ComConsult Research

Der Netzwerk Insider

Dezember 2008

Systematische Weiterbildung für Netzwerk- und IT-Professionals

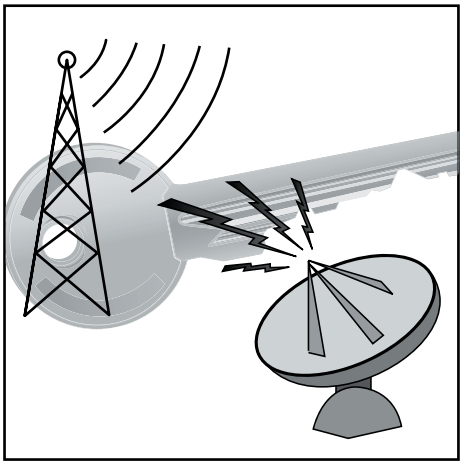
Schwerpunktthema

Sicherheitsaspekte öffentlicher Mobilfunknetze

Teil 1: Gefährdungen im öffentlichen Mobilfunk

von Dominik Zöller, Dr. Michael Wallbaum, Dr. Frank Imhoff

Der öffentliche Mobilfunk hat sich im Laufe seiner fünfzigjährigen Geschichte stark gewandelt. Vom handvermittelten, analogen A-Netz der 50er Jahre hin zum heutigen UMTS stieg die Leistungsfähigkeit der Netze im selben Maß wie ihre Beliebtheit. Mit der Einführung von GSM Anfang der 90er Jahre explodierten die Nutzerzahlen in ungeahntem Maß. Fallende Gebühren, die durch die günstigere digitale Netz-Technologie und die Entwicklung von Endgeräten als Massenware möglich wurden, trugen ebenso zu dieser Entwicklung bei, wie der steigende Mobilitätsdruck auf Arbeitnehmer wie Privatpersonen.



Mittlerweile ist das Mobiltelefon zur weltweiten Nummer Eins in Sachen Sprachkommunikation avanciert. Gerade im geschäftlichen Umfeld hat der Mobilfunk den Arbeitsalltag revolutioniert. Nie zuvor waren Mitarbeiter - unabhängig von ihrem Aufenthaltsort - derart in ihre Unternehmen eingebunden wie heute. Die Vorteile liegen auf der Hand. Anstelle starrer Terminplanungen kann jederzeit flexibel umdisponiert werden.

weiter auf Seite 25

Zweitthema

DCE, CEE, FcoE, iSCSI: zum Dritten

von Dr. Franz-Joachim Kauffels

Switch-Hersteller locken z.Zt. die Corporate Kunden mit erweiterten Funktionen der Ethernet-Basis, wie z.B. der Möglichkeit des Transports von Fibre Channel Daten zur allgemeinen Restrukturierung und Kostensenkung der RZ-Netze. Dabei fallen Schlagworte wie „Enhanced Converged Ethernet“ oder „Data Center Ethernet“.

Von der puren Leistung her gibt es sicherlich keinerlei wirklichen Probleme, denn mit 10 GBASE-LRM bekommen wir sehr viel Leistung zu einem geringen Preis und 40 GBASE ist schon näher als viele glauben. Sieht man sich aber die Funktionen genauer an, gibt es durchaus kritische Bereiche, wie „Lossless Ethernet“ oder „Congestion Control“, die längst noch nicht ausdiskutiert sind, und weitere Fragestellungen, wie z.B. was passiert, wenn man die räumlichen Grenzen des RZ verlassen möchte, sei es aus Gründen der asynchronen Datenspiegelung bis hin zur synchronen Desaster Recovery. Das sind spannende Themen, die alle Unternehmen und Organisationen ab einer gewissen Größenordnung betreffen.

weiter auf Seite 11

Neue Kongresse

Verkabelungs- und Infrastrukturforum 2009

Netzwerk Redesign Forum 2009

ab Seite 5

Geleit

Green-IT: hört auf mit dem Unfug!

ab Seite 2

Report-Neuerscheinungen

Videokonferenztechnik 2009

Microsoft Office Sharepoint Server

ab Seite 9

Zum Geleit

Green-IT: hört auf mit dem Unfug!

Mit jeder Veröffentlichung zu diesem Thema steigt mein innerlicher Ärger. Insbesondere, da die meisten Veröffentlichungen jeder systematischen und sachlichen Grundlage entbehren. Die absolute Spitze ist sicher die Diskussion über Green-Phones mit dem Hinweis, dass die großen Displays zu viel Strom verbrauchen (frei nach dem Motto: es lebe die Wählscheibe).

Hier treiben offensichtlich Aufmerksamkeit heischende „Experten“ und Journalisten, die auf der Suche nach einer Story jeden Müll unkontrolliert abdrucken, ein peinliches Spiel mit dem Markt.

Um dies auch sofort klar zu stellen: Umweltbewusstsein ist mir wichtig. Auch steht außer Frage, dass alle wirtschaftlich sinnvollen Maßnahmen zu Einsparungen ergriffen werden. Und wenn Maßnahmen zur Stromeinsparung speziell im Rechenzentrum wirtschaftlich sind, dann sollten sie auch unbedingt stattfinden.

Tatsächlich ist die gesamte Diskussion über Green-IT aber nicht nur durch zweifelhafte Studien mit häufig konstruierten Ergebnissen geprägt, sie ist vor allem dazu angetan, der Umwelt zu schaden.

Betrachtet man die Diskussion in anderen Ländern, dann wird man schnell auf den Begriff des ökologischen „Footprints“ kommen. Damit ist die Gesamt-Umweltbilanz eines Unternehmens gemeint. Und damit sind wir genau beim Thema.

Wer Umwelt ernst nimmt, der wird versuchen, mit einem optimalen Mitteleinsatz in möglichst kurzer Zeit ein möglichst optimales Gesamt-Ergebnis zu erreichen. In diesem Sinne ist es erforderlich, das Unternehmen im Rahmen einer Gesamtbilanz alle Bereiche möglicher Optimierungen zu analysieren.

Dazu gehören:

- Heiung und Klima
- Strom
- Warmwasser
- Reisekosten
- Abwasser

- Abluft
- alle anderen Formen von Umweltbelastungen

Kennt man die Umweltbilanz eines Unternehmens, kann man untersuchen, welche Investitionen zu welchem Umfang an Verbesserung führen. Der Witz an dieser Vorgehensweise ist, dass das Geld in die Projekte gesteckt wird, die am meisten aus dem Geld machen.

Green-IT ist neben den vielen falschen Berechnungen insofern kritisch, als dass mit diesem Begriff ein einzelner und noch dazu Mittel-intensiver Bereich herausgegriffen wird.

Hier besteht ein hohes Risiko, dass erhebliche Geldmittel in Projekte gesteckt werden, die an anderer Stelle wesentlich mehr bringen würden (siehe Solar-Anlagen für Heißwasser, Kraft-Wärme-Kopplungen usw). Hinzu kommt, dass fast alle Rechnungen die Umweltbelastung durch die Produktion und Entsorgung ignorieren. Es kann umwelttechnisch durchaus Sinn machen, eine weniger optimale Technologie weiter zu betreiben, da unter Berücksichtigung von Produktion und Entsorgung die neue Technologie keine messbaren Vorteile bringt.

Ein anderer Effekt der isolierten Green-IT-Betrachtung ist, dass wichtige technische Projekte blockiert werden. Das Paradebeispiel ist hier das Green-Phone. Mal unabhängig von der gerade hier nachweisbaren Manipulation von Zahlen muss man doch feststellen, dass gerade moderne Telefonie-Lösungen in der Regel das Ziel haben, die Effizienz von Kommunikation zu verbessern. Eine erhöhte Effizienz in der Team-Kommunikation kann aber erhebliche Auswirkungen auf ein Umwelt-Profil haben: Reisekosten können eingespart werden, Fehler in Entwicklung und Produktion können reduziert werden, Produkte können besser am Bedarf des Kunden ausgerichtet werden.

Auch wenn diese Einsparungen durch Team-Effizienz häufig nicht in Euro belegt werden können, erscheint es ein wenig absurd, wenn Einspar-Potenziale von wenigen Watt (dann auch noch auf der falschen Seite des Netzteiles gemessen) pro Endgerät als Argument vergewaltigt werden, solche Effizienz-Ziele in Frage zu stellen. Eine einzige eingesparte Dienstreise pro Jahrzehnt würde vermutlich ausreichen, um diese an den Haaren herbei gezogene Argumentation zum Kippen zu bringen.

Also zum Abschluss und Fazit:

- ein klares Statement für Wirtschaftlichkeit: wenn die Einsparung von Strom im Rahmen der normalen Berechnung wirtschaftlich ist, sollte sie sofort umgesetzt werden. Dies gilt insbesondere bei sowieso stattfindenden Neubeschaffungen (natürlich ist die Entwicklung von Netzteilen mit einem höheren Wirkungsgrad oder von Server-Intensivierung durch Virtualisierung zu begrüßen)
- ein klares Bekenntnis zur Umwelt: Unternehmen sollten im Rahmen eines Gesamt-.Umwelt-Profils ihre Investitionen in Umweltmaßnahmen an den Stellen tätigen, die am meisten Umwelt-Ertrag erbringen und nicht in Bereichen, in denen am lautesten geschrieen wird

In diesem Sinne auf ein umweltbewusstes Jahr 2009

Ihr
Dr. Jürgen Suppan

Top-Seminar

Sonderveranstaltung Wireless Technologie

Die ComConsult Akademie veranstaltet vom 15.12. - 16.12.08 ihre Sonderveranstaltung „Wireless Technologie“ in Düsseldorf.

Die Verfügbarkeit neuer Chip-Generationen hat den Markt für Wireless-Produkte speziell im Bereich Controller-basierter 802.11n-Lösungen über die letzten Wochen und Monate explodieren lassen. Aktuelle Tests aus den USA zeigen eine Verzehnfachung des Durchsatzes gegenüber der älteren 11a und 11g-Technologie.

Mit den neuen Produkten und der gestiegenen Leistung steigen aber auch die Herausforderungen:

- die Einbindung alter Technologien ist eine Herausforderung
- Planung ist deutlich aufwendiger geworden
- Fehlersuche und Messtechnik müssen sich der neuen Situation stellen
- die Produktangebote der Hersteller wirken immer ähnlicher, unterscheiden sich aber im Detail erheblich

Unter anderem werden folgende Themen aufgegriffen:

Industrial WLAN / WLAN in der Automatisierung
- Warum sich das Design unterscheidet
- Wie mit Echtzeitanforderungen umgegangen werden kann
- Welche spzifischen Mechanismen zur Absicherung erforderlich sind

Mesh Networks
- Wie funktioniert IEEE 802.11s?
- Welche Herstellerlösungen gibt es und wie unterscheiden sie sich vom kommenden Standard?
- Planung von Mesh Networks
- Problembereiche Durchsatz und Delay
- Anwendungsbereiche von Mesh Networks

Controller Design
- Vor und Nachteile eines Tunnels für den Nutzerverkehr
- Absicherung der Kommunikation zwischen Access Points und Controller
- Architekturvarianten für den Aufbau von Controller-Lösungen
- Wo unterscheiden sich die Hersteller?
- Was bringt CAPWAP und was unterstützen hier schon die Hersteller?

Fixed Mobile Integration
- Planung sprachtauglicher WLAN
- Lösungen der Hersteller im Vergleich
- Sicherheitsproblematik bei der Integration von Smartphones

WLAN-Planung
- Frequenzplanung
- Aufbau eines Frequenzstandards
- Betrieb mehrerer geographisch benachbarter / überlappender WLANs
- Trennung von Nutzergruppen
- Werkzeuge zur WLAN-Planung
- Techniken zur Ausleuchtung und Simulation

Fremdsysteme bei 2,4 GHz
- Störungen im 2,4 GHz und wie man damit umgeht
- Welche anderen Systeme bei 2,4 GHz operieren und wie ein WLAN dadurch beeinflusst werden kann
- Wie moderne Bluetooth-Systeme die Störung von WLAN-Systemen vermeiden können
- Herstellerspezifische Bluetooth-Erweiterungen
- RFID bei 2,4 GHz
- ZigBee

Werkzeuge zur WLAN-Überwachung
- Was wird wirklich gebraucht?
- Empfehlungsliste für Unternehmen
- Werkzeug-Einsatz

Versäumen Sie nicht, sich jetzt noch in dieser herausragenden Sonderveranstaltung einen Platz zu sichern.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Wireless Technologie

Ich buche die Sonderveranstaltung
☐ **Wireless Technologie**
15.12. - 16.12.08 in Düsseldorf
zum Preis von € 1.490,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer

vom_____ bis_____08

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

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

Programmübersicht Wireless Technologie

Montag, den 15.12.2008

10:00 - 11:00 Uhr
Industrial WLAN / WLAN in der Automatisierung
- Warum sich das Design unterscheidet
- Wie mit Echtzeitanforderungen umgegangen werden kann
- Welche spezifischen Mechanismen zur Absicherung erforderlich sind

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

11:30 - 12:15 Uhr
Fremdsysteme bei 2,4 GHz
- Störungen im 2,4 GHz und wie man damit umgeht
- Welche anderen Systeme bei 2,4 GHz operieren und wie ein WLAN dadurch beeinflusst werden kann
- Wie moderne Bluetooth-Systeme die Störung von WLAN-Systemen vermeiden können
- Herstellerspezifische Bluetooth-Erweiterungen
- RFID bei 2,4 GHz
- ZigBee

Björn Korall, ComConsult Beratung und Planung GmbH

12:15 - 13:00 Uhr
Werkzeuge zur WLAN-Überwachung
- Was wird wirklich gebraucht?
- Empfehlungsliste für Unternehmen
- Werkzeug-Einsatz

Björn Korall, ComConsult Beratung und Planung GmbH

14:30 - 16:00 Uhr
Mesh Networks
- Wie funktioniert IEEE 802.11s?
- Welche Herstellerlösungen gibt es und wie unterscheiden sie sich vom kommenden Standard?
- Planung von Mesh Networks
- Problembereiche Durchsatz und Delay
- Anwendungsbereiche von Mesh Networks

Dr. Franz-Joachim Kauffels, unabhängiger Unternehmensberater

16:30 - 17:15 Uhr
WLAN-Planung
- Frequenzplanung
- Aufbau eines Frequenzstandards
- Betrieb mehrerer geographisch benachbarter / überlappender WLANs
- Trennung von Nutzergruppen
- Werkzeuge zur WLAN-Planung
- Techniken zur Ausleuchtung und Simulation

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

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

Dienstag, den 16.12.2008

9:00 - 9:45 Uhr
Controller Design: Stand der Technik und Trends
- Vor- und Nachteile eines Tunnels für den Nutzerverkehr
- Absicherung der Kommunikation zwischen Access Points und Controller
- Architekturvarianten für den Aufbau von Controller-Lösungen
- Wo unterscheiden sich die Hersteller?
- Was bringt CAPWAP und was unterstützen hier schon die Hersteller?

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

9:45 - 10:30 Uhr
Controller Design im Detail: Vergleich einer Planung mit Cisco und Trapeze

Michael Schneiders, ComConsult Beratung und Planung GmbH

Herstellerpräsentationen WLAN Controller
- Positionierung zu CAPWAP
- IEEE 802.11n und Pre-N im Controller-basierten Design
- Unterstützung von IEEE 802.1X Supplicants im Access Point
- Mehrwert für Wireless Unified Communications durch Controller-design?
- Wie passen Mesh und Controller zusammen?
- Security und schnelles Roaming: Einschätzung von IEEE 802.11r
- Controller-basiertes WLAN-Design und Automatisierung (WLAN in PROFINET und Ethernet/IP)?

11:00 - 11:30 Uhr
Cisco Systems GmbH, Wolfram Maag

11:30 - 12:00 Uhr
Enterasys Networks Deutschland GmbH, Dipl.-Ing. Markus Nispel

12:00 - 12:30 Uhr
LANCOM Systems GmbH, Frank Janssen

12:30 - 13:00 Uhr
Wireless LAN-Komponenten in der Automation
- Anforderungen an WLAN-Komponenten im Automatisie-rungsbereich
- Profinet-Integration
- Projektbeispiele
- Rolle von IEEE 802.11n

Hirschmann Automation & Control GmbH, Olaf Schilperoort

14:30 - 15:15 Uhr
Fixed Mobile Integration
- Planung sprachtauglicher WLAN
- Lösungen der Hersteller im Vergleich
- Sicherheitsproblematik bei der Integration von Smartphones

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:15 - 16:00 Uhr
Wirtschaftlichkeit der Nutzung von WLAN zur Telekommunikation

Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH

Kaffeepause: 10:30 - 11:00 Uhr
Mittagspause: 13:00 - 14:30 Uhr
Ende der Veranstaltung: 16:00 Uhr

Der Veranstalter behält sich Änderungen im Programm vor!

Aktueller Kongress

Netzwerk-Redesign Forum 2009

Die ComConsult Akademie veranstaltet vom 09.03. - 12.03.09 ihren Kongress „ComConsult Netzwerk-Redesign Forum 2009“ in Königswinter.

Netzwerke sind der Lebensnerv unserer Unternehmen. Sie unterliegen einer permanenten Weiterentwicklung und Veränderung. Aus einem Mix aus Bedarf und technischen Möglichkeiten muss das individuelle Optimum für ein Unternehmen gefunden werden. Dieses Optimum muss zugleich an der Zukunft orientiert sein, da Netzwerk-Komponenten über einen langen Zeitraum stabil und ohne permanente Änderungen betrieben werden müssen.

Hier setzt das ComConsult Netzwerk-Redesign Forum 2009 an. Es analysiert die wichtigsten Bedarfsentwicklungen, stellt diesen die neuesten Netzwerk-Technologien gegenüber und erarbeitet Empfehlungen für ein erfolgreiches Netzwerk-Design, eine Zukunfts-oriente Auslegung und einen stabilen und zuverlässigen Betrieb.

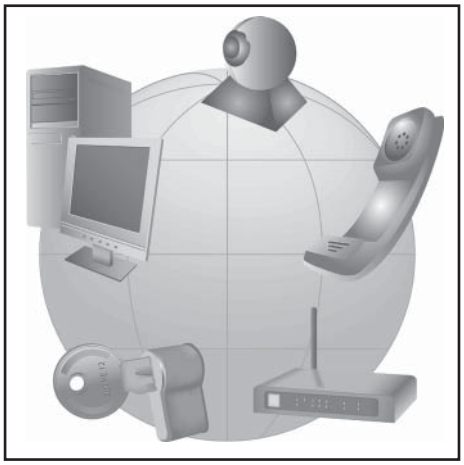
Die Schwerpunktthemen des ComConsult Netzwerk-Redesign Forums 2009 sind:

Neue Redundanz-Verfahren
Wieder einmal sind Redundanz-Verfahren im Mittelpunkt der Diskussion. Immer wieder wird in Projekten eine Art von Netzwerk-Redundanz gefordert, die laufende Sprach- und Video-Verbindungen nicht unterbricht. Dies wird häufig mit Umschaltzeiten von unter 100 ms verbunden. Traditionelle Redundanz-Verfahren leisten sich Umschaltzeiten bis in den Minuten-Bereich und stehen immer häufiger in der Kritik.

Wir analysieren:

- Was ist Stand der Redundanz-Technik in Layer-2 und Layer-3?
- Was kommt auf uns zu?
- Was passiert im direkten Umfeld von Server und Speicher-Systemen?
- Welchen Stellenwert haben Hersteller-Spezifische Lösungen?
- Cisco, Enterasys, Extreme, Foundry, HP, Juniper, Nortel: wer macht was?
- Standardisierung: was ist Zukunfts-orientiert, wie können Investitionen und ein stabiler Betrieb geschützt werden?

Layer-2 kontra Layer-3
Ein altes Thema, aber wieder hochaktuell. Immer wieder besteht der Bedarf nach großen und auch Flächen-deckenden Layer-2-Netzwerken. Zum Teil wird auch eine Layer-2-Verbindung zwischen Standorten



gefordert. Rechenzentren, Industrie-Umgebungen und Remote Speicher-Kopplungen sind Beispiele dafür.

Wir analysieren:

- Große Layer-2-Netzwerke: wo liegen die Probleme heute?
- Integration oder Parallelbetrieb mit Layer-3: welche Optionen bestehen?
- Standort-Kopplungen mit Layer-2: Proprietär kontra Standard, welcher Weg ist Zukunfts-orientiert?

Verkabelung 2009
Cat 6, 6a, 7, 7a, immer mehr Stecker-Alternativen, Multimode OM2, OM3, OM4, auch hier immer mehr Alternativen im Stecker. Dies kombiniert mit Anforderungen im Rechenzentrum für 10 und zukünftig 40 Gigabit: wie sieht die Zukunfts-sichere Verkabelung aus? Betrachtet man die zu erwartende Nutzungsdauer von 10 Jahren und mehr, dann muss bei Neuinstallationen auch 100 Gigabit berücksichtigt werden. Die aktuellen und in Arbeit befindlichen Standards bieten viele Alternativen, doch welche werden sich durchsetzen? Schon heute unterstützen nicht alle Hersteller alle Varianten.

Wir analysieren:

- Verkabelungstechnik 2009: wo stehen wir?
- Twisted Pair: welche Kabel-Qualität, welcher Stecker?
- Glasfaser: Multimode kontra Singlemode, OM2 kontra OM3 kontra OM4, welcher Stecker prägt die Zukunft?
- Was unterstützen die Hersteller?
- Hoher Bestand aus Cat 5 oder Cat 6 und OM2: was ist zu tun?

MPLS kontra Carrier-Ethernet kontra OSPF
Mit Carrier-Ethernet geht ein neuer Stern am Horizont auf. Dabei ist der Name mehr als irreführend, da die Technologie nicht auf Carrier begrenzt ist. Real ist die Technologie in verschiedensten Einsatz-Szenarien interessant. Diese reichen vom Corporate-Netzwerk zwischen verschiedenen Standorten über große Backbone-Netzwerke bis hin zu Spezial-Anwendungen im Industrie-Bereich. Carrier-Ethernet realisiert standardisierte Layer-2-Netzwerke mit extrem kurzen Umschaltzeiten in der Redundanz. Damit ist auch die Basis für jede denkbare Diskussion gelegt (siehe: Layer 2 kontra Layer 3).

Wir analysieren:

- Was ist Carrier-Ethernet, für wen ist es eine Option?
- CE kontra MPLS: ist dies das Ende von MPLS?
- CE im Unternehmens-Backbone: wirklich eine Alternative?
- Große Layer-2-Netzwerke in der Industrie: wird CE die bisher dort dominierenden Verfahren verdrängen?

Wireless-Netzwerke
Atheros hat das Ende von 802.11g eingeläutet. 802.11n ist nun das Maß aller Dinge. Gleichzeitig werden Wireless-Switches in professionellen Installationen fast unvermeidbar. Dies kombiniert mit besonderen Anforderungen spezieller Umgebungen von der Industrie bis zur Filial-Organisation ergibt einen brisanten Technologie-Mix.

Wir analysieren:

- Was passiert zurzeit bei Wireless-Technologien, wohin geht der Weg?
- Was leistet 802.11n? Als Ersatz für Kabel-gebundene Netzwerke geeignet?
- Strombedarf der Access-Points: ein Auswahl-Kriterium?
- Wie viele Radioteile sind für eine Zukunfts-Orientierung sinnvoll?
- Was leisten Wireless-Switches? Wo unterscheiden sich die Produkte? Zeit für einen Standard, wo steht CAPWAP?
- Ist MESH die Zukunft? Ist dies mehr als eine Wireless-Technologie, ist dies die Basis für eine neue Art von Kommunikations-Architektur?
- Wireless LAN in der Industrie: was ist anders?
- Wireless LAN in Filial-Organisationen: welche Technologie ist optimal?

Netzwerk-Redesign Forum 2009

Sicherheit
Der Bedarf nach Sicherheit wächst immer weiter. Dies umfasst sowohl die Kontrolle des Zugangs zu wichtigen Servern, Applikationen und Daten als auch die Verhinderung einer gegenseitigen Beeinflussung von Applikationen im Netzwerk. In keinem Fall darf ein Fehlverhalten einer Applikation oder eines Benutzers andere Applikationen oder Benutzer stören. Die technologischen Ansätze im Bereich Sicherheit sind weitreichend und vielfältig, aber zum Teil Hersteller-gebunden und inkompatibel. Wie kann man hier zu einer sinnvollen und noch beherrschbaren Lösung kommen?

Wir analysieren:

- Was bietet der Markt?
- Was leisten neue Standards wie MACsec und 802.1X-REV?
- Wie können Benutzer- und Applikationstrennung realisiert werden?
- NAC, 802.1x und ähnliche Technologien: wie kann in diesem Wald aus Hersteller-spezifischen und zum Teil nicht kompatiblen Lösungen ein sinnvoller und angemessener Weg gefunden werden, der nicht zum Overkill wird?

Integration mobiler Mitarbeiter/Fixed-Mobile-Konvergenz
Einbindung aller relevanten Mitarbeiter in die wichtigen Geschäftsprozesse, egal wo sich diese befinden. Das Thema ist nicht neu, aber die technischen Möglichkeiten verändern sich. Mehr Bandbreite, neue Gerätetechnologien, andere Applikations-Architekturen schaffen die Voraussetzung für mehr Effizienz und Erfolg mobiler Mitarbeiter.

Wir analysieren:

- Fixed-Mobile-Konvergenz: was bedeutet das?
- Wohin geht der weitere Weg? Wie groß sind die Potenziale wirklich?
- Wie gut und nutzbar sind die Produkte?

WAN-Redesign
Weiterverkehrs-Konzepte sind im Umbruch. Das zunehmende Angebot von Gigabit Ethernet in Ballungsräumen, der weitere Verfall der Preise, das alles schafft die Basis für neue IT-Architekturen. Wichtige neue Anwendungsbereiche wie SOA basieren auf dieser Weiterentwicklung. Desaster Recovery bekommt ohne Frage eine neue Dimension.

- Wir geben den Überblick: was passiert im WAN?
- Welche Leistungen entstehen, wie weit kann das gehen?

Das ComConsult Netzwerk-Redesign Forum 2009 ist die zentrale Netzwerk-Veranstaltung des Jahres 2009. Sie ist für jeden Entscheider, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Sichern Sie sich rechtzeitig einen Platz in dieser herausragenden Veranstaltung!

Netzwerk-Redesign Forum 2009
Frühbucherrabatt
bis 31.12.2008

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2009

Ich buche den Kongress
Netzwerk-Redesign Forum 2009
09.03. - 12.03.09 in Königswinter

☐ mit „Ein-Tages-Intensiv-Trainings zum Preis von € 2.090,-* zzgl. MwSt.

☐ ohne „Ein-Tages-Intensiv-Trainings zum Preis von € 1.690,-* zzgl. MwSt.

*gültig bis zum 31.12.08 - dann regulärer Preis € 2.290,- bzw. 1.890,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Neuer Kongress

ComConsult Verkabelungs- und Infrastrukturforum 2009

Die ComConsult Akademie veranstaltet vom 27.04 - 28.04.09 ihren Kongress „ComConsult Verkabelungs- und Infrastrukturforum 2009“ in Bonn.

Ist die Planung und Realisierung einer anwendungsneutralen Kommunikationsverkabelung nach fast 15 Jahren Standardisierung noch eine Herausforderung? Die Frage ist mit „ja“ zu beantworten. Die für den Bürobereich entwickelte und normierte „Datenverkabelung“ hat einen Erfolg und einen Verbreitungsgrad ohnegleichen erlebt, sie wird als passive Basis eingesetzt zur Sprachkommunikation, Rechenzentrumsverkabelung, Vernetzung von Industrieanlagen und mehr. Doch lassen sich die bisherigen, allseits bekannten Regeln auch auf diese Bereiche übertragen? Die Antwort muss „nein“ sein, die Anforderungen in diesen Bereichen unterliegen nicht immer den gleichen Anforderungen, die Maxime „Gigabit/s-und-mehr“ um jeden Preis ist out. Datenrate ist nicht mehr alleine ein Kriterium für eine gute IT-Verkabelung, verstärkt wird auf Einfachheit und Zuverlässigkeit gesetzt. Dieses erfordert aber teilweise eine Abkehr von bisherigen Planungs- und Realisierungsumsetzungen, nur mit Kenntnis dieser veränderten Technologieanforderungen kann die IT-Verkabelung der Zukunft den neuen Herausforderungen begegnen.

