Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 78 (2000)

Heft: 12

Artikel: Konvergenz von Sprache und Daten auf einem Netz

Autor: Schmid, Andreas

DOI: https://doi.org/10.5169/seals-876497

IP Virtual Private Networks

Konvergenz von Sprache und Daten auf einem Netz

IP-VPNs über ein IP-Netz eines Providers können als Ersatz für kostspielige, lange Mietleitungen durch ein klassisches Overlay-Modell verwirklicht werden. Allerdings skalieren dadurch bereits realisierte Lösungen nicht oder sehr schlecht. Mit dem Einsatz von MPLS (Multi Protocol Label Switching) im Providerbackbone erhält man ein hoch skalierbares Peer-Modell für VPNs.

ANDREAS SCHMID

MPLS bietet vielversprechende Ansätze an für die Bereitstellung von Servicedifferenzierungen (mit Hilfe von QoS-Mechanismen) in IP-Netzen. Somit ist ein weiterer Meilenstein auf dem Weg zu einer umfassenden Konvergenz von Sprache und Daten auf einem Netz vorhanden. Die Chancen stehen gut, dass IP-VPNs die traditionellen Mietleitungen in absehbarer Zeit verdrängen werden.

IP Virtual Private Networks gestern, und heute

Bis heute waren Unternehmen gezwungen, ihre verschiedenen Standorte mit Hilfe von teuren Mietleitungen zu einem privaten Netz zu verbinden. Die Administration der Leitungen wurde in der Regel in den Unternehmen selber durchgeführt, was zwar einfach, aber sehr teuer zu stehen kam.

Mit der Einführung von Layer-2-Netzen konnten die Provider billigere Verbindungen verkaufen, ohne Netzressourcen explizit von Kundenstandort zu Kundenstandort zu reservieren. Dabei wurden virtuelle Verbindungen über das physikalische Netz gelegt. Die Administration des Services erfolgte weiterhin bei den Unternehmen.

Heute entwickelt sich eine Tendenz zu «managed Services» auf IP-Basis wie Intranet, Extranet, Internet, E-Mail, Webhosting und RAS. Diese bieten den Serviceprovidern eine grosse Chance, neue und extensive Einkommensströme zu erlangen. Der IP-VPN-Dienst wird nicht als einzelner Dienst verkauft. Vielmehr lässt sich damit eine leistungsfähige Plattform bilden, die es erlaubt, einfach und relativ schnell den bestehenden Kunden zusätzliche Dienste auf IP-Basis anzubieten. Der Dienst tritt also als «Enabler» für «value added» IP Services auf.

