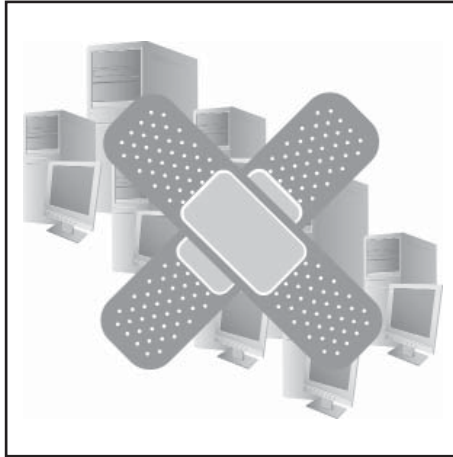


Schwerpunktthema

Verwundbarkeitsmanagement (Leitfaden anhand eines Projektbeispiels)

von Dipl.-Inform. Andreas Meder

Jede IT-Infrastruktur ist heute vielfältigen Gefahren ausgesetzt. Ständig werden neue Sicherheitslücken in Systemplattformen und/oder Anwendungen bekannt, für die die Hersteller in der Regel kurzfristig entsprechende „Security-Fixe“ zur Verfügung stellen. Mitunter ist zu diesem Zeitpunkt der Schaden im Einzelfall zwar bereits angeordnet, aber je nach Verbreitungsgrad der betroffenen System- bzw. Anwendungsumgebungen lässt sich unter Umständen bei einer Vielzahl von ebenfalls gefährdeten Systemlandschaften ähnliches Ungemach verhindern – oder doch zumindest hinsichtlich der Auswirkungen begrenzen – schnelles, konsequentes und gleichzeitig planvolles



Handeln vorausgesetzt. In diesem Artikel werden basierend auf Erfahrungen aus realen Projekten Grundzüge einer möglichen Herangehensweise dargestellt.

Umfeld und Prinzipien

Wie eingangs schon angesprochen, ist es mehr als nur eine sinnvolle Überlegung, potentielle Verwundbarkeiten der in der eigenen Systemlandschaft zur Anwendung kommenden Betriebssysteme und Anwendungen frühzeitig durch Gegenmaßnahmen zu entschärfen; ...

weiter auf Seite 7

Zweitthema

40 GBASE-T: jetzt kommt es doch!

von Dr. Franz-Joachim Kauffels

Bereits im Jahr 2008 gab es Diskussionen um die nächste Evolutionsstufe der kupferbasierten Übertragungssysteme. Danach wurde es aber so still um das Vorhaben, dass man auch angesichts der vielen Fortschritte hinsichtlich der preiswerten Übertragung über Glasfasern annehmen konnte, dass diese Entwicklung nicht mehr

statt findet. Mittlerweile hat sich das Rad aber weitergedreht und die Arbeiten bei EIA/TIA sowie ISO 11801 wurden Ende 2011 mit erheblichem Elan wieder aufgenommen. Renommiertere Hersteller wie Siemon und Nexans haben bereits geeignete Verkabelungssysteme und Komponenten vorgestellt.

Der Druck für die Weiterentwicklung der kupferbasierten Lösungen für 40 GbE kommt von den Serverherstellern. Wie auch schon für 10 GbE wollen sie eine preisgünstige Lösung für das Rack.

weiter auf Seite 15

Geleit

Gigabit-Wireless: erste Produkte angekündigt, es geht los, aber wohin?

auf Seite 2

Aktueller Kongress

Netzwerk-Redesign Forum 2012

ab Seite 4

Neues Seminar

BYOD: Sichere Integration von mobilen Privatgeräten in die IT-Infrastruktur

auf Seite 13

Standpunkt

Erfahrung statt Technik!

auf Seite 14

Zum Geleit

Gigabit-Wireless: erste Produkte angekündigt, es geht los, aber wohin?

IEEE 802.11n hat die lange erwartete solide Basis für Wireless LAN Lösungen gelegt. Es ging um einen riesigen Markt, so dass die Streitereien zwischen den Beteiligten den Standard um Jahre unnötig verzögert haben. Nun geht das ganze Spiel wieder los. Zwei verschiedene Wireless-Standards streiten um die Gunst des Kunden, beide sind rückwärts-kompatibel. Bisher war das ein Wettkampf hinter den Kulissen, aber die gerade in Las Vegas laufende Consumer Electronic Show CES hat den Knoten platzen lassen. Nachdem bisher nur einige kleinere Anbieter Ankündigungen platziert hatten, ist jetzt Broadcom auf das Parkett getreten und hat seine ersten 802.11ac-Chips noch für dieses Jahr angekündigt. Hersteller wie Netgear haben dann auch sofort Produkte für das zweite Halbjahr angekündigt.