Das ComConsult Verkabelungs- und Infrastrukturforum 2009 analysiert die Technologie-, Markt- und Produktsituation für neue und zukünftige Verkabelungsstrategien und gibt wesentliche Empfehlungen sowohl zur Aktualisierung bestehender als auch zur Umsetzung neuer Infrastrukturen.

Im Einzelnen geht das Forum auf folgende Fragen ein:

- Welche Anforderungen müssen Verkabelungslösungen erfüllen, um die Einführung von neuen Techniken der Gebäudemelde- und Leittechnik zu vereinfachen, warum kann der Normungsansatz der EN50173 hier nicht vollständig greifen?
- Haben die Verkabelungsnormierungen einen Stand der Vollständigkeit erreicht, wo steht die EN 50173 heute?
- Nichts neues aber trotzdem für viele etwas Unbekanntes: Warum gehört in ein Rechenzentrum eine strukturierte Verkabelung und wie ist diese sinnvoll aufzubauen?

- Lassen sich vorhandene und neue Verkabelungssysteme mit Kupferverkabelungen für 40 Gbit/s oder 100 Gbit/s nutzen, wo wird die Leistungsfähigkeit von Twisted Pair das Ende erreicht haben?
- Für welche Bereiche in der Industrieverkabelung muss mit einem neuen Planungsansatz gerechnet werden, warum kann die Technik der Office-Verkabelung nur bedingt in einer Industrie-Umgebung eingesetzt werden?
- Warum stellt der Consolidation Point ein wenig bekanntes, aber effizientes „neues“ Teilelement der Datenverkabelung dar?
- Wie sehen moderne Installationsrichtlinien aus, welche typischen Fehler müssen durch diese verhindert werden? Wie weit lassen sich Richtlinien international nutzen?
- Welche neuen Entwicklungen gibt es in der Messtechnik für Kupfer und LWL?
- Arbeitsplatzverkabelung: Glasfaser kontra Kupfer. Ist eine Abkehr von der Lösung „Glasfaser bis zum Arbeitsplatz“ festzustellen? Haben sich die Prognosen zur Zukunftssicherheit bei beiden Medien bewahrheitet?
- Dokumentation mit EXCEL und CAD, reicht das aus? Welchen Mehrwert bringen komplexe Dokumentationslösungen, wie lassen sich intelligente Verkabelungssysteme einsetzen?

Dieses Forum bietet die ideale Basis für eine Standortbestimmung. Wer immer sich für die zukünftigen neuen Aufgaben einer Kommunikationsverkabelung vorbereiten muss, wer nach sinnvollen Alternativen und Empfehlungen für optimale Lösungen sucht, der sollte dieses Forum nicht verpassen.

ComConsult-Foren zeichnen sich durch ein hohes Maß an Herstellerneutralität und ein großes Potenzial an kontrovers geführten Diskussionen aus, zögern Sie nicht, sich einen Platz auf dieser herausragenden Veranstaltung zu sichern.

Folgende Vorträge sind geplant (Änderungen vorbehalten!):

- Videoüberwachung mit Hilfe von Lokalen Netzwerken
- Gigabit-Netzwerk-Technologien und ihre Anforderungen an Kabel und Anschlusstechnik: Anforderungen bei Einführung von mehr als 10 Gbit/s über Kupfer
- Kabelstandardisierung: was ist neu, was passiert hinter den Kulissen
- Installations-„Sünden“ bei der Kommunikationsverkabelung
- Nutzbarkeit von modernen Kommunikationsverkabelungen für Meldeanlagen und Automatisierungsbereiche
- Sanierung bestehender Verkabelungen in Rechenzentren und Serverräumen: wo und wann besteht Bedarf, welche Vorgehensweise ist zu empfehlen, welche Alternativen bestehen
- Elektrische Sicherheit beim Redesign von RZ-Infrastrukturen
- Green IT im RZ
- Netzwerk-Dokumentation gestern & heute
- Normen und Standards zur Messtechnik: Notwendigkeit, Defizite und Ergänzungen
- Zukunftssicherheit durch Glasfaser bis zum Arbeitsplatz, Illusion oder Realität?
- Moderner Brandschutz bei IT-Verkabelung; Lösungen, Techniken und Gefahren

ComConsult Verkabelungs- und Infrastrukturforum 2009

Frühbucherrabatt bis 15.01.09

ComConsult Verkabelungs- und Infrastrukturforum 2009

27.04. - 28.04.09 in Bonn

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir Ihnen exklusiv eine Vorbuchungsphase für das ComConsult Verkabelungs- und Infrastruktur-forum 2009 bis zum 15.01.2009 für eine rabattierte Teilnahmegebühr an.

ComConsult Verkabelungs- und Infrastrukturforum 2009
zum Preis bei Buchung bis 15.01.09 von € 1.490,-
statt regulär € 1.690,- zzg. MwSt.

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

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult Verkabelungs- und Infrastrukturforum 2009

Ich buche den Kongress
☐ **ComConsult Verkabelungs- und Infrastrukturforum 2009**
27.04. - 28.04.09 in Bonn
zum Preis von € 1.490,-* zzgl. MwSt.

*gültig bis zum 15.01.09 - dann regulärer Preis € 1.690,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer

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

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

Neuer Report

Videokonferenztechnik 2009:
Wie finde ich das optimale Produkt für mein Unternehmen?

Soeben ist die neue Studie „Videokonferenztechnik 2009: Wie finde ich das optimale Produkt für mein Unternehmen?“ von Dr. Jürgen Suppan erschienen.

Dieser Report dient nicht zur Bewertung einzelner Produkte, auch wenn der Begriff Telepresence im Markt eng mit der Firma Cisco Systems in Verbindung gebracht wird. Real bieten zurzeit mehrere Hersteller Telepresence- und HD-Konferenz-Produkte an. Tatsächlich beobachten wir einen Trend, in dem nahezu alle Anbieter anfangen, diesen Begriff für neue Produkte zu nutzen.

Ziel dieses Reports ist es, eine Hilfestellung bei der generellen Technologie-Entscheidung pro oder kontra Telepresence bzw. pro oder kontra HD-Videokonferenz zu liefern. Gleichzeitig haben wir analysiert, von welchen Faktoren die Akzeptanz und die Wirtschaftlichkeit von Videokonferenz-Lösungen geprägt sind.

Videokonferenz-Lösungen liefern heute eine Qualität, die vor kurzer Zeit noch undenkbar war. In Kombination mit einer deutlich vereinfachten Bedienung bieten moderne Produkte somit fast die Qualität eines persönlichen Gesprächs. Speziell Telepresence-Lösungen haben dabei in den letzten Monaten erheblich dazu beigetragen, dass die Akzeptanz von Videokonferenzen wieder deutlich gestiegen ist. Hohe Raumauslastungen sind die Folge. Dabei kann Akzeptanz mit Wirtschaftlichkeit gleichgesetzt werden. Im Endeffekt kann Wirtschaftlichkeit nur in Kosten pro Sitzung berechnet werden. Auch sehr teure Lösungen können dabei Kosten von unter 300 Euro pro Sitzung erreichen. In Kombination mit den stetig fallenden Preisen der Produkte sollte somit die Voraussetzung für eine goldene Zukunft der Videokonferenzen gelegt sein.

Folgende Themenschwerpunkte werden in diesem Report behandelt:

- Wir analysieren die Bausteine einer Gesamtlösung für verteilt arbeitende Teams und speziell den Stellenwert der Telepresence und der HD-Videokonferenz innerhalb dieser Bausteine
- Wir untersuchen die Anforderungen an eine hohe Akzeptanz von Videokonferenz-Lösungen
- Wir diskutieren den Bereich Offenheit und seine Auswirkungen auf Wirtschaftlichkeit
- Wir erklären die Bedeutung von Telepresence und die technischen Unterschiede zwischen 720p und 1080p-Technologie und leiten daraus die Antwort zur Frage ab, ob wir Telepresence brauchen
- Wir erläutern typische Ansätze zur Wirtschaftlichkeitsberechnung und zeigen an einem Ansatz im Detail, wie groß die Potenziale von Videokonferenztechnik auch für kleinere Unternehmen inzwischen sind

Die Aussagen in diesem Report basieren auf Tests mit mehreren Videokonferenz-Produkten in unseren Labors in Aachen und Christchurch. Parallel wurden diverse Gespräche und Diskussionen mit führenden Herstellern geführt, um deren Strategien zu evaluieren und technische Fragen zu klären.

---------- SUBSKRIPTIONSANGEBOT ----------

Bei Bestellung bis zum 05.12.08 zahlen Sie nur € 168,-- zzgl. MwSt. und Versand

Fax-Antwort an ComConsult 02408/955-399

Bestellung
Videokonferenztechnik 2009

Ich bestelle den Report
☐ **Videokonferenztechnik 2009:**
zum Subskriptionspreis von € 168,-*
*gültig bis zum 05.12.2008 -
dann regulär € 198,-

(Preise zzgl. MwSt. und Versand)

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Neuer Report

Microsoft Office Sharepoint Server

In diesem Monat erscheint der neue Report „Microsoft Office Sharepoint Server“ von ComConsult Research.

Mit dem Microsoft Office Sharepoint Server (MOSS) bietet Microsoft ein umfangreiches Kollaborations-Portal. Dieses deckt eine große Spannbreite an Einsatzszenarien ab. So werden verteile Projektteams ebenso optimal unterstützt wie diverse lokale Intranet-Szenarien. Doch gerade die große Spannbreite wirft auch Fragen auf: wie komplex ist die Einrichtung, wie gut die Integration in die normalen Arbeitsabläufe, wie leicht die Bendienung durch den Endbenutzer, wie sieht die technische Integration in Office, Outlook und andere Tools aus?

Dieser technisch orientierte Report wendet sich an Entscheider und Planer, die eine Kollaborations-Plattform im Unternehmen einführen wollen. Er beschreibt und analysiert, welche Möglichkeiten der Kollaboration sich durch den Einsatz einer

Microsoft MOSS 2007 Farm im Unternehmen ergeben.

Der Report beschreibt die Funktionsbereiche des MOSS 2007 und analysiert den Mehrwert bei der Verwendung dieser Features. Es wird dargestellt, wie die Integration des MOSS 2007 in das Microsoft Office erfolgen kann und welche Rolle der SharePoint Designer bei der Erstellung von MOSS 2007 Webseiten einnimmt. Empfehlungen für den leistungsgerechten Aufbau der notwendigen Server-Farm werden genauso ausgesprochen wie die Vorstellung der dabei nutzbaren Hilfsmittel. Weiterhin wird der Frage nach der Rolle des MOSS 2007 in der UC-Strategie von Microsoft nachgegangen und es erfolgt ein Rechenbeispiel für die Lizenzierungskosten.

Die nachfolgend aufgeführten Kapitel sind Teil des Reports:

- Funktionsumfang
- MOSS 2007 und Microsoft Office
- Planungsaspekte
- Customizing & Design von Portalseiten mit SharePoint Designer

Der Autoren dieses Reports sind Spezialisten der ComConsult Beratung und Planung GmbH.

---------- SUBSKRIPTIONSANGEBOT ----------

Bei Bestellung bis zum 05.12.08 zahlen Sie nur € 348,-- zzgl. MwSt. und Versand - danach den regulären Preis von € 398,-- zzgl. MwSt. und Versand

Fax-Antwort an ComConsult 02408/955-399

Bestellung
Microsoft Office Sharepoint Server

Ich bestelle den Report
☐ **Microsoft Office Sharepoint Server**
zum Subskriptionspreis von € 348,-*
*gültig bis zum 05.12.2008 -
dann regulär € 398,-

(Preise zzgl. MwSt. und Versand)

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

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

Zweitthema

DCE, CEE, FcoE, iSCSI : zum Dritten

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.

Im Insider des Monats Juni gab es bereits einen Artikel von Dr. Moayeri zum Thema iSCSI vs. FCoE und von mir zu I/O-Konsolidierung und FCoE. Diese Artikel haben neue Fragestellungen aufgeworfen, die hier betrachtet werden sollen. Niemand kann garantieren, dass das der letzte Artikel zu diesem Thema ist. Erschwerend könnte noch hinzukommen, dass uns durch Allianzen von Herstellern in bestimmten Umfeldern eine bestimmte Technologie vor die Nase gesetzt werden könnte.

Heute geht es um folgende Fragestellungen:

- Die Herstellerstrategien wie DCE oder CEE führen mit FCoE neue Übertragungsalternativen im RZ ein. Die dadurch entstehenden Vorteile der I/O-Konsolidierung sind einleuchtend und wurden in den o.g. Artikeln dargestellt. Allerdings wird in diesem Zusammenhang der Begriff „Lossless Ethernet“ ziemlich locker eingeführt. Schaut man genau hin, merkt man, dass „Lossless“ noch nicht einmal ordentlich definiert ist und die Herbeiführung von „Lossless Ethernet“ alles andere als trivial ist.

- Die Hersteller geben in weitgehender Übereinstimmung mit aktuellen Arbeiten von IEEE 802.1 einen Weg an, mit dem „Lossless Ethernet“ erreicht werden soll. Die Basis hierbei ist Prioritäts-basierendes Congestion Management, aufgeteilt in Congestion Control und Congestion Notification. Funktioniert dieser Weg wirklich? Und vor allem: funktioniert er hier und jetzt?

- Was müssen wir machen, wenn der Weg der Hersteller sich als Sackgasse erweist? Müssen wir dann die I/O-Konsolidierung knicken oder gibt es realistische Alternativen?

- Was passiert, wenn wir im Rahmen einer Motivationslage, die ein weites Spektrum umfassen kann, das geographisch eng umgrenzte Gebiet des RZs verlassen möchten? Können wir dann immer noch auf iSCSI und/oder FciE setzen oder brauchen wir da wieder etwas anderes?

Die ersten drei Fragestellungen werden wir hier und heute nach aktuellem Stand der Technik komplett abarbeiten. Die letzte kann nur in Form einer Übersicht angerissen werden. Zunächst möchte ich aber etwas den Wind aus der Diskussion „FCoE versus iSCSI“ nehmen.

1. iSCSI vs. FCoE: Unentschieden!

Wem DCE, CEE und FCoE zu kompliziert ist, kann natürlich iSCSI für den Transport von Speicherdaten über ein RZ-Netz nehmen, weil hier durch die Einbeziehung der TCP-Schicht die Lossless-Problematik nicht evident ist. Da gibt es ja im Internet wüste Diskussionen, ich sehe aber in keinem Falle wirklich eine Substitutionskonkurrenz. Wer heute mit Systemen bis zum mittleren Leistungsbereich arbeitet und iSCSI einsetzt, hat überhaupt keinen Grund, auf FCoE zu gehen. Wer seit Jahren FC betreibt, findet FCoE spannend, aber wird kaum auf den Gedanken kommen, auf iSCSI zu migrieren. (siehe Abbildung 1.1)

Persönlich sehe ich den Kampf der Systeme iSCSI vs. FCoE erst beginnen, wir befinden uns hier noch bei Scharmützeln im Vorfeld. Viele sind ja immer noch der Meinung, dass iSCSI ohnehin nur für geringere Leistungsanforderungen geeignet ist, weil es einen Prozessor, z.B. in einem Server, erheblich belastet. Aber schon im Sommer 2008 wurde klar, dass man das auch anders machen kann. HP hat mit „Accelerated iSCSI“ eine Lösung gezeigt, die auf Hardware-Beschleunigung in entsprechenden Adapterkarten basiert. Diese Lösung konnte auf einer 1 GbE-Verbindung das theoretische Durchsatzmaximum von fast 900 Mbit/s. Speicherverkehr erreichen. Dabei wurde die Belastung des Server-Prozessors deutlich

	iSCSI	**FC**	**FCoE**
Einsatzbereich	Heute <= 2 Gbps	Heute > 2 Gbps	Ziel > 2 Gbps
Reifegrad	Ausgereift, bewährt	Ausgereift, bewährt	Neu
Vorzüge	Stabil auf TCP	Stabil, viele Zusatzfunktionen	FC-Funktionen auf Ethernet
Komplexität im Netz	Wie jede TCP-Anwendung	Sehr gering	Gering
Anforderungen an Ethernet	Wie jede TCP-Anwendung	N/A	Lossless Ethernet
Anforderungen an Prozessor	Hoch, TCP-Abarbeitung muss schnell sein	Mittel wegen sehr hoher Strukturierung	Kein wesentliches Premium gegenüber gleichem FC
Netz mindestens	1 GbE	2 oder 4 GbFC	10 GbE

Abbildung 1.1: iSCSI vs FC vs FCoE

um über 50% gesenkt. Es gab auch Versuche mit einer Duplex-Verbindung, die es immerhin auf fast 1,6 Gbit/s. Speicherverkehr gebracht haben. Wenden wir nun Moore´s Law auf diese Konstruktion an, wird es weniger als drei Jahre dauern, bis man iSCSI auch mit 10 GbE sinnvoll betreiben kann. Also, ca. 2010 können wir damit bestimmt rechnen.

Ein wesentliches Argument gegen iSCSI ist ja, dass die Abarbeitung des TCP-Protokolls zu lange dauert und den Prozessor des betroffenen Speichersystems oder Servers zu stark belastet. Eine Hardware-Beschleunigung mit eigenen Prozessoren auf den entsprechenden Adaptern löst diese Argumentation in Luft auf. Ein Beispiel dafür sehen wir in Abbildung 1.3

Blickt man aber auf die Prozessorentwicklung insgesamt und löst die Konzentration vom Hersteller HP, wird deutlich, dass es Netzwerk-Prozessoren gibt, die schon heute in der Lage wären, einen iSCSI-Speicherverkehr mit 10 GbE abzuwickeln, denn schon vor 7 Jahren gab es welche, die 10 GbE-Verkehr verzögerungsfrei mit Triple-DES verschlüsseln konnten. Die Komplexität der 3DES-Verschlüsselung und der iSCSI-TCP-Bearbeitung fallen in die gleiche Klasse. Solche Lösungen sind nach meinem Kenntnisstand noch nicht auf dem Markt, aber offensichtlich eher deshalb, weil die iSCSI-Welt sie noch nicht benötigt.

Von der strategischen Perspektive her sind also FCoE und iSCSI absolut gleich gerüstet und es ist noch völlig unklar, wie das am Ende ausgeht. Wahrscheinlich bleibt es bei einer Koexistenz beider Lösungen. iSCSI hat jedoch den enormen Vorzug, dass es gegenüber FCoE kein „Lossless Ethernet“ benötigt, um sauber zu laufen. Eine generell erhöhte Qualität eines RZ- oder Corporate-Networks käme allerdings auch iSCSI zugute. Sieht man sich nämlich die Tests genau an, wird klar, dass die Lösungen auf bestehender Hardware noch deutlich schneller werden könnten, wenn das TCP nicht ab und an gezwungen wäre, verloren gegangene Pakete nochmals zu senden, was ja letztlich den Fluss immer wieder unterbricht.

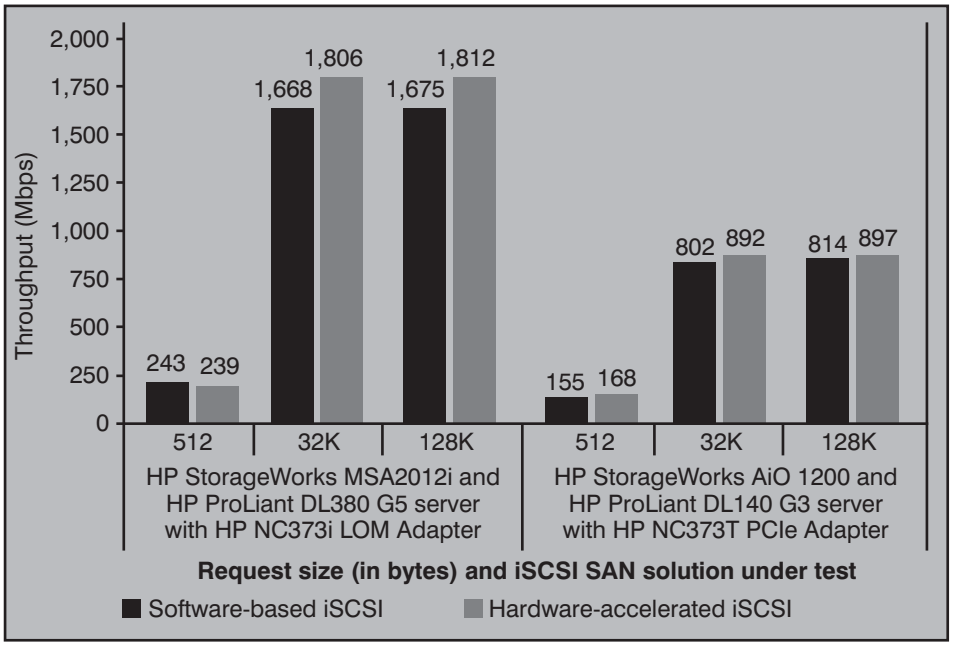


Abbildung 1.2: Wirkung von iSCSI-Hardware-Beschleunigung (Durchsatz) Quelle: HP und Tolly Group

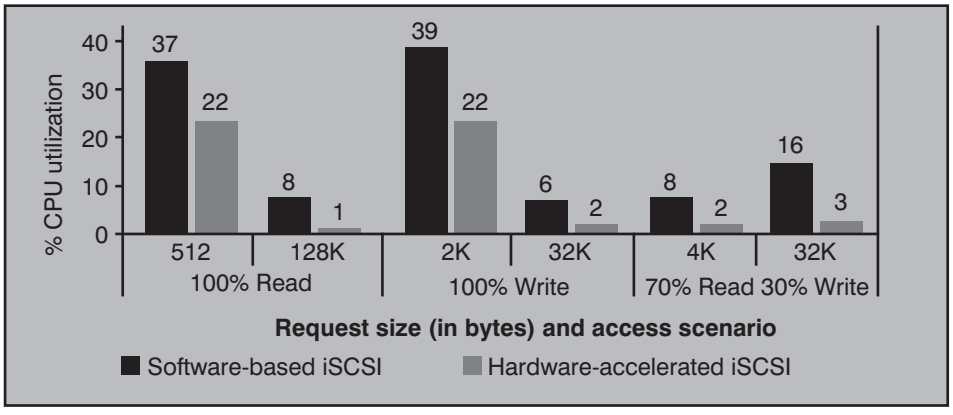


Abbildung 1.3: Wirkung von iSCSI-Hardware-Beschleunigung (Prozessor-Entlastung)
Quelle: HP und Tolly Group

2. Lossless, Enhanced und Converged

In heutigen RZs benutzen Unternehmen üblicherweise Ethernet für die TCP/IP-Netze und Fibre Channel für Storage Area Networks SAN. Ethernet-Netzwerke werden üblicherweise dazu aufgebaut, dass Benutzer relativ geringe Datenmengen über LANs oder auch größere Distanzen bekommen können. Storage Area Networks in Unternehmen und Organisationen werden implementiert, die für Anwendungen wie Booting, Mail Server, File Server oder große Datenbanken den Zugriff auf Block-I/O benötigen.

Die Vorteile der SANs sind

- zentralisiertes Management
- hohe Sicherheit sinnfälliger Verwaltung der Speicher-Ressourcen
- einheitliche Darstellung und Implementierung spezieller Storage Services, wie periodische Backups und
- Unterstützung des Betriebs effektiver Benutzungsniveaus der Speicher-Ressourcen

Ein weiterer interessanter Bereich in Rechenzentren ist der stärkere Wunsch nach Virtualisierung. Dieser führt aber nach steigendem Bedarf an FC-Konnektivität für die Virtuellen Hosts auf ihren Servern. Die Anforderungen an FC werden in diesem Fall durch die Funktion der Hypervisor getrieben, die virtuelle Betriebssysteme mit virtualisiertem Speicher erzeugen. Und dieser virtuelle Speicher muss ja irgendwo effektiv realisiert werden, üblicherweise auf einer dafür spezialisierten Maschine, die man eben über FC erreicht. Denkt man das zu Ende, wird das Netz zum Systembus und man kommt zu einer virtuellen Infrastruktur über diesem „Netz-Systembus“.

2.1 I/O-Konsolidierung

Die Konvergenz von LAN und SAN im RZ bringt eine Reihe möglicher Vorteile. Die Konvergenz beruht auf der Abbildung von „Speicherverkehr“ auf die Ethernet Switching Fabric mittels iSCSI oder FCoE.

iSCSI ist bewährt und problemlos. FCoE klingt zunächst einmal gut, stellt aber zusätzliche Anforderungen an die Ethernet Switching Fabric, die ggf. komplex und kritisch werden können, obwohl sie sich zunächst trivial anhören:

- Lossless Ethernet
- Congestion Notification & Control

Es ist kritisch zu prüfen, inwieweit die Hersteller diese Anforderungen erfüllen können, wenn nicht, kann man das Konvergenzthema mit FCoE vorläufig knicken!!!!

Die in diesem Zusammenhang auch so genannte I/O-Konsolidierung ist von der Konzeption her sehr einfach: man bringt SAN- und Ethernet-Verkehr auf das gleiche Kabel. In Fällen, wo die Trennung dieser Netze aus welchen Gründen auch immer gewünscht ist, bleibt immer noch der Vorzug, dass man die gleiche Hardware für beide Typen von Netzlast flexibel nutzen und zuordnen kann.

Die Vorzüge dieser einfachen Idee für die Anwender sind enorm. Unternehmen, die eine derartige I/O-Konsolidierung vornehmen, werden

- erhebliche Gewinne in der Slot-Effektivität von Servern haben
- mit Multifunktions Netzwerk- und Storage Adaptern die Verkabelung eines Racks erheblich vereinfachen und
- die Abwärme, die ein Server erzeugt, reduzieren (und damit den Stromverbauch)

ABER: natürlich nur wenn alles so funktioniert, wie uns die Hersteller das erzählen wollen.

Heute benutzt man 4, 6, oder sogar 8 Netzwerk-Adapter in kritischen Servern. Das können z.B. 2 FC-Host Bus-Adapter und 2 Ethernet NICs sein, bei virtuellen Maschinen je nach Vorgaben des VM-Herstellers auch bis zu vier NICs zusätzlich.

I/O-Konsolidierung bedeutet, dass ein Kunde statt dessen Multifunktions-Netzwerk/Speicher-Adapter anstelle der Netzwerk-spezifischen Karten einsetzen kann, und zwar nur zwei. Dadurch spart man bei

- Rack-Verkabelung
- Verkabelung generell
- Switchports
- I/O-Stromverbrauch
- Switch-Stromverbrauch
- Kühlung

Es gibt grundsätzlich vier Alternativen zur I/O-Konsolidierung:

- iSCSI setzt auf TCP/IP auf und geht erst damit auf die Ethernet-Schicht. Damit kann es alle Kontrollfunktionen von TCP/IP benutzen
- FCIP ist eine Möglichkeit, FC-Funktionalität auf TCP/IP aufzusetzen. FCIP kann alle Kontrollfunktionen von TCP/IP benutzen, ist aber nicht marktgängig
- iFCP ist eine ähnliche Konstruktion und ebenfalls nicht marktgängig
- FCoE ist ein neuer Standard, bei dem die TCP/IP-Schichten nicht durchlaufen werden müssen. Dafür werden erhöhte Anforderungen an die Ethernet-Schicht gestellt: Lossless Ethernet

Alternativen heute sind also iSCSI oder FCoE. (siehe Abbildung 2.1)

FCoE bedeutet schlicht, dass das Fibre Channel System auf einer anderen physikalischen Verbindung, nämlich Ethernet in einer verbesserten Form, laufen kann. Dazu sind Anreicherungen des Ethernets nötig, Basis ist mindestens 10 GbEthernet mit „Lossless“ Funktionalität. Statt physikalischer FC-Links werden Ethernet-Links eingesetzt, aber Fibre Channel bleibt voll und ganz Fibre Channel. Der Standard durch INCITS T11 Fibre Channel Technical Commitee wird Ende 2008 fertig. Die FCoE Protokollspezifikation bildet FC unmittelbar auf Ethernet ab und ist unabhängig von der eigentlichen Ethernet Forwardíng Funktion. FCoE erlaubt eine wesentliche Weiterentwicklung hinsichtlich der I/O-Konsolidierung, weil er alle Eigenschaften des FC bewahrt, für die gleiche (geringe) Latenz sorgt, die Vorzüge des FC in Sicherheit und Verkehrsmanagement stützt und somit alle Investitionen in Fibre Channel Systeme, Tools, Training und SANs bewahrt.

2.2 Lossless Ethernet, Congestion Control & Priority Based Congestion Control: die komplizierte Nullrunde

Wenn man jetzt den schönen Darstellungen der Hersteller auf den Grund gehen möchte, kommt man schnell in komplexe Untiefen.

