Dr. Suppan International Institute

Der Netzwerk Insider

März 2001

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Ethernet Everywhere

von Dr. Franz-Joachim Kauffels

Seit die Firma Extreme Networks etwa im September 2000 diesen Schlachtruf durch ihren CEO bei einer wichtigen Investorenkonferenz ins Leben gerufen hat, geht die Idee des allumfassenden Ethernet-Päckchens niemandem mehr so richtig aus dem Kopf. Zu verlockend ist der Gedanke, endlich mit all den heute existierenden Formaten und Systemen aufräumen zu können und eine einheitliche Infrastruktur für alle Kommunikationsbedarfe zu schaffen.

Ab der Schicht drei aufwärts ist dies mit der TCP/IP-Protokollfamilie schließlich auch weitestgehend gelungen.

Für die unternehmens- und organisationseigenen Netze ist das Thema durch. Niemand käme auf die Idee, ernsthafterweise ein neues Netz oder eine Migration mit etwas anderem als der Ethernet-Technologie durchzuführen.

Extreme Networks wies den Weg: Ethernet Everywhere

Im Bereich der Storage Area Networks hat heute noch der Fibre Channel die Oberhand, allerdings liegt das nur an einer Leistung deutlich über einem Gbps.

Sobald der 10 Gbps Ethernet Standard wirklich fertig ist, werden auch die SAN-Hersteller wie Brocade und EMC das Ethernet-Format in weiten Bereichen adoptieren.

Wer dies unbedingt wünscht, kann heute auch über Ethernet telefonieren. Voice über IP bedeutet in letzter Konsequenz, dass die IP-Päckchen im Ethernet Format transportiert werden. Überhaupt ist "IP Everywhere" der Wegbereiter für Ethernet Everywhere. ATM ist nicht zuletzt deshalb gestorben, weil beim Transport von IP-Strömen ein zu hoher Overhead von bis zu 50% entstanden ist.

weiter Seite 8

Sicherheit

Encrypting File System (EFS) unter Windows 2000 Nicht für Gruppen geeignet?

von Michael van Laak

Dieser Artikel behandelt das in Windows 2000 enthaltene Datei-Verschlüsselungs-Produkt EFS (Encrypting File System).

Es erfolgt eine kritische Bewertung besonders mit Blickrichtung auf einen Gruppenansatz.

Die Informationen beruhen sowohl auf Ergebnissen aus dem ComConsult Beratung und Planung GmbH Testcenter als auch auf der Analyse für Kunden.

weiter Seite 14

Stichworte

- DESX (56-bit, 128-bit)
- Verschlüsselung und Entschlüsselung
- unterstützte Dateisysteme (Verhalten bei Kopieren und Verschieben)
- Verschlüsselung und Komprimierung
- Verschlüsselung von lokalen und servergespeicherten Daten
- Übertragen von verschlüsselten Daten über ein Netzwerk
- Wiederherstellung verschlüsselter Daten
- Recovery Agents
- Recovery (Group) Policy
- EFS für bestimmte Computer deaktivieren (Verschlüsselung verhindern)
- Gruppenkonzept
- Vergleich mit Verschlüsselungssoftware anderer Hersteller

Zum Geleit

Ist eine Ein-Hersteller-Strategie noch sinnvoll?

In den meisten Fällen werden Netzwerke heute mit den Komponenten eines Herstellers realisiert. Eine gezielte Mischung von Komponenten verschiedener Hersteller wird in der Regel abgelehnt.

Meiner Ansicht nach ist diese Strategie nicht mehr zeitgemäß und für viele Anwender ein sehr teurer Weg.

Impressum

Verlag:
Dr. Suppan
International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland
Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber
und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich,
12 Ausgaben im Jahr

Bezug:
Kostenlos
als PDF-Datei
über den eMail-
VIP-Service
der ComConsult Akademie

Für unverlangt
eingesandte Manuskripte
wird keine Haftung übernommen

Welche Vorteile hat eine Reduzierung auf einen Hersteller?

Im Endeffekt stammt die Strategie aus einer Zeit mit zwei wesentlichen Rahmenbedingungen:

- es gab keine akzeptierten Standards für Switch-Systeme, die Produkte hatten stark Hersteller-individuelle Eigenschaften
- es gab einen Direktvertrieb der Hersteller und eine Ein-Hersteller-Strategie war zur Erreichung eines adäquaten Service-Levels unverzichtbar

Beide Annahmen entsprechen mindestens im Layer-2-Bereich nicht mehr der im Markt gegebenen Situation:

- durch die stark ausgeweiteten Standards der letzten Jahre entsprechen sich die Switch-Systeme im Layer-2-Bereich immer stärker (man vergleiche: Bay/Nortel 350/450, CISCO 35xx, HP 25xx, Intel 510), ein technischer Unterschied zwischen diesen Geräten ist kaum feststellbar. Trotzdem unterscheiden sich die Preise pro Port um bis zu 100%
- die Hersteller vertreiben überwiegend über Händler. Eine Konzentration des Services auf einen Händler ist auch bei einer Mehr-Hersteller-Strategie möglich. Im Gegenteil würde dies durchaus dem Interesse einiger Händler entsprechen, da damit eine stärkere Profilierung möglich wäre

Was spricht also noch ansonsten für eine Ein-Hersteller-Strategie?

Gemeinhin werden folgende Vorteile aufgeführt:

- Reduzierung auf ein Betriebs-Know-How
- Eine gemeinsame Konfigurations-Oberfläche im Rahmen eines durchgängigen Konfigurations-Managements
- Ein gemeinsames Überwachungs- und Alarm-Management
- Nutzung Hersteller-spezifischer Verfahren, für die kein Norm-Äquivalent existiert oder die deutlich besser sind als die Norm
- Eine einzige Support-Strategie mit der Möglichkeit, auch auf den Direkt-Support des Herstellers zurück zu greifen

Sind diese Vorteile heute noch relevant?

Folgende Argumente sprechen dagegen:

- im Layer-2-Bereich ist das Know-How beliebig austauschbar, ich habe bei der Vernetzung unserer Grundschule den Selbstversuch gewagt: aus Finanzgründen musste nach reinen Preisgesichtspunkten ein Layer-2-Switch mit allen üblichen Features gekauft werden (VLAN, Link Aggregation, Management, Web-Konfiguration, Monitor-Port, Gruppen Konfiguration für mehrere Switches unter einer Adresse). Das Produkt war mir vorher völlig unbekannt. Nach nicht einmal 3 Stunden war mir jedes Feature bekannt
- eine gemeinsame Konfigurations-Oberfläche über alle angebotenen Layer-2 und Layer-3-Geräte ist bei den meisten Herstellern nicht gegeben. Im Gegenteil, häufig wird den Kunden eine stark Geräte-individuelle Konfiguration zugemutet, der Grad an Konfigurations-Komfort bewegt sicht nicht selten auf Steinzeitniveau
- Alarm- und Überwachungs-Management realisiert kein Hersteller in adäquater Form, in de Regel wird OpenView

Ist eine Ein-Hersteller-Strategie heute noch sinnvoll?

oder Netview für diesen Bereich eingesetzt. Neue Anbieter wie RiverSoft oder Smart werden diesen Trend verstärken, wünschenswert wären vielmehr seitens der Switch-Hersteller die Unterstützung von SNMP-Version3 sowie das Angebot eines Discovery-Protokolls inkl. der Erfassung der Layer-2-Verschaltung. SNMP-Version3 würde alle Inventarisierungs-Probleme sowie die gegebenen Alarm-Parameter-Engpässe der aktuellen SNMP-Version lösen,

- die von den Herstellern angebotenen individuellen Verfahren mit starken Vorteilen gegenüber einer Norm sind kaum noch feststellbar. CISCO hat marginale Vorteile im Bereich des VLAN-Managements über mehrere Switches hinweg, Extreme hat eine interessante Alternative zu VRRP, Avaya hat im Bereich Switch-Management mit SMON zur Zeit einen deutlichen Marktvorsprung. Aber reicht das für eine Entscheidung aus? Klare Differenzierungen gibt es im wesentlichen bei den sehr großen Layer-3-Systemen, dort werden Leistungsunterschiede in der Zahl unterstützter und pro Sekunde berechenbarer Routen immer deutlicher,

- die Support-Strategie eines Herstellers über den Lieferanten hinaus kann ein Vorteil sein, hier sehe ich zum Beispiel eine Stärke von CISCO. Nur wiegt dieser Vorteil nicht im Layer-2-Bereich sondern hat seinen Reiz primär im Layer-3-Bereich und den entsprechenden Verfahren

- eine Sonderrolle bei den Hersteller-Strategien kann Voice-over-IP einnehmen. Auch wenn jede VOIP-Lösung jedes Herstellers mit den Netzkomponenten jedes anderen Herstellers laufen sollte, können Vorteile durch die verfügbaren Interface-Karten für eine breite Zahl von Netzwerk-Komponenten sowie die Art der Stromversorgung der Telefone entstehen. Diese Vorteile hat zur Zeit sicherlich vorrangig CISCO auf seiner Seite.

Welche Nachteile hat eine Ein-Hersteller-Strategie, was würde für eine gezielte Mischung der Komponenten mehrerer Hersteller sprechen?

Diese Frage ist so pauschal nicht zu beantworten, da die Umgebung eines Kunden starke Einflüsse auf die Entscheidung haben kann. Deshalb zuvor einige Rahmenbedingungen, ich unterstelle:

- einen Layer-3-strukturierten Gigabit-Backbone mit OSPF

- eine Layer-2-Realisierung der Etagenbereiche mit folgenden Merkmalen
  – keine VLAN-Nutzung
  – kein Spanning-Tree auf der Etage
  – Switches werden auf der Etage weitestgehend wie Repeater behandelt, auf eine individuelle Konfiguration wird so weit möglich verzichtet

- Redundanz zwischen Etage und HVT nur über VRRP oder ein gleichwertiges Verfahren

Unter diesen Rahmenbedingungen kann eine Ein-Hersteller-Strategie folgende signifikante Nachteile haben:

- hohe Portkosten auf der Etage, wenn der Hersteller in diesem Bereich nur sehr teure Geräte anbietet

- hohe Layer-3-Kosten, wenn ein Hersteller keine kleinen und leistungsstarken Layer-3-Systeme anbieten kann

- generell hohe Kosten, wenn die von einem Hersteller angebotene Portdichte in den Geräten nicht mit dem gegebenen Bedarf überein stimmt

Hinzu kommt, dass für spezielle Anwendungsbereiche die Produktauswahl sehr eingeschränkt sein kann. So hat sich Hirschmann als Anbieter eindeutig auf Geräte für die Fertigungsumgebung spezialisiert. Geräte dieser Art sind bei den meisten anderen Anbietern nicht zu finden.

Meine persönliche Konsequenz?

Ich würde meine Kernentscheidung auf den Layer-3-Backbone-Bereich beschränken und hier meine konkreten und individuellen Anforderungen definieren. Hier werden Leistung und Stabilität eines Netzwerks entschieden. Die Entscheidung für die Layer-2-Systeme auf den Etagen würde ich primär an den Portkosten orientieren.

Fazit

Mit der zunehmenden Vereinheitlichung der Leistungen von Switch-Systemen insbesondere im Layer-2-Bereich werden die Geräte deutlich austauschbarer als bisher. Auch die technische Gesamtleistung dieser Geräteklasse nähert sich zwischen den Herstellern immer mehr an. Eigentlich fehlt nur noch der Einsatz gemeinsamer Chip-Sätze mit einer Reduzierung der Individualisierung auf den Bereich der Konfigurations-Software. Eine Einarbeitung in die Layer-2-Konfiguration ist in der Regel in wenigen Stunden möglich. In dieser Situation ist ein starker monetärer Nachteil einer Ein-Hersteller-Strategie nicht mehr hinzunehmen. Dementsprechend gibt es nur zwei Alternativen: eine Trennung der Investition zwischen den Layer-2 und den Layer-3-Bereichen oder aber eine Reaktion der besonders betroffenen Hersteller im Sinne einer deutlichen Preisreduzierung.

Ihr

Dr. Jürgen Suppan

Ihre Meinung ist gefragt!

Haben Sie dazu eine Meinung, dann schreiben Sie mir eine Mail. Vielleicht entsteht eine nette kontroverse Meinungsvielfalt, die wir in der nächsten Ausgabe präsentieren können.

drsuppan@comconsult.de

Sicherheits-Event 2001

Hochaktuelle Sicherheitsthemen in Theorie und Praxis: Netzwerk-Sicherheits-Forum 2001

Vom 7. bis 9. Mai 2001 in Königswinter bietet die ComConsult Akademie mit dem Netzwerk-Sicherheits-Forum ein herausragendes Event, das für jeden Sicherheitsverantwortlichen, Server- oder Netzwerkadmininstrator eine unverzichtbare Plattform für aktuelle Informationen, Produktvergleiche und Fachdiskussionen darstellt.

Das Netzwerk Sicherheits-Forum 2001 konzentriert sich auf die für den täglichen Betrieb relevanten Sicherheits-Maßnahmen. Es liefert Erfahrungsberichte und umsetzbare Empfehlungen zum sicheren Betrieb von IT-Umgebungen zu.Folgende Themenschwerpunkte prägen das ComConsult Sicherheits-Forum 2001:

Content-Security

Die Probleme bei der Nutzung von Internetdiensten, die einen Datenimport ermöglichen, werden immer gravierender. Der alleinige Einsatz von Virenscannern reicht schon lange nicht mehr aus, je nach Sicherheitsbedürfnis müssen zusätzliche Maßnahmen ergriffen werden. Dies betrifft zunehmend auch die Kontrolle von "Mobile Code", wie er z.B. bei Java oder Java-Script vorkommt. Neben einer realistischen Einschätzung der Bedrohungen sollen abgestufte Gegenmaßnahmen diskutiert werden. Hierzu gehört auch die Vorstellung und Bewertung von Produkten und Einsatztopologien.

Secure Web-Applications

Anwendungen, die über Netzgrenzen hinaus gehen, werden nicht nur im eCommerce immer häufiger eingesetzt. Dabei greifen zumeist externe Mitarbeiter oder Kunden auf Daten im internen Netz zu, wobei ein Web- oder Web-Application-Server zur Vermittlung genutzt wird. Sicherheitsbetrachtungen müssen deshalb die gesamte Kommunikationskette vom Client bis zum Backend-Server betrachten. Neben Realisierungserfahrungen sollen grundsätzliche Probleme bei Authentisierung und Verschlüsselung aufgezeigt werden.

Einsatz von PKI-Lösungen

Beim Aufbau von sicheren Web-Applikationen, aber auch beim alleinigen Einsatz im internen Unternehmensbereich taucht immer häufiger der Begriff PKI (Public Key Infrastructure) auf. Neben der fachlichen Aufbereitung dieses Themas sollen besonders Praxiserfahrungen bei Implementierungen vermittelt werden. Für wen lohnt sich heute bereits das Thema PKI? Was kostet es? Ist der Aufbau einer eigenen CA sinnvoll? Was bieten Firmen wie VeriSign oder Entrust?