Stellen wir also fest:

- Die Gigabit-Wireless-Welle läuft los.
- Produkte kommen noch in 2012, obwohl der Standard noch nicht verabschiedet ist.
- Die wesentlichen Marktteilnehmer bringen sich in Position.
- Die Entscheidung über den Weg in die Zukunft fällt auf jeden Fall im Konsumer-Markt, hier liegen die Stückzahlen.

Aber worum geht es und wieso brauchen wir überhaupt einen neuen Standard? Sollen wir das ganze Getöse ignorieren und gelassen abwarten?

Fangen wir mit dem Bedarf aus der Sicht eines normalen Unternehmens an. Der ist identisch mit den Mängeln von 802.11n:

- Das benutzte Medienzugangsverfahren ist eines der schlechtesten jemals in einem Standard definierten, es skaliert nicht mit hohen Teilnehmerzahlen pro Zelle, im theoretischen Extremfall kann der Verkehr in einer Zelle zusammen brechen.
- Die Übertragungs-Kapazität pro Zelle ist bezogen auf die typische Abdeckung von 150 bis 200 qm in Büroumgebungen (je nach Dämpfung und Reflexion durch Wände oder Me-



tall) deutlich zu klein, theoretisch sind Rohdatenraten bis 600 Mbit/s im Standard möglich, doch bisher sind nur 450 Mbit/s-Systeme auf dem Markt und deren reale Nutzdatenrate liegt bedingt durch die geringe Effizienz des Medienzugangsverfahrens deutlich darunter (eine gute Faustformel sind 50%).

- Eine Lösung für mehr Parallelität der Kommunikation innerhalb einer Zelle wäre ideal.
- Die Service-Qualität innerhalb einer Zelle schwankt extrem je nach Entfernung zum Access-Point. Teilnehmer mit Sichtkontakt zum AP und Entfernungen unter 2m haben sehr gute Durchsatzraten, Teilnehmer am Rande der Zelle können froh sein, wenn sie stabil kommunizieren können, auf jeden Fall haben sie deutlich niedrigere Durchsätze.

Das war für viele Unternehmen bisher ok, war doch die Teilnehmerzahl überschaubar. Probleme gab es eher bezogen auf die Umsetzung von Wireless-Switch-Systemen und den damit verbundenen Produkteigenschaften bei beweglichen Teilnehmern.

Warum reicht IEEE 802.11n denn nun mit den genannten Mängeln als Basis für eine Zukunftssichere Installation nicht mehr aus?

Wir stehen vor einer bisher noch nie da gewesenen Welle von mobilen Teilnehmern. Die Marktvorhersagen für die nächsten 5 Jahre sind so erschütternd, dass wir nur hoffen können, dass sie nicht eintreffen. Aber wir alle kennen

iPhones, iPads, Androids und beobachten gleichzeitig die Entwicklung bei den Laptops, wo gerade die Ultrabooks als Kopie des MacBook Air mal wieder den Markt anzuschleichen versuchen. Wir müssen also davon ausgehen, dass die Anzahl mobiler Teilnehmer in den Unternehmen zunimmt. Was bedeutet das für die Planung von WLAN-Installationen?

Im Prinzip sind wie immer schon drei Kernfragen zu beantworten:

- Wie groß soll die Zellabdeckung sein (inklusive der notwendigen Überlappung mit Nachbarzellen für bewegende Teilnehmer)?
- Wie viele Teilnehmer pro Zelle werden erwartet?
- Wie viel Bandbreite soll jedem Gerät zugewiesen werden?

Die subjektiven Antworten dazu aus meiner Sicht:

Die bisherige Zellgröße hat sich eigentlich in der Praxis bewährt. Eine bessere Ausleuchtung und eine stabilere Service-Qualität wären wichtiger als noch größere Zellen. Auch die Schaffung von Parallelität würde helfen.