2.2.1 Was ist nun „Lossless“?

Bis dahin ist ja alles schön und gut, aber bei „Lossless“ geht es schon mit dem Begriff selbst los. Der Begriff ist nicht sauber definiert. Es handelt sich NICHT um Verlustfreiheit bei der Bitübertragung. Üblicherweise werden Übertragungssysteme so definiert, dass sie ca. im Bereich von 10 exp -15 ... 10 exp -18 für die Bitfehlerwahrscheinlichkeit liegen. Derartige Verluste können über Prüfsummen kompensiert werden. Es handelt sich NICHT um

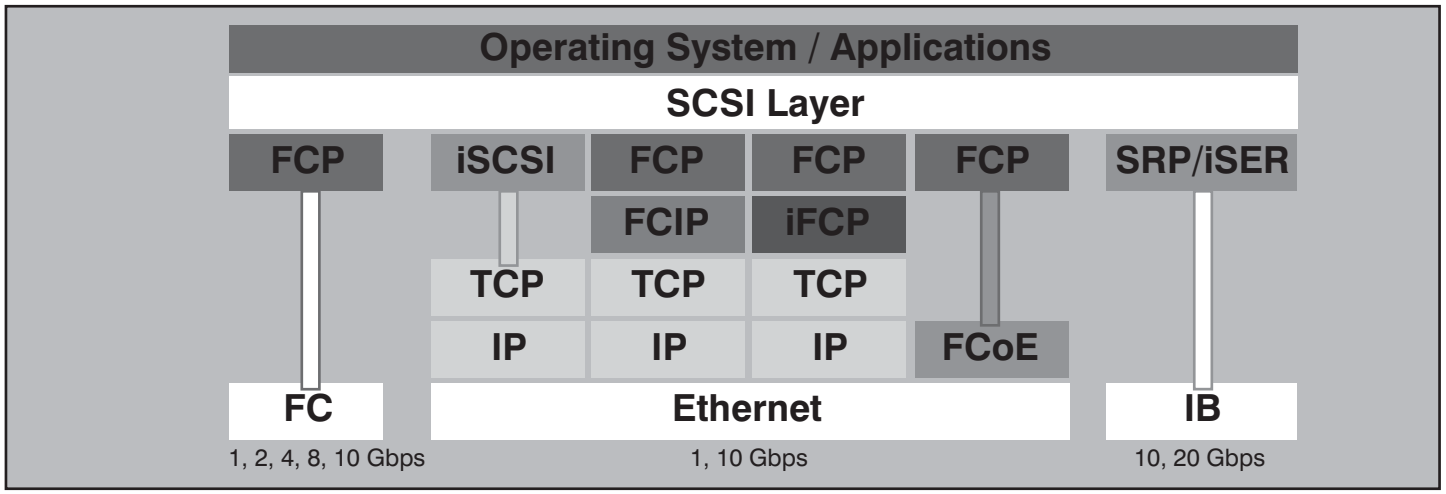


Abbildung 2.1: Protokollstapel

Graphik: INTICS

Verlustfreiheit bei der Ablage von Bits in Speichermedien (oder von den Speichermedien zu Hosts), denn diese wird üblicherweise durch fehlererkennende und -korrigierende Codes implementiert. Es handelt sich einfach darum, dass ALLE zur Übertragung anstehenden Datenpakete auch heil durch die Switching Fabric laufen, ohne dass ein einziges weggeworfen wird, was Ethernet Switches gerne in Überlastsituationen machen. Das hört sich trivial an, ist es aber nicht! Wirklich ALLE Datenpakete? Oder kann man doch Verluste hinnehmen? Wenn ja, wie viele bezogen auf die Gesamtzahl zu übertragender Pakete?

Momentan fühlt sich irgendwie niemand dafür zuständig, „lossless“ wirklich zu definieren. Das liegt hauptsächlich daran, dass der Begriff jeweils in einem gewissen Kontext gesehen werden muss. Ein Hersteller wie Cisco z.B. positioniert den Begriff momentan noch im Zusammenhang mit Ethernet auf den Server-Speicher-Verbindungen, ohne aber auch hier konkret zu sagen, wie viele Pakete denn nun verloren gehen dürfen, um dennoch von „lossless“ sprechen zu dürfen.

Wir können uns der Thematik aber anders nähern, und dann finden wir auch eine Aussage, auch wenn wir dafür den Bereich völlig wechseln müssen, nämlich vom RZ-Netz zu einem Provider-Netz. Ein SONET-Netz eines Providers verliert, außer wenn es atomar zerstört wird, eigentlich überhaupt keine Pakete. In einem SONET steht sozusagen eine ständig umlaufende synchrone Übertragungsressource in Form von Containern bereit, auf die man Daten abbilden kann. Möchte ich nun z.B. einen 4 Gigabit Fiber Channel über ein SONET laufen lassen, muss ich, Overhead eingerechnet, ca. 5 Gigabit SONET fest reservieren, das wäre ein virtueller OC-96 Schaltkreis. Das Providernetz kann Tausende derartiger Schaltkreise parallel unterstützen. Damit kann rein gar nichts schiefgehen, es sei denn, ein Operator im OAM&P-Center macht einen Fehler.

Großkunden sind nun diese Art von Service gewöhnt und bezahlen dafür. Im Rahmen der Service Level Agreements benötigen Provider also ein Maß für „lossless“, damit sie derartige Dienste verkaufen können.

Es gibt aus sehr großen Feldversuchen im Zusammenhang mit der Weiterentwicklung von Providernetzen eine Reihe von Untersuchungen, die zeigen, was passiert, wenn man ein sehr großes Netz mit Routing betreibt. Etwa ab einer Auslastung von 50% geht die Kurve für die Paketverluste steil nach oben. Das ist auch der wirkliche Grund dafür, warum man für Neukonstruktionen eine reine L2-Struktur bevorzugt. Abbildung 2.2 zeigt eine solche Kurve.

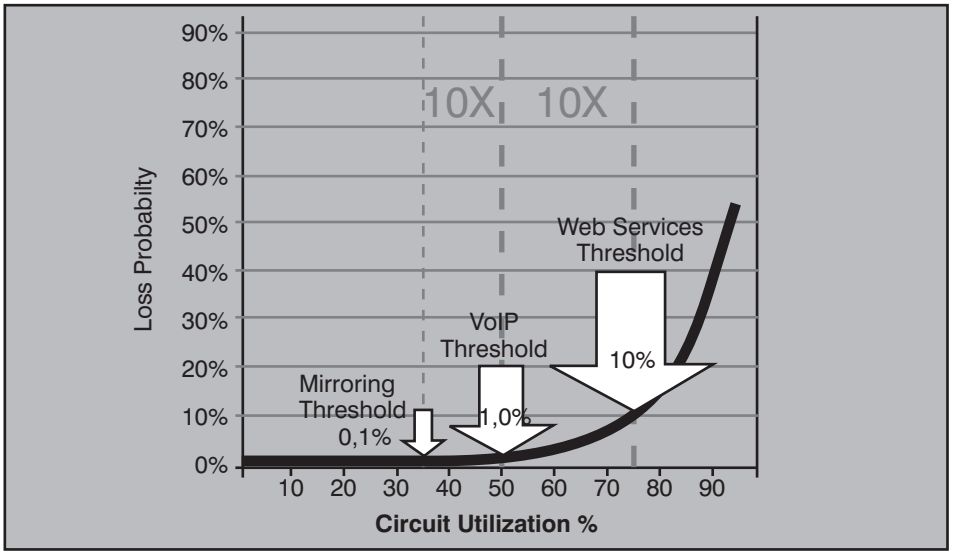


Abbildung 2.2: Verlustraten bei Netzen mit Routing Quelle: Infoworld

Gleichzeitig sehen wir aber auch Schwellen, ab denen ein bestimmter Service nicht mehr ordentlich gewährleistet werden kann. Normaler IP-Verkehr verträgt durchaus bis zu 10% Paketverlust. VoIP ist da schon empfindlicher und reagiert bei 1% Verlust verschnupft. Der Verkehr zwischen Speichern oder zwischen Speichern und Servern wird als Dienst bei Providern häufig als Mirroring bezeichnet, ausgehend von der entsprechenden Grundfunktion bei Speichernetzen. Und hier kommt man auf einen Wert von 0,1 %, der die Grenze der Erträglichkeit beschreibt.

Von daher bedeutet das in diesem Kontext, dass eine Behinderung des Services dann beginnt, wenn ein Paket von 1000 verloren geht. In unserer gewohnten Nomenklatur bezeichnen wir das als eine Paketfehlerrate von 10 exp -3. In der Nachrichtenübertragung hat es sich eingebürgert, ein System hinsichtlich einer grenzwertigen Fehlerrate dann als funktionell zu bezeichnen, wenn es von dieser Grenze mindestens eine Zehnerpotenz wegbleibt. Also erhalten wir:

Im Zusammenhang von Providernetzen spricht man von einem „Lossless“-Pakettransport genau dann, wenn die Paketverlustrate 10 exp -4 oder besser ist.

Jetzt haben wir endlich etwas in der Hand. Ob ein Corporate Netzwerk-Betreiber mit diesem Wert zufrieden ist, hängt unter anderem davon ab, welche Paketfehlerrate die angeschlossenen Speichersysteme durch ihre fehlererkennenden und -korrigierenden Codes verkraften. Da gibt es unterschiedliche Aussagen der Hersteller. Insgesamt ist es aber natürlich in der Praxis so, dass auch bei einer Fiber Channel Übertragung oder bei einer Übertragung über eine unmittelbare Parallelschnittstelle Fehler auftreten können, die von den angeschlossenen Systemen kompensiert werden müssen.

Wenn ich jetzt gemein wäre, würde ich fordern, dass sich

- Hersteller insgesamt darauf einigen, welche Paketverlustrate real dahinter steckt, wenn sie von „Lossless“ sprechen
- Hersteller genau darlegen, wie sie es erreichen

2.2.2 Congestion Management & Control

Um zu erreichen, dass kein Paket weggeworfen wird, setzen Hersteller und Standardisierung auf die sog. Congestion Control. Wenn in einem Switch ein Problem entsteht, sollen alle anderen Switches benachrichtigt werden können und ebenfalls die Aussendung von Paketen ganz oder teilweise unterlassen oder einschränken. Sowohl Hersteller als auch Standardisierung arbeiten in einem solchen Fall mit priorisierten Warteschlangen. Wir werden noch sehen, wohin das führt. (siehe Abbildung 2.3)

Der Hund liegt im Detail begraben, wie so oft.

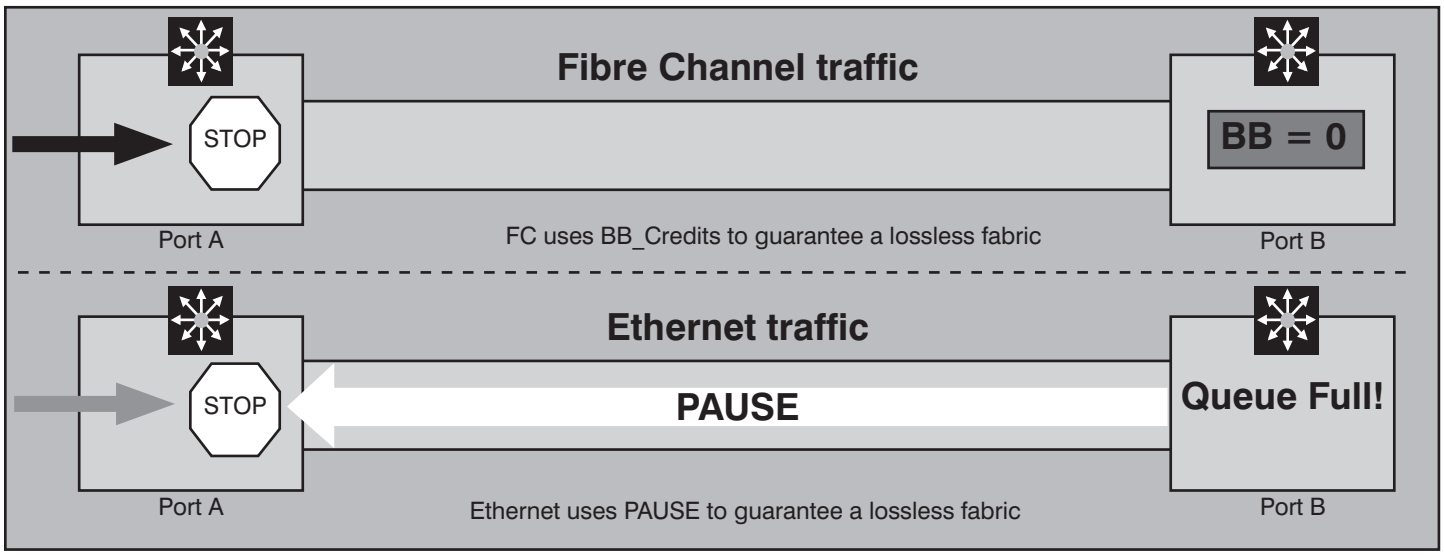


Abbildung 2.3: Problem: „Lossless“ bei FC und Ethernet

Grafik: Cisco

- **Arbeitsweise FC:** ein Empfänger gibt einem Sender mit den BB_Credits eine Reihe von Credits für die Anzahl von Datenblöcken, die er empfangen kann. Beim Senden zählt der Sender die Credits herunter und muss aufhören zu senden, wenn er keine mehr hat. Um eine Art Sliding Window zu erzeugen, sendet der Empfänger neue Credits, bevor die alten aufgebraucht sind.

- **Arbeitsweise Ethernet:** ein Sender sendet immer weiter in der Hoffnung, dass der Empfänger die Pakete auch immer verarbeiten kann. Ist das aus irgendeinem Grund nicht mehr der Fall, kann der Empfänger mit einer PAUSE-Nachricht um eine solche bitten.

D.h. im Klartext: die Arbeitsweise von Ethernet und FC in einem solchen Fall sind *genau invers zueinander!!!*

Sowohl von z.B. Cisco als auch von IEEE gibt es nun Äußerungen dazu, wie ein Lossless Ethernet trotzdem funktionieren soll und zwar auf Basis der sog. Congestion Control.

O-Text Cisco: „Die Cisco IOS Congestion Management Eigenschaften erlauben Ihnen, die Stausituation dadurch zu kontrollieren, dass die Reihenfolge von Paketen, die über eine Schnittstelle ausgesendet werden, durch Prioritäten, die diesen Paketen zugeordnet werden, bestimmt wird.“

O-Text IEEE 802.3ar Congestion Management: „Es wird ein Verfahren entwickelt, das für die Verbreitung von Staumeldungen sorgt und gleichzeitig eine Begrenzung des Verkehrs auf Ethernet-Strecken erlaubt, ohne dass sich am MAC/PLS Interface etwas ändert.“ Und das machen sie dann auch mit priorisierten Warteschlangen.

Sowohl bei Cisco als auch bei IEEE gibt es dann verschiedene, abgestufte Verfahren, ABER: alle diese Verfahren sind NICHT DETERMINISTISCH und benachteiligen nachrangig priorisierte Pakete enorm.

Die Verfahren von Cisco und IEEE unterscheiden sich heute noch leicht. Es ist aber kein Grund zu sehen, warum sie nicht in absehbarer Zeit zu einem vereinheitlichten, standardisierten System konvergieren sollten. Wir brauchen die Unterschiede hier nicht zu differenzieren, sondern betrachten zur generellen Funktionsweise einfach einmal ein Beispiel, siehe Abbildungen 2.4 bis 2.8.

Zur Erläuterung brauchen wir von einem Switch folgende Komponenten: Eingangswarteschlangen, Ausgangswarteschlangen, eine Switchmatrix und einen Puffer, siehe Abbildung 2.4.

In Abbildung 2.5 sehen wir den Staubeginn. Die Kommunikationsrichtung ist von links nach rechts. Am Zielswitch gibt es ein Problem, so dass dieser seine Eingangswarteschlange nicht mehr entleeren kann. Also sendet er dem Quell-Switch ein PAUSE-Signal, damit dieser mit der

Seminar

Internetworking: optimales Netzwerk-Design mit Switching und Routing
09.02. - 13.02.09 in Aachen

Dieses 5-Tages-Intensiv-Seminar vermittelt Netzwerkbetreibern und Planern Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt.

Referenten: Dipl.-Inform. Petra Borowka, Markus Geller
Preis: € 2.290,- zzgl. MwSt.

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

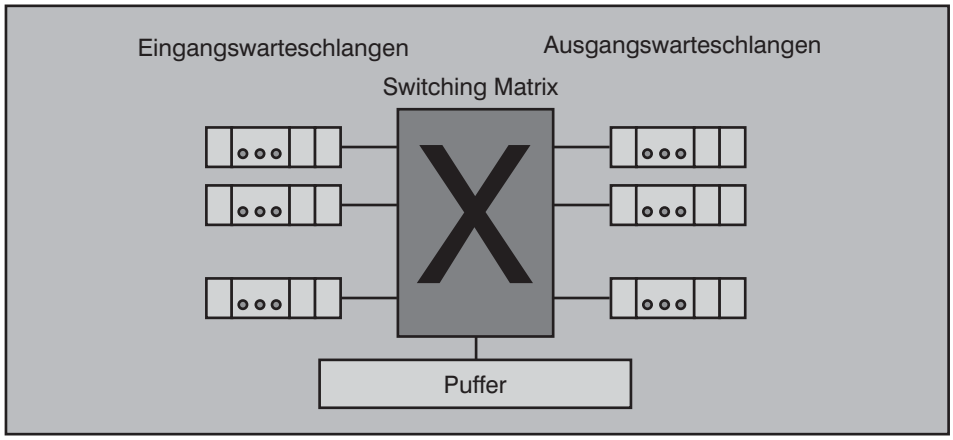


Abbildung 2.4: Congestion Mgmt. (1): Switchkomponenten

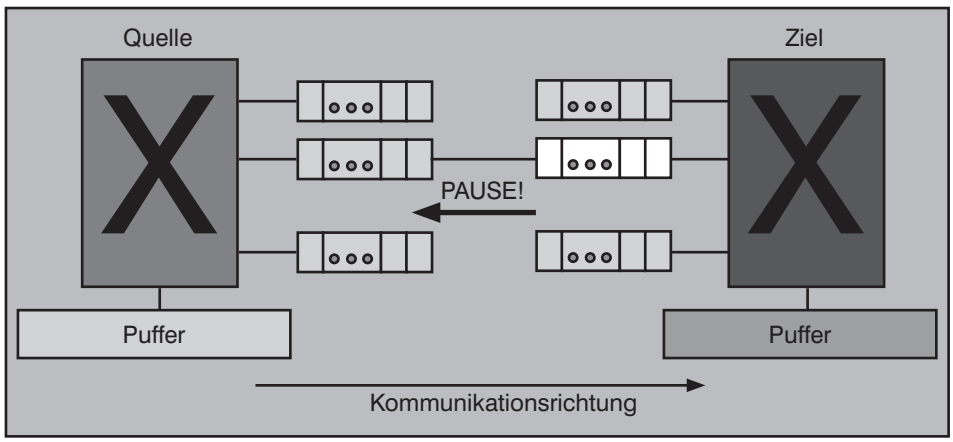


Abbildung 2.5: Congestion Mgmt. (2): Staubeginn (1)

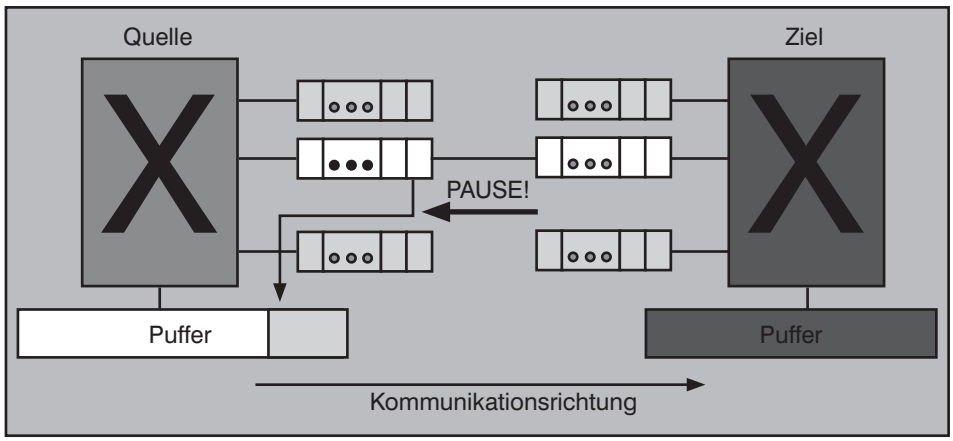


Abbildung 2.6: Congestion Mgmt. (3): Staubeginn (2)

Übertragung über seine Ausgangsschnittstelle aufhört.

Da wegen der PAUSE-Nachricht die Ausgangsleitung nicht mehr benutzt werden kann, muss der Switch die Datenpakete in einen Puffer umleiten, weil sie ja sonst verloren gehen würden, was ja nicht sein darf. Mit der Zeit wird der Puffer immer voller. Bei einer 10 GbE-Schnittstelle kommen 1,25 Gbyte pro Sekunde zusammen. Das kann der Switch nicht unbegrenzt fortsetzen, siehe Abbildung 2.6.

Ist der Puffer weit genug vollgelaufen, hat der Switch selbst ein schwerwiegendes Problem und es bleibt ihm gar nichts anderes übrig, als selbst seine Eingangsleitungen zu sperren, und zwar alle, da er ja nicht weiß, welche Kommunikationsverbindung nun zu dem eigentlichen Problem geführt hat. Das sehen wir in Abbildung 2,7, die Abbildung stellt einen Linksschwenk entgegen der Kommunikationsrichtung zu den Switches, die „vor“ dem bislang betrachteten Switch liegen, dar.

Die ganzen in Kommunikationsrichtung zurückliegenden Switches (Abbildung 2.8) müssen ebenfalls ihre Ausgangswarteschlangen in Puffer umleiten, da sonst ja Pakete verloren gehen könnten. Wenn diese Puffer voll sind, müssen sie ebenfalls ihre Eingangspuffer sperren und der Effekt schlägt immer weiter nach hinten durch, bis das ganze Netz steht!!

Das Beispiel hat gezeigt, dass es vollkommen unerheblich ist, ob ein Stau in einem Switch nun in einer einzelnen „normalen“ Warteschlange entsteht oder innerhalb einer Warteschlange in einer Gruppe von Eingangswarteschlangen. Zwei Switches „nach hinten“ ist der Unterschied nicht mehr differenzierbar. Der Standard IEEE 802.3ar möchte erreichen, dass die Switches einer Switching Fabric sofort informiert werden, wenn irgendwo ein Stau ist. Erstens ist das gar nicht so einfach, zweitens ist es ja schön, dass die Switches das dann wissen, die Frage ist nur, ob es etwas nützt.

Der Gedanke von Standard und Herstellern ist jetzt, in Stausituationen die Pakete priorisiert abzuarbeiten. Dazu braucht man zusätzliche Komponenten, und zwar den dunkelgrauen Block neben dem „X“ in Abbildung 2.9 einmal für JEDE Ausgangsschnittstelle.

Die Frage ist nun, welchen Nutzen eine derartige Konstruktion hat. Die Warteschlangentheorie lehrt, dass bei einer Priorisierung die höchste Prioritätsstufe einen (relativ geringen) Gewinn gegenüber einer ungesteuerten Lösung hat, dass die zweite Prioritätsstufe einen (relativ hinnehmbaren) Verlust gegenüber einer ungesteuerten Lösung hat, die dritte und noch niedrigere Stufe allerdings mit einem schweren Nachteil belegt werden. In der Praxis bedeutet das, dass beim Start der Priority Flow Control Pakete oder Datenströme, die ggf. gar nichts mit dem Stau zu tun haben, auf das schwerste benachteiligt werden können.

Priority Flow Control kann nur dann etwas bewirken, wenn die Ursache der Congestion eine kurze temporäre Degradation einer Ausgangsschnittstelle ist. Dann kann der Rückstau damit einigermaßen elegant aufgelöst werden.

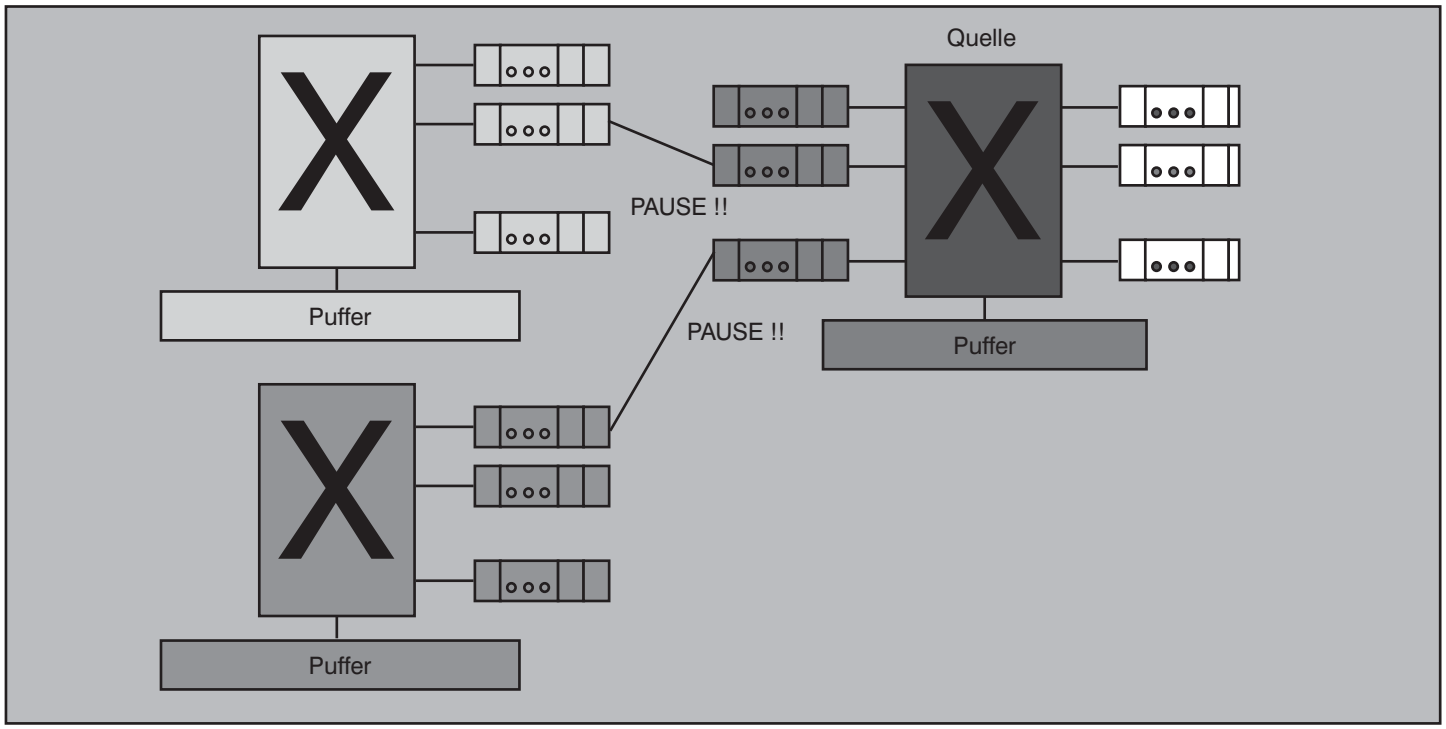


Abbildung 2.7: Congestion Mgmt. (4): Rückstau (1)

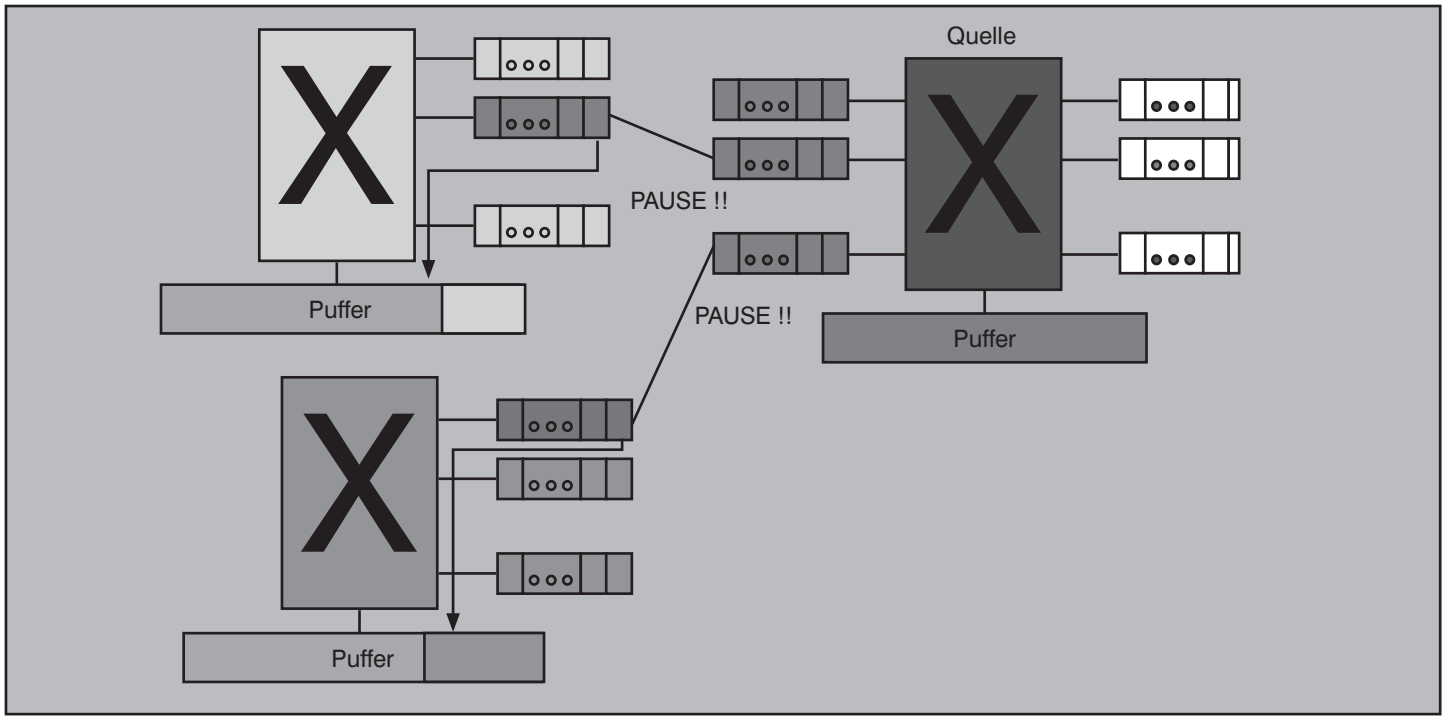


Abbildung 2.8: Congestion Mgmt. (5): Rückstau (2)

In anderen Fällen nützt das Verfahren GAR NICHT !!