Secure Remote Access

Remote Access Möglichkeiten wird heute wohl fast jedes Unternehmen bieten. Eigene Mitarbeiter, aber auch Fremde wie Servicetechniker oder Entwickler bekommen, zumeist nur schwach gesichert, Zugang zum internen Netz. Durch attraktive Konditionen (xDSL) wird zunehmend auch der RA-Zugang über Internet attraktiver. Fragen die dabei zu beantworten sind: Welche Sicherheitsmaßnahmen sind im Grenzbereich, zur Authentisierung und zur Verschlüsselung einzusetzen? Welche Probleme gibt es beim Aufbau von VPN-Lösungen? Wie kann man eine effiziente Nutzerverwaltung aufbauen?

Perimetersicherung

Netzübergänge aller Machart stellen immer potentielle Schwachpunkte dar und müssen deshalb besonders gut gesichert werden. Die für eine Schutzzone typischen Zugangskomponenten wie Firewall, Router, RAS-Server sollen in ihrer Funktion ebenso dargestellt werden wie der Einsatz zusätzlicher Kontrollmöglichkeiten durch Proxies, Content-Scanner oder Intrusion-Detection-Systeme.

Security Outsourcing
(Bereiche, Verträge, SLA,...)

Viele bekannte Hersteller von Sicherheitsprodukten und -Lösungen wenden sich einem neuen Feld zu: den Security-Services. Vom Online-Support über die Alarmzentrale bis hin zum vollständigen Outsourcing des Security-Managements wird fast alles angeboten. Welche Vor- und Nachteile gibt es? Was ist unbedingt bei Vertragsabschluss zu beachten?

Neben diesen Schwerpunkten sind weitere Beiträge zu folgenden Themen geplant:

Secure E-Mail

Technische und organisatorische Anforderungen an die Sicherung von E-Mail im geschäftlichen Umfeld.

Windows 2000

Vorstellung der Sicherheitsmaßnahmen bei Windows-2000 und erste Erfahrungen.

Betriebsaspekte

Von der Security-Policy bis zur realen Lösung: Wie geht man am besten vor?

Security Management Lösungen

Die Sicherheitsmaßnahmen werden immer umfangreicher, die Verwaltungstools halten damit leider nicht Schritt. Wie ist der Stand im Security-Management?

Rechtliche Aspekte und Datenschutz

Nicht nur die technische Seite muss beherrscht werden, Fragen zu rechtlichen Folgen von Sicherheitsmaßnahmen und -verletzungen werden immer wichtiger.

Hackerszene, DDoS, Spying Trojans, ...

Was gibt es Neues aus der Szene?

In mehreren parallel angebotenen Workshops werden darüber hinaus Betriebsthemen vertieft, aber auch Produktvergleiche nach festgelegtem Präsentations-muster zusammen mit unterschiedlichen Herstellern durchgeführt.

Dieses Security-Event, geleitet von dem Sicherheits-Experten Dipl-Inform. Detlef Weidenhammer, bietet den Teilnehmern wie in jedem Jahr eine vollendete Mischung aus Erfahrungsberichten, Fachvorträgen und Produktempfehlungen.

Da auch in diesem Jahr die Mehrzahl der Teilnahmeplätze schon in der Frühbucherphase vergeben worden sind, wird jedem Interessenten jetzt eine rasche Anmeldung empfohlen, um sich seinen Platz auf diesem Kongress zu sichern.

Netzwerk Sicherheits-Forum 2001

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk Sicherheits-Forum 2001

☐ Ich melde mich an für den Kongress **Netzwerk Sicherheits-Forum 2001** vom 07.05.-09.05.01 in Königswinter zum Preis von EUR 1.590,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Hotel, Königswinter (Übernachtung/Frühstück DM 211,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

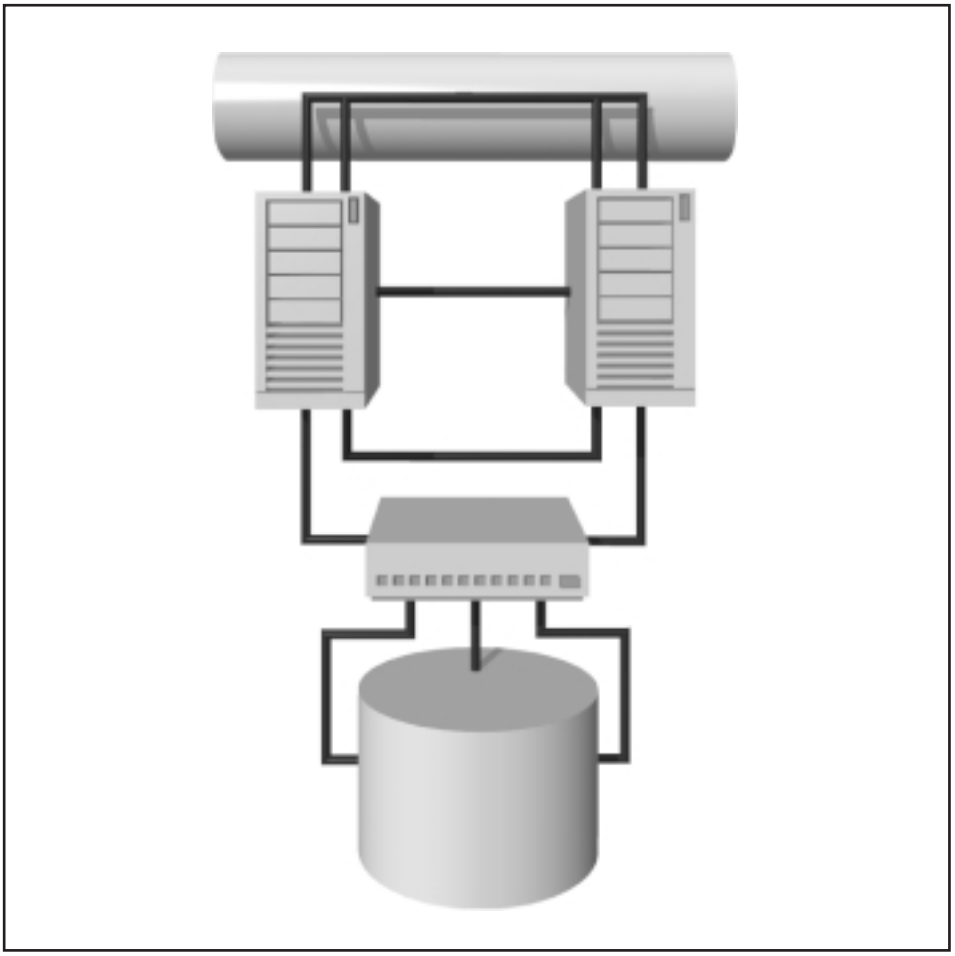
Neues Seminar

Optimale Netzwerk-Anbindung hochverfügbarer Windows-Serverfarmen

Am 7. und 8. Mai 2001 veranstaltet die ComConsult Akademie im Maritim Hotel Königswinter zum ersten Mal ihr neues Seminar "Optimale Netzwerkanbindung hochverfügbarer Windows-Serverfarmen" für Planer, Betreiber und Anwender von hochverfügbaren Rechenzentren und deren Netzanbindungen.

Zum Thema

Windows-Server-Systeme werden zunehmend für Anwendungen mit höheren Verfügbarkeits-Erwartungen eingesetzt. Gleichzeitig besteht für viele Betreiber die Zielsetzung, die Benutzer-Zahlen pro Server drastisch zu erhöhen und damit die Zahl der eingesetzten Server zu senken. Tatsache ist, dass einerseits die Microsoft-Betriebssysteme Windows NT und Windows 2000 eine zum Teil dominierende Präsenz in den Rechenzentren der meisten Firmen behaupten und andererseits immer wichtigere Arbeitsprozesse von der Verfügbarkeit dieser Serversysteme abhängig gemacht werden. Die optimale Anbindung der Server an Lokale Netzwerke ist dabei einer der entscheidenden Faktoren zurErreichung einer hohen Verfügbarkeit, niedriger Betriebskosten und hoher Benutzerzahlen.



Das Seminar behandelt eine Reihe sehr ernst zu nehmender Fragen, die wesentlich die Qualität der Netzwerk-Anbindung beeinflussen, diskutiert die bestehenden Alternativen, beschreibt die Vor- und Nachteile und gibt Empfehlungen aus der Sicht derPraxis.

Die Teilnehmer lernen in diesem Seminar, wie Windows Server Cluster aufgebaut werden und wie die Netzanbindung aussehen sollte, ob eine Layer-2- oder Layer-3-Anbindung zu bevorzugen ist, wie die Redundanzmechanismen funktionieren und welche DNS-Strukturen bei der Anbindung von Servern aufgebaut werden müssen, wie der Windows Load Balancing Service funktioniert und was davon zu halten ist. Und sie lernen, wie Storage Area Networks aufgebaut werden.

Die Referenten diese Seminars haben einen betont praxisorientierten Background und können aufgrund ihrer Projekterfahrung wertvolle Tipps und Erfahrungswerte vermitteln.

Dipl.-Ing./MCSE Kambiz Alikhah betreut bei der ComConsult Beratung und Planung u.a. Kunden beim Aufbau von hochverfügbaren Server-Farmen und deren Migration in modernen Netztopologien.

Markus Holländer (MCSD) ist Kompetenz Center Leiter Backoffice bei der ComConsult Beratung und Planung und besitzt langjährige Projekterfahrung im Design und im Betrieb von Windows NT und Windows 2000, sowie weiterer BackOffice Produkte. Er hat zahlreiche Projekte privater und öffentlicher Auftraggeber in diesem Umfeld erfolgreich geleitet.

Dipl.-Inform. Michael van Laak hat bei der ComConsult Beratung und Planung als Berater im Kompetenz Center Backoffice seinen hauptsächlichen Einsatzbereich in der Konzipierung und Umsetzung von Migrationsprojekten auf Windows NT 4 und Windows 2000. Seine Schwerpunkte sind Domänen-, IP-Management- und (Fern-) Administrationskonzepte.

Dipl.-Ing. Frank Krauthausen ist bei der ComConsult Beratung und Planung GmbH im Backoffice Kompetenz Center als Berater für die Konzipierung von Netzwerkbetriebssystemen und den Einsatz von Produkten aus der BackOffice-Familie beschäftigt. Seine Kenntnisse hat er in der Projektarbeit und der Migration von Netzwerken bei Kunden erworben.

Optimale Netzwerkanbindung hochverfügbarer Windows-Serverfarmen

Optimale Netzwerkanbindung hochverfügbarer Windows-Serverfarmen

Inhaltlicher Aufbau

Hochverfügbarkeit von Serversystemen - Allgemeine Definition
• Verfügbarkeitsstufen (VS) •Redundanzen • RAID-Systeme • Cluster • Loadbalancing

Netzanbindung hochverfügbarer Serversysteme
• Layer-2 vs. Layer-3-Anbindung • Redundanzmechanismen

Namensauflösung bei der Anbindung hochverfügbarer Systeme
(mit Betonung auf DNS-Strukturen)

Detaillierte Beschreibung von Clusterlösungen
• Welche Clusterkonfigurationen gibt es? (Aktiv/Passiv, Aktiv/Aktiv, shared, non shared ...) • Produkte am Clustermarkt - Beispiele für die einzelnen Konfigurationen

Windows 2000 Cluster
• Aufbau • Hardware• Konfiguration

SAN (Storage Area Network)
• Herleitung (Gründe für den Einsatz) • Aufbau • Technik • Backuplösungen im SAN

Der Veranstalter behält sich Änderungen im Programm vor.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Optimale Netzwerk-Anbindung hochverfügbarer Windows-Serverfarmen

☐ Ich melde mich an für das Seminar **Optimale Netzwerkanbindung hochverfügbarer Windows-Serverfarmen** vom 07.05.-08.05.01 in Königswinter zum Preis vo n EUR 1.290,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Hotel, Königswinter (Übernachtung/Frühstück DM 211,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Ethernet Everywhere

Fortsetzung von Seite 1

Es gibt heute zwei wesentliche Bereiche, in denen die Diskussion über Ethernet noch zu führen ist:

- Ethernet im WAN und Access-Bereich
- Ethernet in der "First Mile", die ja hier auch als "letzte Meile" bezeichnet wird

10 Gigabit Ethernet wird ein Konvergenzstandard für den ersten Problemkreis. Aber auch hinsichtlich der Ethernet First Mile EFM haben sich die Interessenten mit dem Ziel der Gründung einer entsprechenden Standardisierungsgruppe getroffen.

Über die Bedeutung und Ausführung des 10 GbE Standards habe ich bereits ausführlich geschrieben, so dass wir hier nur den neuesten Stand rekapitulieren müssen. EFM ist allerdings wirklich Zündstoff, denn meiner Ansicht nach gibt es auch in jedem Unternehmen große Bereiche, die eher nach einer Art haushaltsmäßiger Versorgung rufen als nach der individuellen Versorgung, wie man sie heute betreibt. Ein Erfolg dieser Initiative würde die Preise für Komponenten durch dramatische Erhöhung von Stückzahlen noch weiter in den Keller treiben. Viel verlockender erscheint aber die Aussicht auf systematische, genormte Steuerungsmechanismen, wie sie Carrier benötigen, um die Versorgung von Haushalten kontrollieren zu können.

10 Gigabit Ethernet

Im November 2000 und im Januar 2001 gab es weitere Treffen der Standardisierungsgruppe, die allerdings nicht viel verwertbare Neuigkeiten hervorgebracht haben. Seit den Abstimmungen beim Treffen Ende September 2000 in San Diego sind von den vielen Vorschlägen für die PMD folgende Varianten übrig gelieben:

10GBASE-LX 1550

Serielle Übertragung von 10 Gbps, woraus allerdings durch Codierung auf der Leitung 12,5 Gbps werden, auf 9 oder 10 Micron Singlemode-Fasern bis zu 40 km ohne Zwischenverstärker. Dies ist die hochqualitative Variante für den Einsatz in MANs oder beim WAN Access.

10GBASE-LX 1310

Auch hier hat sich die serielle Übertragung durchsetzen können, allerdings mit etwas

Der Autor

Dr. Franz-Joachim Kauffels ist einer der bekanntesten und erfahrensten Referenten der Netzwerkszene. Bekannt geworden durch vielfältige Publikationen, Seminare und Kongresse setzt sich der selbständige Unternehmensberater für eine fortschrittliche und wirtschaftliche Nutzung der neuen Technologien ein.

geringeren Leistungseckdaten. Auf 9 oder 10 Micron Singlemode-Fasern kommt man bis zu 10 km weit, auf neuentwickelten Multimodefasern wie z.B. Lucent LazrSpeed rechnet man mit ca. 300 m Übertragungsdistanz. Verschiedene Papiere bei den letzten Sitzungen befassen sich mit dem Einsatz von 1310 nm VCSELs.

Diese Vertikalemitterdioden könnten den Preis für diese Variante erheblich senken. Allerdings würde man dazu einen neuen Durchbruch in der Forschung benötigen, mit dem eher nicht zu rechnen ist. 10 GBASE-LX 1310 ist der Favorit für organisationseigene Backbones.

