gesamte Bandbreite bekommt. Ist eine Brücke so spezifiziert, dass sie Prios auf Verkehrsklassen abbildet, braucht diese Abbildung nicht geändert zu werden. Man muss dann lediglich definieren, welche Bandbreite die jeweiligen Verkehrsklassen bekommen sollen.

Es gibt eine Reihe von Empfehlungen für DCB-Geräte:

- DCB-Geräte sollten mindestens 3 Prio-Gruppen unterstützen
- DCB-Geräte sollen die Abbildung auf und die Zuordnung zu einer einzigen Prio-Gruppe mit PBIB=15 gestatten
- DCB-Geräte sollen mindestens eine Prio-Gruppe mit Bandbreitezuordnung erlauben, bei der Priority Flow Control aktiviert ist
- DCB-Geräte sollen mindestens eine Prio-Gruppe mit Bandbreitezuordnung erlauben, bei der PFC deaktiviert ist
- DCB-Geräte sollten eine Konfiguration der Bandbreitezuordnung mit einer Granularität von 1% erlauben
- DCB-Geräte sollten ein Verfahren zur Übertragungsselektion unterstützen, welches keine Bandbreite verschwendet. Sollte eine der Prio-Gruppen ihre Bandbreite nicht aufbrauchen, muss diese für andere Prio-Gruppen verfügbar werden

Interessant ist auch eine Fußnote. Da steht: die Spezifikation der Präzision eines Schedulers ist außerhalb der Perspektive dieses Dokuments. Wir erwarten aber, dass die Genauigkeit eines Schedulers im Bereich von +/- 10% liegt. Als Konsequenz davon kann eine Prio-Gruppe mit PG% 0% dennoch bis zu 10% der verfügbaren Gesamtbandbreite erhalten, auch wenn die anderen Gruppen zusammen an und für sich die 100% ausschöpfen.

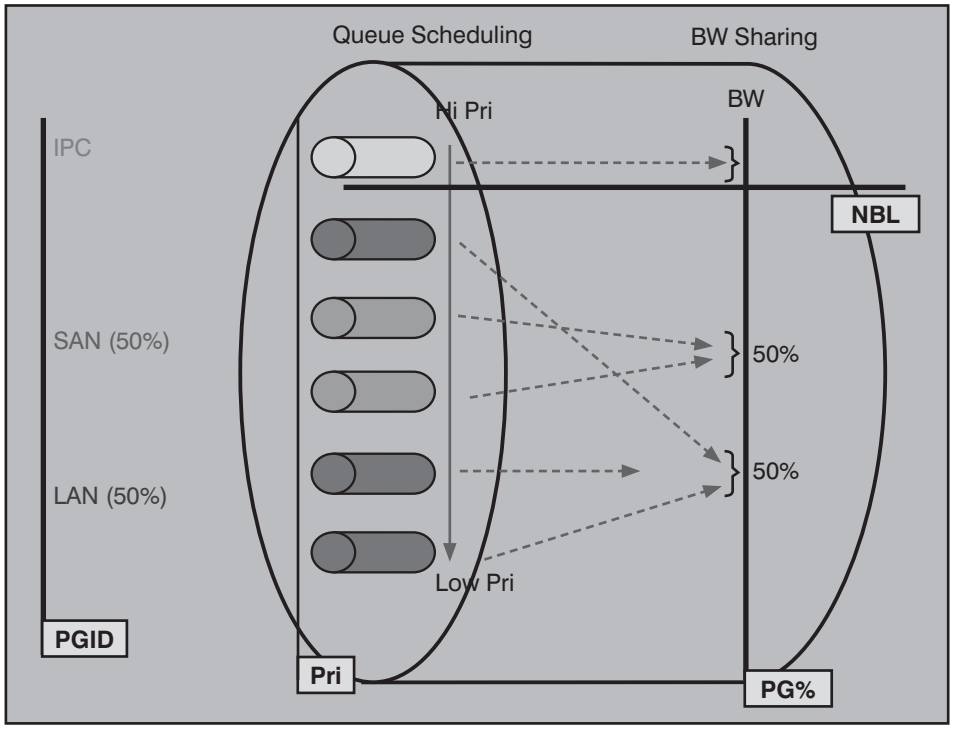


Abbildung 13: Parameter für die Konfiguration einer konvergierten Verbindung Quelle: IEEE

Der Kampf ums RZ: die nächste Runde - Teil 1

5. Zwischenfazit

Die Frage ist jetzt: bekommen wir durch DCBX und ETS das, was dringend für DCB notwendig und erforderlich ist ? Die Antwort lautet: nur zum Teil !