Damit sind die Probleme aber noch nicht zu Ende. Angenommen, wir haben ein Verfahren, welches die Meldung über einen Stau an alle Switches und schließlich auch an die Endgeräte weitergibt. Dann stellt sich die Frage:

Welche Frames sollte ein Rate Limiter verlangsamen????

Ausgangswarteschlangen von Endgeräten sind nach unterschiedlichen Design-Kriterien organisiert:

- reiner L2-Service
- Offload
- L4/L5-Service
- eine Mischung davon

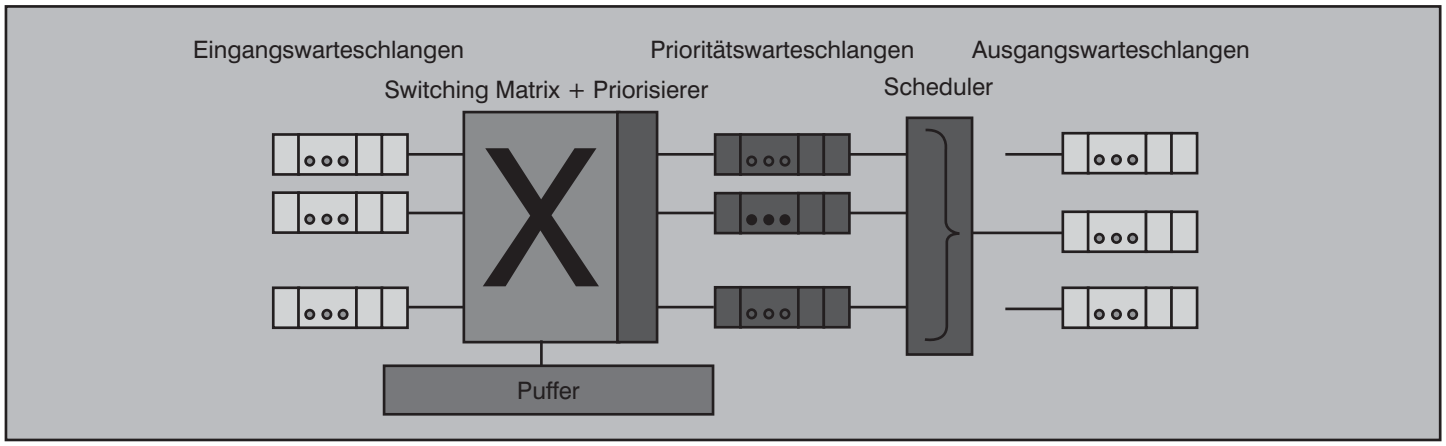


Abbildung 2.9: Priority Flow Control

- verschiedene physikalische und/oder virtuelle PortsSpeicher auf dem Chip, dem Chip direkt zugeordnet oder Host-Speicher

Ein entsprechendes Modell zur Steuerung der Auflösung von Congestions müsste für einen weiten Bereich von Designs entworfen werden.

Die meisten Datenquellen benutzen universelle Sendeschlangen, die in ihrer Datenrate nicht limitiert sind. Datenquellen könnten in dynamisch zugeordneten Sendeschlangen organisiert werden, die in der Datenrate limitiert werden können.

Dazu könnte es für spezielle Anwendungen (FCoE, iSCSI) Ausgangsschlangen geben, die je nach Bedarf in ihrer Datenrate limitiert werden könnten. Jede Sendeschlange ist für genau eine virtuelle NIC und genau eine Verkehrsklasse. Siehe dazu auch Abbildung 2.10.

Die Frage ist aber ganz klar, welche Endgeräte so etwas heute schon unterstützen. Selbst wenn der Standard fertig wäre (wovon er noch weit entfernt ist) und selbst wenn die Hersteller ihn implementieren würden (wovon sie noch weit entfernt sind), würde es 5-10 Jahre dauern, bis alle Endgeräte auf dem Stand wären, dass sie ALLE auf Congestion Control Nachrichten entsprechend reagieren würden. Denn das ist ja ein weiterer Teil des Debakels: *nur wenn ALLE Geräte sich daran halten, kann so etwas wirklich funktionieren. Wenn nur einige Geräte auf Congestion Control reagieren und andere nicht, entsteht genau denen, die nicht reagieren, ein Vorteil, weil sie weiterhin ungehemmt ihre Nachrichten herausblasen, während sich die kontrollierten Stationen vornehm zurückhalten.*

Eine Station ohne Congestion Control Funktionen hat das Problem, dass sie nichts „sieht“, sondern nur irgendwie „merkt“, dass die Pakete nicht mehr in der üblichen Weise abtransportiert werden können. Congestion Management bedeutet, die Station hinreichend in Kenntnis zu setzen, damit sie idealerweise alle Datenströme, die in Richtung der Problemstelle liegen, herunterfährt. Dazu müsste die Station aber in letzter Konsequenz Routing-Informationen bekommen, weil die Problemstelle ja auf dem Weg zwischen Quelle und Ziel liegt. Abgesehen von den technischen Problemen, die so etwas aufwerfen würde, widerspricht das ganz und gar einem Layer-2 Ansatz.

Es gibt eine weitere Initiative von IEEE, 802.1au, die die prioritätsbasierte Congestion Control in Zonen schachtelt. Abgesehen davon, dass es dadurch end-

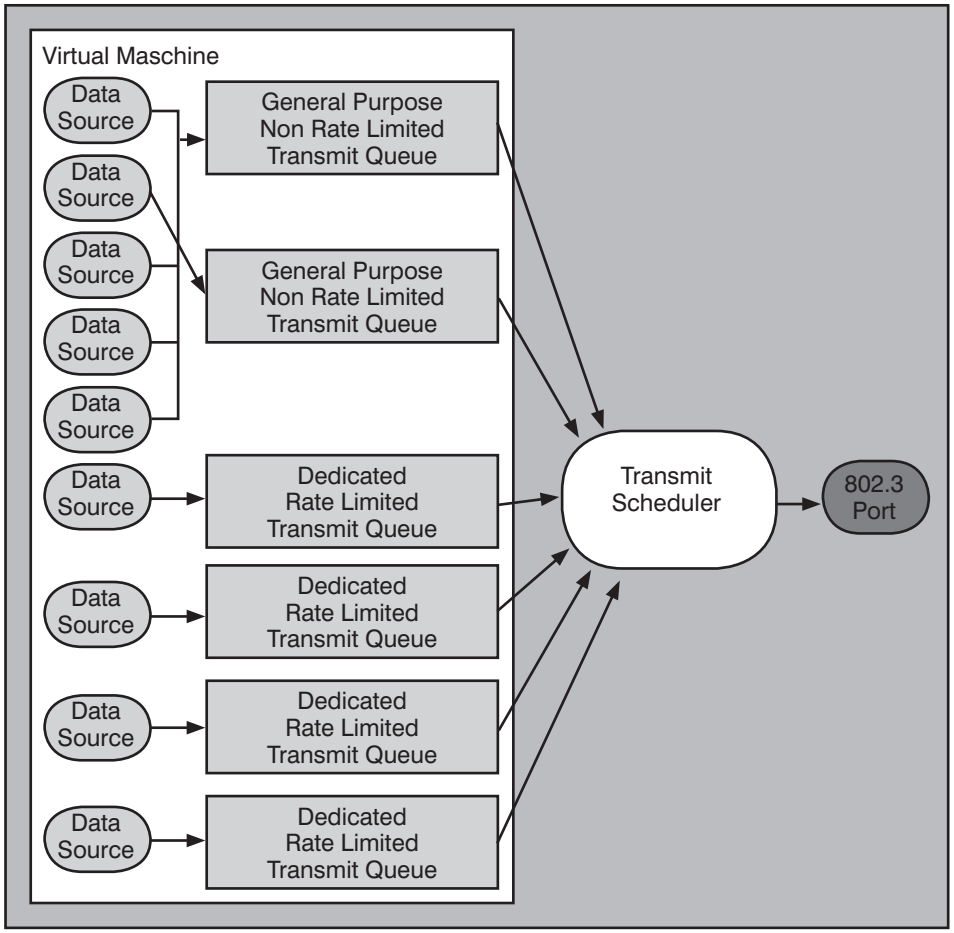


Abbildung 2.10: Endgeräte-Organisation

gültig völlig unübersichtlich wird und eine solche Zonenbildung wenn überhaupt für sehr große Netze in Frage kommt, ändert diese Schachtelung nichts an den grundsätzlichen Grenzen der Konstruktion.

Man hat in der Vergangenheit dazu geneigt, prioritätsbasierte Verfahren immer dann einzusetzen, wenn die Ressourcen zur eigentlichen Datenübertragung knapp werden, also z.B. in der Phase, wo Gigabit Ethernet neu war und man überlegte, ob man mit Fast Ethernet in Kombination mit Priorisierung nicht auch weiter käme. Wir wissen alle, wie so etwas ausgeht: die komplizierte Priorisierung wird ganz und gar überflüssig, wenn man eine neue Leistungsstufe in der Übertragungstechnik einführt.

Aber jetzt kommt noch etwas ganz Neues in diese Diskussion.

In der Vergangenheit wurde Priority Flow Control vor allem dazu entwickelt, einen relativ schmalbandigen, aber wichtigen Datenstrom davor zu schützen, von breitbandigem, aber weniger wichtigem Verkehr, untergebuttert zu werden. Dafür funktioniert es hervorragend, ob nun als Herstellerverfahren oder im Rahmen von IEEE 802.1p. Wegen der unterschiedlichen Bandbreiten tritt die warteschlangentheoretisch zu erwartende Leistungsdegradation kaum messbar ein.

Jetzt haben wir aber eine umgekehrte Problemlage: wir wollen einen breitbandigen Datenstrom, nämlich FCoE schützen. Dafür liegen keine praktischen Erfahrungen vor. Die Warteschlangentheorie zeigt dann aber schnell, dass in einem solchen Fall alle anderen, nachgeordneten Verkehrsströme praktisch still gelegt werden. Sie gibt aber keinen Hinweis darauf, ob wenigstens der breitbandige Verkehr heil durchkommt.

Fazit: Die aktuellen Verfahren wie Priority Based Flow Control können bei einer Congestion im günstigsten Falle leicht abfedern, im ungünstigsten Falle richten sie nichts aus. Ein Congestion Management, welches tatsächlich bis in die Endgeräte reicht, ist zwar theoretisch vorstellbar, wird aber mindestens noch einige Jahre benötigen, wenn es überhaupt dazu kommt. Die von IEEE 802.3ar angestrebte Benachrichtigungsfunktion ist aber in jedem Falle sinnvoll, auch wenn man mit der Nachricht nicht immer etwas anfangen kann.

Ansonsten gilt: das beste und einzig wirkungsvolle Congestion Management ist die völlige (soweit möglich) Vermeidung von Congestions durch konstruktive Maßnahmen. Alles andere führt ggf. zu einem Stillstand des Netzes.

3. Lösungsmöglichkeiten

Bei der Suche nach anderen Lösungsmöglichkeiten fiel mir zunächst folgendes auf.

Der wesentliche Unterschied zwischen iSCSI und FCoE in diesem Kontext wird immer wieder daran festgemacht, dass iSCSI TCP benutzen kann, um einen gestörten Paketfluss zu reparieren, indem es bei der Übertragung verloren gegangene Pakete nochmals sendet und am Ziel wieder richtig eingliedert. FC arbeitet mit einem Sliding Window. Völlig vergessen wurde aber offensichtlich, dass es bei Ethernet die Connection Mode Service LLC Typ 2, kurz LLC2, gibt, jedenfalls im Standard seit weit über 20 Jahren. Der verbindungsorientierte Transportdienst der LLC2 ermöglicht einer Arbeitseinheit der Vermittlungsschicht Sendung und Empfang von Schicht-2 Dateneinheiten (LSDU Link Service Data Unit) und leistet Sequencing, Flusskontrolle und Wiederaufsetzen nach Fehlern. LLC2 hat dazu wie TCP einen Sliding Window Mechanismus, weil sie konstruktiv auf HDLC/SDLC basiert. Diese Verfahren waren für die Sicherung der Kommunikation auf zwischen Terminals und Cluster Controllern (SDLC) oder Daten-Endeinrichtungen und Datenübertragungseinrichtungen (HDLC) über alte, unzuverlässige und langsame Leitungen gedacht. Der Sliding Window von HDLC und SDLC umfasst standardmäßig meist 8 Pakete. Es gibt aber auch eine HDLC-Variante mit 256 Plätzen im Fenster. Sie wurde für die Satellitenübertragung entwickelt. LLC2 benutzt den sog. asynchronen balancierten Modus von HDLC, bei dem das Sequencing über 128 Rahmen geht, und nicht über 8. Für das Abfangen kleinerer Störungen wäre LLC2 durchaus hilfreich, eine größere Störung wäre dann ein Fehler, der normalerweise ja ohnehin durch ein herstellerspezifisches Umschaltverfahren behoben wird. Zwischen der kleineren und der größeren Störung gibt es eine Grauzone. Und genau in dieser wäre PBCC eine echte Hilfe. Wenn man nicht in den Höchstleistungsbereich vordringen will, ergibt die Kombination aus LLC2, PBCC und Umschaltverfahren eine weitest gehend durchgängige Lösung auf der Basis von Komponenten, die wir bereits haben. Erstaunlicherweise spricht aber heute niemand mehr von der LLC2. Eine extrem elegante Lösung für Lossless Ethernet wäre eine LLC2 mit einem erweiterten Fenster.

Die Frage ist jetzt: über welche Zeiträume kann LLC2 einen Verkehr bei einer Störung retten? Wir können davon ausgehen, dass bei der Abbildung von FC-Verkehr auf Ethernet maximal lange Ethernet Pakete entstehen. In den Unterlagen von SNIA und INTICS spricht man davon, dass eine Implementierung sowieso am besten funktioniert, wenn ein Switch auch Jumbo Frames verarbeiten kann.

Bei einer Übertragungsrate von 1 Gbit/s werden bis zu 83.333 maximal lange Ethernet-Pakete erzeugt, also 83 pro Mil-

Seminar

Ethernet-Netzwerke: Techniken, Einsatzgebiete und Betrieb
20.04. - 22.04.09 in Aachen

Dieses Seminar stellt die aktuellen Ethernet-Themen vor und zeigt, wie etablierte und neue Techniken in bereits wohlbekannten und zukünftigen Anwendungsgebieten eingesetzt werden können. Zu den analysierten Sonderanwendungsgebieten gehören insbesondere VoIP, Gefahrenmeldetechniken, Industrienetze und Rechenzentrumsbereiche. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, Planungsregeln vorgestellt, Möglichkeiten und Grenzen von Quality of Service und Risiken durch Fehlentscheidungen bei der Technikauswahl aufgezeigt.

Referenten: Dipl.-Inform. Oliver Flüs, Dipl.-Ing. Hartmut Kell
Preis: € 1.690,- zzgl. MwSt.

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

lisekunde. LLC2 könnte uns in diesem Fall also grob über die ersten 2 msec eines Congestion-Problems hinweghelfen. Dann warten wir gespannt auf das Einsetzen des Recovery-Verfahrens, was spätestens nach 50 msec passieren sollte, weil es sonst keine Voice Grade Qualität im Netz garantieren könnte. Außerdem kann das SONET über mehrere Tausend km schon seit 20 Jahren, also 50 ms sind eher die Grenze, an der sich ein Recovery Verfahren der Lächerlichkeit preisgibt. Wenn wir Speicherverkehr übertragen, müsste das Recovery Verfahren viel eher eingreifen und da wir im RZ ohnehin nur kurze Wege und schnelle Switches haben, ist es keine völlig überzogene Anforderung, dass das Recovery Verfahren eher im Bereich von 10 - 20 msec einsetzt. Zu diesem Punkt müssen sich die Hersteller irgendwie einmal offenbaren, weil die standardbasierten Recovery Verfahren in diesem Umfeld zu langsam sind.

Nehmen wir einmal an, dass zwischen dem Ende der Möglichkeiten der LLC und dem Beginn der Wirkung des Recovery Verfahrens 20 msec liegen. Ein Speicher in einem Switch müsste in dieser Zeit 1660 Pakete zwischenlagern, das wären knapp 20 Mbit. Das ist nun wirklich nicht viel, die Pufferspeicher bei guten Switches liegen allesamt im Gigabit-Bereich. In diesem Zusammenhang ist die Abarbeitung der Schlangen mit PBCC sicherlich hilfreich.

Bei 1 Gbit/s. können wir also ein „Lossless Ethernet“ durchaus mit Mitteln herbeiführen, die wir schon haben, dazu wäre es lediglich nötig, dass das heute unsauber in die Schichtenstrukturierung herein gequetschte FCoE-Modul, welches die FC-Pakete in Ethernet-Pakete umpackt, automatisch den LLC2 SABM-Befehl ausführt und somit die LLC2 nutzt.

Ich wundere mich wirklich, warum bislang niemand darüber spricht.

Bei 10 GbE nutzt LLC2 dann nur innerhalb der ersten 0,2 msec. Unter gleichen Voraussetzungen müsste der Pufferspeicher dann 0,2 Gbit groß sein. Auch das ist absolut im Rahmen der heutigen Möglichkeiten.

Außerdem gibt es noch andere Lösungsmöglichkeiten für „Lossless“. Das Congestion Thema wurde vor vielen Jahren bereits im Rahmen optischer Providernetze diskutiert. Dabei ist zu Tage getreten, dass die Wahrscheinlichkeit für Congestions durch normalen Verkehr immer dann ins Bodenlose sinkt, wenn grundsätzlich für alle Verbindungen in der Switching Fabric die doppelte Leistung der eigentlich angestrebten Maximalleistung verbaut wird. Alle Stillstandssituationen, die trotz dieser Überdimensionierung auftreten, sind Fehler im eigentlichen Sinne und müssen von den Fehlerkontroll- und -Umgehungsmechanismen des Netzes aufgefangen werden. SONET-Systeme schalten in einem solchen Fall in höchstens 50 msec so um, dass als fehlerfrei erkannte Wege als Ersatzwege benutzt werden können. Normalerweise führt die SONET-Umschaltung zu einer Halbierung der Leistung. Das macht aber wegen der doppelten Dimensionierung eben nichts aus.

Ist dieses Ergebnis aus den SONET-Providersystemen auch auf RZ Ethernet Switching Fabrics übertragbar? Ja, und zwar durch kombinierten Einsatz von

- Überdimensionierung und
- schnellem Redundanzverfahren

Die Überdimensionierung erreicht man einfach dadurch, dass man genau eine 2 oder 4 Gbps FC-Verbindung auf genau eine 10 GbE-Verbindung abbildet. Das schnelle Redundanzverfahren dient dazu, eine hartnäckige Staustelle als Fehler zu klassifizieren und zu umgehen, eine geeignete Grundkonfiguration vorausgesetzt. Dann kann eigentlich kein Paket mehr verloren gehen. Eigentlich.

Letztlich ist das Problem nur dann durch Priority Based Flow Control zu lösen, wenn Failover-Verfahren und Pufferspeichergröße in einer bestimmten Relation zueinander stehen.

Nehmen wir einmal an, wir haben tatsächlich ein Failover-Verfahren mit einer maximalen Arbeitszeit von 50 msec. Wir sind jetzt extrem pessimistisch und geben nochmal die gleiche Zeit hinzu, bis alle wissen, dass wieder alles normal läuft, also kämen wir dann auf 100 msec. In dieser Zeit möchte ein 10 GbE-Adapter 1 Gigabit an Daten loswerden, so ist er nun einmal gebaut. Das sind über 800.000 maximal lange Ethernet-Pakete und ca. 20 Millionen minimal lange Ethernet Pakete. Jeder Puffer muss also mindestens 0,125 GigaByte groß sein. Außderdem sehen alle prioritätsbasierten QoS-Verfahren acht Warteschlangen vor, diese Anzahl hat sich irgendwie eingebürgert. Also benötigen wir pro Ein- und Ausgangsport jeweils 1 GB Puffer. Das ist nicht weiter tragisch, aber im schlimmsten Fall muss ein Steuerprozessor in 0,1 Sekunden die priorisierte Abarbeitung von 20 Millionen Paketen ausrechnen, und zwar für JEDEN Port des Switches. Sagen wir einmal, er benötigt für jede Zuordnung 10 Fließpunktoperationen, dann wäre für jeden Port ein 0,2 Teraflop-Prozessor notwendig.

Diese Darstellung ist durchaus realistisch und auch der Grund dafür, warum der neue SONET-Switch der Reihe 15000 von Cisco keinen zentralen Prozessor mehr besitzt, sondern jeder 40 Gigabit-Einschub einen eigenen kräftigen Prozessor hat und darüber hinaus eine verteilt arbeitende Switching-Matrix, die mit jedem Einschub wächst. Sie sehen, dass nichts unmöglich ist, aber das führt uns ggf. auf eine völlig neuartige Switch-Architektur.

4. Zwischenfazit

Im RZ haben wir eine Reihe von günstigen Voraussetzungen:

- kurze Übertragungswege
- extrem leistungsfähige Übertragungstechnik
- sehr schnelle Switches
- sehr schnelle proprietäre Redundanzverfahren
- übersichtliche redundante Netzstruktur

Die Einführung einer „Lossless Ethernet“ Übertragungsmöglichkeit für die letztliche Herbeiführung einer gewinnbringenden Konvergenz von normalem Datenverkehr und Speicherverkehr wird durch diese Voraussetzungen erheblich begünstigt. Die prioritätsbasierte Congestion Control kann dabei ein nützlicher Baustein sein, reicht aber alleine nicht aus. Es ergeben sich folgende konstruktive Alternativen:

- Leitungsgeschwindigkeit 1 GbE:
  - LLC2 + Puffer minimal 2,5 MB/Port + schnelles Redundanzverfahren
- Leitungsgeschwindigkeit 10 GbE
  - LLC2 + Puffer minimal 25 MB/Port + PBCC + schnelles Redundanzverfahren
  - Überdimensionierung + schnelles Redundanzverfahren

Sie sehen, dem schnellen Redundanzverfahren kommt eine erhebliche Bedeutung zu.

Andererseits beschränken sich die eigentlichen Integrationsverfahren auf iSCSI und FCoE. Blickt man in Richtung Hardwarebeschleunigung, sind diese Verfahren trotz aller wüsten Diskussionen theo-

retisch fundamental betrachtet äquivalent. Der Unterschied liegt letztlich nur in der Schicht, in der bestimmte notwendige Funktionen bearbeitet werden.

Das bedeutet: jeder Kunde hat die völlige Wahlfreiheit zwischen iSCSI und FCoE. Die Wahl kann ausschließlich darauf beruhen, welches System er letztlich aus Gründen des Schutzes der bisherigen Investitionen in zusätzliche Werkzeuge und/oder des generellen Leistungsumfangs bevorzugt. Natürlich spricht auch nichts gegen den Parallelbetrieb beider Varianten im RZ.

Beide Varianten werden von der aktuellen Netzwerktechnik hinreichend unterstützt. Bei Einführung von FCoE auf einer 10 GbE-Struktur werden allerdings High End Switches notwendig. Das liegt aber nicht an FCoE, sondern daran, dass die Switches intern konstruktiv in der Lage sein müssen, viele 10 GbE-Schnittstellen zu aggregieren, unabhängig vom „Inhalt" der Ethernet-Päckchen, und diese letztlich auch über 40 GbE-Schnittstellen weiterzuverarbeiten. Es gibt hierfür schon mehrere Kandidaten auf dem Markt. Ich möchte aber in diesem Zusammenhang darauf hinweisen, dass die beliebte Serie 6500 von Cisco in diesem Zusammenhang an ihre Grenzen stößt, weil es nach Angaben des Herstellers höchstens eine einzige doppelt ausgeführte 40 GbE-Schnittstelle für dieses System geben wird.