10GBASE-SX4 850CWDM

Diese Variante ist mein persönlicher Favorit. Die kurzwellige kompakte Technologie mit Wellenlängenmultiplex, bei der vier 2,5 Gbps Kanäle für die gewünschte Übertragungsrate sorgen, lässt die Verwendung preiswerter Komponenten, besonders VSCELs, zu. Die ursprünglich im Standard verfolgten Distanzziele werden überschritten:

100 m auf installierter 62,5 Mikron Multimode Faser mit 160 MHz*km

300 m auf 50 Mikron Multimode Faser mit 500 MHz*km

500 m auf 50 Mikron Multimode Faser mit 1000 MHz*km

Damit ist 10GBASE-SX4 850CWDM die günstigste Variante für "worst case FDDI cabling", der aus der Perspektive des Standardisierungsgremiums schlechtmöglichsten bestehenden Verkabelung. Multiplexer und Demultiplexer können als passive PHASARe in preiswerter Kunstoff-Spritzguss Optik ausgeführt werden. Mit den VCSELs entsteht dadurch eine sehr preiswerte, stromsparende Bauart.

Man darf aber auch nicht vergessen, daß CWDM-Systeme optisch skalierbar sind, weil sie in einem weiten Bereich von der Modulationsrate unabhängig sind. Momentan benutzt man VSCELs mit 2,5 Gbps "Datenrate", noch in diesem Jahr kommen aber 5 Gbps-VSCELs an den Markt und der nächste Schritt sind 10 Gbps VCSELs. Erhöht man die Kanaldirchte dann von heute vier auf z.B. 10 Kanäle, kommt man z.B. zum 100 Gigabit Ethernet.

10 GBASE-SX4 850 CWDM Komponenten sind nach Aussagen der Hersteller mit Serienqualität im ersten Quartal 2001 verfügbar.

Abgewählt wurden folgende Varianten: 1310nm WWDM (schlechter als 850 nm CWDM), 850nm seriell (wesentlich schlechter und teurer als 850 CWDM) und parallele Fiber (technologischer Unfug).

Momentan bilden sich bei den Herstellern zwei Fronten. Eine Gruppe favorisiert die seriellen Lösungen auch aus Kostengründen. Infineon Technologies, einer der weltweit führenden Anbieter vom 10 Gbps Transceivern und auch Kreator des z.Zt. kleinsten 10 Gbps Transceivers rechnet vor, ab welchen Stückzahlen serielle 10 GbE Module genauso günstig wie CWDM-Module hergestellt werden können. Dagegen stehen Firmen wie BLAZE Technologies, die erhebliche Kostenvorteile bei CWDM sehen. Ich persönlich favorisiere für den LAN-Bereich CWDM, alleine wegen der besseren Anpassbarkeit an Multimodefasern. Wer allerdings ohnehin nur Monomodefasern hat, kann sich der seriellen Fraktion anschließen.

Sobald sich wirklich etwas Neues bei IEEE 802.3 ae tut, werde ich es in diesem Medium sofort aufgreifen.

Ethernet Everywhere

Anfang Januar 2001 tagte zum ersten Male eine neu gebildete IEEE 802.3 Arbeitsgruppe zum Thema "EFM" Ethernet First Mile. Wenn wir davon ausgehen, dass die optischen Netze eine neue Leistungs-Dimension in der WAN-Technik erschließen und dabei via des 10 GbEthernet Standards auch hier das Ethernet Päckchen das Maß aller Dinge ist, ist es nur logisch, darüber nachzudenken, wie man dies sinnvoll zum Endteilnehmer durchschleifen kann.

Es ist sehr zu begrüßen, dass sich die Arbeitsgruppe in einem Stadium konstituiert hat, in dem es noch nicht "zu spät" ist, entsprechende Entwicklungen zu koordinieren. Es ist jedem klar, dass ATM in Zukunft auch für die Versorgung von Endteilnehmerschleifen keine Alternative mehr sein kann, dass aber auch Lösungen wie die xDSL-Technik früher oder später deutlich an ihre Grenzen stoßen werden. Es geht jetzt darum, die Netze der nächsten Jahre mit entsprechenden Standards vorzubereiten.

Das Marktpotential ist gewaltig. US und Europäische Telcos und Kabelbetreiber sind an einem Standard interessiert. Für den Heimmarkt ergeben sich über 200 Millionen Haushalte, allerdings können mit dem gleichen Ansatz auch Unmengen kleinerer und mittlerer Büros bedient werden. IEEE 802.3 hat natürlich Interesse daran, Switched Ethernet als DEN Standard für den Aufbau von heimischen Netzumgebungen zu forcieren.

Direkt beim ersten Treffen waren außerordentlich viele wirklich maßgebliche Hersteller wie Nokia, ADC, Lucent, Picolight, Alloptic, 3Com, Nortel, Extreme und Cisco anwesend. Ausgangsszenario ist das Multiservice Operator Network z.B. eines value-addenden Telco Providers, der neben der Basisleistung entweder selbst Mehrwerte anbietet oder dies Dritten ermöglicht und für die technische Realisierung sorgen muss. Dienstleistungen in einem typischen Multiservice-Operator-Netzwerk sind:

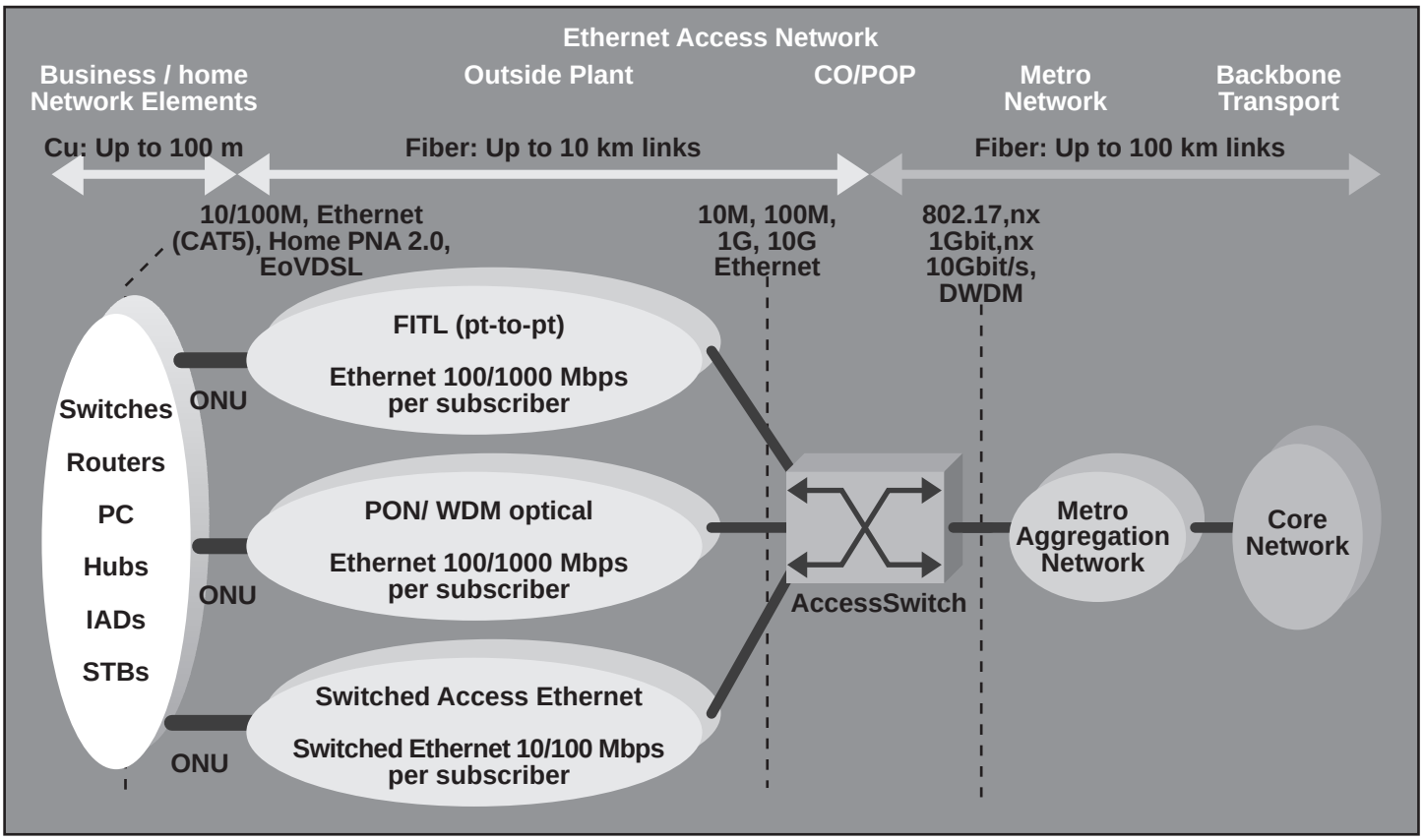
- paketisierte Sprache
- geswitchtes Digital-Video: Broadcast, Pay per View, VOD, Videotelefonie, HDTV
- Daten: Internet Access, VPNs, ...

An das Zugriffsnetz der Endteilnehmer werden dann folgende Anforderungen gestellt:

- Bandbreite 100 Mbps oder 1 Gbps per Haushalt, 10 Mbps oder weniger sind nicht ausreichend um in der Qualität mit CATV vergleichbare Video-Dienstleistungen anbieten zu können, vor allem vor dem Hintergrund mehrerer zu unterstützender Endgeräte in einem Haushalt
- Alle Dienstleistungen über IP (über Ethernet) mit einer IP Kontrollebene
- Genügend QoS-Verfahren, um die Dienstleistungen, geringe Verzögerung, Dienstleistungen mit geringen Verlusten zu gewährleisten, wobei allerdings IP DiffServ mit Zugriffskontrollen ausreichend erscheint
- Passive Komponenten werden bevorzugt (Ethernet Passive Optical Network EPON)
- Bestehende Telefonleitungen und CATV-Coax sollten nach Möglichkeit ebenfalls benutzt werden können.

Der Sichtbereich des Standards wird aus Bild 1 deutlich.

Bild 1



Ethernet Everywhere

Hauseigene Kupfernetze gehören üblicherweise dem Hauseigentümer. Neue Häuser werden normalerweise mit strukturierten Verkabelungssystemen der CAT 5 ausgestattet.

Ältere Häuser haben CATV-Kabel für die Verteilung analoger Fernsehsignale oder sogar nur Telefonleitungen. Über den Standard HomePNA 2.0 (PNA = Physical Network Access) können diese Telefonleitungen auch für die Datenübertragung genutzt werden. Das Problem mit HomePNA ist es, dass sich verschiedene Geräte die ohnehin geringe Datenrate von 10 Mbps auch noch teilen müssen.

Eine andere Möglichkeit wäre die Nutzung von VDSL.

Betrachtet man aber die physikalischen Randbedingungen näher, erscheint auch eine Standardisierung für die Auslieferung von Ethernet-Paketen über CATV erfolgversprechend für eine einigermaßen dauerhafte Übergangslösung.

Eine solche Spezifikation sollte folgende Eigenschaften haben:

- Unterstützung von mindestens 100 Mbps Datenrate
- Unterstützung von Distanzen von mindestens 100 m
- Bidirektionale Übertragung
- 4-8 Endgeräte
- 4-8 Serviceklassen
- Bandbreitezuordnung via Gerät und Klasse
- Braucht allerdings dann nicht noch die parallele Übertragung analoger Videosignale

Grundsätzlich ist die Verwendung von Kupfer nur mehr ein politischer Kompromiss und es gibt eine Reihe von Gründen, in den nächsten Jahren die Optische Übertragungstechnik bis zum Endkunden durchzuleiten. Bereits im Zusammenhang mit ATM hat es Überlegungen gegeben, passive Optische Netze, die ATM-PONs oder kurz APONs zu implementieren. Die Verwendung von ATM bedeutet jedoch die unsinnige und unnütze Notwendigkeit, Pakete zu shreddern und wieder zusammenzusetzen, fügt mindestens 20% Overhead hinzu und ist insgesamt nur für Anwendungen bis hin zu mittleren Geschwindigkeitsbereichen zu nutzen.

Generell muss man sich bei einem PON überlegen, dass es nicht wirklich eine skalierbare Architektur bietet. Ein PON besteht letztlich aus einem Link zu einem größeren Netzwerk, einem passiven Verteiler und Leitungen zu den Endknoten. Der Link muss in jedem Fall mehr als 1 Gbps können, denn wenn man z.B. 32 Endteilnehmer mit einem PON bedient, dann kämen bei einem Gbps ja nur ca. 30 Mbps beim Endteilnehmer an, dafür könnte man gleich VDSL nehmen. Allerdings, welchen Wert man auch immer nimmt, einen größeren Technologieschritt macht das PON nicht ohne größere Änderungen in der Struktur mit. Die Fiber Optic selbst ist dabei nicht so sehr ein Problem wie die Verlegung.

Diesen Bedenkenbereichen stehen allerdings auch eine große Zahl von Vorteilen gegenüber. PONs reduzieren wegen ihres Konzentrator-Charakters die Anzahl der Leitungen in den Links. Man benötigt keine aktiven Komponenten beim Kunden, anders als bei VDSL und man benötigt keinerlei Stromversorgung. Hinsichtlich der Kapazität sind PONs eher den flexiblen Architekturen zuzuordnen. Der Standard G.983 für APONs ist verfügbar und wäre auch für das Ethernet Protokoll Profil nutzbar. Allerdings ist er über 10 Jahre alt und müsste ohnehin renoviert werden.

PONs, VDSL- und CATV-Netze liegen nicht so weit auseinander, dass es völlig unmöglich wäre, für sie eine gemeinsame MAC-Layer zu schaffen. Insgesamt geht man aber davon aus, dass die Kupferinfrastruktur an Boden gegenüber der Fiber Optic verliert.

Die natürliche Erweiterung eines Glasfasernetzes ist die Einbeziehung von Wellenlängenmultiplex WDM. Das geht natürlich auch bei PONs. WDM-PON Access würde bedeuten, dass man z.B. jedem Haushalt eine Wellenlänge zuordnet. Das ist ideal vom Standpunkt der Skalierbarkeit hinsichtlich der Kapazität. Man kann Geräte gezielt mit Dienstleistungen versorgen und dabei auch hohen Sicherheitsanforderungen genügen, weil ja nicht alle Endgeräte die gleichen Wellenlängen empfangen können müssen. Außerdem kann die Bandbreite pro Wellenlänge noch dadurch modifiziert/erweitert werden, dass das Equipment des Subscribers mehr oder weniger kann. Allerdings ist das noch etwas fernere Zukunftsmusik, denn es würde voraussetzen, dass Endteilnehmer billige durchstimmbare Netzwerkabschlussgeräte bekämen oder man mit festen Filtern arbeiten kann. Außerdem ist zu befürchten, dass passive WDM-Systeme recht anfällig gegen Temperaturschwankungen sind.