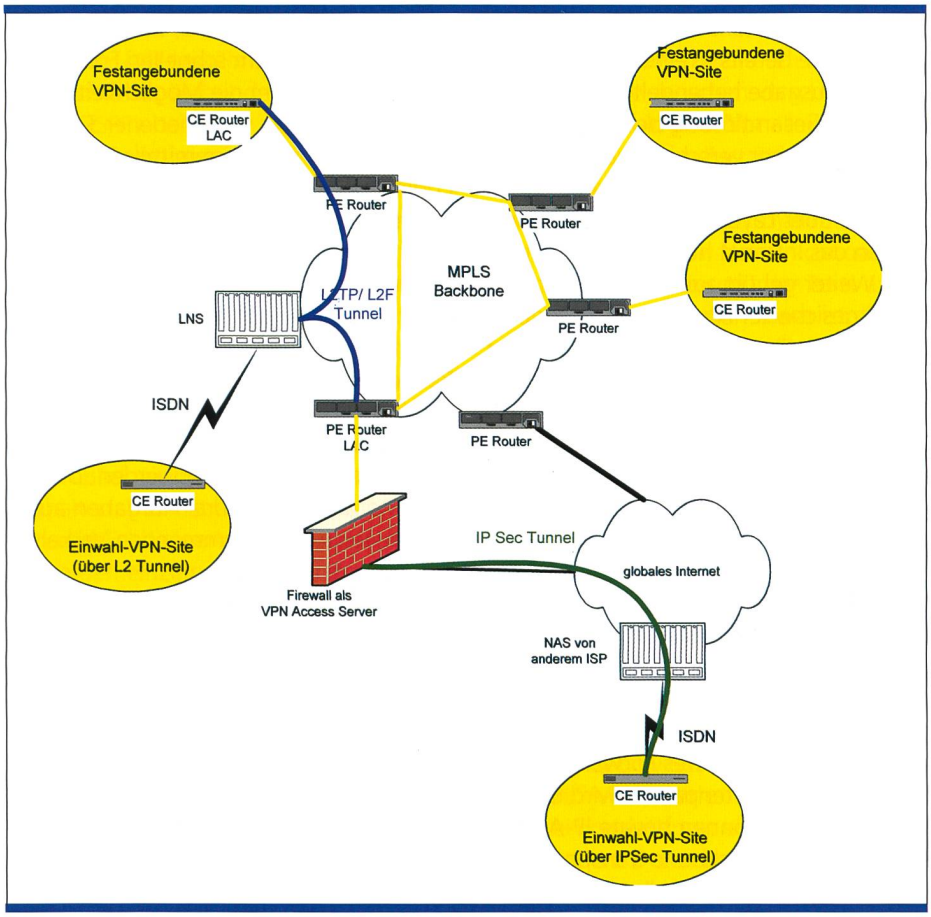


Bild 1. Architektur einer VPN-Gesamtlösung. Die L2-Tunnelvarianten sind entweder als L2-Tunnel zum CE oder als L2-Tunnel zum PE zu verstehen.

Die hier dargestellten Fakten basieren auf Erfahrungen, die der Autor während eines halbjährigen Aufenthalts bei der ehemaligen 50%-Swisscom-Tochter «tesion» Telekommunikation in Stuttgart machen konnte. Dort hat sich der Autor mit der hier beschriebenen Technologie intensiv beschäftigt, Tests durchgeführt und Konzepte entworfen. Als Folge davon entschied sich «tesion» für diese Technologie und baut nun ein deutschlandweites MPLS/VPN-Netz auf.

IP-VPNs können durch existierende Layer-2-Technologien oder durch Layer-3-Tunnels gebildet werden. Auf dem traditionellen Overlay-Modell basierende Konzepte skalieren aber nicht und sind oft mit einem grossen Konfigurationsaufwand verbunden. Deshalb ist es erforderlich, den IP-VPN-Service mit einem Peer-Modell auf das Netz zu bringen. Das

Netz muss sozusagen IP-VPN «enabled» werden. Dies kann mit Hilfe der BGP/MPLS-Technologie [1] geschehen. Der Konfigurationsaufwand reduziert sich damit von einer exponentiellen zu einer linearen Abhängigkeit pro neuer Site in einem VPN. Cisco verwendet diese Technologie in seiner MPLS/VPN-Architektur.

Konzepte für VPNs

Grundsätzlich wird zwischen zwei Arten von VPNs unterschieden, die sich zu einer vollständigen VPN-Lösung ergänzen:
- Site-to-Site-VPNs oder Intranet-VPNs
- Remote Access VPNs (NAS initiated oder Client initiated)

Bei Site-to-Site oder Intranet-VPNs werden verschiedene Niederlassungen einer Firma über den IP-Backbone eines Serviceproviders miteinander verbunden, sodass ein logisches privates Netz entsteht. Der Kunde des Providers benötigt nicht mehr eine teure Mietleitung zwischen den einzelnen Niederlassungen, sondern nur noch eine Mietleitung pro Niederlassung bis zum nächsten IP-POP (Point of Presence) des Providers. Es sind natürlich auch andere Zugangsverfahren über Kabelmodem, xDSL, Powerline und WLL möglich (je nachdem, was der Provider anbietet). Der Provider sorgt dann für den korrekten Transfer der Daten durch Tunnels zwischen den einzelnen POPs. Die MPLS-Technologie in Verbindung mit iBGP (internal BGP) bietet eine einfache und gut skalierbare Möglichkeit für den Aufbau dieser Tunnels. Dabei wird eine spezielle Nomenklatur für die involvierten Routers eingeführt. Man spricht von CEs (Customer Edge Routers) bei den CPE-Routers, von PEs (Provider Edge Routers) bei den POP-Routers und von Ps (Provider Routers) bei den Core-Routers. Um kleinere Niederlassungen und Teleworker an das Intranet-VPN anzubinden, kommen meist Einwahlverbindungen zum Einsatz. Dazu muss vom Einwahlserver (NAS) auf Layer-2-Ebene (L2TP oder L2F-Tunnel) oder direkt vom Client aus auf Layer-3-Ebene durch Verschlüsselung mit IPsec ein Tunnel in das VPN hinein aufgebaut werden. Auf einem Homegateway werden die Tunnels zentral terminiert. Bei Verwendung von L2-Tunnels kann zusätzlich mit IPsec verschlüsselt werden. Bei Remote Access VPNs spricht man von VPDNs oder NAS-iniziierten VPNs, wenn L2-Tunnelingmechanismen verwendet werden, und von Client-inizierten VPNs, wenn nur auf Layer-3-Ebene