DCBX ist eine notwendige Funktion, die man offensichtlich zu Beginn vergessen hatte. Sie ist so substantiell wie Autonegotiation.

ETS liefert aber eines immer noch nicht: eine Garantie für „Lossless“. Es können immer noch Pakete verloren gehen. Begünstigt wird das vor allem durch die erlaubte Toleranz der von den Herstellern zu entwickelnden Scheduler. ETS hält immer noch an dem mittlerweile mehrfach widerlegten Irrglauben fest, dass Priorisierung und Congestion Control alles regeln könnten, wenn man sie nur genügend häufig aufeinanderstapelt.

Was soll der interessierte Anwender nun machen ? Klar ist, dass bei FCoE immer noch ein, wenn auch geringes, Restrisiko für einen Paketverlust besteht. Dieses Risiko kann man minimieren, indem man wirklich üppige Bandbreite spendiert und ausgesprochen übersichtliche Konfigurationen benutzt.

Spendiert man also einem 5 Gbps-Speicherverkehr 10 GbEthernet auf einer Verbindung, die von einem Speicher über einen einzigen Switch zu einem Server-HBA führt, ist der Paketverlust unwahrscheinlicher als dass man mitten in Aachen von einem sibirischen Tiger verspeist wird.

Damit könnte man ja durchaus leben, aber ein modernes iSCSI mit Entlastungsprozessoren auf den Adapterkarten kann durchaus mehr: es würde in Projektion bisheriger Möglichkeiten bis zu 8 Gbps aus einer 10 GbE-Leitung herausholen.

Ich habe ja immer gesagt, dass es zwischen FCoE und iSCSI keine wirkliche Substitutionskonkurrenz gibt. Interessant ist aber doch die Frage, was wir nun in den Fällen machen können, in denen es bereits hohe Investitionen in eine bestehende SAN-Infrastruktur mit Fibre Channel gibt. Die Weisheit der Werbung lautet: „Nimm FCoE zur I/O-Konsolidierung“. Wir wissen, dass das nach wie vor mit Risiken behaftet ist.

Also gehen wir in der nächsten Folge der spannenden Frage nach, wie sich die Hersteller das nun insgesamt vorstellen und ob es nicht noch im Falle einer bestehenden SAN-Infrastruktur eine neue Alternative gibt, die hinsichtlich ihrer Eigenschaften alles in den Schatten stellen könnte, worüber wir heute berichtet haben: EoFC!

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Sicherheit im LAN mit IEEE 802.1X, 15.06. - 16.06.09 in Stuttgart

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes.

Preis: € 1.390,- zzgl. MwSt.

Office Communications Server 2007 R2, 15.06. - 16.06.09 in Stuttgart

Das Seminar richtet sich in erster Linie an IT-Entscheider, die einen detaillierteren Blick in den OCS werfen wollen, sowie Administratoren, die einen ersten etwas tieferen Blick in die Thematik wünschen.

Preis: € 1.390,- zzgl. MwSt.

IP-Telefonie: Vorbereitung, Migration, Management, 15.06. - 17.06.09 in Stuttgart

Dieses Seminar richtet sich an die Verantwortlichen für die Planung und Einführung von IP-Telefonieumgebungen. Grundkenntnisse in Netzen und Telefonie werden vorausgesetzt.

Preis: € 1.690,- zzgl. MwSt.

Sicherheit 3: Zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs, 15.06. - 19.06.09 in Aachen

Dieses einmalige Seminar vermittelt intensiv innerhalb von 5 Tagen den praktischen Umgang mit Firewalls, VPNs, Windows-Sicherheit und WLAN-Sicherheit. Im Rahmen von praktischen Live-Übungen werden typische Konfigurationen analysiert und vermittelt.

Preis: € 2.290,- zzgl. MwSt.