Zusammenfassend hat die IEEE Arbeitsgruppe folgende Grobziele ins Auge gefasst:

- Definition eines Standards für Fiber-To-The Home FTTH und andere Nutzer
- Benutzung der einfachsten Protokolle, die Flexibilität und schnelle Upgrades berücksichtigen
- Möglichst einfaches CPE Equipment (Customer Premises Environment)
- Möglichkeit, mit existierender Technologie zu beginnen
- Einbeziehung von Kupfervarianten
- Einbeziehung möglichst vieler Anbieter (Telcos, CATV, ...)
- Möglichkeit der Einbeziehung normalen Telefonverkehrs
- Standardisierung der Erweiterungsmethode
- Garantierte Bandbreite mit hochverfügbarem Service für den Endnutzer
- Symmetrische, skalierbare und leicht änderbare Bandbreite
- Für den Betreiber: leichte Verwaltbarkeit (Abrechnungsmöglichkeit, flexible Subnetzgranularität, Kontrolle und Feedback über Latenz, Statistik und Security)
- Möglichkeiten zur schnellen Fehlerisolation
- Schnelle und flexible Konfiguration

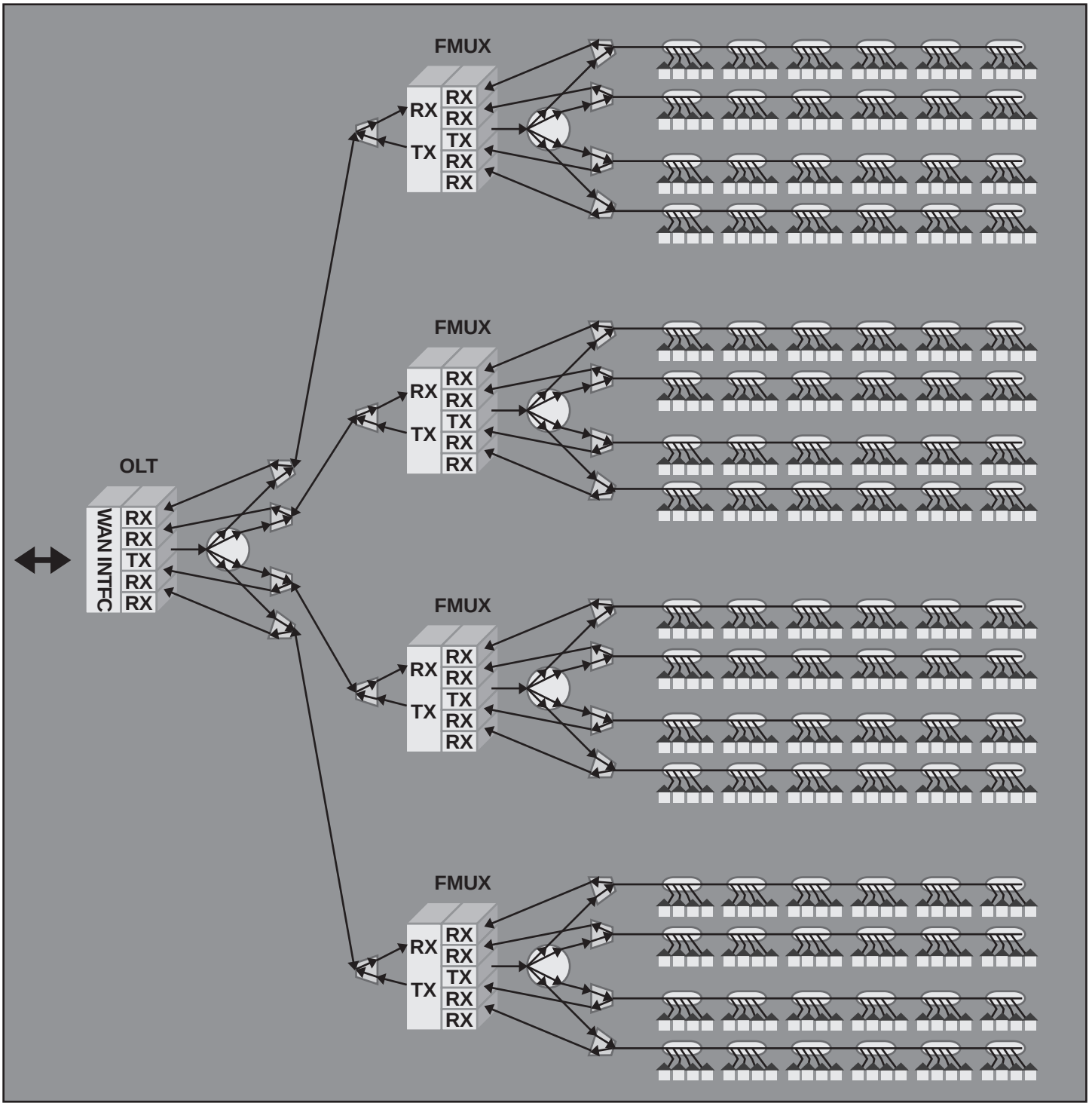
Für das zu entwickelnde Protokoll hat IEEE 802.3 EFM folgende Ziele:

- Kein Transport von Kontrollinformation via der codierten Ethernet-Pakete, was bedeutet: weniger SNMP Agenten als Subscriber, weil das Headend Equipment der SNMP Agent für das angeschlossene Feldequipment ist, das CPE benötigt weder MAC- noch IP Adresse und erhöhte Sicherheit und Robustheit
- Das Protokollschema muss einfach sein, aber mit mehr Sicherheit als die, die durch VLAN Tags gewährleistet wird
- QoS wird über die Bandbreite realisiert: die totale Bandbreite, die den Endkunden zugesagt wird, überschreitet nicht die Möglichkeiten der WAN Infrastruktur

- Protokollunabhängiger Transport der Ethernet Pakete
- Vollständige vorwärtsgerichtete Wegbestimmung an den Headends
- Garantierte Minimalbandbreite von 10 oder 100 Mbps
- Integration der 64 kbps Telefonie
- CPE muss aus generischen Plug In Komponenten bestehen können
- Das Headend muss Gigabit Ethernet, 10 Gigabit Ethernet und SONET unterstützen
- EFM Transport ist transparent für 802.3 Features wie IEEE Standard VLANS, Spanning Tree, Link Aggregation Control Protocol

Bild 2 zeigt, wie man z.B. 384 Häuser mit einem ordentlichen optischen Link Transceiver, vier Multiplexern und 4-fachen TAP-Ketten versorgen könnte.

Bild 2



Ethernet Everywhere

Insgesamt konzentriert sich die Diskussion momentan stark auf die EPONs. (Ethernet Passive Optical Network). Ein EPON hat eine Punkt-zu-Vielpunkt-Struktur und kann für Fiber to the Building, Home, Office usf. benutzt werden. Dynamisch skalierbare Bandbreite hilft bei der systematischen Versorgung der ONUs, der Optical Network Units. Im Bild 3 sehen wir nochmals vereinfacht die Grundstruktur, die Voice, Daten- und Video-Dienste anbietet. Ein Switchrouter stellt die Schnittstelle zum Metropolitan Area Network Equipment dar. Passive optische Splitter ersparen aktive Elektronik in der lokalen Schleife. Normalerweise hat man heute bis zu 32 ONUs hinter einem Splitter und benutzt eine Lichtwellenlänge von 1550 bzw. 1510 nm für den Downstream und 1310 nm für den Upstream, wenn man nur mit einer Faser arbeitet. Man sieht natürlich sofort, dass dann für den Upstream ein Synchronisationsprotokoll fällig wird, weil ja hier verschiedene Nachrichtenwege in einem Punkt zusammenlaufen. Dies widerspricht natürlich schon den o.g. Zielen, wo ja z.B. eine symmetrische Kommunikation vorgesehen wird. Allerdings kann man darüber lange streiten: für die Services bei normalen Endkunden dient der Rückkanal nur dem Auswählen und Bezahlen oder sonstigen Kontrollfunktionen wie Browsen, braucht also eine wirklich wesentlich geringere Bandbreite. Hier nur wegen der Symmetrie mit erheblich erhöhtem Aufwand zu arbeiten, lohnt sicher vielfach nicht.

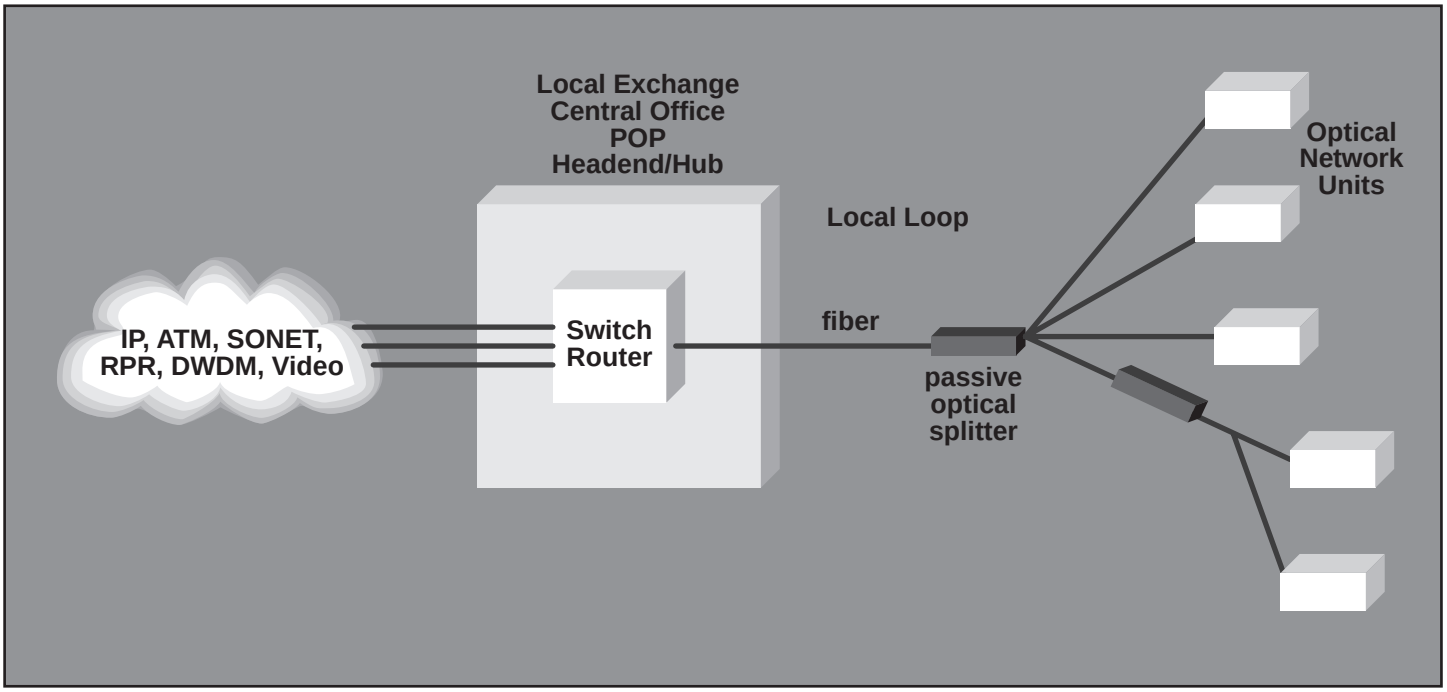
Verschiedene Hersteller, wie die Firma Alloptic, haben schon entsprechende Verfahren vorgestellt, an dieser Stelle sei daran erinnert, dass Ethernet ja einmal ein Netz mit Wettbewerbsverfahren war und es außer CSMA/CD immerhin noch ca. 4000 andere Algorithmen gibt, mit denen man eine solchen Mehrfachzugriffssteuerung realisieren könnte. CSMA/CD selbst kommt wohl nicht in Frage, weil man eine Bandbreitegarantie für den Rückkanal haben muss.

Einer der wesentlichen Nachteile von ADSL oder VDSL ist die extreme Abhängigkeit der realisierbaren Bandbreite von der Leitungslänge. Erzielt man über 300 m mit VDSL ohne weiteres 50 Mbps, so fällt dies mit ADSL über 6.000 m auf 1,5 Mbps ab. Hersteller sprechen davon, in den interessanten Bereichen zwischen 2 und 6 km mit vollständig passiver, preiswerter Technologie Datenraten im Gbps-Bereich realisieren zu können. Die optischen Modems auf der Seite der Teilnehmer werden dabei aber nicht dumm sein müssen, sondern können Funktionen wie Firewalling, Routing, Switching und dynamische Bandbreitezuordnung beinhalten.

Über die Integration von Kupfertechnik indes gibt es ganz unterschiedliche Vorstellungen. Viele Hersteller denken daran, wie beschrieben einen Standard für EFM zu formulieren, der auf Koax, Cat. 5 und Optik gleich gutartig funktioniert. Das ist aber irgendwie auch unstimmig wegen der enormen Leistungsunterschiede der Technologien. Viel besser gefällt mir die Idee, einen EPON-Standard zu definieren, der die alte Verkabelung ganz ans Ende setzt. Ein Optisches Modem ist sozusagen der Eingang zur bestehenden Hausverkabelung, siehe Bild 4. Dieser Ansatz würde es ermöglichen, ein Carrier Netz ganz in optischer Technologie auszuführen und gleichzeitig die Investitionen in bestehende Verkabelungen zu retten. Hausbesitzer sind in diesem Punkt sicherlich eine wesentlich schwierigere Klientel als z.B. Industriekunden und werden es gar nicht einsehen, die irgendwann einmal teure Infrastruktur, grade bei größeren Mietshäusern, gegen irgendwelche ominösen Glasfasern einzutauschen, nur weil diese jetzt angeblich modern seien. Der Autor ist selbst Limited Partner bei US-Immobilienfonds und kennt die Diskussionen um solche Punkte. Aus dieser Erfahrung kann man es als absolut undurchführbar ansehen, Kunden zwangsweise ältere Verkabelungen stillzulegen und durch Inhouse-Glasfasern zu ersetzen.