Unter normalen Umständen sollte von maximal 10 bis 20 Teilnehmern pro Zelle ausgegangen werden. Dieser Wert ist in der Tat kritisch, da das Zugangsverfahren nicht skaliert und zu viele Teilnehmer das Netzwerk theoretisch destabilisieren können.

Bei der Kalkulation der Bandbreite sind fünf verschiedene Aspekte zu berücksichtigen:

- Die zunehmende Bedeutung von Video inklusive mobiler Video-Konferenzen. Hier wird die notwendige Datenrate weiter sinken. Der SVC-Standard wird Konferenzen mit 512 Kbit/s möglich machen, das heutige Maximum ist bei 2 Mbit/s für mobile Geräte anzusiedeln. Theoretisch stellen Video-Übertragungen in Blueray-Qualität noch höhere Anforderungen, aber das macht für mobile Teilnehmer eigentlich keinen Sinn.
- Die mobilen Teilnehmer werden in Zukunft in Private oder Public Cloud-Infrastrukturen eingebunden sein. Dies

Schwerpunkthema

Verwundbarkeitsmanagement (Leitfaden anhand eines Projektbeispiels)



Dipl.-Inform. Andreas Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

Fortsetzung von Seite 1

... andernfalls muss zwar nicht, kann aber ein – möglicherweise existenzbedrohender – Schaden durch Ausnutzen einer solchen Schwachstelle entstehen.

Allgemein kann gesagt werden, dass es zur Aufrechterhaltung der Sicherheit der IT-Infrastruktur im laufenden Betrieb notwendig ist, zumindest solche Security-Fixe zu installieren, bei denen das Schadensrisiko, d.h. die Eintrittswahrscheinlichkeit eines Schadens in Verbindung mit der erwarteten Schadenshöhe, eine bestimmte Grenze überschreitet. Bei der Festlegung dieser Grenze in Form eines Schwellenwertes ist u.a. naturgemäß immer auch der Aufwand für die Implementation eines Security-Fixes zu berücksichtigen.

Um dabei systemübergreifend ein einheitliches und angemessenes Sicherheitsniveau erreichen zu können, müssen grundlegende Verfahrensweisen und Kriterien im Rahmen des Verwundbarkeitsmanagements festgelegt werden. Soweit die Theorie. In der Realität hingegen existiert in vielen (um nicht zu sagen: den meisten) Fällen keine einheitliche Vorgehensweise zum Verwundbarkeitsmanagement. Es fehlen sowohl entsprechende Vorgaben hinsichtlich der Bewertung und Kategorisierung von Schwachstellen als auch die notwendigen Prozesse, die den Umgang mit festgestellten Sicherheitslücken in konkret in der eigenen IT-Landschaft im Einsatz befindlichen IT-Systemen in Abhängigkeit von der Kategorie und damit verbunden der Dringlichkeit verbindlich regeln. Maßnahmen zum Schließen solcher Sicherheitslücken werden stattdessen – wenn überhaupt – individuell von den jeweils für den Betrieb der betroffenen Systeme verantwortlichen IT-

Mitarbeitern recherchiert und umgesetzt. Als Konsequenz resultiert hieraus ein uneinheitlicher Stand in Bezug auf installierte Sicherheitsupdates, der in aller Regel obendrein nicht in seiner Gesamtheit dokumentiert ist. Daher fehlt typischerweise auch ein Gesamtüberblick über die jeweils aktuelle Bedrohungslage.

Wir wollen im Folgenden etwas genauer betrachten, wie ein solches Verwundbarkeitsmanagement angelegt sein kann. Da es hierfür selbstverständlich im Detail sehr unterschiedliche Varianten geben kann und gibt, werden wir uns beispielhaft an einem realen Projekt orientieren; dabei aber sollte aber stets bedacht werden, dass die beschriebene Lösung nur eine von vielen möglichen ist.