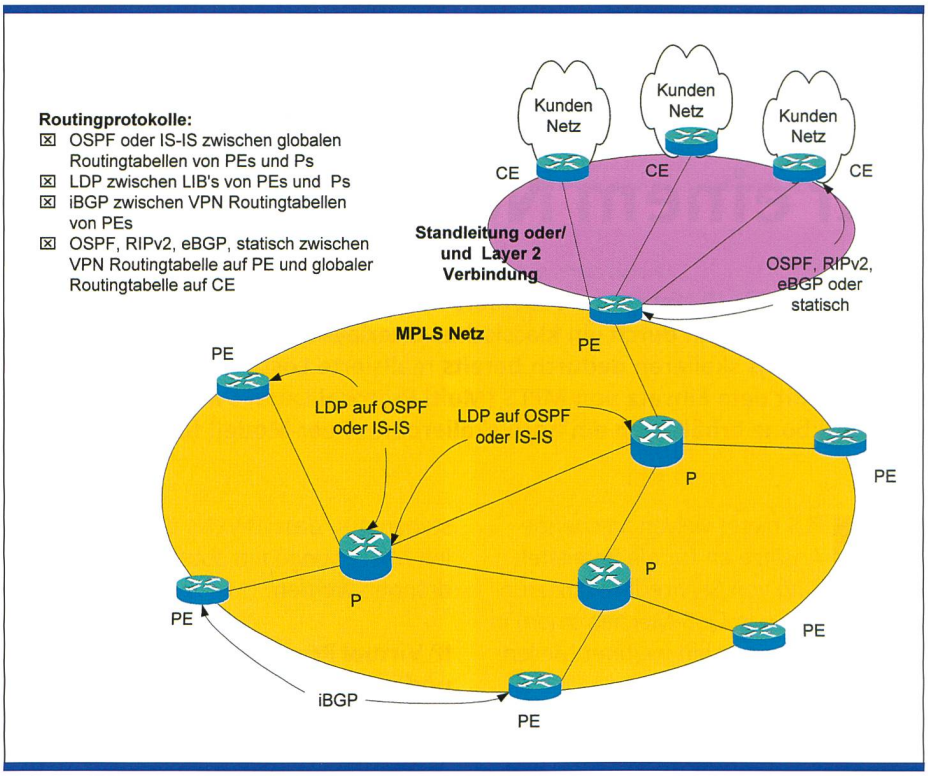


Bild 2. Zusammenspiel der verschiedenen Routingprotokolle in einem MPLS/VPN-Netz.

verschlüsselt wird. Die L2-Tunnelingprotokolle an sich haben nichts mit Verschlüsselung zu tun. Das Thema Ipsec-VPNs wurde bereits in einer früheren comtec-Ausgabe behandelt [2].
Eine VPN-Gesamtlösung beinhaltet oft ein Intranet über verschiedene, fest angebundene und sich einwählende Standorte, die über Layer-2- oder Layer-3-Tunnels an das Intranet herangeführt werden. Weiter gehört auch ein über eine Firewall gesicherter Ausgang ins Internet dazu. Bild 1 zeigt das Zusammenspiel der verschiedenen Komponenten.