Insgesamt taucht auch mehrfach der Vorschlag auf, völlig unabhängig von der Verwendung von EPONs zunächst einmal Ethernet auf VDSL zu definieren, um ein klares Signal gegen ATM zu setzen. Von Extreme Networks kam der berechtigte Einwand, dass eine Konzentration auf eine Ethernet-TECHNOLOGIE für die First Mile falsch sei, man solle sich stärker darauf be-

Bild 3



Ethernet Everywhere

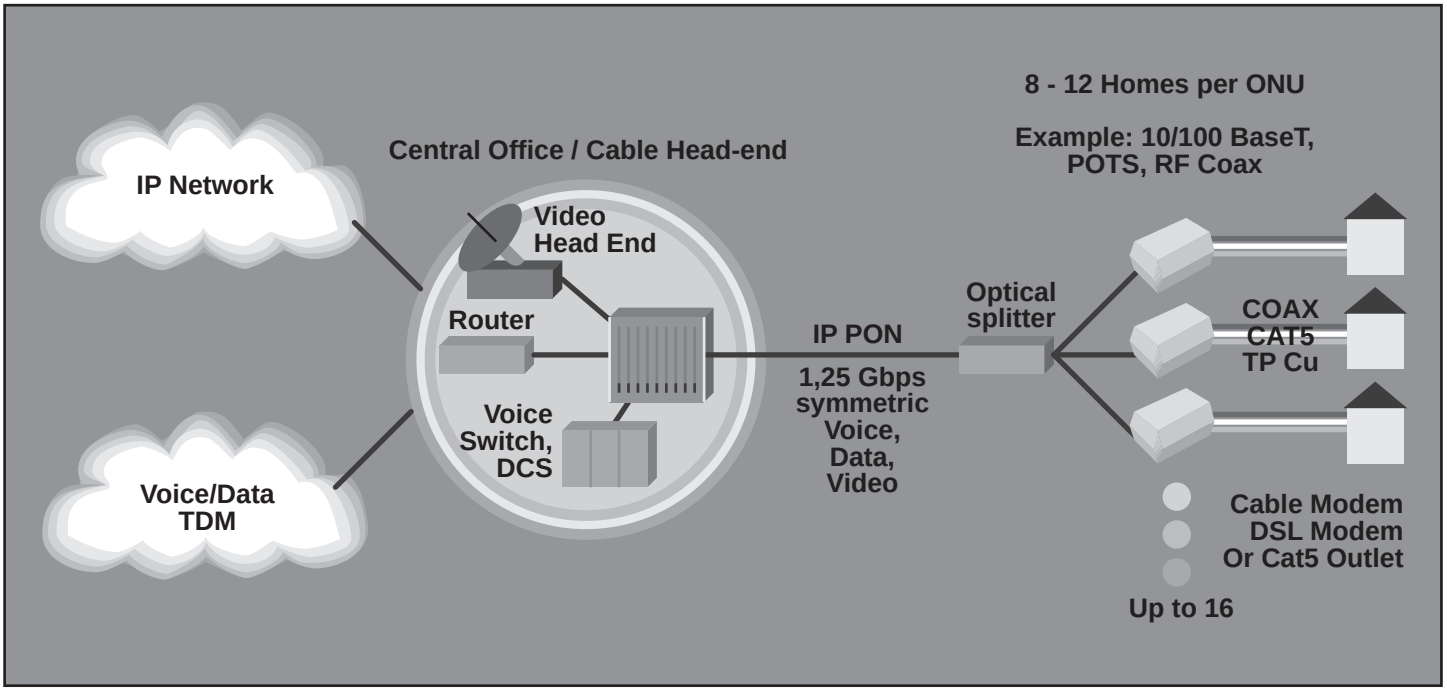


Bild 4

sinnen, Ethernet-SERVICES zu liefern, und dies über einen weiten Bereich von Technologien. Wenn man an den Endpunkten des Netzes verbindungslosen Datentransfer im Ethernet Paket Format implementieren möchte, kann das Netz aus Circuit Switches, Zellen, Ringen oder sonst was bestehen. So könne man die Front der ATM-orientierten Carrier am ehesten aufbrechen. Wesentlich sei es, die betrieblichen Vorteile von Ethernet herauszuarbeiten, was Monitoring, Betrieb und Management betrifft und sich als Standardisierungsgremium vor allem auf die Dinge konzentrieren, die den Betreibern, also den kleinen und großen Carriern eine Nutzung der Fortschritte in der Technologie bei gleichzeitiger Reduktion des täglichen Aufwandes ermöglichen könnte. Dazu müsse man die physikalischen Randbedingungen der EFM von den Anforderungen eines Netzwerkmodells mit Provider und Abonnent trennen. Dazu gehöre unzweifelhaft die Definition neuer technischer Übertragungswege unterhalb der Ethernet MAC. Andererseits müsse die Hinzufügung neuer Qualitäten dezent geschehen, um nicht das einfache und klare Gesamtbild "Ethernet" zu verwässern. Cisco Systems hatte dem noch hinzuzufügen, dass der Markt für EFM aus besonders qualifizierten Kunden bestehe, die sich letztlich nur von massiven, nachweisbaren Vorteilen beeindrucken ließen. Zu diesen gehöre ein "Versorgungsmodell vom AOL-Typ", welches Kunden durch besonders billige Bandbreite locken könne.

Interessant sind auch die Einlassungen von Kundenseite. BT (British Telecom) hat bereits 50% der Haushalte in GB mit ADSL versorgt. Man bemerkt natürlich mit Recht, dass ein System nicht automatisch billiger oder erfolgreicher werde, weil man es Ethernet nenne. Die Erfahrungen mit DSL zeigen jedenfalls, dass dies keine besonders geeignete Methode für preiswerten Zugriff sei, und für EFM stehe der Beweis ja auch noch weit aus. Man benötigt eigentlich radikal billigere Komponenten oder eine radikal andere Infrastruktur. FTTH sei sehr teuer und kleinere Betreiber könnten das auch in näherer Zukunft gar nicht bezahlen. Der Markt für neue Gebäude sei vergleichsweise schmal. Daraus zieht man die Konsequenz, dass FTTH insgesamt nicht so schnell kommen wird. Allerdings würden Kostenstudien auch zeigen, dass die Passiven Optischen Netze, wenn sie vor der Gebäudeverkabelung enden, wie wir dies weiter oben ja schon angesprochen haben, der einzige gangbare und bezahlbare Weg für die nähere Zukunft seien. Allerdings gebe es jetzt erst einmal immense Investitionen in Kupfertechnik, besonders xDSL, und ein nur marginaler Kostenvorteil sei kein Grund, sich davon zu verabschieden. Die Standardisierungsgruppe sei gut beraten, sich mit Ethernet über DSL zu befassen und ansonsten nicht nur auf die Vorgaben des US-Marktes zu starren, sondern auch die Verkabelungssituation in EMEA und ROW zu berücksichtigen und die generellen Anforderungen wie Skalierbarkeit, Zuverlässigkeit und die Möglichkeit, wirklich große Teilnehmerzahlen bedienen zu können nicht aus den Augen verlieren.

In der Frage QoS ist man sich eigentlich darüber einig, dass jedes PON eine übersichtliche Umgebung ist, bei der die benötigten Bandbreiten festliegen und eigentlich immer eine sehr hohe Versorgungsqualität gesichert werden kann. Sollten darüber hinaus dennoch weitergehende Ansprüche bestehen, werden die einfachen Verfahren wie DiffServ und RSVP im Layer 3, sowie 802.1 p und q in Layer 2 als ausreichend angesehen.

Fazit

Ethernet Everywhere ist auf dem Vormarsch. Kleinere Carrier wie z.B. TELIA in Schweden haben schon umfangreiche Betriebserfahrungen auch in der letzten Meile. EFM und xDSL-Techniken werden sich ergänzen und sind kein Widerspruch. Gleichermaßen erwarte ich von der Standardisierung eine Lösung für CATV-Systeme. Für die LAN-Anwendung hochinteressant sind aus meiner Sicht die EPONs. Hier könnte letztlich ein Weg geebnet werden, der Glasfasern zum Arbeitsplatz zu Kosten einer Kat. 5 Verkabelung möglich macht. Das bleibt ganz spannend.

Encrypting File System (EFS) unter Windows 2000 – Nicht für Gruppen geeignet?

Fortsetzung von Seite 1

Wozu Verschlüsselung?

Der Zugriff auf sensitive Daten wird üblicherweise durch restriktive Konfiguration der NTFS-Berechtigungen gesteuert. Dies ist jedoch oft unzureichend, insbesondere wenn auch Administratoren keinesfalls Einblick in die Daten erhalten dürfen. Ein weiterer Risikofaktor ist gegeben, wenn Unbefugte physikalischen Zugriff auf den Rechner mit den zu schützenden Daten erhalten. Dann ist es sofort möglich, beispielsweise mit Hilfe einer DOS-Bootdiskette und einem Tool wie NTFSDOS.SYS direkt und unter Umgehung sämtlicher NTFS-Berechtigungen auf die Daten zuzugreifen. Diese Gefahr ist natürlich besonders beim Einsatz von Notebooks gegeben.

Abhilfe kann hier durch den Einsatz von Verschlüsselung geschaffen werden. Dies implementiert eine zusätzliche Sicherheitsstufe, indem gewährleistet wird, dass selbst bei erfolgreichem Zugriff auf die verschlüsselten Daten durch Unbefugte keine verwertbaren Informationen erkennbar sind.

Ansätze

Tools zur Dateiverschlüsselung werden von verschiedensten Herstellern teilweise sehr kostengünstig angeboten. Mit Hilfe dieser Programme lassen sich Dateien unter Verwendung zumeist wählbarer Verschlüsselungsalgorithmen kodieren. Problematisch beim Einsatz von Verschlüsselung auf Applikationsebene sind oft die folgenden Unsicherheitsfaktoren:

1. Falls z.B. eine Textdatei verschlüsselt wird, ist zu beachten, dass ggf. zur Laufzeit einer Textverarbeitungssoftware erstellte Temporärdateien nicht verschlüsselt werden.

2. Oft ist der Benutzerschlüssel in der Auslagerungsdatei zu finden.

3. Die Verschlüsselungssoftware verwendet in der Regel eine eigene Passwortverwaltung, welche nicht automatisch in eine ggf. bestehende (Domain-)Policy integriert werden kann. Somit entfällt die zentrale Kontrolle über Komplexität und Änderungsintervall des verwendeten Passwortes. Erfahrungsgemäß wird der Anwender dauerhaft ein kurzes, leicht zu merkendes Passwort wählen, zumal die Authentifizierung bei der Verschlüsselungssoftware zusätzlich zum Windows-Login erfolgt.

4. Falls der Benutzer doch sein Passwort vergisst oder beispielsweise beim Ausscheiden aus der Firma versäumt, verschlüsselte Produktivdaten zu entschlüsseln, können die Daten nicht wiederhergestellt werden.

Diese Unsicherheitsfaktoren werden durch die Verwendung von EFS folgendermaßen umgangen:

1. Bei Verschlüsselung eines gesamten Ordners werden auch die temporären Kopien der verschlüsselten Dateien verschlüsselt.

2. Benutzerschlüssel werden im "nonpaged memory" abgelegt und gelangen niemals in die Auslagerungsdatei.

3. EFS arbeitet mit benutzerspezifischen Zertifikaten, so dass keine separate Authentifizierung erfolgen muss. Somit ist die Einhaltung einer ggf. implementierten Passwort-Policy gewährleistet.

4. Zu jeder verschlüsselten Datei existiert (mindestens) ein "Recovery Agent", welcher den für die Wiederherstellung notwendigen Schlüssel besitzt.

Das Encrypting File System (EFS)

Das Encrypting File System arbeitet mit dem "expanded Data Encryption Standard" (DESX) Algorithmus. Hierfür wird standardmäßig eine Schlüssellänge von 56-bit für die DES Verschlüsselung verwendet, welche allerdings laut Microsoft durch die Installation des "High Encryption Pack" auf 128-bit erweitert werden kann. Hierbei ist allerdings unklar, welcher Verschlüsselungsalgorithmus anschließend verwendet wird, zumal keine offizielle DES-Implementierung mit 128-bit existiert. Für zukünftige Versionen von EFS ist die Unterstützung weiterer Verschlüsselungsalgorithmen geplant. Die Erweiterung des DES Algorithmus auf DESX besteht in der Einführung eines zusätzlichen 64-bit Schlüssels. Dieser Schlüssel wird auf zwei 64-bit Sequenzen K1 und K2 erweitert. Diese beiden Schlüssel werden für jeweils eine XOR Operation verwendet, und zwar K1 für den Klartext und K2 für den mittels DES gewonnenen Schlüsseltext. Somit wird der DESX definiert als:

C = K2 xor DES (K3, K1 xor P),

wobei P der Klartext (Plaintext), C der Schlüsseltext (Ciphertext) und DES (K, P) die Verschlüsselung mittels DES von P unter Verwendung des Schlüssels K ist.

Bei der Verschlüsselung werden symmetrische und asymmetrische Verfahren kombiniert, indem für die Verschlüsselung der Daten ein pro Datei zufällig generierter Dateicodierschlüssel für die symmetrische Verschlüsselung mittels DESX verwendet wird, welcher daraufhin asymmetrisch sowohl mit dem öffentlichen Schlüssel des Erstellers als auch mit den öffentlichen Schlüsseln aller Recovery Agents verschlüsselt wird. Dieses kombinierte Verfahren wird sehr häufig für die Dateiverschlüsselung eingesetzt, da eine symmetrische Verschlüsselung in der Regel etwa um den Faktor 100 bis 1000 mal schneller ist als eine asymmetrische Verschlüsselung. Sämtliche auf diese Weise entstandenen verschlüsselten Versionen des Dateicodierschlüssels werden der codierten Datei vorangestellt. Jeder Benutzer, der mindestens eine Version des Dateicodierschlüssels mit seinem privaten Schlüssel entschlüsseln kann, erhält somit Zugriff auf die Datei, d.h. der Ersteller selbst sowie alle eingerichteten Recovery Agents.

Der Autor

Dipl.-Inform. Michael van Laak ist seit 1999 bei der ComConsult Beratung und Planung GmbH als Berater im Kompetenz Center Backoffice tätig.
Sein hauptsächlicher Einsatzbereich liegt in der Konzipierung und Umsetzung von Migrationsprojekten auf Windows NT 4 und Windows 2000. Schwerpunkte hierbei sind Domänen-, IP-Management- und (Fern-) Administrationskonzepte.

Encrypting File System (EFS) unter Windows 2000 – Nicht für Gruppen geeignet?

Bild 1 Verschlüsselung über den Windows Explorer aktivieren.

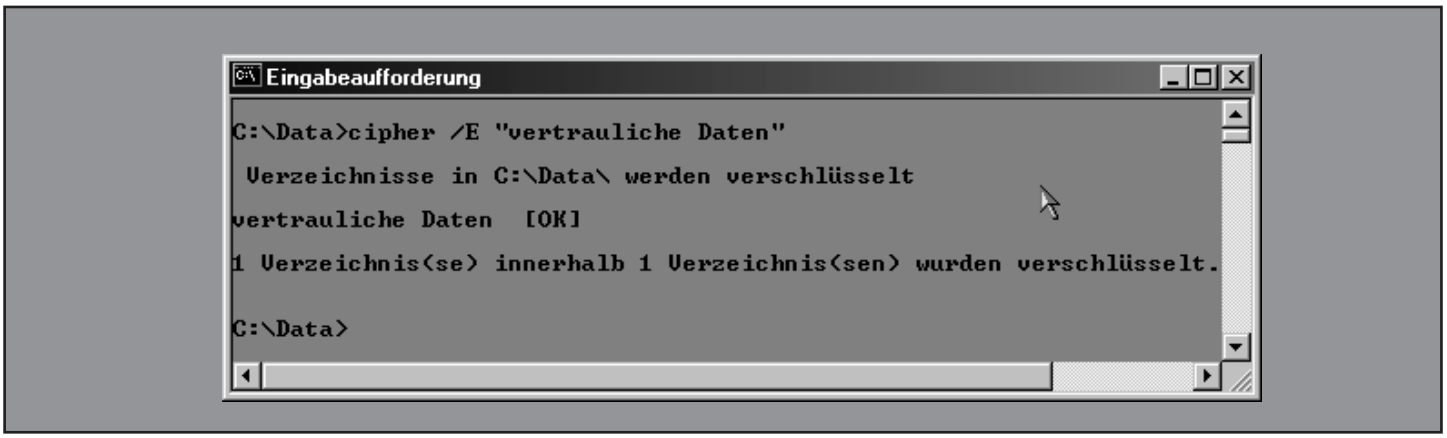
Hierbei sind folgende Bedingungen zu beachten:

- Nur Dateien auf NTFS5 Datenträgern können verschlüsselt werden.
- Systemdateien und -ordner können nicht verschlüsselt werden.
- Wenn Daten auf einem Windows 2000 Server von einem Clientrechner aus verschlüsselt werden sollen, so muss diesem Server "zu Delegierungszwecken vertraut werden" (im Verwaltungstool "Active Directory Benutzer und Computer" einstellbar).
- Komprimierte Ordner oder Dateien können nicht verschlüsselt werden.