Zunächst bedarf es einer Definition des Begriffs „Verwundbarkeitsmanagement“. Hierunter wird im Folgenden eine Beschreibung des geregelten Umgangs mit Sicherheits-Schwachstellen in IT-Systemen mit dem Ziel verstanden, solche Schwachstellen zu eliminieren bevor sie zu negativen Vorfällen wie Ausspähung, Manipulation oder Zerstörung von Daten führen. Ein derartiges Verwundbarkeitsmanagement verfolgt typischerweise folgende Ziele:

- Herbeiführung und Erhalt eines einheitlichen und angemessenen Sicherheitsniveaus der IT-Systeme
- Nachvollziehbarkeit des Sicherheitsniveaus durch übersichtliche Dokumentation geschlossener bzw. nicht geschlossener Sicherheitslücken
- Schnellere Reaktionszeiten und geringerer Aufwand bei der Behandlung von

Sicherheitslücken durch abgestimmte und etablierte Verfahren

Vor dem Hintergrund der oben dargestellten typischen Ausgangslage empfiehlt es sich, bei der Herangehensweise an die Spezifikation des Verwundbarkeitsmanagements darauf zu achten, dass alle Abläufe, die im Rahmen des zu definierenden Prozesses zu beschreiben sind, einen hohen Standardisierungsgrad aufweisen und für alle Involvierten verbindlich sind. Nur so lässt sich ein hinreichend hoher Qualitätsstandard auf Basis vorhandenen Personals und etablierter Strukturen überhaupt erzielen. Aus ähnlichen Beweggründen sind insbesondere individuelle Recherchen und ähnliche Arbeitsschritte, die Expertenwissen erfordern, auf Ausnahmefälle zu beschränken, was wiederum den Einsatz externer Informationsquellen (insbesondere sogenannte „Verwundbarkeitsdatenbanken“, s.u.) zu bekannten Sicherheitslücken und empfohlenen Maßnahmen angeraten erscheinen lässt. Der bewusste Verzicht auf Expertenwissen gestattet es insbesondere, das Verwundbarkeitsmanagement – zumindest in Bezug auf Standard- bzw. Routineaufgaben (also das sprichwörtliche „Massengeschäft“) personell in Bereichen anzusiedeln, in denen solche Expertise nicht vorausgesetzt werden kann, etwa im Umfeld von Help Desk & Co.

Da das Verwundbarkeitsmanagement nicht im luftleeren Raum existiert, sondern sich in bereits bestehende Prozessstrukturen eingliedern soll, sind beim Design des entsprechenden Prozesses neben den zuvor schon dargelegten Zielen (siehe oben) vor allem die Schnittstellen zu kooperierenden Prozessen darzustellen. Aber auch der Geltungsbereich, also die

Verwundbarkeitsmanagement (Leitfaden anhand eines Projektbeispiels)

Bereiche der IT, innerhalb derer die Regelungen des Verwundbarkeitsmanagements zwingend zu beachten bzw. befolgen sind, ist ebenso festzulegen wie das Prozedere zur Aktualisierung der Prozessbeschreibung: Die Regelungen des Verwundbarkeitsmanagements müssen einem kontinuierlichen Reviewprozess unterliegen mit dem Ziel einer sukzessiven Optimierung und ständigen Anpassung an zukünftige Rahmenbedingungen; vor allem in der Anfangsphase ist bei Etablierung eines neuen Prozesses mit Nachbesserungsbedarf zu rechnen, etwa hinsichtlich der Ausgestaltung der Schnittstellen zu anderen Prozessen aber auch in Bezug auf Fristen, Schwellwerte etc.. Werden im Zuge solcher Reviews Defizite, Optimierungspotenziale oder Anpassungsbedarfe konkret festgestellt, ist die Prozessspezifikation des Verwundbarkeitsmanagements geeignet fortzuschreiben. Diesbezügliche Änderungen – soweit sie autorisiert sind – erlangen dabei sinnvollerweise unmittelbar Gültigkeit, soweit nicht besondere Gründe dafür sprechen, einen speziellen Termin zur Inkraftsetzung zu spezifizieren. Jegliche Änderung ist allen in das Verwundbarkeitsmanagement involvierten Personen und Gremien selbstverständlich unverzüglich bekanntzugeben.

Der Prozess

Die nachfolgende Skizze eines Prozesses zum Verwundbarkeitsmanagement mag – wie eingangs bereits dargestellt – als Beispiel dafür dienen, wie ein solcher hinsichtlich benötigter Rollen, Abläufe, Schnittstellen, Werkzeuge usw. aussehen kann – aber natürlich nicht muss. Im Rahmen des hier Pate stehenden Projekts hat sich das dargestellte Verfahren als der optimale Kompromiss im Spannungsfeld personeller Zwänge einerseits und angestrebtem Resultat andererseits herauskristallisiert. Anders gelagerte Rahmenbedingungen mögen hier entsprechend andere Vorgehensweisen im Detail ratsam erscheinen lassen; somit können die untenstehenden Ausführungen nur eine Anregung sein, an der man sich bei Bedarf orientieren mag.