5. Storage Extension: wir verlassen das RZ

Innerhalb des RZs haben wir jetzt sozusagen Friede, Freude, Eierkuchen. Jetzt bleibt als Frage übrig, wie sich die Situation außerhalb des RZs darstellt. Es gibt hier einen weiten Bereich von Anforderungen vom einfachen asynchronen Backup bis hin zum vollständigen synchronen Betrieb eines Ausweichrechenzentrums. Dadurch ergeben sich natürlich hinsichtlich der einzusetzenden Technologien Unmengen von Alternativen für die jeweiligen Zwecke. Diese Diskussion können wir gerne führen, aber nicht hier und jetzt. Ab einer gewissen Ansammlung von Anforderungen und Leistungsmerkmalen ist ohnehin am Ende der Wellenlängenmultiplex (DWDM oder CWDM) die einzige Lösung. Das Abbildung 5.1 zeigt eine Lösung, bei der ein ganzes IBM-Rechenzentrum vermöge DWDM repliziert wurde. Die Lösung ist sieben Jahre alt, aber am Prinzip hat sich mittlerweile nichts geändert. Bei einer solchen Replikationslösung spielen neben den Speicherschnittstellen ja auch noch andere Schnittstellen eine Rolle, wie ESCON-Kanalverlänge-

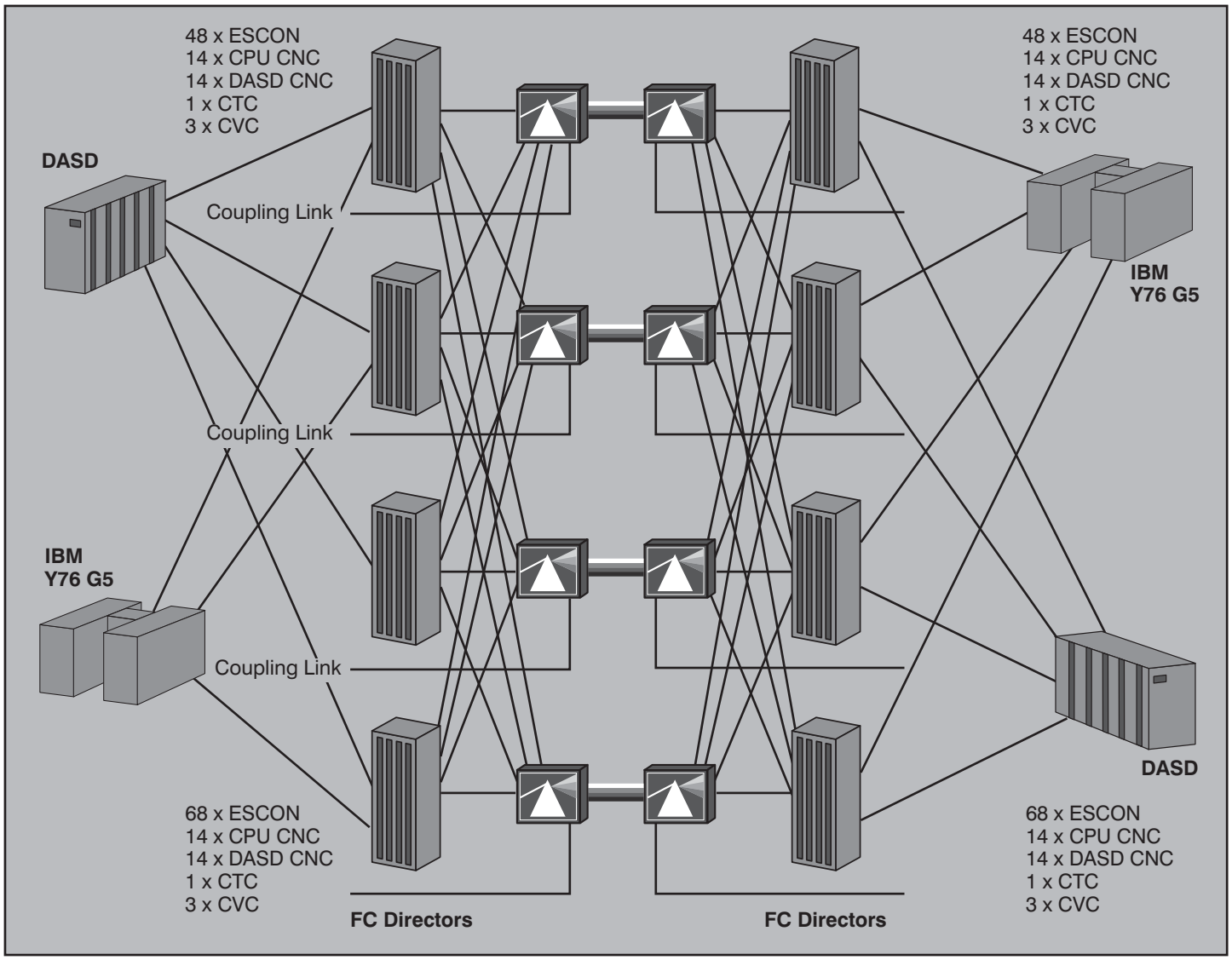


Abbildung 5.1: DWDM-FC-SAN Data Center Replication

Quelle: Cisco

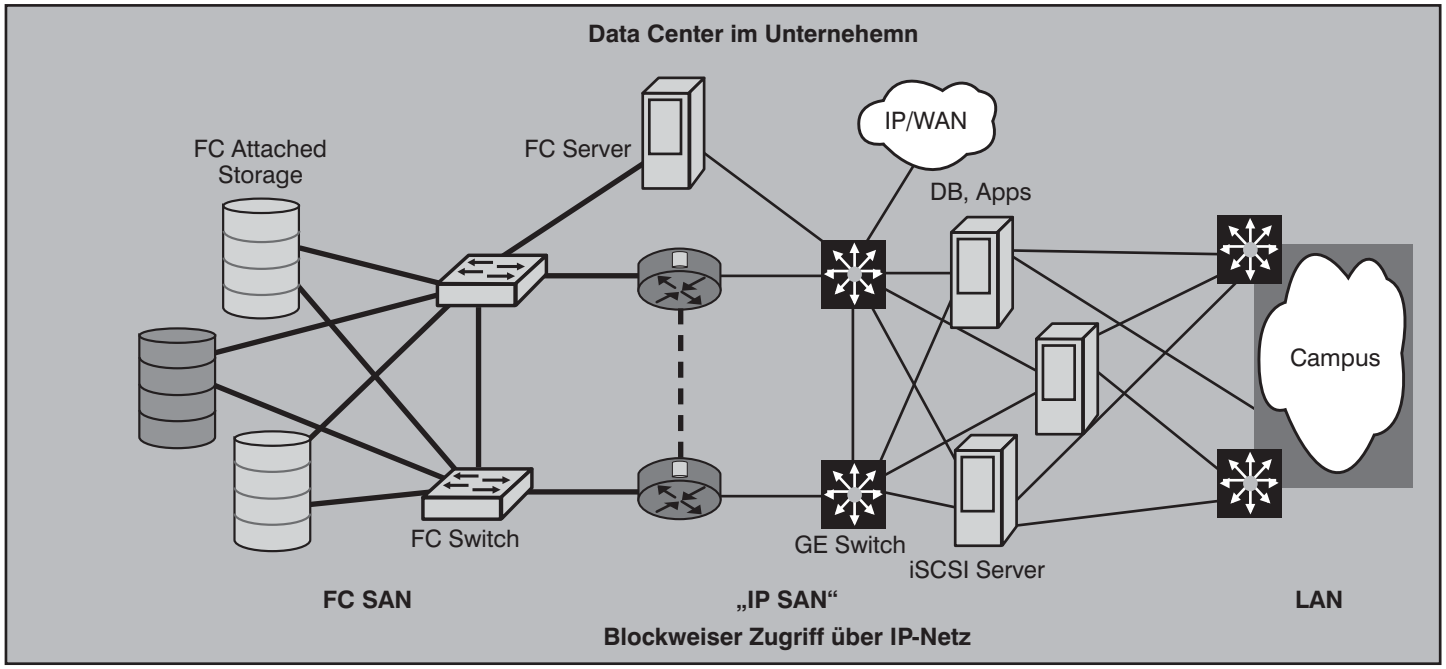


Abbildung 5.2: IETF iSCSI Storage über IP

rungen, deren Existenz man auch heute noch nicht unterschätzen sollte.

Auf der Abbildung 5.1 sieht man eine ältere Lösung von Cisco. Es gibt da natürlich mittlerweile viele Alternativen. Am besten gefällt mir persönlich in diesem Zusammenhang die Reihe 4200 von Ciena und zwar wegen ihrer hochgradigen Modularität und Skalierbarkeit. Von IP-Verkehr über FC, ESCON, FICON und Infiniband bis hin zu DS-1 Video frisst sie alle in einem solchen Zusammenhang denkbaren Datenströme und kann sie dann über CWDM, DWDM, SONET, ATM und 10 oder 40 GbE weitertransportieren.

Das führt aber jetzt nicht weiter, ich möchte vielmehr eine eher generelle Differenzierung hinsichtlich FCoE und iSCSI durchführen.

5.1 iSCSI und das Verlassen des RZs

Sieht man sich ältere Dokumente aus der Frühzeit der Entwicklung von iSCSI an, sieht man sofort, dass iSCSI ursprünglich genau dafür gedacht war, eine Speicherverlängerung über das RZ hinaus zu realisieren. So ein älteres Bild sehen sie in Abbildung 5.2.

Links haben wir die Komponenten des RZs. Der dominierende Verkehr ist FC. Rechts sehen wir ein gewöhnliches IP/Ethernet-Netz. In der Mitte gibt es Switches, die in geheimnisvoller Weise den FC-Verkehr in iSCSI-Verkehr umwandeln. Das ist auch an sich gar keine schlechte Idee, den sowohl FC als auch iSCSI machen definitiv das Gleiche: sie packen SCSI-Datenströme in Pakete, FC eben in FC-Pakete, iSCSI in Ethernet-Pakete. Und deshalb ist auch ein FC/iSCSI-Konverter eine durchaus denkbare und sinnvolle Komponente.

Eine weitere Idee an iSCSI war eben dann, dass iSCSI für den Weitertransport der Daten ein gewöhnliches Ethernet verwenden könne. Damals haben sich zwei unterschiedliche Welten gebildet: die Storage Area Networks SAN, eben FC-Netze, die, wie der Name sagt, im Bereich des RZs Speicher und Hosts unter- und miteinander verbinden und die Network Attached Storages NAS, die kein besonderes Netz benötigen, sondern einfach vermöge iSCSI an Ethernet angeschlossen werden können.

Von daher ist iSCSI von Konstruktion und Grundsatz her eine Technik, die so aufgebaut ist, dass sie ein irgendwie geartetes Ethernet mit all seinen bekannten Mängeln benutzen kann. Dadurch, dass iSCSI

Seminar

Sicherheit im LAN mit IEEE 802.1X
16.02. - 17.02.09 in Bonn

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.

Referent: Dr. Simon Hoff
Preis: € 1.490,- zzgl. MwSt.

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

von sich aus schon Elemente der Schichten 3 und 4 benutzt, ist auch die Harmonisierung mit Schicht 3-Verfahren wie OSPF, die heute in Unternehmen und Organisationen vornehmlich dazu dienen, die Fehler und Funktionslücken des Ethernets zu kompensieren, problemlos möglich.

Lange Zeit hat man iSCSI eine zu hohe Rechenkomplexität unterstellt und es daher auf einen unteren Leistungsbereich fixiert. Das ist aber von der Konstruktion her unberechtigt, wie man leicht sieht, wenn man den Gedanken der Hardwarebeschleunigung zu Ende denkt.

5.2 FCoE: Stirb langsam 27 (ohne Bruce Willis)

Anders sieht die Situation für FCoE aus. Manche werden denken: „fein, wenn FC auf Ethernet abgebildet wird, kann ich das ja nicht nur im RZ nutzen, sondern auch auf meinem ganzen Corporate Backbone“.

Das ist definitiv unrichtig. Zunächst einmal muss man deutlich klarstellen, dass FCoE von der Standardisierung durch SNIA und INTICS ausschließlich für die Verwendung in Switching Fabrics innerhalb des RZs gedacht ist. Es kann nun sein, dass ein Vertriebsbeauftragter eines Herstellers irgendwie zu viel Optimismus getankt hat und diesen Punkt übersieht. Kein seriöser Hersteller wird bewusst diese falsche Darstellung verfolgen.

Um es zusammenzufassen: *schickt man einen FCoE Datenstrom auf ein ausgedehntes normales Ethernet, wird der mit diesem zu übermittelnden SCSI-Datenstrom langsam aber sicher zugrunde gehen.*

Das glauben Sie mir jetzt natürlich nicht ohne weitere Erläuterung. Dazu muss ich leider erst ein paar Begriffe klären, damit es verständlich wird.

Um die Details des Speicherverkehrs richtig zu verstehen, ist es wichtig, die Begriffe **synchron, asynchron** und **plesiochron** auseinanderzuhalten. In einer Menge synchroner Signale geschehen die digitalen Transitionen innerhalb der Signale exakt mit der gleichen Taktrate. Es darf aber eine Phasendifferenz zwischen den Transitionen der zwei Signale geben, solange sie innerhalb spezifizierter Grenzen liegt. Diese Phasendifferenzen können durch Verzögerungen in der Ausbreitung des Signals oder Jitter liegen, der im Übertragungsnetz entsteht. In einem synchronen Netz können alle Uhren (Takte) auf eine zentrale Referenzuhr (Takt) **PRC** zurückgeführt werden. Die Genauigkeit der PRC ist höher als +/-1 in 10 exp. 11 und wird von einer Cäsium-Atomuhr abgeleitet. Bei zwei plesiochronen Signalen geschehen die Transitionen meist mit der gleichen Rate, wobei jede Abweichung in Grenzen liegen muss. Das tritt z.B. dann auf, wenn zwei Netze zusammenarbeiten müssen, die auf verschiedenen Referenzuhren basieren. Obwohl diese Uhren extrem genau sind, gibt es Unterschiede zwischen ihnen. Dies ist als plesiochrone Differenz bekannt. Man kann sich das auch anders merken: im Altgriechischen heißt plesiochron „vieluhrig“. Bei asynchronen Signalen müssen die Transitionen der Signale nicht notwendigerweise in den gleichen Nominalraten geschehen. Asynchron bedeutet in diesem Fall, dass die Differenz zwischen zwei Uhren wesentlich größer ist als im plesiochronen Fall. Das ist z.B. der Fall, wenn zwei Uhren von verschiedenen freilaufenden Quartzoszillatoren abgeleitet werden.

Zwischen Speichern und Servern wollen wir einen SCSI-Informationsstrom laufen lassen. SCSI ist ein Übertragungsprotokoll, welches ursprünglich auf einem möglichst breiten Systembus innerhalb eines einzigen Rechners oder eines Racks läuft. Diese Umgebung zeichnet sich dadurch aus, dass sie entweder synchron (in einem Rechner) oder plesiochron (getrennte Geräte in einem Rack) ist. Möchte man also einen SCSI-Informationsstrom auf etwas anderes abbilden, muss man dies berücksichtigen.

Ein Ethernet arbeitet grundsätzlich völlig asynchron. Bleibt das Ethernet, wie im RZ, räumlich klein, gibt es kaum Laufzeitprobleme und Jitter. Ist dann auch noch die Schaltgeschwindigkeit der Switches so ausgelegt, dass ein Ethernet-Paket gar nicht merkt, ob es nun grade über eine Leitung oder durch einen Switch läuft, kann man die Übertragung auch als plesiochron klassifizieren. Moderne Switches haben damit kaum ein Problem. Es ist ja lediglich notwendig, dass die Switching-Latenz in einem vernünftigen Verhältnis zur Daten- bzw. Paketrate steht.

Fibre Channel hat sich genau das zunutze gemacht. FC wurde für geringe Entfernungen, breite Übertragungswege und schnelle Switches mit vergleichsweise wenigen Ports definiert. FC ist somit ein „unechtes“ plesiochrones System. So kann man denn auch FCoE in diesem Zusammenhang sinnvoll betreiben, wenn die plesiochrone Qualität durch die Konstruktion der Switching Fabric gegeben ist.

Der SCSI-Informationsstrom verträgt zwar Unterbrechungen, aber keinesfalls ein zu großes Delay oder gar eine große Delayvarianz zwischen den einzelnen Teilen eines zu übertragenden Blocks, was die Grundeinheit für diese Technik ist.

FCoE hat aber von sich aus absolut gar keine Mittel, um Delay oder Delay-Varianz zwischen den einzelnen FCoE-Ethernet-Paketen zu verhindern. Wachsen diese Werte in einem großen und/oder verzweigten Netz zu stark an, kann sich FCoE nicht dagegen wehren und als Konsequenz reißt der SCSI-Informationsstrom mit einem Fehler ab, obwohl alle Pakete übertragen wurden. Damit kommen wir nochmal auf „Lossless“. Wir haben schon gesehen, dass es relativ mühsam ist, „Lossless“ in einer sehr überschaubaren Umgebung innerhalb des RZs zu implementieren. In einem verzweigten und/oder ausgedehnten Ethernet ist dies mit den bisher verfügbaren Hilfsmitteln praktisch ausgeschlossen. Außerdem sehen wir jetzt, dass „Lossless“ für FCoE eine notwendige, aber keinesfalls hinreichende Voraussetzung ist.

Wenn Sie tatsächlich FCoE über eine größere Distanz übertragen möchten, müssen Sie SONET mit ANSI „Ethernet over SDH“ nehmen. Das klappt gut, weil SONET ein plesiochrones System ist und Sie für diesen Zweck dort einige der permanent umlaufenden Transportcontainer nutzen können, die natürlich auch lossless arbeiten. Aber das ist natürlich von hinten durch die Brust nach vorne: FC-Abbildung auf Ethernet via FCoE, danach Ethernet-Abbildung auf SONET-Ocx via ANSI EoSDH und zurück. Da soll nochmal einer etwas über die Komplexität von iSCSI sagen.

Ach, ja: wie hilft sich nun iSCSI? Hier greift man auf einen Trick zurück. Das TCP schiebt alle Daten aus den Ethernet-Paketen, die zu einem SCSI-Block gehören, zusammen, bevor diese an das Ziel-SCSI übergeben werden. SCSI kennt Pausen zwischen den Blocks, es mag nur gar keine Unterbrechungen *innerhalb* eines Blocks. TCP ist schlauer als SCSI und täuscht diesem die Plesiochronität vor.

Es gibt noch eine Entwicklung, die man in diesem Zusammenhang erwähnen kann. Carrier Ethernet CE. CE ist eine auf mehreren Standardisierungsgremien basierende Bemühung, das Ethernet um bestimmte Qualitäten des SONET wie schnelles Wiederaufsetzen nach Fehlern, grundsätzliche Redundanz, Lossless und deterministische Arbeitsweise für Durchsetzung von CoS/QoS anzureichern. Primäres Ziel ist, dass Provider ein günstiges L2-Netz mit dieser angereicherten

Ethernet-Technik aufbauen können. Sie werden von CE in den nächsten Monaten noch viel hören, das weiß ich sicher. Aber auch führende Hersteller innerhalb der CE-Bewegung zweifeln daran, dass es gelingt, CE in gleichem Maße plesiochron zu gestalten wie SONET. Damit wäre auch CE für FCoE-Übertragung ungeeignet.

6. Konsequenzen für die Unternehmensnetze

Die Untersuchungen haben Folgendes zutage gefördert:

- Es gibt im Kontext eines RZ-Netzes keinen technologisch zu begründenden Vorteil für FCoE oder iSCSI. Beide Technologien können gleichermaßen - auch zusammen - im Rahmen der strategischen Ziele genutzt werden, wobei der Investitionsschutz im Vordergrund stehen kann.

- Es gibt im Kontext eines RZ-Netzes keinerlei Vorbehalte gegen den hinsichtlich der I/O-Konsolidierung gewinnbringenden Einsatz der FCoE-Technologie an den Stellen, an denen sie sinnvoll erscheint. Dabei sind allerdings bestimmte Voraussetzungen zu erfüllen, wie lossless-Übertragung und die Möglichkeit des Einsatzes von Jumbo-Frames.

- Es gibt im Kontext eines RZ-Netzes keine unlösbaren Probleme hinsichtlich der Erfüllung der Voraussetzungen für FCoE. Vielmehr gibt es sogar unterschiedliche Lösungswege, die natürlich auch kombiniert werden können.

- Es kann dabei allerdings passieren, dass die bisherigen Switches über die Grenzen ihrer Leistungsfähigkeit belastet werden und neue, leistungsfähigere Switches angeschafft werden müssen. Dies muss im Rahmen einer Kostenbalance mit dem Gegengewicht I/O-Konsolidierung bestimmt werden. Der Ausgang hängt extrem vom Einzelfall ab, man kann hier leider noch nicht einmal grundsätzliche Hinweise geben.

- Außerhalb des RZs ist FCoE völlig überfordert und konzeptionell unbrauchbar, auch wenn vielleicht in Einzelfällen eine entsprechende Verbindung rein zufällig funktioniert. Hier ist und bleibt iSCSI die einzig verfügbare Technologie für den Transfer von Speicherdaten.

Kongress

Netzwerk-Redesign Forum 2009
09. - 12.03.09 in Königswinter

Netzwerke sind der Lebensnerv unserer Unternehmen. Sie unterliegen einer permanenten Weiterentwicklung und Veränderung. Aus einem Mix aus Bedarf und technischen Möglichkeiten muss das individuelle Optimum für ein Unternehmen gefunden werden. Dieses Optimum muss zugleich an der Zukunft orientiert sein, da Netzwerk-Komponenten über einen langen Zeitraum stabil und ohne permanente Änderungen betrieben werden müssen.

Hier setzt das ComConsult Netzwerk-Redesign Forum 2009 an. Es analysiert die wichtigsten Bedarfsentwicklungen, stellt diesen die neuesten Netzwerk-Technologien gegenüber und erarbeitet Empfehlungen für ein erfolgreiches Netzwerk-Design, eine Zukunfts-oriente Auslegung und einen stabilen und zuverlässigen Betrieb.

Einige Schwerpunktthemen des ComConsult Netzwerk-Redesign-Forums 2009 sind:

Neue Redundanz-Verfahren
- Was ist Stand der Redundanz-Technik in Layer-2 und Layer-3?
- Was kommt auf uns zu?
- Was passiert im direkten Umfeld von Server und Speicher-Systemen?
- Welchen Stellenwert haben Hersteller-Spezifische Lösungen?
- Cisco, Enterasys, Extreme, Foundry, HP, Juniper, Nortel: wer macht was?
- Standardisierung: was ist Zukunfts-orientiert, wie können Investitionen und ein stabiler Betrieb geschützt werden?

Layer-2 kontra Layer-3
- große Layer-2-Netzwerke: wo liegen die Probleme Heute?
- Integration oder Parallelbetrieb mit Layer-3: welche Optionen bestehen?
- Standort-Kopplungen mit Layer-2: Proprietär kontra Standard, welcher Weg ist Zukunfts-orientiert?

Verkabelung 2009
- Verkabelungstechnik 2009: wo stehen wir?
- Twisted Pair: welche Kabel-Qualität, welcher Stecker?
- Glasfaser: Multimode kontra Singlemode, OM2 kontra OM3 kontra OM4,
- welcher Stecker prägt die Zukunft?
- Was unterstützen die Hersteller?
- Hoher Bestand aus Cat 5 oder Cat 6 und OM2: was ist zu tun?

MPLS kontra Carrier-Ethernet kontra OSPF
- was ist Carrier-Ethernet, für wen ist es eine Option?
- CE kontra MPLS: ist dies das Ende von MPLS?
- CE im Unternehmens-Backbone: wirklich eine Alternative?
- Große Layer-2-Netzwerke in der Industrie: wird CE die bisher dort dominierenden Verfahren verdrängen?

Integration mobiler Mitarbeiter / Fixed-Mobile-Konvergenz
- Fixed-Mobile-Konvergenz: was bedeutet das?
- Wohin geht der weitere Weg? Wo groß sind die Potenziale wirklich?
- Wie gut und nutzbar sind die Produkte?

WAN-Redesign
- Wir geben den Überblick: was passiert im WAN?
- Welche Leistungen entstehen, wie weit kann das gehen?

Moderation: Dr. Jürgen Suppan
Preis: € 2.090,- zzgl. MwSt.* - gültig bis 31.12.08 - dann regulär € 2.290,- zzgl. MwSt.

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

Schwerpunktthema

Dominik Zöller ist seit 2006 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich auf die Themengebiete der Kommunikationsnetze und der Betriebssysteme. Bei ComConsult ist er vorwiegend mit der Evaluierung, Planung und Ausschreibung professioneller Unified Communications, Kollaborations- und Videokonferenz-Systeme befasst.

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

Sicherheitsaspekte öffentlicher Mobilfunknetze Teil 1: Gefährdungen im öffentlichen Mobilfunk

Fortsetzung von Seite 1

Der Mitarbeiter steht immer in Kontakt zu seinem Heimatstandort oder der koordinierenden Zentrale. Kein Unternehmen kann es sich heute noch leisten, auf diese Flexibilität zu verzichten. Im Nachsatz zur Sprachkommunikation wurden in der Unternehmenswelt sehr bald auch mobile Datendienste populär. Heute ist der mobile Zugriff auf Email, Internet und Unternehmensdaten fast selbstverständlich. (siehe Abbildung 1)

Doch was ist der Preis der Mobilität? Wie steht es um den Schutz der Privatsphäre? Welche Eingriffe in die vermeintlich vertrauliche Unterhaltung am Mobiltelefon sind technisch möglich, welche gar erlaubt? Welche Konsequenzen hat die mobile Datenkommunikation für das Unternehmensnetz? Und wie kann die Vertraulichkeit technisch sichergestellt werden? Dieser zweiteilige Artikel soll die Risiken des Mobilfunks beleuchten und Anregungen geben, um eine sichere Nutzung zu ermöglichen. Der vorliegende erste Teil beschäftigt sich hierbei mit technischen Aspekten von Netzen und

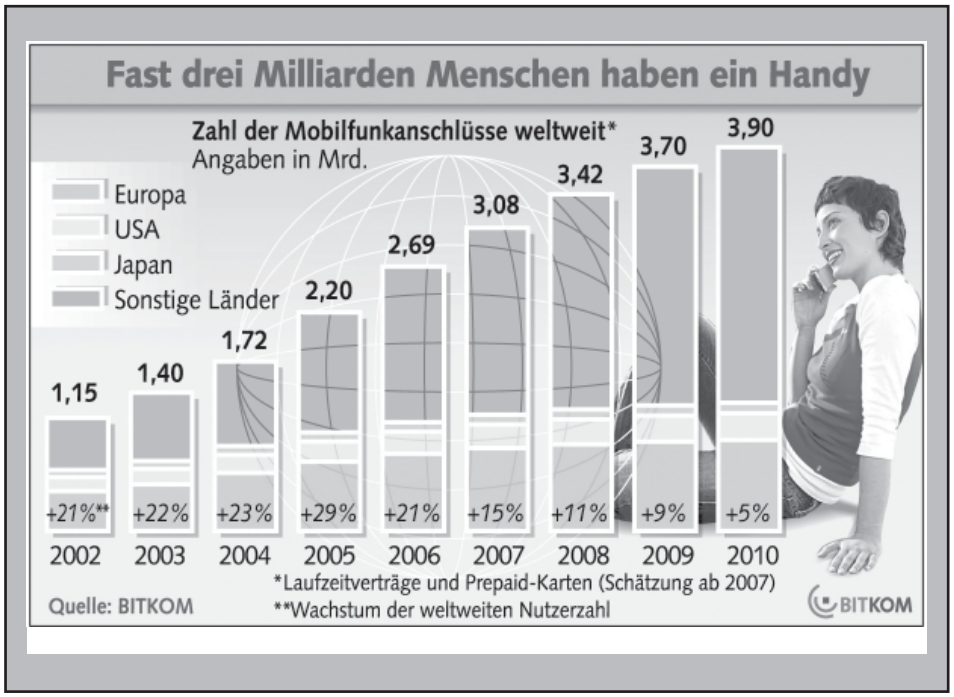


Abbildung 1 Weltweit steigen die Nutzerzahlen der Mobilfunknetze (Quelle: BITKOM)

Diensten und den hieraus erwachsenden Gefährdungen für Privatsphäre und Datensicherheit. Im zweiten Teil werden dann Anregungen zur organisatorischen und technischen Absicherung mobiler Kommunikationsinfrastruktur gegeben.

Die Netze

Mobilfunknetze, wie wir sie heute kennen, basieren in erster Linie auf dem GSM-Standard. Zunächst nach der mit der Standardisierung befassten Group Spéciale Mobile benannt, steht GSM heute für „Global System for Mobile Communications“. Im GSM Standard sind sowohl die eingesetzten Verfahren zur Modulation der Übertragungskanäle und der Sprachcodierung als auch die grundlegende Architektur eines GSM-Netzes festgeschrieben. Zur Funkübertragung werden - in international verschiedenen Ausprägungen – die Frequenzbänder 900 MHz, 1800 MHz und 1900 MHz verwendet. Die verschiedenen Frequenzbänder werden anhand von Zeit- und Frequenzmultiplexing in einzelne Kanäle unterteilt (siehe Abbildung 2). So kann jede Basisstation (Base Transceiver Station, BTS) im BSS gleichzeitig einer Vielzahl von Endgeräten den Zugriff ermöglichen.