Die Verschlüsselung kann über den Windows Explorer erfolgen, indem unter den erweiterten Eigenschaften eines Ordners oder einer Datei die Option "Inhalt verschlüsseln, um Daten zu schützen" ausgewählt wird (s. Bild 1) oder es kann alternativ das Kommandozeilentool cipher verwendet werden (s. Bild 2).

Wie der Name "Encrypting File System" (verschlüsselndes Dateisystem) schon andeutet, setzt EFS direkt auf das Dateisystem von Windows 2000 auf und ist somit in seiner Funktionalität für den Benutzer völlig transparent. Bei der erstmaligen Verwendung von EFS wird dem jeweiligen Benutzer automatisch ein EFS Zertifikat ausgestellt, welches das für die Verschlüsselung benötigte Schlüsselpaar – öffentlicher und privater Schlüssel – enthält. Das Zertifikat wird im Benutzerprofil gespeichert. Falls keine servergespeicherten Profile verwendet werden, bedeutet dies, dass der Benutzer auf verschlüsselte Dateien (lokal oder auf einem Windows 2000 Server) nur von dem Rechner aus zugreifen kann, auf welchem sich sein zum Zeitpunkt der Verschlüsselung verwendetes lokales Profil befindet. Sollte der Zugriff von verschiedenen Rechnern aus benötigt werden, ohne dass servergespeicherte Profile verwendet werden, so muss das EFS Zertifikat inklusive des privaten Schlüssels zunächst auf der primären Arbeitsstation exportiert und anschließend auf sämtlichen sekundären Arbeitsstationen wieder importiert werden.

Bild 2 Verschlüsselung über das Kommandozeilentool cipher.



Encrypting File System (EFS) unter Windows 2000 – Nicht für Gruppen geeignet?

Bei der Arbeit mit verschlüsselten Daten - insbesondere bei der Verschlüsselung von Dateien auf einem Windows 2000 Server von einer Arbeitsstation aus sollten folgende Eigenschaften von EFS berücksichtigt werden:

- Die Übertragung von verschlüsselten Daten über ein Netzwerk erfolgt unverschlüsselt.
- Beim Kopieren einer unverschlüsselten Datei in einen verschlüsselten Ordner wird die Datei ebenfalls verschlüsselt. Entsprechendes gilt auch umgekehrt.
- Beim Verschieben einer unverschlüsselten Datei in einen verschlüsselten Ordner bleibt die Datei unverschlüsselt. Entsprechendes gilt auch umgekehrt.
- Bei der Bewegung von verschlüsselten Dateien in ein anderes Dateisystem als Windows 2000 NTFS (z.B. auf Diskette) hebt sich die Verschlüsselung auf.
- Ein Benutzer (insbesondere ein Administrator), welcher über NTFS Sicherheitseinstellungen ändernden Zugriff auf eine verschlüsselte Datei eines anderen Benutzers erhält, kann diese weder öffnen noch umbenennen, wohl jedoch löschen.

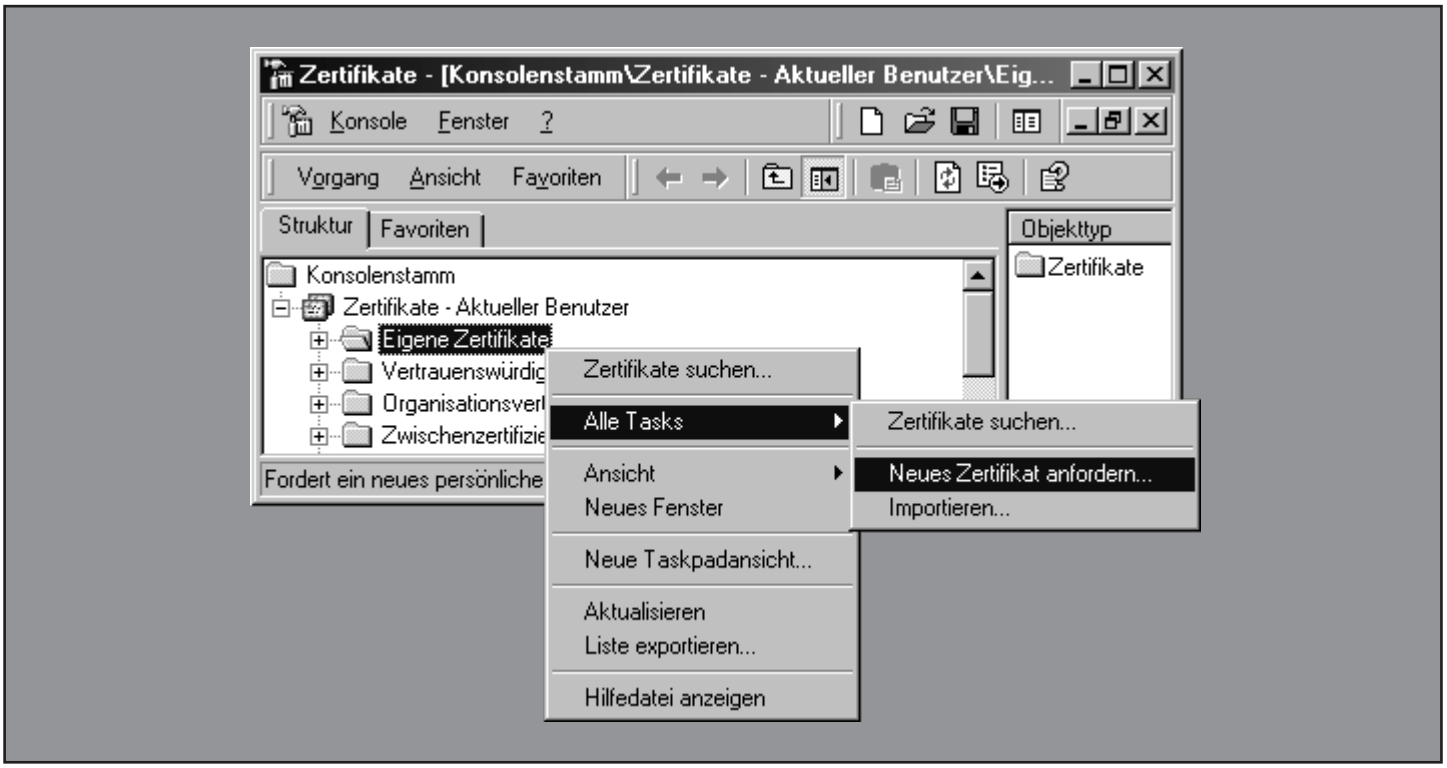
Wiederherstellung von verschlüsselten Daten

Falls keine eigenen Recovery Agents eingerichtet werden, übernimmt standardmäßig der Administrator diese Funktion. Für alle lokalen Benutzer eines Standalone PCs ist dies der lokale Administrator. Sobald der PC Mitglied einer Windows 2000 Domäne ist, übernimmt der erste Domänenadministrator die Rolle des Recovery Agents. Der zugehörige private Schlüssel befindet sich nur auf dem ersten eingerichteten Domänenkontroller.

Beim großflächigen Einsatz von EFS sollten statt des Administrators eigene Recovery Agents definiert werden, um eine Trennung der Zuständigkeiten für die Wiederherstellung sensitiver Daten und für das administrative Tagesgeschäft zu gewährleisten. Auch bei kleinen Netzen, in denen es vielleicht nur einen einzigen Administrator für sämtliche Aufgabengebiete gibt, sollte zumindest ein zusätzliches Konto für einen weiteren Recovery Agent eingerichtet werden - spätestens dann, wenn der Administrator selbst Daten verschlüsselt. Um sicherzugehen, dass ein Recovery Agent sein Amt nicht missbrauchen kann, sollte sein Zertifikat inklusive des privaten Schlüssels zunächst z.B. auf Diskette exportiert und an zwei verschiedenen sicheren Orten gelagert werden. Wenn anschließend das Zertifikat auf dem Domänenkontroller gelöscht wird, kann ein Recovery Agent nur dann verschlüsselte Daten wiederherstellen, wenn ihm vorher die Diskette mit seinem Zertifikat ausgehändigt wird.

Recovery Agents können nicht nur für die gesamte Active Directory Domäne, sondern auch nur für bestimmte Organisationseinheiten definiert werden. Auf diese Weise kann die Datenwiederherstellung beispielsweise auf jeweils eine vertrauenswürdige Person innerhalb jeder Abteilung delegiert werden. Diese Person würde dann in einer entsprechenden Recovery Group Policy für die jeweilige Organisationseinheit als Wiederherstellungsagent definiert werden. Um dies zu erreichen, muss zunächst eine Zertifizierungsstelle für das Unternehmen eingerichtet werden, indem auf einem Domänenkontroller die Zertifizierungsdienste (Enterprise CA) installiert werden. Anschließend muss jeder Benutzer, welcher als Wiederherstellungsagent definiert werden soll, ein Zertifikat für die Dateiwiederherstellung beantragen. Dies geschieht über die Microsoft Management Console (MMC) mit Hilfe des Snap-Ins "Zertifikate" (vgl. Bild 3), wobei als Modus "für den aktuellen Benutzer" ausgewählt werden muss.

Bild 3 Anfordern eines neuen EFS Recovery Agent Zertifikates



Das so erhaltene Zertifikat sollte nun zunächst ohne den privaten Schlüssel in eine CER-Datei exportiert werden, welche dann von einem Domänenadministrator zu der Recovery Policy hinzugefügt werden kann. Anschließend ist das Zertifikat mit dem privaten Schlüssel in eine mit Passwort gesicherte PFX-Datei zu exportieren und an einem sicheren Ort zu lagern.

Nun kann ein Domänenadministrator mit Hilfe des MMC Snap-Ins "Active Directory Benutzer und Computer" in den Eigenschaften einer gewünschten Organisationseinheit eine Recovery Group Policy anlegen (s. Bild 4)

Innerhalb dieser Gruppenrichtlinie können anschließend die zuvor ausgestellten Zertifikate zur Dateiwiederherstellung verwendet werden, um die gewünschten Agenten für die Wiederherstellung von verschlüsselten Daten zu definieren (vgl. Bild 5).

Auf diese Weise kann jedoch andererseits auch der Einsatz von EFS für eine bestimmte Organisationseinheit oder sogar für die gesamte Domäne unterbunden werden. Dies kann erreicht werden, indem der vordefinierte Recovery Agent aus der Recovery Group Policy gelöscht und somit eine leere Recovery Group Policy für den gewünschten Bereich definiert wird. Weiterhin sollte die Übernahme in untergeordneten Organisationseinheiten erzwungen werden, falls der Einsatz von EFS im gesamten Organisationszweig verhindert werden soll.

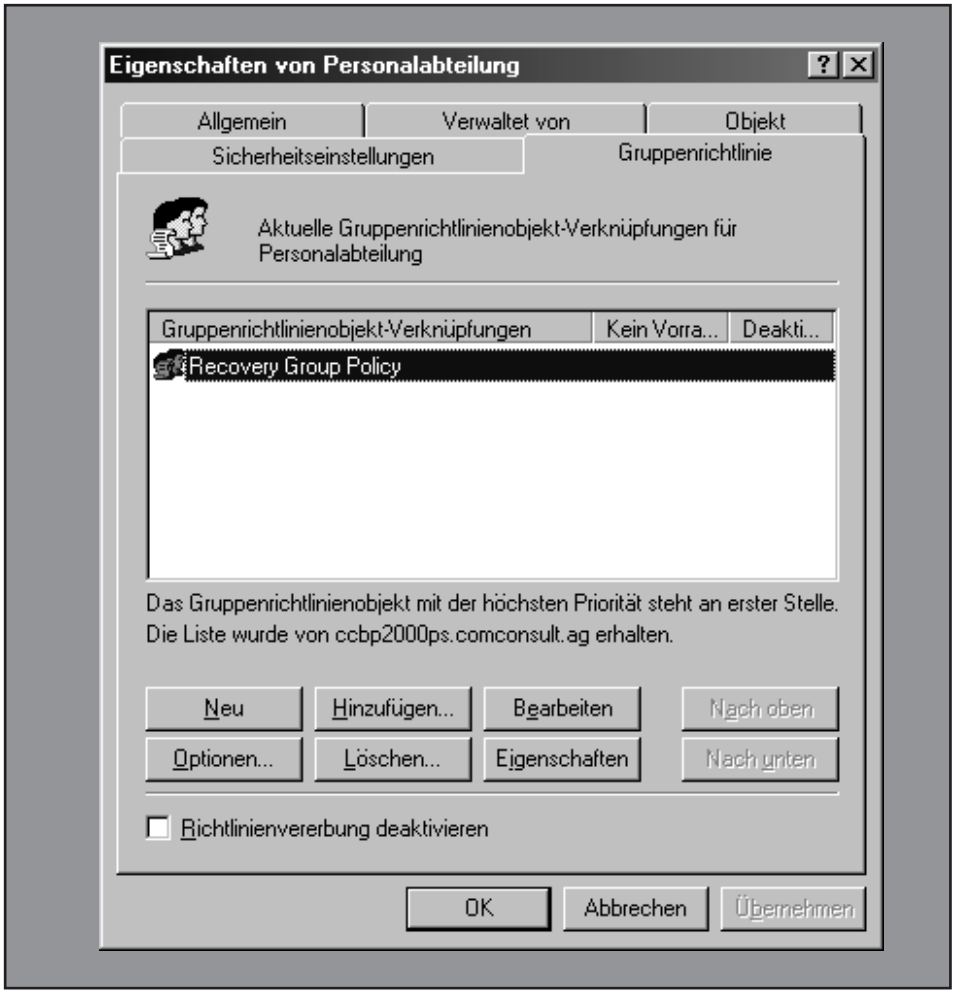
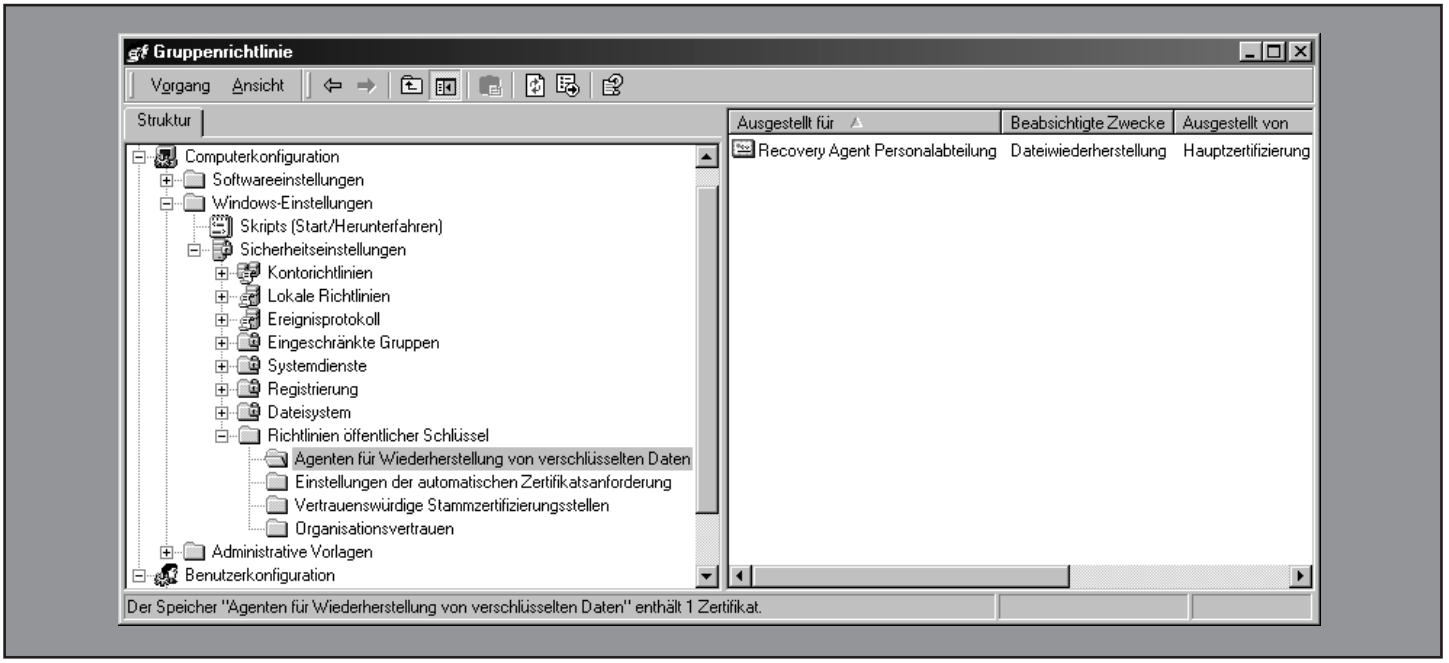


Bild 4 Definition einer Recovery Group Policy für eine Organisationseinheit

Bild 5 Hinzufügen des Zertifikates für den definierten Wiederherstellungsagenten



Durch diese Maßnahme wird der gewünschte Effekt erzielt, da die Verschlüsselung ohne mindestens einen gültigen Wiederherstellungsagenten vom System verweigert wird.