Technologie für MPLS/VPNs

Für den Aufbau von MPLS/VPNs werden grundsätzlich die zwei Bausteine MPLS (Forwarding, Tunnelling) und iBGP (VPN-Routing) benötigt. MPLS ist eine Initiative des IETF (Internet Engineering Task Force), die eine Arbeitsgruppe für dieses Thema eingesetzt hat. Die Technologie vereint die Vorteile von ATM und IP. Sie arbeitet mit kurzen Labels statt mit IP-Adressen. Ein schnelleres Forwarding (Switching) der Datenpakete wird dabei möglich. Damit können private IP-Adressen über den IP-Backbone transportiert werden. Diese Labels werden von einem Routingprotokoll (LDP) über das ganze Netzwerk verteilt. In den Routers werden die Labels in einer Label Information Base (LIB) verwaltet. LDP kann per Huckepack auf ein bestehendes Routingprotokoll (OSPF oder IS-IS) aufgepackt werden. Neben dem schnellen Forwarding sind vor allem die Möglichkeiten für die Unterstützung verschiedener Serviceklassen (unter anderem mittels Traffic Engineerings) und das mit MPLS ermöglichte Peer-Modell für den Aufbau von VPNs interessant. MPLS ist unabhängig vom Layer-2-Protokoll. Man kann ATM, POS, Frame Relay oder Gbit-Ethernet benützen [3].
Bei der Verwendung von MPLS werden administrativ getrennte Netzwolken festgelegt, in denen mittels LDP Labels zugeordnet und ausgetauscht werden. Die Edge Routers führen drei Aufgaben aus:
- Sie teilen den einkommenden Verkehr bestimmten FECs zu.
- Sie fügen den Paketen Labels bei.
- Sie leiten diese weiter zu ihrem nächsten Hop.

Traditionell würde der Edge-Router FECs pro IP-Präfix verteilen. Im MPLS-Netz können nun FECs pro Serviceklasse, pro VPN oder pro speziell definierter Verkehrsart vergeben werden. Die FEC-Vergabe und die Zuweisung eines IP-Pakets zu einer FEC können dadurch sehr komplex werden. Damit lässt sich zum Beispiel auch ein Forwarding entlang eines spezifischen Pfades durchführen (eine

Links

MPLS Working Group bei IETF:
Homepage: www.ietf.org/html.charters/mpls-charter.html

MPLS Resource Center:
Homepage: www.mplsrc.com

Multi Layer Routing Übersichtsseite:
Homepage: www.infonet.aist-nara.ac.jp/member/nori-d/mlr

Cisco, VPN Solutions for Serviceproviders:
Homepage: www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/index.shtml

Art Source Routing). Die Core-Routers führen kein Processing mehr durch, sondern leiten die Pakete nur noch anhand des Labels weiter, wobei auch Priorisierungen abgehandelt werden können. Damit wird die ganze «Intelligenz» in die Edge-Routers gelegt. Die Core-Routers sind nur noch «dumme», aber schnelle Forwarder.
Die PEs, welche die Intelligenz darstellen, verwalten pro VPN je eine separate Routingtabelle mit allen Routingeinträgen der VPNs. Diese VPN-Routingtabellen werden gefüllt mit Routinginformationen, die von anderen PEs oder von CEs kommen können. Unter den PEs wird diese Funktion mit iBGP (Multiprotocol Extension, [4]) gewährleistet. Zwischen PEs und direkt verbundenen CEs kann eBGP, OSPF oder RIPv2 als Routingprotokoll verwendet werden. Eine Alternative ist hier ebenfalls der Einsatz von statischem Routing. Der Kunde ist mit dem POP-Standort über eine Standleitung direkt verbunden. Diese kann mit Layer-2-Technologie (ATM, Frame Relay usw.) zur physikalischen Lokation des PEs verlängert werden (Bild 2).
Das Verwalten verschiedener Routingtabellen auf einem Router scheint auf den ersten Blick ein Sicherheitsproblem zu enthalten. Dem ist aber nicht so. Es finden nämlich keinerlei Interaktionen zwischen den einzelnen Routingtabellen statt (weder zwischen einer globalen Tabelle und VPN-Tabellen noch zwischen den einzelnen VPN-Routingtabellen). Ein von Swisscom in Auftrag gegebener Hackertest konnte diese theoretische Aussage auch praktisch bestätigen.