Ein GSM-Netz besteht aus verschiedenen Subsystemen, die unterschiedliche Aufgaben übernehmen. Das Base Station Subsystem (BSS) dient dabei den Nutzern als Zugriffspunkt. Es verbindet das Mobile Endgerät mit dem Network Subsystem (NSS) und dem Operations and Support System (OSS). Während das OSS alle

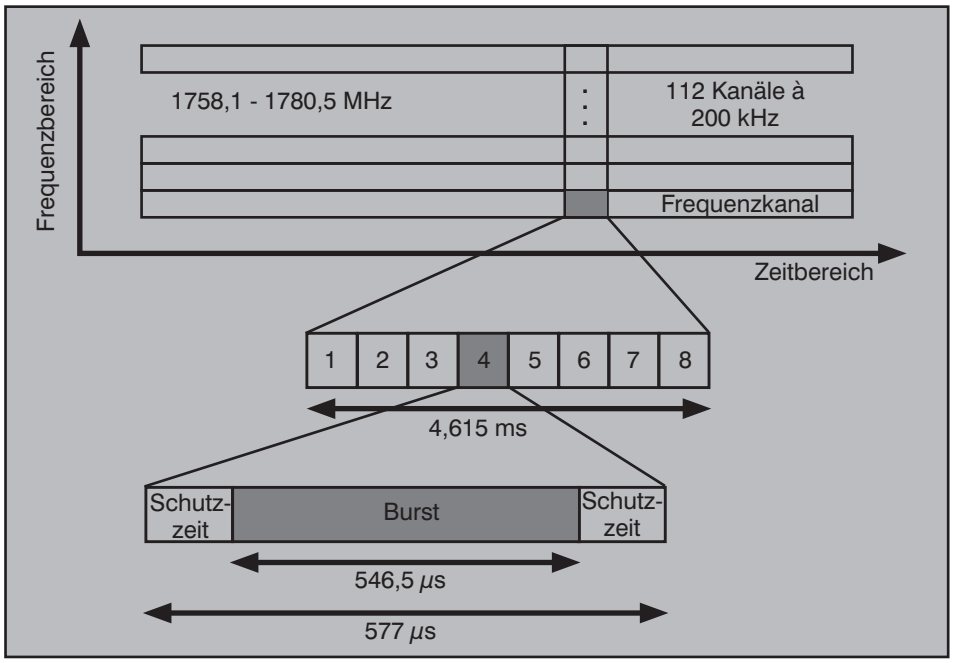


Abbildung 2: Kanalmodellierung bei GSM – Acht Zeitscheiben pro Frequenzkanal

für die Verwaltung eines Mobilfunknetzes notwendigen Komponenten enthält, bildet das NSS den eigentlichen Kern eines GSM-Netzes. In ihm werden Teilnehmer verwaltet, Authentisierungs- und Ortsinformationen gespeichert sowie die Vermittlung sämtlicher Sprachverbindungen vorgenommen.

Datendienste als Innovationstreiber

Um auch Datenanwendungen auf mobilen Endgeräten zu ermöglichen, wurde der Standard nachträglich um ein weiteres Subsystem erweitert, das so genannte GPRS Core Network. General Packet Radio Service (GPRS) ist ein Standard, der das GSM-Netz zu paketvermittelter Datenübertragung befähigt. Das GPRS Core Network stellt dabei mittels entsprechender Gateways die Anbindung zu den Datennetzen anderer Provider und dem Internet her. (siehe Abbildung 3)

Die zunehmende Nutzung mobiler Datendienste zeigte aber bald die Grenzen des

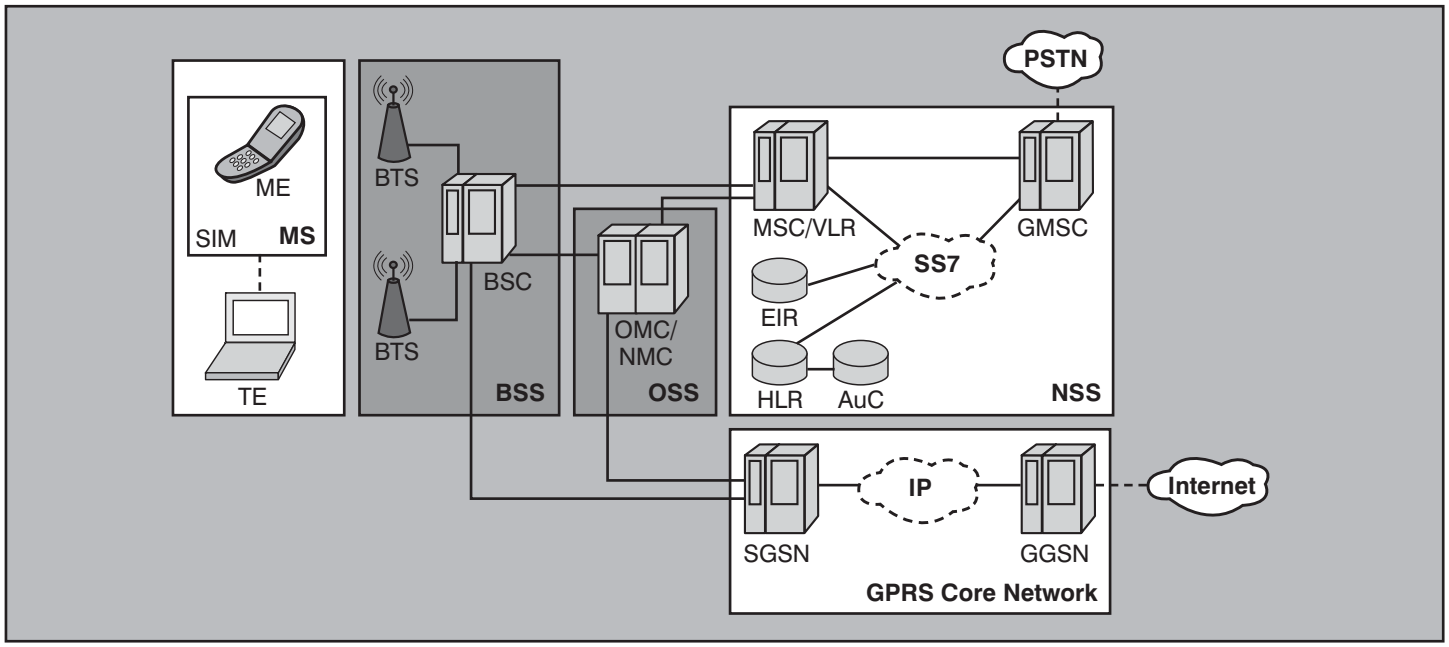


Abbildung 3: Architektur eines GSM- und GPRS-Netzes

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

GSM-Standards auf. Mit einer Nettodatenrate von acht bis 20 kbit/s pro Kanal und begrenzter Kanalbündelung (maximal vier Kanäle für den Downlink) ergibt sich ein Maximaldurchsatz von 80 kbit/s pro Endgerät – ohne jegliche Fehlerkorrektur! Hinzu kommt, dass pro Funkzelle – abhängig von der Lizenz des Netzbetreibers – nur um die 100 Trägerfrequenzen mit je 8 Kanälen zur Verfügung stehen. Das begrenzt die Gesamtdatenrate auf in der Praxis höchst illusorische 16 MBit/s – für alle in der Zelle befindlichen Endgeräte. In Zeiten hochbitratiger Internetverbindungen muten diese Werte geradezu antiquiert an. Da verwundert es nicht, wenn es – insbesondere in Ballungsräumen – zu Engpässen kommt. Eine Weiterentwicklung der zweiten Generation der Mobilfunknetze (2G), wie GSM und GPRS auch genannt werden, war also dringend notwendig.

Attraktive Krücke

Die erste Stufe der Weiterentwicklung ist das so genannte EDGE, was für „Enhanced Data Rates for GSM Evolution“ steht. Ziel dieses Verfahrens war es, mit minimalen Änderungen am GSM-Netz eine Erhöhung der Datenraten zu erzielen. Hierzu setzt EDGE ein anderes Modulationsverfahren ein, was wahlweise zum GSM-spezifischen Verfahren verwendet werden kann und das – je nach verwendetem Codierungsschema – rund die dreifache Datenrate ermöglicht. Dabei bleiben Architektur und Multiplexing-Verfahren des GSM-Netzes unangetastet, was die Kosten für einen Ausbau niedrig hält. In vielen Fällen ist die Aufrüstung mit einem Software-Update erledigt. Daher rührt auch die häufige Bezeichnung 2.5G für EDGE, das in der Einführung preiswert und deshalb als Fallbacklösung beliebt ist, wenn sich der Ausbau von Netzen der dritten Generation wirtschaftlich (noch) nicht rechnet.

Da geht noch was!

Die aktuelle, dritte Generation der mobilen Kommunikationsnetze stellt das Universal Mobile Telecommunications System (UMTS) dar. UMTS bedient sich eines grundlegend anderen Multiplexing-Verfahrens, was die Extrapolation sich überlagernder Funksignale ermöglicht. Hierdurch ist keine Aufteilung in starre Kanäle mehr notwendig und die Datenrate kann auf Werte zwischen 144 und 384 kbit/s pro Endgerät erhöht werden. Im Gegensatz zu EDGE basiert UMTS nicht auf den herkömmlichen GSM-Netzen. Auch wenn sich architekturelle Gemeinsamkeiten finden, so unterscheiden sich doch sowohl die verwendeten Frequenzbänder (1920,3-1979,7 MHz und 2110,3-2169,7 MHz) als auch die Übertragungstechnik grundlegend voneinander. Des Weiteren wurde in der Architektur der gestiegenen Bedeutung mobiler Datendienste Rechnung getragen, was sich im Zusammenführen der paketvermittelten und der leitungsvermittelten Dienste im UMTS Core Network niederschlägt.

Durch beständige Weiterentwicklung der Modulations- und Codierungsverfahren wurden die Datenraten der UMTS-Netze nochmals gesteigert, so dass heute mit dem High Speed Download Access (HSDPA) und dem High Speed Uplink Access (HSUPA) zwei Verfahren zur Verfügung stehen, mit denen Datenraten von momentan bis zu 3,6 MBit/s möglich sind. Diese als 3.5G bezeichneten Techniken stellen eine weitere Evolutionsstufe auf dem Weg zu zukünftigen Mobilfunknetzen dar. Der nächste Schritt wird das vom Standardisierungsgremium 3GPP (Third Generation Partnership Project) zum Kronprinz erklärte High Speed Orthogonal Frequency Division Multiplexing Packet Access (HSOPA) sein. Hinter diesem schwerfällig anmutenden Titel verbirgt sich eine Technologie, die maximale Datenraten in der Größenordnung moderner WLANs und darüber hinaus verspricht. All diesen Verfahren ist gemein, dass sie auf der Netzarchitektur des UMTS-Standards basieren und zu diesem kompatibel sind. Ob dies auch für die zukünftige vierte Generation der Mobilfunknetze gelten wird, ist unklar. Heiße Anwärter darauf, sich als Basistechnologie für diese zukünftigen Netze zu qualifizieren, sind neuere WLANs der 802.11- und 802.16-Familien. Welche Technik hier schließlich das Rennen machen wird, liegt in der Hand der Arbeitsgruppe 3GPP Long Term Evolution (3GPP LTE).

Evolution? Aber sicher!

Das Tuning der Mobilfunk-Netze für schnelle Datendienste ist nur ein Aspekt von UMTS. Vielmehr wurden sowohl die Architektur als auch einzelne, teils sicherheitsrelevante Funktionen des Standards einer Generalüberholung unterzogen. Dabei zog man zum Teil die Konsequenzen aus bekannt gewordenen Sicherheitslücken des GSM-Standards und trug gleichzeitig dem - gerade im Geschäftsbereich - steigenden Bedarf an gesicherter Datenübertragung Rechnung.

Beispielhaft sieht man dies am Vergleich der eingesetzten Authentisierungs- und Verschlüsselungsverfahren. Zur Authentisierung wird vom Netzbetreiber eine Zufallszahl generiert und an das zu authentisierende Endgerät geschickt. Sowohl auf Seiten des Netzbetreibers als auch auf Endgeräteseite wird hieraus ein 32 Bit langer Wert berechnet. Dies geschieht nach GSM-Spezifikation anhand des Algorithmus A3. Im Endgerät ist hierfür die SIM-Karte zuständig, die neben dem für diese Berechnung zuständigen Prozessor auch den Subscriber Authentication

Seminar

Office Communications Server 2007

08.12. - 09.12.08 in Bonn

Un diesem Seminar werden sowohl die technischen als auch die strategischen Aspekte des Office Communications Servers analysiert. Unsere herstellerunabhängigen und neutralen Experten haben sich sehr ausführlich mit den technischen Details befasst und verfügen über langjährige Erfahrung bei der Implementierung von Microsoft-Lösungen, bei der Konzeption von TK-Lösungen sowie bei der Bewertung von Kommunikationstechnologien.

Moderation: Markus Holländer, Dr. Frank Imhoff, Dipl.-Inform. Michael van Laak
Preis: € 1.390,- zzgl. MwSt.

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

Key Ki des Mobilfunkteilnehmers enthält. Dieser liegt auch auf Seiten des Netzbetreibers (im so genannten Authentication Center (AuC), einer Entität im NSS) vor und wird auf beiden Seiten mit in die Berechnung einbezogen. Nach erfolgreicher Berechnung sendet das Endgerät den Wert an das Authentication Center, wo ein Vergleich stattfindet. Stimmt das Ergebnis mit dem im AuC generierten Wert überein, gilt das Endgerät als erfolgreich authentisiert und darf sich am Netz anmelden. Nach demselben Verfahren wird anhand des Algorithmus A8 ein 64 Bit langer Sitzungsschlüssel generiert. Dieser wird dann von beiden Seiten zur Verschlüsselung von Sprach- und Datenverkehr auf der Luftschnittstelle eingesetzt. Die Verschlüsselung findet mit Hilfe von Algorithmus A5 statt, von dem verschiedene Varianten existieren. (siehe Abbildung 4)

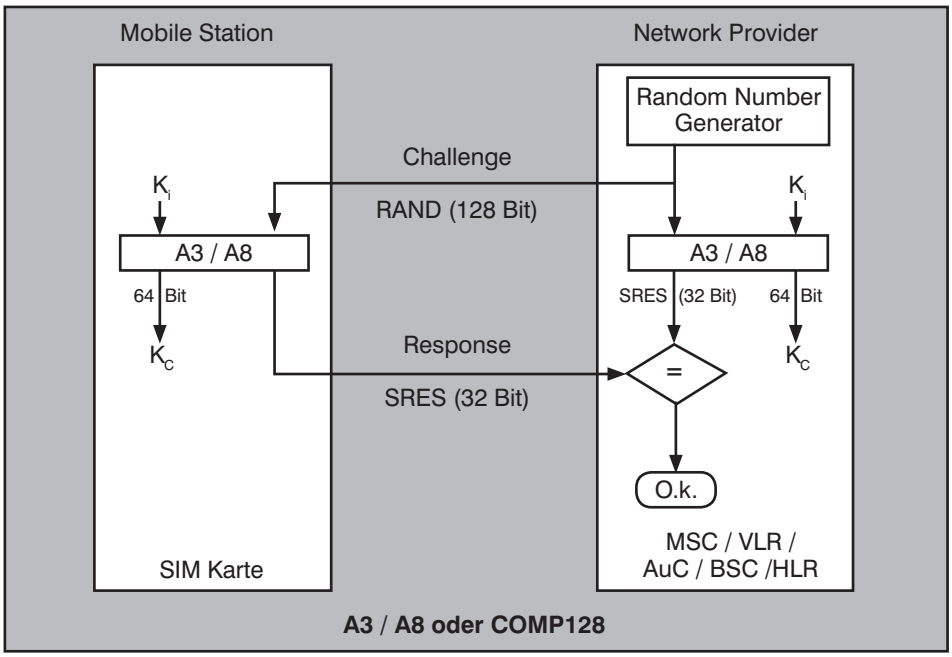


Abbildung 4: Authentisierung und Schlüsselgenerierung nach den Algorithmen A3 und A8

An den oben beschriebenen Verfahren gibt es eine Reihe von Kritikpunkten:

- Der Subscriber Authentication Key ist ein so genanntes Shared Secret: Die Kenntnis dieses Schlüssels ermöglicht die Übernahme der Identität eines Mobilfunkteilnehmers. Wenn also das Network Subsystem unzureichend abgesichert ist, könnte ein Angreifer oder Innentäter Zugriff auf sämtliche Shared Secrets erhalten. Damit wäre er in der Lage, innerhalb des GSM-Netzes die Identität jedes beliebigen Kunden anzunehmen.

- Die Algorithmen A3 und A8 sind im GSM Standard nicht exakt festgeschrieben. Der Netzbetreiber kann eine „geeignete“ Implementierung wählen. Diese Idee stammt offensichtlich aus einer Zeit, als proprietäre Implementierungen noch als implizit sicher galten.

- Einige Varianten des zur Verschlüsselung verwendeten Algorithmus A5 sind unsicher. Variante A5/0 beispielsweise ist eine Platzhalter-Funktion, die überhaupt nicht verschlüsselt. Die Varianten A5/1 und A5/2 sind Stromchiffren, die heute als unsicher gelten. Da ein Wechsel der verwendeten Variante durch das Betreibernetz initiiert werden kann, ist eine zuverlässige Verschlüsselung nicht gewährleistet. Erst die im Zuge von UMTS auch für GSM standardisierte Variante A5/3 (auch Kasumi genannt) ist nach heutigem Stand der Technik als sicher anzusehen.

- Die Authentisierung ist einseitig: Zwar wird der mittels A3 generierte Wert vom Endgerät an das AuC geschickt und dort auf Richtigkeit überprüft. Umgekehrt findet eine solche Überprüfung aber nicht statt.

Der Grund für den letzten Kritikpunkt liegt auf der Hand: Beim Entwurf von GSM stand offensichtlich im Fokus, das Netz vor seinen Teilnehmern zu schützen. Es sollte sichergestellt werden, dass kein Teilnehmer sich unberechtigt Zugriff auf das Mobilfunknetz erschleicht und damit den kommerziellen Interessen der Netzbetreiber schadet. Auf die Idee, dass es nötig sein könnte, den Teilnehmer vor dem Netz zu schützen, kam zu diesem Zeitpunkt wohl niemand.

Catch me, if you can!

Ein Beispiel für einen Missbrauch dieser Schwachstelle ist der so genannte IMSI-Catcher. IMSI steht hierbei für International Mobile Subscriber Identity, also der weltweit eindeutigen Kennung des Mobilfunkteilnehmers. Das Prinzip ist einfach: Der IMSI-Catcher verhält sich gegenüber dem Endgerät wie die Basisstation eines Mobilnetzbetreibers. Durch erhöhte Sen-

Verbesserte Sicherheit durch UMTS

Authentisierung: Im Gegensatz zu GSM findet bei UMTS eine gegenseitige Authentisierung von Endgerät und Basisstation (Node-B) statt. Dadurch werden Man-in-the-Middle Attacken wirkungsvoll unterbunden.

Verschlüsselung: Während ursprünglich für GSM nur nicht offengelegte und - nachgewiesenermaßen - unsichere Stromchiffren (A5/1, A5/2) zur Verfügung standen, wurde im Zuge der Standardisierung von UMTS ein neuer Blockchiffre eingeführt. Der „KASUMI“ (japanisch „verschleiert“) genannte Algorithmus fand im Nachhinein als A5/3 auch bei GSM Verwendung. Aus Gründen der Abwärtskompatibilität kann aber auf alte, unsichere Verfahren zurückgegriffen werden.

Verschlüsselte IMSI: Im Gegensatz zu GSM findet die Übertragung der IMSI (International Mobile Subscriber Identity) niemals im Klartext, sondern immer in Form der verschlüsselten EMSI (Encrypted Mobile Subscriber Identity) statt. Das erschwert die Zuordnung von Kennung und Teilnehmer und das Fälschen der Teilnehmererkennung erheblich.)

Temporäre IMSI: Wie auch in neuen Releases des GSM Standard vorgesehen, wird im Laufe der Verbindung zum Mobilfunknetz die IMSI regelmäßig gewechselt. Was bei GSM die TMSI (Temporary Mobile Subscriber Identity) ist, nennt sich unter UMTS TEMSI (Temporary Encrypted Mobile Subscriber Identity). Das regelemäßige Durchwechseln der TEMSI erschwert die Entschlüsselung der EMSI zusätzlich.

deleistung „unterdrückt“ er das Signal der in der Umgebung befindlichen Basisstationen (BTS). Dadurch versucht das Endgerät, sich am IMSI-Catcher anzumelden. Dieser erhält so Kenntnis über die IMSI eines Teilnehmers. Ortung und Zuordnung der IMSI zu einer Person stellen dann kein Problem mehr dar. Außerdem können die Anmeldeinformationen vom IMSI-Catcher zur echten BTS durchgeleitet werden, er verhält sich also gegenüber dem Netzwerk wie ein Endgerät. So passieren alle relevanten Daten den IMSI-Catcher, statt direkt zwischen Endgerät und BTS ausgetauscht zu werden – eine klassische Man-in-the-Middle Attacke. Falls das Endgerät und die Basisstation es zulassen, kann die Verschlüsselung auf A5/0, also unverschlüsselte Übertragung zurückgefahren werden. Andernfalls können die mitgelesenen Informationen nach einer der bekanntgewordenen Angriffsmethoden auf die Stromchiffren A5/1 und A5/2 in Echtzeit entschlüsselt werden.

Für den behördlichen und nachrichtendienstlichen Einsatz eingeschränkt zulässig, ist der Betrieb solcher Geräte in Deutschland für Privatpersonen und Unternehmen untersagt. Aber zu glauben, ein Angreifer mit der notwendigen kriminellen Energie ließe sich hiervon abhalten, wäre mehr als blauäugig. Die notwendige Technik ist zwar alles andere als preisgünstig, aber je nach Ausführung ist sie teilweise sogar im europäischen Ausland legal zu beziehen – bequem per Internet und frei Haus. Was gerade im Bereich der Industriespionage mit einem abhörtauglichen IMSI-Catcher angerichtet werden kann, mag sich niemand gerne vorstellen. Gespräche sensiblen Inhalts zwischen Mitgliedern der Geschäftsleitung aufzeichnen? Ein Bewegungsprofil der Patrouille des Werkschutzes erstellen? Vertrauliche Geschäftsbeziehungen anhand sozialer Netze rekonstruieren? Mit dem Zugriff auf Teilnehmerkennungen und Ortsinformationen sind solche Attacken auf ein Unternehmen problemlos möglich.

All das würde verhindert, wenn sich die Basisstation ihrerseits gegenüber dem Endgerät authentisieren müsste. Dem wurde mit dem UMTS-Standard Rechnung getragen. Die Authentisierung des Endgeräts wird erst initiiert, wenn sich die Basisstation (in UMTS-Nomenklatur Node-B) anhand eines Authentication Token erfolgreich gegenüber dem Endgerät ausgewiesen hat. Das grundlegende Verfahren entspricht im Prinzip dem von GSM, ist aber durch die beidseitige Authentisierung deutlich sicherer. Zusätzlich werden personenbezogene Daten wie die IMSI niemals unverschlüsselt übertragen und können so nicht in die Hände eines Angreifers gelangen. Nach dem Aushandeln der Verbindung und Authentisierung anhand der Encrypted Mobile Subscriber Identity (EMSI) wird im Folgenden auf die TEMSI (Temporary EMSI) zurückgegriffen. Diese wird anhand von zufälligen Parametern zyklisch gewechselt, was ein Abhören und Orten des Nutzers zusätzlich erschwert. Die Aufgaben der SIM-Karte bei Authentisierung und Verschlüsselung übernimmt im UMTS-Standard das so genannte Universal Subscriber Identity Module (USIM), welches eine Teileinheit der Universal Integrated Circuit Card (UICC), der Nachfolgerin der herkömmlichen SIM-Karte, ist. Auch die Verschlüsselung wurde verbessert, der unter dem Namen Kasumi (japanisch für „verschleiert“) bekannte Algorithmus ist ein Blockchiffre, dessen Quellen komplett offen gelegt wurden. Er wurde unter dem Namen A5/3 nachträglich in den GSM-Standard aufgenommen.

Flashback

All diese Verbesserungen könnten die Luftschnittstelle nach heutigem Stand vor unbefugtem Zugriff schützen. Wenn da nicht das Problem der Abwärtskompatibilität wäre. Aus wirtschaftlichen Gründen erfolgte kein kompletter Austausch der bestehenden GSM-Infrastruktur durch UMTS-Technologie. Weder sind UICC und USIM flächendeckend im Einsatz, noch wurden alle BTS durch UMTS Node-B ausgetauscht. Selbst wenn dies kostenneutral zu realisieren wäre – ein Teil der Kunden verfügt zwar bereits über UMTS-fähige Endgeräte nutzt dieses Netz aber für kaum mehr als gelegentliches Surfen. Die höheren Kosten schrecken viele Anwender gerade im privaten Bereich noch ab. Sicherheitsaspekte fallen bei Vertragsabschluss in der Regel kaum ins Gewicht. Auch wenn die Zahlen der UMTS-Nutzer beständig steigen (siehe Abbildung 5), ist ein Großteil der Verträge noch auf die Nutzung von GSM beschränkt.

So bleibt den Netzbetreibern nur eine Möglichkeit: Der Austausch der Infrastruktur wird stückweise vollzogen, so dass lange Zeit ein Parallelbetrieb notwendig ist. Viele der neuen Sicherheitsfeatures wurden auf diesen Mischbetrieb ausgelegt. Netz wie Endgeräte unterstützen gleichermaßen den Rückfall in alte GSM-Marotten. Dieser Sachverhalt wird sich erst ändern, wenn alle Kunden auf die neue UMTS-Technologie umgestellt wurden. Doch bis dahin wird vermutlich bereits ein Netz der vierten Generation im Aufbau begriffen sein. Wenn man davon ausgeht, dass in der Zukunft auch bei UMTS Sicherheitsmängel aufgedeckt werden, so stünde man hier erneut vor derselben Problematik.

Intelligente Infrastruktur

Auch wenn die Luftschnittstelle der Mobilfunkkommunikation natürlich besonderen Gefährdungen ausgesetzt ist: auch die fest verdrahtete Infrastruktur der Netzbe-

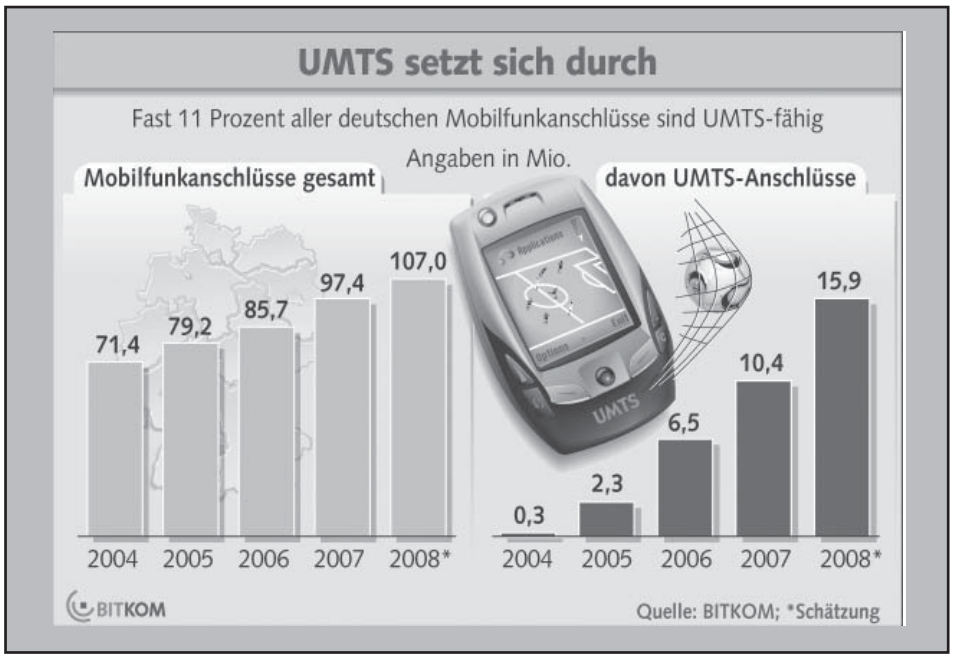


Abbildung 1 Weltweit steigen die Nutzerzahlen der Mobilfunknetze (Quelle: BITKOM)

treiber bedarf eines kritischen Blicks. Welche Daten werden hier über den Kunden vorgehalten? Wer hat auf welche Daten Zugriff? Wie bereits erwähnt unterteilt sich das Netz eines Mobilfunkbetreibers in verschiedene Funktionsgruppen. Auch wenn sich die Nomenklatur und konkrete Architektur zwischen GSM/GPRS/EDGE und UMTS in Details unterscheiden, so ist der grundlegende Aufbau doch soweit identisch, dass die wichtigsten Komponenten gemeinsam betrachtet werden können.

Die erste Funktionsgruppe, mit der das Endgerät in Berührung kommt, ist das Base Station Subsystem (BSS), dessen UMTS Äquivalent das Radio Network Subsystem ist. Beide bestehen aus mehreren Basisstationen (Base Transceiver Station (BTS) bzw. Node-B) und einem Controller (Base Station Controller (BSC) bzw. Radio Network Controller (RNC)). Die Summe all dieser Subnetze ergibt das GERAN bzw. UTRAN eines Providers (GSM/EDGE Radio Access Network / UMTS Terrestrial Radio Access Network). Hier werden keine Daten über den Teilnehmer vorgehalten. Wichtig ist allerdings, dass jedes dieser Subnetze sich in ein oder mehrere so genannte Location Areas (LA) aufteilt, die über die Location Area Identity (LAI) identifiziert werden können. Hierüber und über zusätzliche Informationen, z.B. die verwendete Basisstation und sogar die zuständige Sektorantenne, kann eine grobe Ortsbestimmung des Teilnehmers geschehen. All diese Informationen werden im Network Subsystem (NSS) für das Routing ein- und ausgehender Anrufe und zu Abrechnungszwecken benötigt.