Der hier entwickelte Prozess sieht zwei **Rollen** vor: den Verwundbarkeitsmanager (VM) und den Produktverantwortlichen (PV); ersterer war (naheliegenderweise) im Rahmen des Verwundbarkeitsmanagements neu zu schaffen, während letzterer in der hier beispielhaft betrachteten Umgebung bereits existierte und somit lediglich eine Erweiterung seines Aufgabenspektrums vorzunehmen war. Daneben sind noch das CERT (Computer Emergency Response Team) und der bestehende Prozess zum Patchmanagement in Form entsprechender Schnittstellen zu berücksichtigen.

Der Verwundbarkeitsmanager bildet dabei die zentrale Rolle innerhalb des Verwundbarkeitsmanagements. Er nimmt dementsprechend eine ganze Reihe von Aufgaben wahr:

- Filterung der aufgelaufenen Meldungen aus der Verwundbarkeitsdatenbank (s.u.) über festgestellte Sicherheitslücken und empfohlene Maßnahmen nach umgebungsspezifischer Relevanz.

Hierzu erfolgt zunächst eine Sichtung der jeweiligen Quellen der Verwundbarkeitsdatenbank, und zwar bei passiven Quellen, die einen aktiven Zugriff durch den Verwundbarkeitsmanager erfordern, regelmäßig einmal je Arbeitstag; bei aktiven Quellen, die Meldungen z.B. per E-Mail an den Verwundbarkeitsmanager übermitteln, unmittelbar nach Kenntnissnahme vom Eintreffen der Meldung.

Im Rahmen der anschließenden Filterung werden alle Meldungen verworfen, deren Merkmale nicht in der jeweils gültigen Positivliste der umgebungsrelevanten Verwundbarkeiten enthalten sind (es liegt nahe, in Umgebungen, in denen beispielsweise keine Solaris-basierten Systeme im Einsatz sind, Meldungen über Solaris-spezifische Verwundbarkeiten von vornherein auszublenden; analoges gilt selbstverständlich in Bezug auf bestimmte Releasestände etc.).

- Vorklassifizierung der empfohlenen Maßnahmen nach Dringlichkeit gemäß aktuell gültiger Kriterienpezifikation (s.u.)
- Eliminierung eventuell vorliegender Dubletten (d.h. Meldungen gleichen Inhalts aus verschiedenen Quellen), soweit zweifelsfrei möglich; dabei bleibt

grundsätzlich die Maßnahme mit der jeweils höchsten Dringlichkeit erhalten.

- Öffnen je eines Tickets je Maßnahme mit Übernahme der zu der Maßnahme gehörenden Informationen: Inhalt der Meldung (Verwundbarkeit, betroffene Systeme, Maßnahmen, etc.) und Dringlichkeit nach Vorklassifizierung.
- Weiterleitung von Maßnahmen, für die entsprechender Bedarf vorliegt, an das CERT; ein Bedarf für die Einschaltung des CERT liegt dabei vor, wenn für eine gemäß den entsprechenden Kriterien als ausreichend dringlich vorklassifizierte Sicherheitslücke noch keine empfohlene Maßnahme vorliegt, oder aber wenn eine solche Maßnahmenempfehlung mit oberster Dringlichkeit gemäß Vorklassifizierung vorliegt, die unter Umständen weitere flankierende Maßnahmen erforderlich macht. Letzteres ist insbesondere kritisch, wenn hierdurch negative Seiteneffekte auf andere IT-Bereiche zu befürchten sind; in solchen Fällen ist eine dedizierte Abwägung von Nutzen und Risiko einer Maßnahme notwendig, die in aller Regel die Sach- wie auch Entscheidungskompetenz des Verwundbarkeitsmanagers übersteigt (wir erinnern uns: innerhalb des Verwundbarkeitsmanagements sollte nach Möglichkeit kein besonderes Expertenwissen erforderlich sein). Das CERT liefert dann – gegebenenfalls übergangsweise – Maßnahmenempfehlungen für den Umgang mit der Sicherheitslücke.
- Weiterleitung von empfohlenen Sicherheitspatches bzw. Maßnahmen an den zuständigen Produktverantwortlichen zur konkreten Klassifizierung und Wei-

Seminar

Interne Absicherung der IT-Infrastruktur 14.03. - 16.03.12 in Köln

Bedingt durch Netzkonvergenz, Mobilität und Virtualisierung hat die interne Absicherung der IT-Infrastruktur in den letzten Jahren enorm an Bedeutung gewonnen. Heterogene Nutzergruppen mit unterschiedlichstem Sicherheitsniveau teilen sich eine gemeinsame IP-basierte Infrastruktur und in vielen Fällen ist der Aufbau sicherer, mandantenfähiger Netze notwendig. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf.