Technische Probleme

Bei den Tests im «tesion»-Labor vom Januar bis Juni 2000 stellte sich schnell heraus, dass MPLS eine junge Technologie ist. Die Basistechnologie hat bereits eine gewisse Reife erlangt. Sobald spezielle Features, Feature Interworking oder Interworking von Equipments verschiedener Hersteller verlangt werden, stösst man immer wieder auf nicht ganz ausgereifte Implementierungen. Im Testlabor traten auch Lösungsansätze zu Tage, die für eine Umsetzung offensichtlich noch weiterentwickelt werden müssen. Die aktuellen Implementierungen sind noch stark mit Fehlern und Problemen behaftet. Speziell problematisch sind das Zusammenspiel von MPLS/VPN PE und L2TP Homegateway auf einem PE. Diese Konstellation bereitete im Labor in mehrfacher Hinsicht Probleme. Sie lässt beim aktuellen Stand (IOS 12.12) auch noch keinen Multilink für die Einwahl zu. Probleme bereiteten ausserdem die Übergänge zwischen verschiedenen Layer-2-Technologien. Vor allem beim Übergang zwischen Fast Ethernet und POS können MPLS-Probleme wegen nicht übereinstimmender maximaler Paketlängen entstehen. Noch nicht ganz bereit war zum Zeitpunkt der Tests auch die QoS-Implementation. Zwar ist die Bereitstellung von QoS für VoIP-Verkehr grundsätzlich schon heute auch bei ausgelasteten Netzen machbar (mittels Priority Queuing), aber die Konfiguration ist ziemlich umständlich, und sie treibt die involvierten Routers sehr rasch an ihre Leistungsgrenzen (CPU Last extrem hoch bei heutigen Routern).

Stolpersteine in Organisation und Betrieb

Die organisatorischen Probleme für die Umsetzung eines VPN-Dienstes bei einem Serviceprovider sind mannigfaltig. Die MPLS/VPN-Plattform muss intern als Multiserviceplattform erkannt und gefördert werden. Deren Potenzial dient vor allem dem Marketing als Instrument. VPN ist nicht ein abgeschlossener Dienst, sondern eine Plattform für zusätzliche, rasch umsetzbare IP-Dienste. Das dadurch vorhandene Personalisierungspotenzial zum Kunden muss ausgeschöpft werden, was zu einer potenziell sehr starken Kundenbindung führen kann. Prozesse müssen definiert und vor allem umgesetzt werden. Produkte und -bundles sollen definiert werden, sodass der Kunde sie noch versteht und als Mehrwert anerkennt. Das Personal aus den Bereichen Verkauf und Customer Care braucht eine Schulung, die von den Technikern unterstützt wird. Wegen der Komplexität des Dienstes darf das nicht unterschätzt werden.
Vor allem aber braucht es eine erarbeitete Managementarchitektur, die umgesetzt und unterhalten wird. Dazu ist eine Reihe von Werkzeugen von verschiedenen Herstellern erhältlich für Fault, Service und Performancemanagement sowie für Billing und Provisioning. Da man sich von einem so genannten «dummen» zu einem servicebewussten Netz hin bewegt, darf das Management nicht beim Elementmanagement stehen bleiben, sondern muss für Servicemanagement bereit sein. Dazu ist unter anderem eine IP-Mediation-Plattform notwendig. Sie sammelt Daten von verschiedenen Datenquellen, beispielsweise Serverlogfiles, Routerlogfiles und Netzwerkprobes. Die Aufgabe dieser Plattform ist dann die Datenaggregation, -korrelation und -konsolidierung für die Serviceapplikationen von Billing, Customer Relationship Management oder Performancemanagement. Der Aufbau einer durchdachten Managementarchitektur ist für Time-to-Market-Aspekte neuer Services kritisch. Sie ist heute aber einer der wichtigsten Faktoren für den Erfolg eines Produkts und damit auch für das Überleben eines Serviceproviders.