Wer weiß was?

Die aktuelle LAI eines Teilnehmers wird im NSS mit anderen Daten des Teilnehmers verknüpft. Dazu zählen das verwendete Endgerät (International Mobile Equipment Identity, IMEI), die Teilnehmer Identifikation (IMSI), Shared Secret sowie allgemeine Verbindungsdaten, wie z.B. Dauer und Ziel eines Telefongesprächs. All diese Daten werden in verschiedenen Datenbanken gespeichert (siehe Kasten „Datenbanken im Mobilfunknetz“), auf die Mobile Switching Center (MSC) und Global MSC (GMSC), welche für das Routing zuständig sind, zugreifen. Aber auch administrative Komponenten aus dem Operations and Support System (OSS) können auf diese Daten zugreifen. Neben der Verwaltung der Teilnehmer und Abrechung der Verbindungen werden in diesem Teil des Netzes auch Mechanismen zur staatlichen Kontrolle der Netze implementiert. Dazu zählen die per Gerichtsbeschluss erwirkbaren Abhörmaßnahmen durch polizeiliche oder geheimdienstliche Stellen (engl. Lawful Interception) ebenso, wie die durch die EU-Richtlinie 2006/24/EG ab dem 01.01.2009 vorgeschriebene Vorratsdatenspeicherung. Lässt man die Bedenken der Datenschützer einmal außen vor und unterstellt die Rechtsstaatlichkeit dieser Maßnahmen, so ändert dies nichts an der Tatsache, dass die Datenbanken der Mobilfunkbetreiber extrem sensible Daten beinhalten.

Die Mehrheit der Mobilfunkteilnehmer wird – vermutlich zu Recht – die Meinung vertreten, dass sie vor dem Staat nichts zu verbergen haben und die Speicherung von Verbindungsdaten oder das gezielte Abhören von Tatverdächtigen einen Beitrag zur Inneren Sicherheit leisten können. Ein Stückchen Privatsphäre im Tausch gegen ein Stückchen Sicherheit. Eine durchaus nachvollziehbare Haltung. Richtig brisant wird es dann, wenn nicht der Staat, sondern eine nicht rechtlich legitimierte Instanz Zugriff auf diese Daten erhält. Für sich genommen ist die IMSI oder LAI eines Teilnehmers noch keine Information von großer Tragweite. Sprengstoff wird daraus erst durch die Verknüpfung der Daten vieler Teilnehmer untereinander. So lassen sich nicht nur Bewegungsprofile Einzelner, sondern ganze soziale Netzwerke mit allen Interaktionen der Individuen, wie etwa persönlichen Treffen an einem bestimmten Ort oder geführten Telefongesprächen, rekonstruieren. Besteht dann noch die Möglichkeit, diese Netze mit Inhalten zu verknüpfen - ob das nun das Konsumentenverhalten oder der Inhalt eines Telefongesprächs ist - lässt sich ein exaktes Bild über Gewohnheiten und Aktivitäten von Mobilfunkteilnehmern erstellen. Dies kann, gerade im geschäftlichen Umfeld, weitreichende Konsequenzen haben. Vertrauliche Informationen zu Geschäftsbeziehungen und Kunden sowie Intellectual Property stehen zur Disposition.

Jenseits aller orwellschen Paranoia wird hieran eines deutlich: Die Nutzung von Mobilfunknetzen setzt Vertrauen voraus. Vertrauen in die Einhaltung rechtstaatlicher Rahmenbedingungen und in die Gewissenhaftigkeit der Mobilfunkprovider. Gewissenhaftigkeit sowohl in Bezug auf die Absicherung der Datenbanken als auch in die Auswahl der Mitarbeiter mit Zugriff auf die sensiblen Kundendaten. Die Möglichkeit von Innentätern, ob sie nun eigene Interessen oder die des Konzerns verfolgen, besteht. Das zeigte im Mai dieses Jahres eindrucksvoll die Affäre um die Deutsche Telekom. Der Vorwurf lautete, dass Mitarbeiter der Deutschen Telekom Kunden- und Verbindungsdaten zur Auswertung an ein externes Unternehmen weitergegeben hätten. Ziel der Aktion war es offensichtlich, Verbindungen von Vorstandsmitgliedern zu Journalisten offenzulegen, um so undichte Stellen im Konzern zu lokalisieren. Auf wessen Betreiben und in welchem Maßstab das geschah, ist eine Frage, die Staatsanwaltschaften und Gerichte noch länger beschäftigen wird. Es ist zu vermuten, dass zumindest Namen, IMSIs und aufgezeichnete LAIs sowie Verbindungsdaten der betroffenen Kunden das Unternehmen verließen. Nicht, dass eine interne Auswertung dieser Daten etwa legal wäre, aber dass die sensiblen Daten ein-

Datenbanken im Mobilfunksetz

AuC - Authentication Center: Neben den Funktionen zur Teilnehmerauthentisierung enthält das AuC auch eine Datenbank mit den Shared Secrets aller Teilnehmer. Insiziert werden sie über die zugehörige IMSI.

EIR - Equipment Identity Register: Enthält die IMEI aller im Netz angemeldeten Endgeräte. Über eine Whitelist, eine Greylist und eine Blacklist wird zwischen zugelassenen, zu überprüfenden und gesperrten (z.B. als gestohlen gemeldeten) Endgeräten differneziert. Dieses Verzeichnis zu führen stellt die GSM-/UMTS-Architektur frei.

HLR - Home Location Register: Im Home Location Register werden alle den Teilnehmer betreffenden Daten dauerhaft gespeichert. Darunter fallen IMSI, Rufnummer des Teilnehmers (Mobile Station ISDN Number) sowie Ortsinformationen in Form der aktuellen Location Area Identity (LAI). Auch für den Teilnehmer freigeschaltete Dienstmerkmale, Gebührendaten und ein Verweis auf das aktuell genutzte VLR sind im HLR enthalten.

VLR - Visitor Location Register: Enthält eine temporäre Kopie der - für das Routing relevanten - Nutzerdaten aus dem HLR, um die Mobilität des Nutzers sicherzustellen. Bei Wechsel in eine Location Area, für die ein anderes VLR zuständig ist, werden die Daten in das ab sofort zuständige VLR transferiert.

fach an einen externen Dienstleister gegeben wurden, macht die Angelegenheit besonders delikat.

Das Beispiel zeigt uns, dass Datensicherheit ein relevantes Thema ist, was - wenn auch oft viel zu spät - den Kunden der Mobilfunkbetreiber am Herzen liegt. Es ist somit zu hoffen, dass die Mobilfunkunternehmen den entstandenen Image-Schaden als Anlass nehmen, um ihre Sicherheitsmaßnahmen einer Revision zu unterziehen. Vielleicht setzt auch der ein oder andere in Zukunft stärker auf Transparenz als Marketinginstrument. Die Kundschaft jedenfalls ist sensibilisiert.

Ferngesteuerte Endgeräte

Neben den unvermeidlich anfallenden Kundendaten gibt es in Mobilfunknetzen auch einige vermeidbare Sicherheitslücken. Was Kunde und Betreiber gleichermaßen zu Komfort verhelfen sollte, erweist sich manchmal als Fallstrick. Moderne Endgeräte sind kleine Computer, die dementsprechend auch über eine Firmware und ein Betriebssystem verfügen. Darüber hinaus kann je nach Endgerät eine Vielzahl von Einstellungen getroffen werden. Falsche Konfiguration kann dazu führen, dass das Endgerät in seiner Leistungsfähigkeit eingeschränkt wird oder ein bestimmter Dienst nicht genutzt werden kann. Dabei kann den wenigsten Kunden zugemutet werden, die neueste Version des Betriebssystems auf ihrem Handy selbst zu installieren. Auch das Wälzen von seitenlangen Konfigurationsleitfäden mit Empfehlungen des Mobilfunkbetreibers ist nicht gerade der Traum jedes Kunden. Den neuesten Sicherheits-Patch für das Betriebssystem installieren? Wäre schön, wenn der Provider das übernehmen könnte.

Technisch ist das ohne weiteres möglich. Neben dem „Branding“, also dem Präparieren der Endgeräte nach Betreibervorgaben, das vor der Auslieferung des Endgeräts an den Kunden vorgenommen wird, setzen viele Anbieter Techniken ein, die unter dem Begriff „Over-the-Air-Programming“ (OTA) zusammengefasst werden. Während beispielsweise per FOTA (Firmware over the Air) Patches und ganze Firmware-Pakete installiert werden können, bietet OTAPA (OTA Parameter Administration) die Möglichkeit, Konfigurationsdaten von Endgeräten zentral zu verwalten. Nur so ist es etwa möglich, die korrekte Konfiguration der GPRS-Verbindung wiederherzustellen, wenn ein Kunde diese durch ein paar unbedachte Tastendrücke ungültig gemacht hat. Kritisch wird es dann, wenn dies vom Teilnehmer unbemerkt und vielleicht auch unaufgefordert passiert.

Die Angriffsmöglichkeiten sind vielfältig. Eine manipulierte Firmware einzuschleusen, die beispielsweise die Aktivitäten des Nutzers am Endgerät protokolliert oder gar Daten kopiert, wäre wohl der Worst Case eines Angriffsszenarios. Aber auch viel trivialere Eingriffe, etwa die Fehlkonfiguration der Internetverbindung, können schwerwiegende Folgen für die Datensicherheit haben. So könnte ein Angreifer die Adresse eines Proxy konfigurieren, über den er die Kontrolle besitzt. Alle Daten würden umgeleitet und könnten - falls sie nicht einer Ende-zu-Ende-Verschlüsselung unterliegen - im Klartext mitgelesen werden. Das gilt gleichermaßen für geschäftliche oder private Emails wie auch für das Surfen im Internet. Beispiele wie dieses ließen sich noch viele nennen. Der Einsatz von OTA und FOTA ist - auch wenn er noch so nutzbringend sein mag - äußerst sensibel und bedarf entsprechender Schutzmechanismen durch den Provider. Eine Offenlegung der Schnittstellen und Sicherungsmaßnahmen und der Verzicht auf „unsichtbare“ Konfigurationsänderungen würden dem Kunden zumindest das Gefühl zurückgeben, die Kontrolle über sein Endgerät zu besitzen.

Kompromittierbare Dienste

Die Benutzung von Mobiltelefonen birgt aber auch andere Gefährdungen, jenseits derer die in der Natur der Netze begründet liegen. Von den Netzbetreibern selbst oder von externen Dienstleistern erbrachte Sprach- und Datendienste haben ebenfalls ihre sicherheitstechnischen Tücken.

Netzbetreiber und Endgerätehersteller bieten ihren Kunden in der Regel eine Vielzahl von Komfortfeatures und Leistungsmerkmalen. Ob Push-To-Talk (PTT) oder automatische Rufannahme: ein vorsichtiger und bewusster Umgang mit solchen Leistungsmerkmalen ist - gerade im geschäftlichen Umfeld - dringend zu empfehlen. Versehentlich oder durch Manipulation eine falsche Rufnummer einer PTT Gruppe hinzugefügt - wer kann schon abschätzen, was der unerwartete Adressat mit dem Gehörten anzufangen weiß? Ein gutes Beispiel sind Telefonkonferenzen, welche als Leistungsmerkmal im Betreibernetz zur Verfügung gestellt werden. Ob ein Anrufer zuvor eine Konferenzschaltung mit einem weiteren - unerwünschten - Zuhörer initiiert hat, ist nicht immer feststellbar. Kurze Piepsgeräusche beim Eintritt in eine Telefonkonferenz werden oft eher als Störung im Netz oder als Akku-Warnung des eigenen Endgeräts interpretiert. Möglichkeiten, sich gegen solche Mithörer zu schützen, hat der einzelne Teilnehmer nicht.

Ähnliches gilt für die Nutzung aller im Mobilfunknetz erbrachten Dienste. Ob Sprach-, Messaging- oder Datendienst: viele Verfahren haben Schwächen, die ein Angreifer ausnutzen kann, um in den Besitz sensibler Informationen zu gelangen.

Report

Office Communications Server 2007

Mit der Ankündigung des Office Communications Server 2007 (OCS) hat Microsoft für eine gehörige Unruhe im Markt gesorgt, war doch damit der Einstieg in den bis dato von Microsoft ignorierten Telefoniemarkt verbunden. Microsoft positioniert das Produkt bewusst als Kollaborations-Produkt und setzt es funktional in die direkte Konkurrenz zu Cisco und Siemens/IBM. Damit liegt das Produkt zentral in einem der größten Zukunfts- und Wachstums-Märkte.

In dem vorliegenden Report analysiert ComConsult Research die aktuelle Unified Communications Strategie von Microsoft, in deren Mittelpunkt der Office Communications Server steht.

Februar 2008 - 141 Seiten
Preis: € 398,- zzgl. 7% MwSt. und Versand

Bestellen Sie über unsere Web-Seite **www.comconsult-research.de**

Wichtig ist, sich klar zu machen, dass Mobil-Telefonie nicht sicherer sein kann als die Festnetz-Telefonie. Zu der Angreifbarkeit der Luftschnittstelle und den Eigenarten des Vermittlungsnetzes gesellen sich dieselben Probleme, die auch im Festnetz existieren. So beschränkt sich die verschlüsselte Übertragung – falls überhaupt eine solche ausgehandelt wurde – ausschließlich auf die Luftschnittstelle. Ab diesem Zeitpunkt unterliegt das Gespräch denselben Gefährdungen wie im öffentlichen Telefonnetz. Eine Ende-zu-Ende-Verschlüsselung muss separat von beiden Teilnehmern ausgehandelt und technisch umgesetzt werden. Der technische und finanzielle Aufwand ist nicht unerheblich und in den seltensten Fällen für Privatleute interessant oder erschwinglich. Aber auch im Geschäftsumfeld lohnt sich die Investition selten, geschweige denn, dass sie flächendeckend für alle potentiellen Gesprächspartner umgesetzt werden könnte. Das Stichwort lautet hier „erhöhter Schutzbedarf“. Welche Informationen derart sensibel sind, dass sie durch teure Investitionen geschützt werden müssen liegt dabei - über die gesetzlichen Bestimmungen, etwa zum Schutz von Kundendaten, hinaus – im Auge des Betrachters.

Nachrichtendienstlich

Ebenfalls unsicher ist die Benutzung von Messaging-Diensten. Der beliebte Short Message Service (SMS) oder auch Enhanced Message Service (EMS, eine Aneinanderreihung von SMS) sind dafür gute Beispiele. Die Kurznachrichten von maximal 160 Zeichen pro SMS werden nicht über die eigentlichen Sprach- oder Datenkanäle des GSM-Netzes übertragen. Vielmehr wird für die Übertragung auf die Steuerkanäle zurückgegriffen, über die normalerweise Aufgaben die Signalisierung von Anrufen abgewickelt werden. Diese unterliegen prinzipiell derselben Verschlüsselung auf der Luftschnittstelle, wie Sprach- und Datenkanäle des GSM-Netzes, sind also als potentiell unsicher einzustufen. Darüber hinaus kann als Fallback auf einen gänzlich unverschlüsselten Steuerkanal zurückgegriffen werden, was beispielsweise bei zu hoher Auslastung der regulären Übertragungswege der Fall ist. Der Inhalt der SMS selbst bleibt unverschlüsselt und geht in dieser Form durch die Luft und über sämtliche Server und Gateways auf dem Weg zum Empfänger. Sich per SMS auf einen Kaffee zu verabreden, ist also bestimmt unkritisch. Auf diesem Wege Geschäftsgeheimnisse auszutauschen, ist mit Sicherheit keine gute Idee.

Was allgemein für Email in puncto Sicherheit gilt, muss so oder ähnlich auch für den mobilen Zugriff auf Email beachtet werden. Bedenkt man, wie wenig verbreitet die Verschlüsselung des Email-Verkehrs momentan ist, scheint hier kein gesteigerter Bedarf nach Schutz zu bestehen. In Wahrheit ist aber eher die fehlende Verbreitung der notwendigen Schutzmechanismen der Hemmschuh. Was nützt es mir, meine Email zu verschlüsseln, wenn der Adressat sie nicht entschlüsseln kann? Während unternehmensintern das Rollout einer sicheren Email Lösung kein Problem darstellt, Bedarf es beim Emailverkehr mit Kunden, Partnern und Zulieferern erheblichen organisatorischen Aufwands, um eine konsistente Lösung zu gewährleisten. Aus diesem Grund wird oft auf Verschlüsselung der Inhalte verzichtet. Solange sich die Übertragung der Emails in einer geschützten Umgebung wie z.B. einem Unternehmensnetz abspielt, ist dies in vielen Fällen hinnehmbar. Im Fall mobiler Email findet dieser Zugriff aber immer von außerhalb statt. Es ist daher wichtig, die Übertragungswege zwischen Mailserver und mobilem Endgerät zu betrachten und hier entsprechende Schutzmaßnahmen zu treffen.

Push Mails

Grundsätzlich unterscheiden sich zwei Verfahren beim mobilen Zugriff auf Emails. Klassischerweise baut der Client in regelmäßigen Abständen eine Verbindung zum Mailserver auf und „fragt“ nach neuen Emails. Dieses Verfahren unterscheidet sich nicht von dem des „normalen“ Emailclients eines externen Mitarbeiters. Der Zugriff kann durch verschiedene architektonische und verschlüsselungstechnische Maßnahmen gegen Manipulation abgesichert werden. Beispiele wären das Bereitstellen eines gespiegelten Email-Servers in der „Demilitarisierten Zone“ (DMZ), Authentisierung per Zertifikat und das Einrichten eines sicheren Übertragungstunnels für den Abruf von Mails. Nachteile des Verfahrens sind die häufigen – und meist überflüssigen – Datenverbindungen, welche zwischen Client und Server etabliert werden. Was im LAN oder auch WAN Bereich kaum ins Gewicht fällt, kann im mobilen Einsatz hohe Kosten verursachen. Da die Netzbetreiber häufig pro angefangene Dateneinheit fester Größe abrechnen, entstehen schnell hohe Verbindungsentgelte. Längere Intervalle für die Serverabfrage sind nur bedingt sinnvoll, da Mails nicht mehr zeitnah empfangen werden und der Sinn des mobilen Einsatzes damit verloren gehen würde

Daher erfreut sich die zweite, passive Variante großer Beliebtheit: Push Mail. Bei diesem Verfahren initiiert nicht der Client, sondern der Server die Übertragung neuer Emails. Das passiert entweder per SMS oder über eine dauerhaft bestehende, virtuelle Netzwerkverbindung. Die verschiedenen Verfahren hierfür wurden von der Open Mobile Alliance (OMA) standardisiert. Für die eigentliche Datenübertragung kommt dann eines von vielen Synchronisierungsprotokollen zum Einsatz. Als Beispiel sei das ebenfalls von der Open Mobile Alliance entwickelte SyncML genannt. Darüber hinaus existiert eine Vielzahl proprietärer Protokolle. Für Signalisierung und Übertragung kann, je nach Vorgaben des Unternehmens und des Netzbetreibers, ein so genanntes Network Operation Center (NOC) zwischengeschaltet werden.

Das NOC wird vom Mobilfunkanbieter oder einem Drittanbieter zur Verfügung gestellt. Der bekannteste Vertreter einer solchen Drittanbieter-Lösung ist

Beim **Advanced Encryption Standard** (AES) handelt es sich um ein symmetrisches Kryptosystem, das als Nachfolger für DES bzw. Triple DES (3DES) im Oktober 2000 vom US-amerikanischen National Institute of Standards and Technology (NIST) als Standard verabschiedet wurde. AES ist ein Blockchiffre und verfügt über eine feste Blockgröße von 128 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit. Anhand der Schlüssellänge wird zwischen den drei AES-Varianten AES-128, AES-192 und AES-256 unterschieden.

Für AES sind bisher keine Master-Keys oder andere Verfahren bekannt, die ein Aufbrechen der AES-Verschlüsselung in einem überschaubaren Zeitraum erlauben. Der Algorithmus ist frei verfügbar und darf ohne Lizenzgebühren eingesetzt werden.

AES wird u.a. bei der Verschlüsselung für Wireless LAN (802-11i / WPA2), bei SSH und bei IPsec sowie zur Verschlüsselung diverser komprimierter Datearchive verwendet (z.B. bei 7-Zip). Auch in der Europäischen Union gehört AES zu den empfohlenen kryptografischen Algorithmen (siehe EU-Projekt NESSIE, IST-1999-12324)

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 1

„Blackberry“ der Kanadischen Firma Research in Motion (RIM). RIM betreibt dazu u.a. NOCs in Kanada und in Großbritannien. Alle zwischen Mailserver und mobilem Endgerät ausgetauschten Daten passieren dabei das jeweils zuständige NOC, so dass hier eine geeignete Ende-zu-Ende-Verschlüsselung genutzt und dem Anbieter eine besondere Vertrauensstellung eingeräumt werden muss. Ansonsten wäre denkbar, dass im NOC Emails zumindest temporär zwischengespeichert und so dritten zugänglich gemacht werden könnten. Blackberry und anderen Push-Mail-Diensten ist diese Befürchtung häufig vorgehalten worden. Vor allem, weil zunächst nur unzureichende Verschlüsselungsmethoden (z.B. Triple DES) verwandt worden sind. Inzwischen bietet Blackberry daher auch für besonders hohe Sicherheitsansprüche eine AES-Verschlüsselung.

Bei Blackberry werden die Private Keys für die Verschlüsselung jedem Benutzer individuell zugewiesen. Vor ihrer Übertragung werden die Daten vom Blackberry Enterprise Server (BES), der sich innerhalb des geschützten Unternehmensbereich, hinter der unternehmenseigenen Firewall mit einem privaten Key verschlüsselt und können erst auf dem Handheld des Empfängers gelesen werden. Jeder Schlüssel wird dabei ausschließlich in der sicheren Sphäre des entsprechenden Endgerätes hinterlegt. Aus diesem Grund ist auch dringend die Nutzung von Blackberry-Endgeräten zu empfehlen, da ansonsten kaum die Unversehrtheit des Schlüssels auf dem Endgerät gewährleistet ist.

Nach heutigem Stand der Technik gibt es keine Mechanismen, an diesen privaten Key heranzukommen. Nur die IT-Abteilung des Nutzers kann auf die Keys der einzelnen Anwender zugreifen, und selbst der Hersteller der Push-Mail-Lösung, bei Blackberry also RIM selbst, ist angeblich unter keinen Umständen in der Lage, Zugang zu dem privaten Key zu bekommen oder die Nachrichten des Kunden zu lesen.

Jedoch hat beispielsweise Frankreichs Staatspräsident Nikolas Sorkozy als eine seiner ersten Amtshandlungen die Nutzung von Blackberry für Regierungsmitglieder verboten. Grund dafür ist die Befürchtung des für die innere Sicherheit in Frankreich zuständige Secrétariat Général de la Défense Nationale (SGDN), geheime Sitzungen könnten allzu leicht von fremden Geheimdiensten abgehört werden, da die Blackberry-NOCs in Kanada und in Großbritannien angesiedelt sind und diese Länder über z.T. sehr großzügige Datenschutzregelungen verfügen, sobald Geheimdienste sich dafür interessieren. Die Befürchtungen sind nach Bekanntwerden der UKUSA-Verträge nicht ganz unbegründet. UKUSA bezeichnet die zwischen Großbritannien (United Kingdom) und den USA 1949 geschlossenen Verträge zur Zusammenarbeit der US-amerikanischen National Security Agency (NSA) und dem britischen GCHQ sowie dem kanadischen CSE, dem australischen DSD und dem neuseeländischen GCSB. Ganz aktuell sind Bestrebungen der britischen Regierung, mit einem Milliardenaufwand jegliche Kommunikation, d.h. auch mobile Email-Kommunikation, zu überwachen und zentral zu speichern. (siehe Abbildung 6)

Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich zunächst kritisch zu Blackberry geäußert, ist dann aber wieder zurückgerudert und hält sich seitdem auffällig mit Stellungnahmen zu diesem Thema zurück. Es wird lediglich darauf verwiesen, dass es bisher keine Möglichkeit gegeben habe, die von RIM verwendeten Algorithmen zu prüfen, so dass keinerlei Erkenntnisse über die verwendeten Sicherheitsmechanismen vorliegen, die fundierte Aussagen ermöglichen.

RIM seinerseits hat 2005 das Fraunhofer Institut für sichere Informationstechnologie (SIT) beauftragt, eine detaillierte Sicherheits-Analyse der Blackberry-Lösung zu erarbeiten. Auf der IDC Security Conference 2006 in Frankfurt hat Fraunhofer SIT bekanntgegeben, dass die erste von drei Testphasen zur Sicherheit von E-Mail-Push-Diensten mit der BlackBerry-Lösung abgeschlossen ist. Dabei sind keine Hinweise auf verborgene Hintertüren, einen bei RIM liegenden Master-Key oder andere Möglichkeiten gefunden worden, wie die E-Mail-Kommunikation mittels der BlackBerry-Enterprise-Lösung von Dritten gelesen oder manipuliert werden könnte. Einige von Fraunhofer empfohlene Sicherheitsoptimierungen sind bereits umgesetzt worden, so dass mit einem endgültigen Abschluss der Untersuchungen noch in diesem Jahr gerechnet wird.