Achtung: eine leere Recovery Group Policy bedeutet, eine Gruppenrichtlinie ohne einen Wiederherstellungsagenten zu definieren. Dies verhindert durch die Vererbung auch den Einsatz von EFS in untergeordneten Organisationseinheiten, selbst wenn dort anderslautende Gruppenrichtlinien definiert wären. Keine Recovery Group Policy zu definieren bzw. die gesamte Recovery Group Policy zu löschen würde ggf. einer untergeordneten Organisationseinheit ermöglichen, mit Hilfe einer eigenen Recovery Group Policy doch EFS einzusetzen.

Einsatz von EFS

EFS ist primär für den Einsatz auf lokalen Computern (insbesondere Notebooks) konzipiert, um sensitive Daten vor unberechtigtem Fremdzugriff - beispielsweise nach einem Diebstahl des Rechners - zu schützen. Bereits die Überlegung, Daten auf Netzwerkservern zu verschlüsseln erfordert weitergehende Konzipierung bezüglich der Verfügbarkeit des privaten Schlüssels für den jeweiligen Anwender, falls er von mehreren Computern aus auf die verschlüsselten Daten auf dem Server zugreifen möchte.

Für einen eventuellen Gruppeneinsatz ist EFS definitiv nicht konzipiert, obwohl theoretisch natürlich eine Notlösung denkbar wäre, indem entsprechende Gruppen in Organisationseinheiten zusammengefasst würden und dort jeweils sämtliche Gruppenmitglieder als Recovery Agents definiert würden. Somit wären alle verschlüsselten Dateien (unabhängig von ihrem Ersteller) von sämtlichen Gruppenmitgliedern lesbar. Dieser Ansatz ist jedoch schon auf Grund des enormen administrativen Aufwands keinesfalls zu empfehlen, insbesondere dann nicht, wenn etwa innerhalb einer Organisationseinheit mehrere Benutzergruppen benötigt werden, welche gegenseitig nicht auf die verschlüsselten Daten der jeweils anderen Gruppe zugreifen dürfen.

Falls derartige Anforderungen gegeben sind, muss weiterhin auf Tools von Drittherstellern zurückgegriffen werden. Weit verbreitet ist hier beispielsweise PGP, welches ab der Version 7 auch den gemeinsamen Zugriff auf verschlüsselte Daten ermöglicht, wobei dies allerdings ebenfalls nicht über echte Gruppenschlüssel sondern über explizite Zugriffslisten für die jeweiligen Daten realisiert wird. Dennoch ist hierdurch mit entsprechendem Aufwand auch eine feinere Strukturierung der Zugriffe unabhängig von existierenden Organisationseinheiten im Active Directory möglich.

Eine komplett eigene Benutzer- und Gruppenverwaltung für eine somit frei konstruierbare Zugriffstruktur ist zum Beispiel mittels LanCrypt realisierbar, indem äquivalent zu NTFS-Sicherheitseinstellungen gruppenbasiert Verschlüsselungsregeln für Ordner und Dateien definiert werden können. Natürlich ist hierfür allerdings eine weitere Benutzer- und Gruppenverwaltung zusätzlich zur Windows-basierten Administration nötig.

EFS ist also sicherlich dann zu empfehlen, wenn mit Hilfe von Windows 2000 Bordmitteln insbesondere auf Notebooks lokale Daten transparent für den Benutzer geschützt werden sollen. Dies gilt z.B. für private oder projektbezogene Daten des Anwenders, die auf Grund des hohen Entschlüsselungsaufwands für einen Dieb uninteressant werden.

Allerdings ist die für die Verschlüsselung verwendete DES-Variante mit 56-bit Schlüssellänge für den Schutz hochsensitiver Daten unzureichend, weshalb hierfür mindestens bis zur angekündigten erweiterten Nachfolgeversion von EFS andere Tools wie z.B. PGP verwendet werden sollten, zumal bislang keine offizielle kryptologische Bewertung der im "High Encryption Pack" eingeführten 128-bit Verschlüsselung vorliegt.

Bereits für den Fall, dass Benutzer ihre eigenen Daten auf einem Netzwerkserver verschlüsseln sollen, steigt der administrative Aufwand, wenn der Benutzer von verschiedenen Computern aus auf die verschlüsselten Daten zugreifen muss und noch keine servergespeicherten Profile verwendet werden. Hinzu kommt, dass die mittels EFS verschlüsselten Daten über ein Netzwerk unverschlüsselt übertragen werden, so dass ggf. zusätzlich der Einsatz weiterer Schutzmaßnahmen wie IPSec konzipiert werden muss.

Möglicherweise ist also bereits in diesem Szenario der Einsatz eines Drittherstellertools zu überlegen, spätestens jedoch, wenn ein gemeinsamer Zugriff auf die verschlüsselten Daten erforderlich ist.

Abkürzungstabelle

E	**EFS**	**Encrypting File System**
D	**DES**	**Data Encryption Standard**
	DESX	**expanded Data Encryption Standard**
M	**MMC**	**Microsoft Management Console**
N	**NTFS**	**Windows NT Dateisystem**

ComConsult Certified Network Engineer

"Damit ich auch weiß, wovon ich rede."

Henning Kruse (28) arbeitet seit Januar 2000 bei der Origin Deutschland GmbH.

Der Netzwerk Insider sprach mit ihm unmittelbar nach seiner bestandenen Prüfung zum ComConsult Certified Network Engineer.

Insider: Was machen Sie in Ihrem Beruf?

Henning Kruse: Ich bin relativ neu bei der Firma, arbeite im Netzwerk-Bereich in der Abteilung Services und Projects. Wir sind eine größere Gruppe, das heißt mehrere Mitarbeiter übernehmen auch die gleiche Aufgabe, das heißt die Aufgaben werden im interdisziplinären Team erledigt. Es geht darum, Projekte, die sich nicht wiederholen, die also neuen Charakter haben, durchzuführen, zu projektieren, Angebote zu bearbeiten und zu erstellen im Netzwerkbereich.

Insider: Wie kamen Sie dahin?

Henning Kruse: Vorher habe ich in der Automatisierungsbranche gearbeitet, Fertigungsstraßen automatisiert, Roboter installiert und programmiert. Dieser Bereich war sehr interessant, aber er hat sich sehr langsam entwickelt. Es gab wenig Neuerungen und weil mich die neuen Technologien sehr interessiert haben, bin ich dann in den Netzwerkbereich gewechselt, weil der gesamte Bereich auf keinen Fall als konservativ zu bezeichnen ist.

Insider: Was haben Sie gelernt?

Henning Kruse: Studiert habe ich Elektrotechnik. Nur studiert, nicht gelernt (lacht).

Insider: Was hat Sie motiviert, die Ausbildung zum ComConsult Certified Network Engineer zu machen?

Henning Kruse: Durch meinen Wechsel bedingt musste ich einige Kenntnisse im Netzwerkbereich auffrischen bzw. mir erstmal aneignen. Ich wusste nicht, welche Ausbildungsmöglichkeiten es gibt und da hat mir meine Chefin die Empfehlung gegeben, was es da gäbe.

Insider: Dann haben Sie das ja ziemlich schnell durchgezogen.

Kruse: Ja. Meine Strategie war: zuerst die Grundlagen der Netze, dann die TCP/IP-Grundlagen durchzunehmen und den dritten Vortrag Internetworking etwas abgesetzt zu belegen, um erst einige Erfahrungen zu sammeln, da Internetworkiung ja weiter noch ins Detail geht.

Henning Kruse
als frischgebackener "ComConsult Certified Network Engineer"

Insider: Wie bewerten Sie die Ausbildung?

Henning Kruse: Grundsätzlich habe ich sehr viel gelernt in den Kursen. Es war sehr intensiv. Die Prüfung fand ich sehr wichtig, weil man sich da nochmal intensiv mit dem Stoff beschäftigen musste und ich da auch das Buch erst das erste Mal angeschaut habe (lacht).

Insider: Wo sehen Sie den praktischen Nutzen Ihrer Ausbilung für Ihre tägliche Arbeit?

Henning Kruse: Ich kann jetzt fundiertere Entscheidungen treffen in der Beratung von Kunden auf welche Technologien sie setzen sollten, wie die Netzwerke ausgelegt werden sollten. Die Ausbildung hilft mir sehr praktisch in meiner täglichen Arbeit. Damit ich auch weiß, wovon ich rede.

Henning Kruse (Mitte) im Kreise der Mitabsolventen

Dr. Kauffels Investment Insider

Dr. Kauffels Investment Insider

Der Dr. Kauffels Investment Insider greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends. Auf keinen Fall haftet der Autor oder der Netzwerk Insider für Investments der Leser, die sich aus diesen Darstellungen ergeben. Eine Haftung, weder für Verluste noch für entgangene Gewinne, wird absolut ausgeschlossen.

Boden oder nicht Boden, das ist hier die Frage ...

Durch die überraschende Warnung von Notel Networks hinsichtlich eines überaus schlechten Ergebnisses, zu deren Folgen wir weiter unten noch etwas sagen sind praktisch alle Werte, die im Sichtbereich dieser Publikation liegen, auf neue 52-Wochen-Tiefs gefallen.

Wir danken Nortel Networks besonders dafür, einer Abwärtsbewegung, die an sich schon seit zwei oder drei Monaten intakt ist, richtigen Schwung gegeben zu haben und dabei insgesamt eine Geldvernichtungskraft entfaltet zu haben, die sonstige Vernichter wie Finanzamt, unterhaltswillige Ex-Ehefrauen oder Neuwagen weit in den Schatten stellt.

Es ist heute überhaupt nicht abzusehen, was passieren wird. Nortel hat eine Reihe völlig unschuldiger Firmen wie JDS Uniphase oder Corning mit ins Verderben gerissen, nur weil sie in enger Geschäftsbeziehung mit den Kanadiern gestanden haben.

Ihr Dr. Franz-Joachim Kauffels

Dr. Kauffels Investment Insider

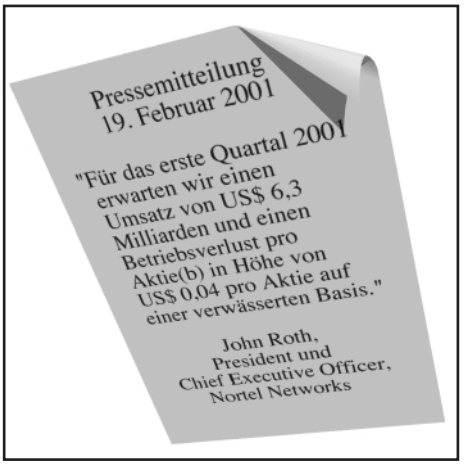
Der Fall (von) Nortel

Es ist unbestritten, dass die Telekommunikationsanbieter wie Carrier oder Internet Provider etwas zurückhaltender in ihren Ausgaben geworden sind. Das kommt einfach daher, dass deren Endkunden vom Privatmann bis zum Unternehmen nicht in dem Maße Geld für Dienstleistungen ausgeben mögen, wie man das bisher vielfach angenommen hatte. Diese Zurückhaltung ist jedoch weniger dramatisch als der Kursverfall der Ausrüster.

Nortel Networks nimmt in diesem Zusammenhang aber eine besonders unrühmliche Rolle ein. Statt eines allgemein erwarteten Gewinns von ca. 16 Cents pro Aktie wurde kurzfristig ein Verlust von 4 Cents im operativen Geschäft angekündigt.

Diese Ankündigung traf nicht nur Kleinaktionäre (wie Sie) oder Hobby-Analysten (wie mich) sondern auch die volle Spannbreite der wirklichen Profis von den Analysten der Investment-Banken bis hin zu den großen Investment Fonds mit voller Wucht.

Während dem Kleinaktionär nichts bleibt als ein ärgerlicher Verlust und der Hobbyanalyst leider in Deutschland durch unterschiedliche Maulkorbhierachien davon



abgehalten wird sagen zu können, was er wirklich denkt, stehen den Profis gewaltvolle Strafmittel zur Verfügung, deren Anwendung in diesem Fall auch wirklich angebracht erscheint.

In den USA gibt es durch die SEC ein starkes Regelwerk für die Behandlung von Unternehmensergebnissen. Dieses Regelwerk setzt Analysten in die Lage, Einschätzungen abzugeben, die dann vielleicht um einige Cents unter- oder übertroffen werden. So hat z.B. Cisco Systems ca. 25 Quartale immer einen Cent über den Erwartungen gelegen. Die Erwartungen werden durch "First Call" kurz vor der Bekanntgabe der eigentlichen Ergebnisse zusammengefasst und stehen z.B. über Reuters oder CNBC der breiten Öffentlichkeit zur Verfügung.

Bei sehr kleinen Firmen können schon einmal wirklich größere Abweichungen auftreten, weil z.B. zu wenige Analysten sich mit dieser Firma befassen. Nortel Networks ist aber ein großes Unternehmen und in seiner Heimat Kanada ein Schwergewicht im TOPIX, dem Index von Toronto. Nortel Networks ist für die Kanadier so etwas wie SAP für den DAX. Es gibt keinen technologieorientierten Analysten, der sich nicht mit Nortel Networks befasst hat. Die Ankündigung von Nortel hat sogar den Kanadischen Dollar unter Druck gesetzt!