Sonderveranstaltung: Ausschreibungen im Informations- und Kommunikationsbereich, 18.06.09 in Bonn

Diese Veranstaltung ist als Leitfaden für öffentliche Auftraggeber gedacht, die in ihren ITK-Vergabeverfahren unter Einhaltung aller gesetzlichen Auflagen und Vermeidung aller rechtlichen Risiken für ihre Verwaltung das optimale Ausschreibungsergebnis erreichen wollen. Planer mit jahrzehntelanger Erfahrung bei Ausschreibungen der öffentlichen Hand vermitteln auf dieser Veranstaltung ihren Erfahrungsschatz. Das juristische Wissen wird von einem renommierten Rechtsanwalt mit dem Spezialgebiet Vergaberecht präsentiert.

Preis: € 790,- zzgl. MwSt.

ComConsult IT-Sicherheits-Forum 2009, 22.06. - 25.06.09 in Königswinter

Das IT-Sicherheits-Forum wird auch in diesem Jahr wieder einen umfassenden Überblick zu aktuellen Themen der IT-Sicherheit in Theorie und Praxis anbieten. An insgesamt vier Tagen wird mit einführenden Tutorien, technischen Workshops und neutralen Fachvorträgen für jeden Interessierten etwas geboten. Dabei wird äußerst hoher Wert auf sofort verwendbare Informationen gelegt, die Teilnehmer sollen die gewonnenen Erkenntnisse möglichst sofort in der eigenen Umgebung anwenden können. Preis: € 2.290,- zzgl. MwSt.

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Projektteams leiten, 22.06. - 26.06.09 in Aachen

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.

Trouble Shooting für Netzwerk-Anwendungen, 23.06. - 26.06.09 in Königswinter

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzte Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.190,- zzgl. MwSt.
bzw. € 2.370,- zzgl. MwSt mit Prüfung

Sommerschule 2009 - Intensiv-Update auf den letzten Stand der Netzwerktechnik, 29.06. - 03.07.09 in Köln

Die Sommerschule gibt den kompakten und intensiven Überblick über die neusten Entwicklungen im Umfeld der Netzwerk-Technologien: Anforderungen an zukunftssichere Netzwerke: was ändert sich?; Neue Technologien und Standards; Design-Verfahren im Vergleich; Ausgewählte Technologien in der Analyse

Preis: € 2.290,- zzgl. MwSt.

Lokale Netze für Einsteiger, 31.08. - 04.09.09 in Frankfurt

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.290,- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
31.08. - 04.09.09 in Frankfurt
23.11. - 27.11.09 in Hamburg

TCP/IP und SNMP
21.09. - 25.09.09 in Bonn

Internetworking
05.10. - 09.10.09 in Frankfurt

Paketpreis für alle drei Seminare € 6.183,-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

ComConsult Certified Trouble Shooter

Trouble Shooting 1
06.10. - 09.10.09 in Aachen

Trouble Shooting 2
23.06. - 26.06.09 in Aachen
03.11. - 06.11.09 in Aachen

Paketpreis für beide Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 4.120.-- zzgl. MwSt.
(Seminar-Einzelpreis € 2.190.--, mit Prüfung € 2.370,-)

ComConsult Certified Security Expert

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
14.09. - 18.09.09 in Köln

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten
26.10. - 30.10.09 in Aachen

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs
15.06. - 19.06.09 in Aachen
23.11. - 27.11.09 in Aachen

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

ComConsult Certified Voice Engineer

Basis-Seminar: Session Initiation Protocol-Basis-Technologie der IP-Telefonie
28.09. - 30.09.09 in Bad Neuenahr
23.11. - 25.11.09 in Hamburg

Basis-Seminar: Sicherheitsmechanismen für Voice over IP
05.10. - 06.10.09 in Frankfurt

Alternative 1: IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
14.09. - 16.09.09 in Köln
02.11. - 04.11.09 in Frankfurt

Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management
15.06. - 17.06.09 in Stuttgart
26.10. - 28.10.09 in Berlin

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
07.09. - 08.09.09 in Aachen
09.11. - 10.11.09 in Königswinter

Basis-Paket Alternative 1: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 1“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Basis-Paket Alternative 2: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 2“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,-- zzgl. MwSt. statt € 1.390,-- zzgl. MwSt.

Impressum

Verlag:
ComConsult Technology Information Ltd.
ComConsult Research
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline 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