Geht man davon aus, dass bei Blackberry wirklich eine korrekte Implementierung des AES-256 vorliegt, bleibt also vor allem die Frage, ob der im eigenen

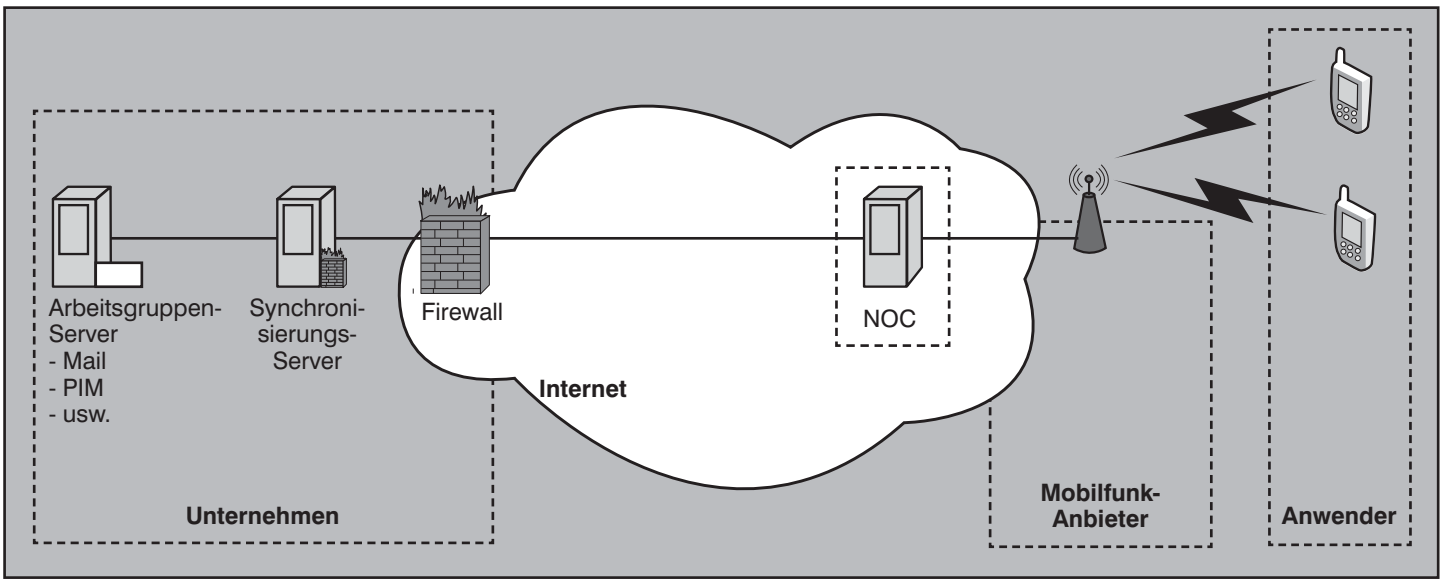


Abbildung 6: Push Mail Synchronisation unter Einsatz eines Network Operation Centers

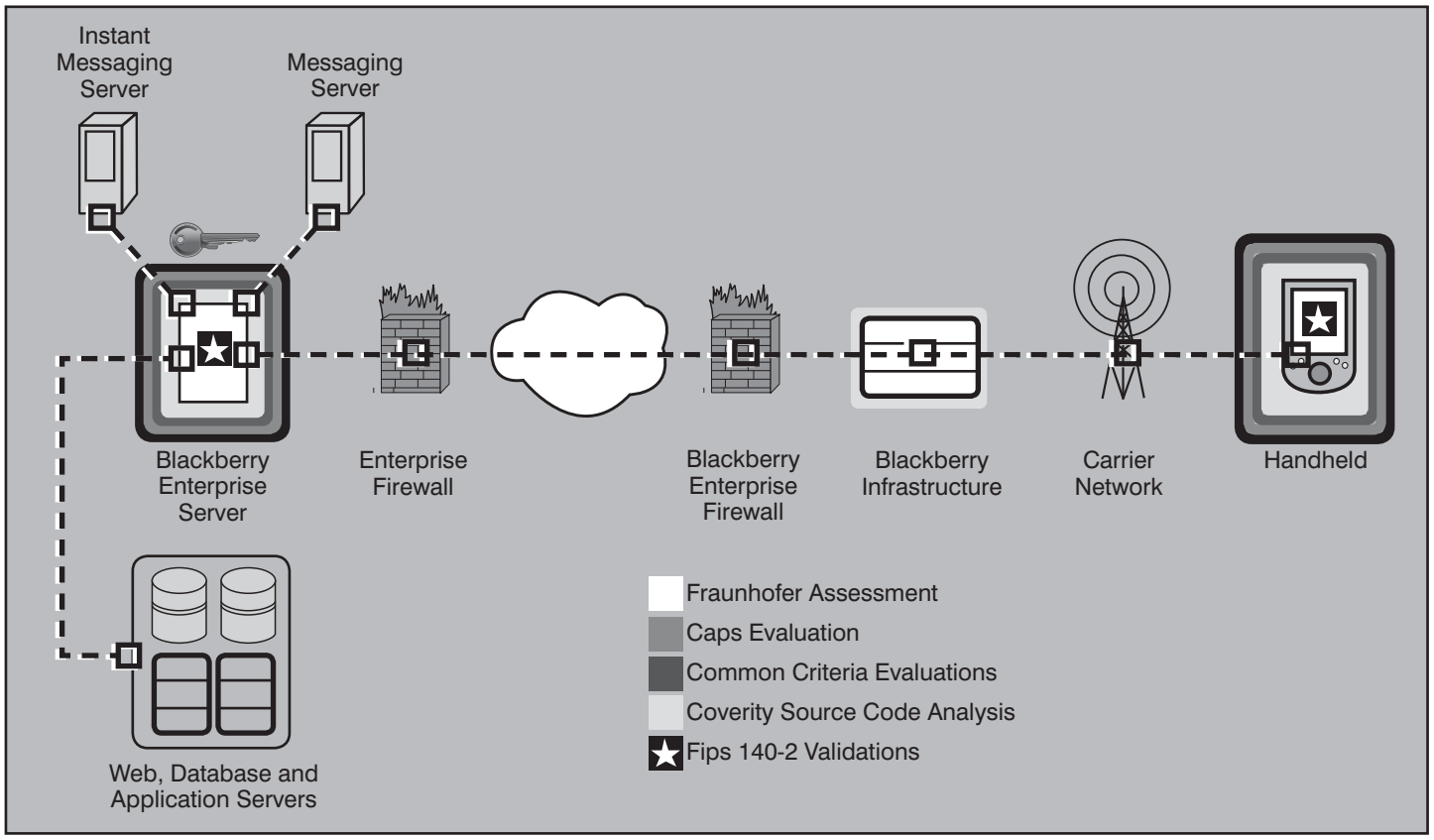


Abbildung 7: Bereiche unterschiedlicher Sicherheitsevaluierungen bei Blackberry

Unternehmen stehende Synchronisierungsserver ein nicht zu kontrollierendes Einfallstor in die gesamte Unternehmenskommunikation darstellt. Zumal dieser Server beispielsweise bei MS-Exchange vollumfänglichen Zugriff auf die gesamte E-Mail-Kommunikation haben muss. Würde also der Server über eine Hintertüre verfügen, wäre die gesamte E-Mail-Kommunikation und nicht nur die Kommunikation von und zu den mobilen Endgeräten dem Zugriff von außen ausgesetzt.
Zwar soll Fraunhofer SIT auch diese Fragstellung klären (siehe Abbildung 7), und RIM hat dazu nicht nur Fraunhofer die entsprechenden Quellcodes zur Verfügung gestellt, aber diese Untersuchungen sind natürlich nur begrenzt aussagekräftig. Denn niemand außer dem Betreiber kann sicherstellen, dass die zur Verfügung gestellte Software wirklich zum Einsatz kommt oder evtl. beim nächsten Update nicht doch wieder eine Hintertür eingebaut worden ist. Zudem stellt sich die Frage, warum RIM nicht auf die Bedenken und Sorgen der Skeptiker eingeht und beispielsweise eine weiter verteilte NOC-Struktur aufbaut. So könnte beispielsweise auch ein NOC in Deutschland bereitgestellt werden, das dann natürlich auch deutschen Datenschutzvorschriften unterliegt. Die Kosten und der Image-Gewinn sollten dafür kaum höher zu bewerten sein, als die ständige Sicherheitsdebatte.

Die Bedenken sind zweifelsohne spitzfindig, treffen teilweise auch auf andere Anbieter als RIM zu und klingen ein wenig paranoid, aber auch hier zeigt die Erfahrung, dass man bei solchen Dingen selten positiv überrascht wird. Bei erhöhtem Schutzbedarf ist also das NOC bzw. der Synchronisierungsserver ein zusätzlicher Risikofaktor. Realisiert man eine Push-Mail-Lösung gänzlich im eigenen Haus, erkauft man sich jedoch die volle Kontrolle über die Datensicherheit mit einem höheren administrativen Aufwand. Angebote für solche eigenen Lösungen sind jedoch schon länger verfügbar und weisen einen ähnlichen Komfort auf wie NOC-basierte Lösungen.

Eventuell sicher surfen

Neben Push Mail und anderen Nachrichten-Übertragungsmöglichkeiten werden mobile Endgeräte zunehmend mehr auch für den mobilen Internet-Zugang genutzt. Auch hier muss daher die Frage gestellt werden, wie sicher dieser Zugang z.B. im Vergleich zu ansonsten intensiv geschützten Unternehmensnetzen aus. Bleibt wenigstens das private Online-Banking oder der Zugriff auf Dokumente im Unternehmensnetz vor unbefugten Augen verborgen? Vielleicht! Unabhängig von der zugrundeliegenden Übertragungstechnologie – GPRS, EDGE oder UMTS-Derivat – erfolgt der Zugriff auf Websites aller Art mithilfe des Wireless Access Protocol (WAP). Ausschließliches Ziel der ersten Versionen dieser Protokollfamilie war die effiziente Übertragung von Websites über schmalbandige Datenverbindungen und deren, für mobile Endgeräte optimierte, Darstellung. Hierzu wurde eine Reihe von Protokollen definiert. Die Inhalte werden in einer für mobile Endgeräte optimierten Version auf Seiten des Webservers bereitgestellt und nach dem Transport per Internet und WAP entsprechend auf dem Endgerät dargestellt. Diese Anwendungsschicht wird in Abbildung 8 mit Wireless Application Environment (WAE) bezeichnet.

Während der Transport durch das Internet mittels der herkömmlichen Protokolle TCP, TLS und HTTP stattfindet, wird der Transport zum Endgerät mithilfe der WAP Protokoll Suite sichergestellt. Hierzu wird ein WAP-Gateway benötigt, welches die Protokolle übersetzt. Problem dabei: sowohl TLS als auch HTTP Protokoll wer-

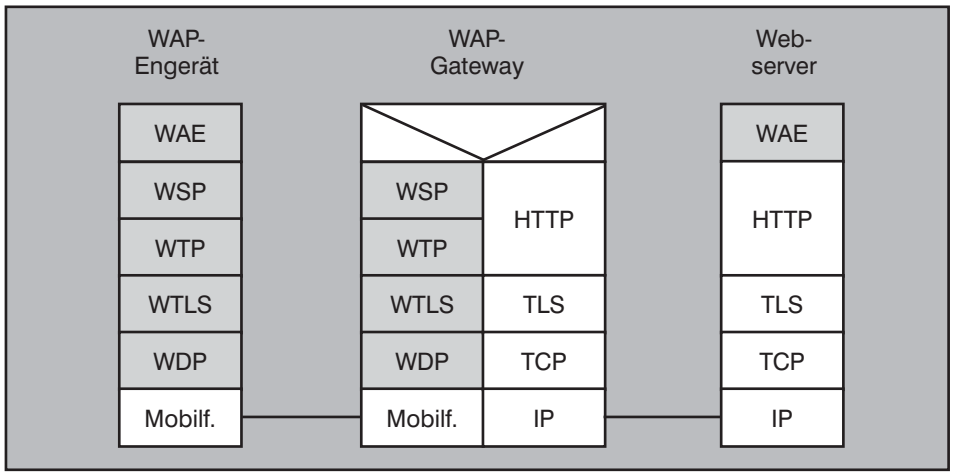


Abbildung 8: Protokoll-Stack der WAP 1.x - Familie

den in ihre WAP-Äquivalente umgesetzt. Die durch TLS gesicherten Inhalte müssen also entschlüsselt und für die Übertragung zum Endgerät per Wireless TLS (WTLS) erneut verschlüsselt werden. Das bedeutet, dass die Ende-zu-Ende Sicherheit von Inhalten am Gateway durchbrochen wird. Das WAP-Gateway stellt hier also die Schwachstelle aller WAP Versionen 1.x dar.

Dieser Umstand wurde mit der aktuellen Version des Standards WAP 2.0 aufgelöst. WAP 2.0 definiert unter anderem eine Variante der Extensible Hypertext Markup Language (XHTML) als neues Format für WAE-Inhalte. Diese Beschreibungssprache erweitert die geläufige Hypertext Markup Language (HTML) um Sprachelemente der für WAP 1.x verwendeten Wireless Markup Language (WML). Die neue Version trägt aber auch der Tatsache Rechnung, dass das primäre Ziel nicht mehr die Optimierung der Übertragungsgeschwindigkeit sein kann. Vielmehr wird davon ausgegangen, dass der genutzte Datendienst IP als Basisprotokoll zur Verfügung stellt. Die Architektur beinhaltet zwar weiterhin ein WAP-Gateway. Das ist aber zum Transport der WAE-optimierten Inhalte nicht mehr zwingend erforderlich. Es kann auch - dann allerdings ohne Protokolloptimierung - direkt auf Inhalte eines WAE zugegriffen werden. Andernfalls übernimmt das WAP-Gateway die optionale Optimierung der Protokolle TCP und HTTP, so dass im Falle einer TLS-gesicherten Verbindung zwar TCP optimiert wird, die darüber liegenden Schichten aber unangetastet bleiben. Die Ende-zu-Ende-Sicherheit bleibt somit gewahrt. (siehe Abbildung 9)

Um beim Surfen und dem Zugriff auf eventuell vertrauliche Inhalte also sichergehen zu können, dass die Daten vor Zugriff durch Angreifer oder Innentäter geschützt bleiben, ist die Verwendung von WAP 2.0 unerlässlich. Die Tauglichkeit eines Endgerätes für WAP 2.0 und der Verzicht auf den Einsatz von WAP 1.x ist für den Anwender allerdings nicht leicht zu überprüfen. Oft klaffen Produktbeschreibung des Herstellers und Realität auseinander. Zudem gibt es diverse Mischformen, z.B. Geräte, die zwar WAP 1.x verwenden, aber sowohl WML als auch XHTML im Browser darstellen können. Der einzige Weg, sich der WAP 2.0 Fähigkeit eines Endgeräts zu versichern, liegt darin, ohne den Umweg über ein WAP-Gateway auf eine WAE zuzugreifen.

Allerdings lässt sich das Zurückgreifen auf WAP-Proxys nicht immer vermeiden. Ein Derivat dieser Protokollfamilie kommt für den Versand von Multimedianachrichten mittels Multimedia Message Service (MMS) zum Einsatz. Die multimedialen Inhalte werden dabei auf Servern zwischengespeichert, während die eigentliche MMS nur die notwendigen Links zu diesen enthält. Dem Empfänger wird die Nachricht mithilfe von WAP Push – einer Push-Technologie ähnlich dem Push Mail Verfahren, die auf WAP basiert – zugestellt. Die eigentlichen Inhalte lädt das Endgerät dann über einen MMS-Proxy von den Servern der Anbieter. Problematisch ist hierbei, dass der MMS Proxy sich gegenüber dem Endgerät nicht authentisieren muss. So können Inhalte gefälscht oder mit Schadsoftware versetzt und die Identität des Urhebers verschleiert werden, falls die MMS über einen kompromittierten MMS-Proxy ausgeliefert wird. Brisant ist auch das MMS-Phishing, bei dem - analog zu dem von Emails bekannten Vorgehen - dem Anwender eine vertrauenswürdige Quelle vorgegaukelt wird, um ihn zur Eingabe persönlicher Daten oder Passwörter zu bewegen. Gegen solche Attacken kann man sich nur durch gesunden Menschenverstand beim Umgang mit MMS schützen.

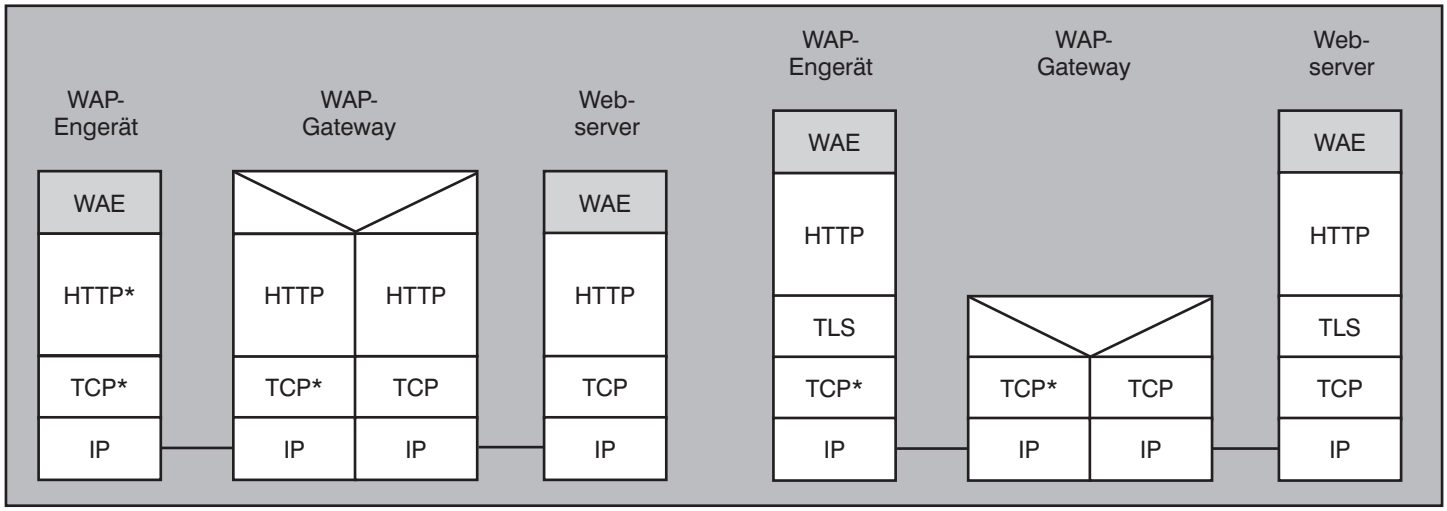


Abbildung 9: WAP 2.0 mit (l.) und ohne (r.) Optimierung höherer Protokollschichten

Umsichtig handeln

Gesunder Menschenverstand ist auch bei der Nutzung von elektronischen Handels- und Bezahlplattformen notwendig. Ob das bequeme Shopping während der U-Bahn-Fahrt nach Feierabend oder das Lösen eines Tickets für selbige per SMS. M-Commerce und M-Payment sind das mobile Gegenstück zu den mittlerweile etablierten E-Commerce und E-Payment Angeboten des Internets. Dementsprechend sind auch die Gefährdungen ähnlich. Die durch das bereits angesprochene Email- oder MMS-Phishing erlangten Zugangsdaten geben dem Angreifer nicht nur Einblick in die Gewohnheiten des Nutzers. Sie können vielmehr ganz konkrete, wirtschaftliche Folgen für den Einzelnen haben. Doch es braucht noch nicht einmal einen gewaltigen technischen Aufwand, um in Besitz der Zugangsdaten zu gelangen. Ein simpler Blick über die Schulter eines ahnungslos Einkaufenden genügt, und schon können Zahlungen von seinem Account aus vorgenommen werden. Ein umsichtiger Umgang mit solchen Angeboten sollte also selbstverständlich sein (gilt übrigens auch für Notebook-Nutzer, denn mit den auf einer einzigen Bahnreise in der 1. Klasse mühelos gewinnbaren Informationen lassen sich ganze Wirtschaftsteile einer Zeitung füllen).

Darüber hinaus ist die Auswahl der genutzten Plattformen ausschlaggebend. Prinzipiell dürfen nur Angebote genutzt werden, bei denen persönliche Daten und Zahlungsinformationen verschlüsselt übertragen werden. Bei für den mobilen Einsatz zugeschnittenen Webplattformen geschieht das meist per Secure Sockets Layer (SSL), das in Kombination mit HTTP in Form von HTTPS Verwendung findet (erkennbar am „https://“ zu Beginn der Adresse). So gesicherte Verbindungen sind prinzipiell unbedenklich. Allerdings muss dennoch auf die Vertrauenswürdigkeit des Anbieters geachtet werden. Denn was nutzt eine sichere Verbindung, wenn die Gegenseite kompromittiert ist. Brauchbare Kriterien sind hier eventuelle Zertifizierungen und die Beständigkeit des Anbieters am Markt. Plattformen für die mobile Nutzung sind durch ihren Komfort sehr attraktiv für den Kunden. Damit können sie für viele Unternehmen eine gewinnbringende Ergänzung der Vertriebswege sein, insbesondere wenn diese mit ihren Produkten den privaten Endverbraucher adressieren. Ein Nachweis der Sicherheit eines solchen Angebots, z.B. durch Security Audits, sollte daher im ureigensten Interesse der Anbieter liegen.

Fazit

Der öffentliche Mobilfunk birgt eine Reihe von Tücken in puncto Sicherheit. Ein bewusster und umsichtiger Umgang mit diesem Medium ist dringend geboten, und das nicht nur, wenn es um den Schutz von Geschäftsgeheimnissen geht. Auf die Sicherheit der verwendeten Netztechnologie hat der Kunde keinen oder nur indirekten Einfluss. Hier ist auf Kundenseite viel Vertrauen in die Gewissenhaftigkeit der Netzbetreiber notwendig. Bleibt zu hoffen, dass diese das Vertrauen auf Vorschuss zu würdigen wissen und dem Kunden in Zukunft ein höheres Maß an Sicherheit und Transparenz gewähren.

Doch die Sicherheit der Netztechnologie alleine hilft nicht, wenn die zur Verfügung gestellten Dienste selbst Teil des Problems sind. Ob Ende-zu-Ende-Sicherheit bei Datendiensten oder Deaktivierung nicht genutzter oder potentiell unsicherer Leistungsmerkmale - der Anwender kann einiges zum Schutz seiner Privatsphäre und seiner Daten beitragen. Mit dem Wissen um die Gefährdungen und ein wenig gesundem Menschenverstand lassen sich viele Fallen der mobilen Datenwelt vermeiden. Eine umsichtige Planung der Nutzung von mobilen Endgeräten und Diensten ist für Unternehmen dennoch unerlässlich. Die Sicherheitsstandards, die auf viele Unternehmensnetze bereits heute angewendet werden, müssen auch die mobilen Teilnehmer erfassen, um die Wirksamkeit des Gesamtkonzepts sicherzustellen.

In der täglichen Praxis fällt jedoch immer wieder auf, dass Unternehmen zwar intensiv den Schutz ihrer eigenen Netze betreiben, den mobilen Zugriffsmöglichkeiten ihrer Mitarbeiter aber vergleichsweise unkritisch gegenüberstehen. Wenn man berücksichtigt, dass die mobilen Endgeräte und öffentlich Mobilfunknetze immer leistungsfähiger werden, ist das aber eine äußerst bedenkliche Herangehensweise. Denn eines ist klar: Gelangt ein ungeschütztes mobiles Endgerät in falsche Hände, bestehen fast alle Möglichkeiten, auf unternehmenskritische Daten zuzugreifen. Dazu gehören nicht nur die Daten auf dem Endgerät selbst, sondern auch die Unternehmensdaten, auf die vom Endgerät aus zugegriffen werden kann.

Es muss demnach als höchst fahrlässig betrachtet werden, wenn sich die IT-Verantwortlichen eines Unternehmens auf die Betreiber von Mobilfunknetzen oder die Anbieter von mobilen Diensten verlassen. Zu groß ist die Gefahr, dass sensible und geschäftskritische Daten aufgrund von inhomogenen Sicherheitskonzepten und arglosem Endanwenderverhalten das Unternehmen verlassen. Ein solches Risiko kann sich kein Unternehmen auf lange Sicht leisten, Unternehmen in einem verschärften Wettbewerbsumfeld nicht mal kurzzeitig. Was der einzelne Anwender und Unternehmen tun können, um sensible Daten vor dem Zugriff Dritter zu schützen, wird das Thema des zweiten Teils dieses Artikels sein.

Literatur

Pressemitteilung „Fast jeder zweite Mensch telefoniert mobil“ vom 05.06.2007, Brachenverband BITKOM, http://www.bitkom.de/de/presse/30739_46282.aspx, (zuletzt überprüft: 22.09.2008)

Technische Referenzen und Mobilfunkstandards der dritten Generation von Mobilfunknetzen, The 3rd Generation Partnership Project, http://www.3gpp.org/specs/specs.htm, (zuletzt überprüft: 22.09.2008)

Pressemitteilung des Bundesministerium der Justiz zum Thema Vorratsdatenspeicherung vom 09. November 2007, http://www.bmj.bund.de/enid/cf71891a0cf2593af66c730,46bdaa706d635f6964092d0934383133093a095f7472636964092d0933303334/Pressestelle/Pressemitteilungen_58.html, (zuletzt überprüft: 22.09.2008)

Deutscher Bundestag Drucksache 16/5846, 27. Juni 2007, „Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ - http://dip.bundestag.de/btd/16/058/1605846.pdf, (zuletzt überprüft: 22.09.2008)

Broschüre „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/literat/doc/oefms/index.htm, (zuletzt überprüft: 22.09.2008)

Artikel „Telekom bespitzelte mehrere Journalisten“ vom 10.09.2008, Onlineangebot des Handelsblattes, http://www.handelsblatt.com/unternehmen/it-medien/telekom-bespitzelte-mehrere-journalisten;2035251, (zuletzt überprüft: 22.09.2008)

Pressemitteilung „Über 10 Millionen UMTS-Nutzer in Deutschland“ vom 10.02.2008, Branchenverband BITKOM, http://www.bitkom.de/de/presse/30739_50446.aspx, (zuletzt überprüft: 22.09.2008)

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Sonderveranstaltung: Wireless Technologie, 15.12. - 16.12.08 in Düsseldorf

Aufgrund der aktuellen Neuheiten bei Wireless Technologien und der großen Bedeutung für laufende Projekte haben wir uns entschlossen, eine Sonderveranstaltung zu diesem Thema anzubieten. Erfahren Sie von ausgewählten Top-Experten, wohin sich die Technologie entwickelt und wo die Stolpersteine in den Projekten liegen.

Preis: € 1.490,- zzgl. MwSt.

Lokale Netze für Einsteiger, 26.01. - 30.01.09 in Aachen

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.

IP-Wissen für TK-Mitarbeiter: was Sie für IP-Telefonie über IP wissen müssen, 02.02. - 03.02.09 in Bonn

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das TK-Mitarbeiter ohne Vorkenntnisse zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen.

Preis: € 1.390,- zzgl. MwSt.

Trouble Shooting in vernetzten Infrastrukturen, 03.02. - 06.02.09 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und 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-Software kommt Wireshark zum Einsatz.

Preis: € 2.190,- zzgl. MwSt.

Sicherheitsmechanismen für Voice over IP, 09.02. - 10.02.09 in Hamburg

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.390,- zzgl. MwSt.

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit, 09.02. - 13.02.09 in Hamburg

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

Preis: € 2.290,- zzgl. MwSt.

Internetworking: Optimales Netzwerkdesign mit Switching und Routing, 09.02. - 13.02.09 in Aachen

Dieses 5-Tages-Intensiv-Seminar vermittelt Netzwerkbetreibern und Planern Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt.

Preis: € 2.290,- zzgl. MwSt.

TCP/IP und SNMP, 16.02. - 20.02.09 in Bonn

LAN-, WLAN- und WAN-Netzwerke sind heutzutage IP-Netze, und ein Verzicht auf Nutzung des IP-basierten Internet undenkbar. Auch für früher nur mit herstellerspezifischen Protokollen in Verbindung gebrachte Anwendungsgebiete wie Telefonie oder Produktionsumgebungen gibt es mittlerweile geeignete IP-basierte Lösungen. Hersteller und Dienstanbieter versuchen den Eindruck zu vermitteln, die Nutzung sei kinderleicht, fast schon plug and play - man trägt ein paar Adressen ein (wenn überhaupt), und es kann losgehen. Falsch!

Preis: € 2.290,- zzgl. MwSt.

Sicherheit im LAN mit IEEE 802.1X, 16.02. - 17.02.09 in Bonn

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.

IP-Telefonie: Vorbereitung, Migration, Management, 16.02. - 18.02.09 in Bonn

Die Vorbereitung der Netze auf IP-Telefonie, die Migration von der klassischen Telekommunikation zu Voice over IP sowie der Betrieb der dadurch entstehenden komplexen Netz- und Anwendungsarchitektur konfrontieren alle Unternehmen mit neuen Herausforderungen. Das Wissen aus verschiedenen Bereichen, von der Netzinfrastruktur bis hin zu neuen und etablierten Kommunikationsapplikationen, muss zu einem interdisziplinären Know-how verdichtet und neu geordnet werden. Diesem Ziel dient das Seminar.

Preis: € 1.690,- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
26.01. - 30.01.09 in Aachen
11.05. - 15.05.09 in Aachen
31.08. - 04.09.09 in Frankfurt
23.11. - 27.11.09 in Hamburg

TCP/IP und SNMP
16.02. - 20.02.09 in Bonn
25.05. - 29.05.09 in Aachen
21.09. - 25.09.09 in Bonn

Internetworking
09.02. - 13.02.09 in Aachen
11.05. - 15.05.09 in Aachen
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
03.02. - 06.02.09 in Aachen
05.05. - 08.05.09 in Aachen
06.10. - 09.10.09 in Aachen

Trouble Shooting 2
17.03. - 20.03.09 in Aachen
16.06. - 19.06.09 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“ € 3.940.-- zzgl. MwSt. (Einzelpreise: je € 2.190.--)

ComConsult Certified Security Expert

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
09.02. - 13.02.09 in Hamburg
14.09. - 18.09.09 in Köln

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten
30.03. - 03.04.09 in Berlin
26.10. - 30.10.09 in Aachen

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs
22.06. - 26.06.09 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
30.03. - 01.04.09 in Berlin
15.06. - 17.06.09 in Stuttgart
28.09. - 30.09.09 in Bad Neuenahr
23.11. - 25.11.09 in Hamburg

Basis-Seminar: Sicherheitsmechanismen für Voice over IP
09.02. - 10.02.09 in Hamburg
14.05. - 15.05.09 in Bonn
05.10. - 06.10.09 in Frankfurt

Alternative 1: IP-Telefonie evaluieren, planen, betreiben
02.03. - 04.03.09 in Stuttgart
25.05. - 27.05.09 in Hamburg
14.09. - 16.09.09 in Köln
02.11. - 04.11.09 in Frankfurt

Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management
16.02. - 18.02.09 in Bonn
15.06. - 17.06.09 in Stuttgart
26.10. - 28.10.09 in Berlin

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
02.02. - 03.02.09 in Bonn
04.05. - 05.05.09 in Königswinter
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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research