Referenten: Dipl.-Inform. Oliver Flüs, Dr. Simon Hoff
Preis: € 1.890,- netto



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

Zweitthema

40 GBASE-T: jetzt kommt es doch!

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.

Die in der Abbildung 1 dargestellte Entwicklung hinsichtlich der notwendigen Anschlussleistungen für x86-basierte Server ist zwar schon etwas älter, hat sich aber bis jetzt präzise bewährt.

In den Backplanes gibt es schon 40 GBASE-KR. Wer sofort 40 GbE auf Kupfer einsetzen möchte, kann natürlich 40 GBASE-CX4 nehmen, was technisch gesehen einfach vier mal 10GBASE-CX ist und sich in seiner Urform durch vier dicke Kabel auszeichnet. Das ist alles andere als elegant, aber es spricht ja nichts gegen die Verwendung aktiver optischer Kabel für 40 GbE, die einfach in das CX-Loch gesteckt werden und ihren Strom für die in die Stecker integrierten Transceiver ebenfalls aus dieser Schnittstelle entnehmen. Es wird immer wieder angeführt, dass die Verwendung aktiver optischer Kabel dem Gedan-

ken eines passiven Netzes widerspricht. Das ist formal korrekt, aber aus der betrieblichen Sicht nicht wirklich nachzuvollziehen.

Also, wer seine 40 GbE-Server anschließen will, hat eigentlich schon heute eine große Auswahl. Warum dann noch 40 GBASE-T?

Es ist letztlich weniger als eine technische Frage, sondern eher eine Frage von Reichweite, betrieblichen Aspekten, grundsätzlicher Systematik und Flexibilität.

Die Reichweite der CX-Schnittstelle ist sehr begrenzt und wenn man aktive optische Kabel verwendet, ist deren mögliche Länge vom jeweiligen Hersteller abhängig. Man geht also an einer Stelle

eine Herstellerbindung ein, wo man sie bestimmt nicht möchte. Die optischen Schnittstellen wie 40 GBASE-SR sind zwar höchst elegant, wenn aber an einem gelieferten Server nur eine Kupferschnittstelle vorhanden ist, was in den meisten Fällen aus Kostengründen so sein wird und die Situation an den Switches ähnlich aussieht, fügt man pro Verbindung genau wie bei den aktiven optischen Kabeln zwei zusätzliche Komponenten hinzu. Diese fallen zwar aus der Erfahrung gesehen kaum aus, aber man muss sie eben doch überwachen. Das gibt also pro Verbindung zwei eigentlich völlig unnütze Wartungspunkte.

Wenn ein Betreiber also nicht mit allen Konsequenzen komplett auf Glasfasern umrüsten möchte, benötigt er unbedingt eine kupferbasierte Übertragungslösung für 40 GbE, die genau so flexibel, universell und zuverlässig ist, wie er das von 10 GbE oder geringeren Datenraten gewohnt ist.

Und genau das würde 40 GBASE-T bieten!

Vor ca. 12 Jahren gab es erhebliche Zweifel daran, dass 10 GbE über Kupfer funktionieren könnte. Wie wir wissen, gab es zwar noch ein ziemliches Gezerre zwischen den Standardisierungsorganisationen, aber am Ende hat es funktioniert.

Im weiteren Verlauf des Artikels erklären wir genau, wie und unter welchen Bedingungen 40 GBASE-T funktionieren kann und wird. Für die Ungeduldigen fassen wir aber die wichtigsten Faktoren hier kurz zusammen.