Nun muss man sich ernsthaft die Frage stellen, welche Einflüsse dazu führen können, dass ganze Hundertschaften von Profis so falsch liegen. Bislang äußert sich die betroffene Firma selbst nur äußerst fadenscheinig "schlechteres Geschäft als erwartet, Zurückhaltung der Stammkunden und bla und öh." Damit möchte ich hier gar keinen Platz verschwenden.

Leider kann ich von den Ideen, die ich habe, nur einige relativ harmlose nennen.

Dr. Kauffels Investment Insider

- Die Firma hat ein schauderliches Rechnungswesen. Bis zum endgültigen Ausrechnen der Zahlen weiß niemand so recht, wie das operative Geschäft läuft. Halten Sie das für wahrscheinlich?

- Die Firma hat eine schreckliche Lagerhaltung. Man ist völlig überrascht davon, dass man plötzlich keinen Platz für Komponenten in den Lagern findet, weil niemand die bereits lagernden Komponenten gekauft hat. Halten Sie das für wahrscheinlich?

- Alle Kunden haben sich gleichzeitig verschworen, nicht mehr zu zahlen. Um weiter produzieren zu können, muss man Miese machen. Halten Sie das für wahrscheinlich?

- Das Management steht plötzlich und unerwartet vor einem riesigen Finanzloch, obwohl es doch bislang fest an den Erfolg geglaubt hat. Wirklich wahrscheinlich?

- In den vergangenen Quartalen wurden Einnahmen absichtlich vorgezogen, z.B. mit Rabatten auf zukünftige Rechnungen. Das ist zwar legitim und in gewisser Weise üblich, wenn z.B. bei einem Carrier ein Auftrag besteht, der sich über mehrere Jahre erstreckt, schönt aber das Ergebnis in erheblicher Weise, denn irgendwann müssen die Komponenten, für die man das Geld bekommen hat, ja einmal geliefert werden und dann bekommt man nicht nochmal Geld dafür. Macht man dies extensiv, nimmt man sozusagen einen Kredit auf die Zukunft auf, in dem Glauben, dass dieses System immer weiter läuft. Außerdem hält man nach außen hin den eigentlichen Unternehmenswert, den man z.B. in Form von Aktien für Akquisitionen benötigt, künstlich hoch. Solange der Markt wächst, geht das gut, stagniert der Markt, ist man plötzlich tot. Und ich halte diese Version für sehr wahrscheinlich.

Ich bin froh, dass ich jetzt nicht Chambers bin, der CEO von Cisco Systems. Dieser hat nämlich seit Monaten immer wieder in kleinen Dosen davor gewarnt, dass der Markt abkühlen könnte. Dafür hat er hingenommen, dass sich der Wert seines Unternehmens kontinuierlich verringert hat. Aber er war wenigstens immer ehrlich und es ist auch für die Zukunft nicht zu erwarten, dass Cisco Systems die Anleger so übel (ent)täuscht. Ich kann mir überhaupt nicht vorstellen, dass Nortel Networks nicht zu den gleichen Zeitpunkten die gleichen Informationen vorgelegen haben. Aber, im Gegensatz zu Chambers hat das kanadische Management einfach auf den Knall gewartet.

Im Nortel-Strudel: Cisco, Corning und JDS Uniphase

Sehen wir uns an, was jetzt passiert. Die US-Großbanken schäumen vor Wut. Merrill Lynch hat Nortel umgehend aus der "Techfolio List of Top 10 Names" verbannt und statt dessen Extreme Networks hinein genommen. Credit Suisse First Boston hat den zu erwartenden Unternehmenswert halbiert und das Kursziel der Aktie von 80 auf 40 US$ herabgesetzt. Die technologieorientierten Lehmann Brothers hatten die Aktie schon vor einigen Wochen von 90 auf 50 US$ herabgestuft, jetzt nehmen sie das Kursziel von 50 auf 26 US$ zurück. Alle Kaufempfehlungen sind um ein oder zwei Stufen zurückgesetzt worden. Die Analysten dieser Banken arbeiten seit Jahren abgesehen von einigen Ausrutschern ordentlich, seriös und zielsicher. In den USA sind die Anforderungen an Analysten sehr hoch, sie dürfen ggf. keine Aktien von Unternehmen haben, die sie analysieren, der Besitz von Aktien in Fonds, die einer analysierenden Bank gehören, muss veröffentlicht sein. Wenn man diese ganzen Profis an der Nase herumführt, darf man sich über nichts mehr wundern.

Nortel kann Prozesse erwarten. Um nicht in laufende Verfahren einzugreifen, zitiere ich lediglich auszugsweise aus einer Meldung von Reuters, 19.02.2001, 4:38 PM:

"Drei US-Anwaltskanzleien vereinigen sich, um Nortel Networks mit einer Sammelklage wegen der Täuschung von Anlegern zu belegen. Rechtsexperten sagen jedoch, dass sich solche Prozesse über Jahre ziehen können und einen ungewissen Ausgang haben ...

Die Kläger haben in den letzten zwei oder drei Monaten Nortel Aktien gekauft ...

Investoren, Analysten und Fondsmanager sind ärgerlich mit Nortel, weil die Warnung gerade drei Wochen kam, nachdem Nortel noch versichert hatte, man werde die 30% angestrebtes Wachstum sicherlich erreichen ...

Die Klageschriften weisen darauf hin, dass Nortels Präsident für E-Business, William Conner und der Präsident für Global Operations, Chahram Bolouri zusammen Nortel Aktien im Wert von mehr als 7 Mio. US$ verkauft haben, bevor die Firma die Warnung herausgegeben hat ...

Conner hat am 31.1.2001 117.050 Aktien zu $ 39,50 verkauft, Bolouri hat am 26.1. 43.400 Aktien zu Preisen zwischen 55 und 57.4 $ verkauft ...

Nortels CEO John Roth hat in einer Rede bereits gesagt, dass man Klagen erwarte, aber ... das sei eine eingespielte Klageindustrie ..."

Man kann eigentlich davon ausgehen, dass Klagen von einzelnen Aktionären kaum wirklich etwas bewegen. Aber Nortel Networks ist auf einer stark nach unten gerichteten Spirale unterwegs. In einem anderen Zusammenhang musste Roth zugeben, dass man "Änderungen der Kundenbudgets in Anbetracht der geänderten Sachlage erwarte". Gegenüber den Höchstständen hat sich der Unternehmenswert mehr als gedrittelt, man hat alleine in den letzten Tagen über 40% verloren. Dies kann nicht ohne Auswirkungen auf die Einschätzungen der Rating Agenturen wie Standard & Poors oder Moodys bleiben. Damit wird es wesentlich teurer für Nortel werden, Geld aufzunehmen. Geld benötigt man aber dringend, so hat man noch wenige Tage vor der Warnung eine Fabrik von JDS Uniphase gekauft. JDS Unphase sieht "zunächst" von einer Klage ab.

Ich gehe nicht davon aus, dass sich der Wert bald erholt, ganz im Gegenteil. Ich habe selbst schon länger keine Aktien von Nortel mehr, weil sie sich für meine Begriffe zu langsam bewegt haben. Hätte ich noch welche, würde ich sie jetzt gegen die Wand knallen und mir damit einen Verlust aus Spekulationsgeschäften schaffen, den ich im Laufe des Jahres dadurch auszugleichen gedenken würde, dass ich kurzfristig Aktien von Firmen kaufe, die unschuldig in den Nortel Sog gekommen sind, aber den Aktionären gegenüber seriöser auftreten, wie Cisco Systems, JDS Uniphase oder Corning.

Das einzige Kreative, was mir noch zu Nortel Networks einfällt, ist die Erzeugung eines Verlustvortrages, den man irgendwann im Jahr nochmal brauchen kann.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Fehlersuche und Betrieb in geswitchten Netzen, 12. - 14.03.01 in der AGIT Aachen

Das Seminar konzentriert sich auf die für Problemspezialisten vertieften Kenntnisse der relevanten Details von Protokollen und Medienzugangsverfahren, Routing-Informationen. Es setzt Grundkenntnisse im LAN-Trouble-Shooting voraus.
Referenten: Dipl.-Inform. Oliver Flüs und Dr. Jochen Wetzlar, ComConsult Beratung und Planung Preis: EUR 1.790,--

Verkabelungssysteme für Lokale Netze, 12. - 13.03.01 im Holiday Inn Bonn

Das Seminar basiert auf der Erfahrung einer Vielzahl aktueller Verkabelungsprojekte und deren Betrieb. Es führt methodisch vom aktuellen Stand der Technik bis zu den Leistungsmerkmalen zukünftiger Lösungen.
Referent: Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung Preis: EUR 1.290,--

Moderne Datenkommunikation, 12. - 16.03.01 im Holiday Inn Bonn

Das Intensiv-Seminar vermittelt Techniken, Verfahren und Systeme der Datenkommunikation für Ein- und Umsteiger. Der Schwerpunkt liegt auf dem erfolgreichen Einsatz der Internet/Intranet-Technologien.
Referent: Dr. Franz-Joachim Kauffels Preis: EUR 1.990,--

Projekt-Management, 12. - 14.03.01 im Holiday Inn Bonn

In diesem Seminar lernen Projektleiter ein Projekt effektiv zu organisieren und überzeugend zu führen. Es basiert auf einem kreativen Mix aus Lehrvorträgen, Erfahrungsaustausch und praktischen Übungen.
Referent: Dr. Ralf Hillemacher Preis: EUR 1.590,--

Switching-Technologien in LANs, 19. - 21.03.01 im Holiday Inn Bonn

Das Seminar vermittelt Teilnehmern mit vorhandenen Grundlagenkenntnissen den erfolgreichen Umgang mit Switching-Technologien sowie den methodischen Einsatz dieser Technologien.
Referent: Mathias Hein Preis: EUR 1.590,--

Internet und E-Business – Durchblick für Manager, 26. - 27.03.01 im Holiday Inn Bonn

Das Seminar versetzt den Teilnehmer in die Lage, die neuen Technologien kennen- und schätzen zu lernen. Techniken und Verfahren, Möglichkeiten und Gefahren, Kosten und Nutzen, Chancen und Risiken werden in kleinem Kreis diskutiert.
Referent: Dr. Franz-Joachim Kauffels Preis: EUR 1.290,--

Neue Ethernet-Technologien, 26. - 30.03.01 in der AGIT Aachen

Das Intensiv-Seminar beschäftigt sich mit dem Ausbau bzw. Umbau dieser Netze in Richtung Fast Ethernet und Frame Switching für alle Betreiber traditioneller Ethernet-Netzwerke. Referenten: Dipl.-Inform Oliver Flüs, Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hartmut Kell, Dipl.-Ing. Harald Krause, Dipl.-Inform. Sven Schumann, Dr. Joachim Wetzlar, ComConsult Beratung und Planung Preis: EUR 1.990,--

Prozess-Optimierung, 26. - 27.03.01 im Holiday Inn Bonn

In diesem Seminar lernen Führungskräfte und Spezialisten die methodischen Grundlagen der Wege zur Optimierung von Geschäftsprozessen um Verbesserungen in unternehmensinternen Strukturen und Abläufen zu realisieren.
Referent: Dr. Ralf Hillemacher Preis: EUR 1.290,--

Highend Switching Verfahren, 26. - 28.03.01 im Holiday Inn Bonn

Das Seminar vermittelt ausgerichtet auf das Umfeld von "mission critical" Client-Server-Anwendungen Technologien, Methoden und Design-Alternativen zum Aufbau hochverfügbarer Netzwerke (Quality-of-Service).
Referentin: Dipl.-Inform. Petra Borowka Preis: EUR 1.590,--

Anmeldung

Titel des Seminars _____ Name _____ Vorname _____

Termin _____ Firma, Abteilung _____ Position, Funktion _____

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Straße _____ PLZ, Ort _____

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

Telefon _____ Fax _____

eMail _____ Unterschrift _____

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerk-Komponenten

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen. Wir bauen für unsere Kunden eine Handelsplattform für gebrauchte Netzwerk-Komponenten auf. Die Spielregeln: Sie melden uns, welche Produkte/Komponenten Sie anbieten/suchen mit Ihrer Preisvorstellung. Ihr Angebot wird in anonymer Form auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de und im Netzwerk Insider veröffentlicht. Interessenten melden sich per Mail, mit dem Fax-Formular (unten) oder über den Web-Server bei uns. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her. Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Fax an 02408/955-399

☐ **Ich biete**
☐ **Ich suche**
☐ **Antwort auf Gesuch**
☐ **Antwort auf Gebot**

☐ ☐

Produkt/Komponente/Release/Software

_____

_____

_____

_____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon, Fax

_____

eMail

Gebote

Hubs
Repeater
Sternkoppler
Concentrator
Ringleitungsverteiler

Smart LAM UTP, 1 Stck., DM 350,-- B0201

Lanstack TR 20 UE, 1 Stck., DM 500,-- B0202

Lanstack TR2L,1Stck., DM 800,-- B0203

Smart LAM STP, 2 Stck., DM 600,-- B0204

Smart Cau Plus 2 (STP), 1 Stck. DM 500,-- B0205

Multiplexer
Steuereinheiten
Controller

IBM 3745-A31A Comm. Contrl. mit 3746-900 Erweiterungseinh. Schaltsystem von Control Ware System Specification auf Anfrage, verfügbar Ende Januar, 5 Stck, VS B0103

Racal Datacom Premnet 5000, jeweils mit: 1x Singlemode 1300 nm, 25 dB, 1x Switch, 5x Ethernet I/O, 1x Dual DS 1A, 1x Network MGT, 2x AC Power Supply, 2 Stck. Gesamtpreis DM 4.000,-- B0104

Switches
Brücken

IMB 8230 TRN-Units, IVS+RJ45 Ports,mehrere Stck., VS B0102

Gesuche

Adapter

IBM, Olicom, Madge TR-Adapter 16/4, PCI, mit Anschluss SUB D-9, bis 100 Stck., DM 20,-- bzw. VS S0201

Hubs
Repeater
Sternkoppler
Concentrator
Ringleitungsverteiler

jegliche managementfähige SNMP/RMON Komponenten (Hub, Router, Switch) mehrere Stck,, VS S0105

Smart LAN Plus Madge Nr:55-50, 1-3 Stck., DM 700,-- S0202

S0203 Smart LAN Plus Madge Nr: 55-29, 1-3 Stck., DM 1.200,-- S0203

Router

Cisco Router, 3000 Serie IOS V. ab. 11.0, 1 Stck., VS S0103

Switches
Brücken

Enterasys (Digital) VNSSwitch 900 CG, DVNCG-MX inkl. 1 Gigabit Ethernet Uplink Modul (GPIM-01)1 Stck., VS S0104

Sonstiges

Kabel für 2 Baynetworks BayStack 28115 um sie zu kaskadieren, 1 Stck., VS S0102

Weitere Gebote/Gesuche

finden Sie auf dem Web-Server
der ComConsult Akademie
unter www.comconsult-akademie.de