- Kabel sind besser als ihr Ruf. Momentan liegt die Grenze für die maximale

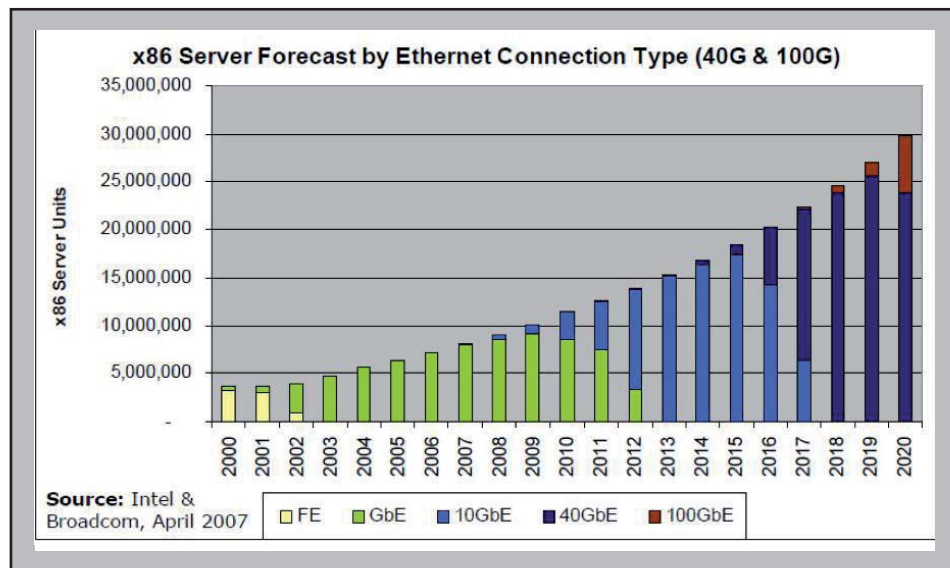


Abbildung 1: x86-Server und Anschluss-Datenraten

40 GBASE-T: jetzt kommt es doch!

Frequenz, die ein Signal auf einem Kabel pro Paar haben darf, bei 600 MHz. Hersteller haben aber schon längst hochqualitative Kabel entwickelt, die durchaus in der Lage sind, Signale mit einer Bandbreite von 1000 MHz sinnvoll zu übertragen. Dazu gehören natürlich auch passende Stecker.

- Um ein Signal mit einer derartigen Bandbreite zu übertragen, sind Maßnahmen in zwei Gruppen erforderlich: die erste Gruppe bereitet das Signal auf seinen beschwerlichen Weg vor, die zweite Gruppe fischt aus dem erheblich verformten Signal am Ende des Übertragungsweges die mittlerweile mit einer Reihe von Störungen gemischten Nutzinformationen wieder heraus.

- Die in diesem Zusammenhang notwendigen digitalen Signalprozessoren unterliegen wie alle integrierten Schaltkreise Moore's Law. Seit der Entwicklung von 10 GBASE-T vor 12 Jahren konnten diese Signalprozessoren also in ihrer Komplexität um den Faktor 256 zulegen, wenn man eine Verdopplung der Transistoren alle 18 Monate zugrunde legt. Dabei sind die Kosten kaum oder gar nicht gestiegen. Das reicht völlig für die Behandlung eines Signals, welches lediglich um den Faktor 4 zugelegt hat.

- Das mit IEEE 802.3ab definierte „Skalierbare Ethernet“ lässt eine beliebige Zerlegung eines Nachrichtenstroms in Unterströme von 2,5 Gbps zu und definiert Standardmechanismen dafür. Jede Art von Transceiverschaltkreisen kann sich das zu Nutze machen, um einen möglichst großen Teil der Logik in preiswerter paralleler CMOS-VLSI-Technik auszuführen. Das ist auch auf die für 40 GbE notwendigen Signalprozessoren übertragbar.

Technisch gesehen sind wir jetzt also für eine Steigerung der kupferbasierten Übertragung auf 40 GbE bestens gerüstet.

In 2008 ist man vor allem dann an technische Probleme gestoßen, wenn man die Länge einer 40 GBASE-T-Verbindung wirklich auf 100m steigern möchte. Die Realität zeigt jedoch, dass die überwiegende Anzahl von notwendigen Verbindungen deutlich kürzer ist. Definiert man also erfolgreich ein System, welches die 100m schafft, besteht ein hinreichender Puffer für evtl. in der Praxis immer wieder auftretende Schwankungen. Die interessante Graphik Abbildung 2 zeigt aber auch, dass ein Ansatz, der nur 10 m überwinden kann, deutlich zu kurz greift.

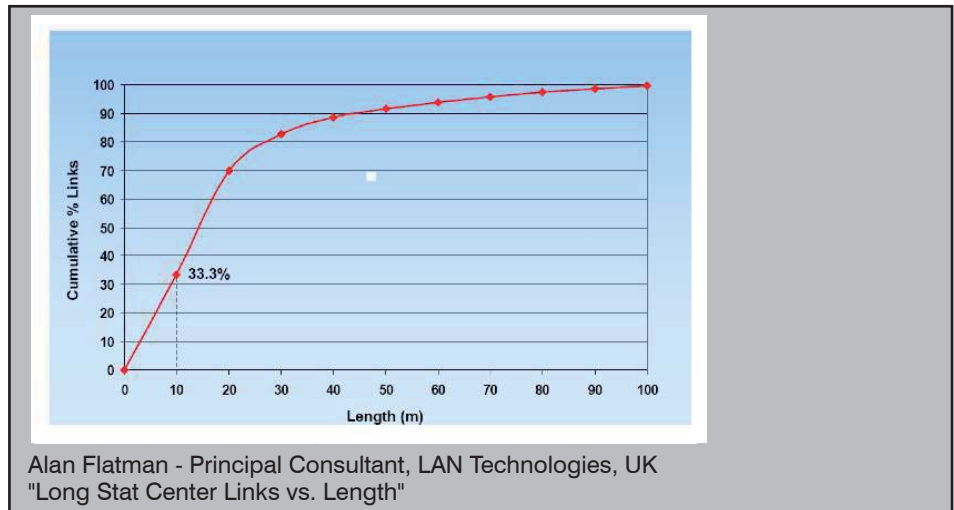


Abbildung 2: Verteilung der notwendigen Kabel-Längen in einem RZ

Man sieht, dass 80% der Verbindungen kürzer als 30 m und 93% kürzer als 50 m sind. Man könnte sogar auf den Gedanken kommen, dass für die kürzeren Verbindungen auch ein Kat. 6A Kabel ausreichend ist. Dieser Gedanke ist aber erheblich verwegen.

Schon im Spätherbst 2008 gelang Wissenschaftlern der Penn State University der eigentliche Durchbruch:

50 Gigabit pro Sekunde über 100m Twisted Pair Kabel der Kategorie 7A!

Damit wurden schon zwei für die Planung enorm wichtige Dinge erarbeitet:

- es gibt ein Twisted Pair Kabel, welches für 40 GBASE-T geeignet ist
- es gibt einen geeigneten Stecker

Es sei allerdings hier direkt angemerkt, dass es einen erheblichen Unterschied zwischen der Standardisierung von 10 GBASE-T und 40 GBASE-T gibt. Im Bereich 10 GbE hat man viel Zeit damit ver-

loren, einen Standard für ungeschirmte UTP-Kabel (Kat 5) zu entwickeln. Bei 40 GbE ist von Anfang an klar, dass es eine Lösung nur für geschirmte STP-Kabel geben kann.

Auch das Kabel der Kat. 7A befindet sich zur Zeit in der Normung. Allerdings gibt es schon einige Hersteller, die ein solches Kabel anbieten. Wir beziehen uns im Folgenden auf das Produkt LANmark 7A von Nexans.

Das 7A-Kabel ist in seinen Eigenschaften bis 1000 bzw. 1200 MHz definiert, geht also weit über den bisher definierten Bereich hinaus. Das 6A-Kabel ist in der Norm nur bis 250 MHz definiert, normtreue Produkte sind bis zu 500 MHz spezifiziert.

Die Eckdaten des 7A-Kabels sind:

- NEXT (Nahnebensprechdämpfung): 60 dB bei 1000 MHz
- FEXT (Fernnebensprechdämpfung): 50 dB bei 1000 MHz

- Cat. 6A für 10 GBASE-T spezifiziert
- Cat. 7A in der Diskussion, aber es gibt schon Produkte, Beispiel Nexans LANmark-7A

	LANmark-7A	Category 6A
• NEXT	60dB at 1000MHz	30dB at 500 MHz
• FEXT	50dB at 1000 MHz	25dB at 500 MHz
• RL	8dB at 1000 MHz	8dB at 500 MHz

- NEXT: Nahnebensprechdämpfung
- FEXT: Fernnebensprechdämpfung
- RL: Return Loss

Abbildung 3: Cat 6A und Cat 7A