Schlussfolgerungen und Ausblick

Der Einsatz von VPNs verspricht ein Integrations- und Sparpotenzial. Die bei «tesion» durchgefürten Tests zeigten, dass Konzepte und Technologie bereits eine Reife erlangt haben, die es den Serviceprovidern ermöglicht, in diesem Markt aktiv zu sein oder zu werden. Stolpersteine sind vor allem im Bereich Management und bei internen Prozessen anzutreffen. Die MPLS/VPN-Technologie wird sich mit der Verabschiedung weiterer Standards im IETF für die Serviceprovider zu einer äusserst attraktiven Möglichkeit als Multiservice-Plattform entwickeln. Vor allem die Standards für das Traffic Engineering in MPLS-Netzen, die Umset-

Abkürzungen

ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol (i = internal, e = external)
CPE	Customer Premises Equipment
FEC	Forwarding Equivalence Class
IETF	Internet Engineering Task Force
IOS	Internetworking Operating System (OS von Cisco-Routers)
IS-IS	Intermediate System-Intermediate System
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator (Homegateway)
LDP	Label Distribution Protocol
LNS	L2TP Network Server (NAS)
MPLS	Multi-Protocol Label Switching
NAS	Network Access Server
OSPF	Open Shortest Path First
POP	Point of Presence
POS	Packet over SONET/SDH
QoS	Quality of Service
RAS	Remote Access Service
VPN	Virtual Private Network
WDM	Wavelength Division Multiplex
WLL	Wireless Local Loop
xDSL	Digital Subscriber Line Technology

zung von DiffServ als QoS-Mechanismus und die Entwicklung neuer Tools für das Management von MPLS-Netzen werden der Technologie zu breiter Popularität verhelfen. Swisscom hat mit dem IPSS-Netz als erster Serviceprovider weltweit ein MPLS-Netz aufgebaut. Und «tesion» wird bis Anfang 2001 sein deutschlandweites IP-Netz mit dieser Technologie aufbauen. Eine interessante Weiterentwicklung von MPLS ist MPLambdaS [5]. Sie verbindet MPLS mit der Flexibilität und der beinahe unbeschränkt verfügbaren Bandbreite der WDM-Technologie im Layer 1. MPLS wird damit zur Steuerungsschicht für Wellenlängen (LambdaS). Die Netzarchitektur wird stark vereinfacht. Allerdings bleibt dahingestellt, ob der Layer 3 mit dem Hinzufügen von mehr und mehr «Intelligenz» irgendwann so komplex ist, dass er nicht mehr zu managen ist. 9.4

Andreas Lukas Schmid *erhielt 1998 sein Elektrotechnikdiplom an der ETH Zürich und arbeitet seither bei Swisscom Corporate Technologie CIT, Outpost OSI-LAB in Zürich. Seine Interessen liegen in den Bereichen IP Networking, IP Services und Management von IP-Netzen.*

Referenzen

[1] E. Rosen, Y. Rekhter: «BGP/MPLS VPNs», IETF RFC 2547, März 1999.
[2] A. Ferchichi: «IPsec VPN: Theory and Practice», comtec 7/8 2000.
[3] E. Zahnd: «What is MPLS», Swisscom interne Präsentation, Okt. 1999. Swisscom Intranet: epweb.swissptt.ch/ep9/web/mpls.pdf
[4] T. Bates, R. Chandra, D. Katz, Y. Rekhter: «Multiprotocol Extensions for BGP-4», IETF RFC 2283, Februar 1998.
[5] D.O. Awduche, Y. Rekhter, J. Drake, R. Coltun: «Multi-Protocol Lambda Switching: Combining MPLS Traffic Engineering Control with Optical Cross-connects», IETF draft: draft-awduche-mpls-te-optical-02.txt, Juli 2000.

Summary

IP-VPNs as a substitution for expensive long-distance leased lines can be implemented with a classical overlay model on an IP network of a Serviceprovider. However, such solutions do not scale well or not at all. With the use of MPLS in a Service Provider Network a highly scalable peer model is introduced. MPLS offers also promising approaches for QoS in IP networks. This is one vital requirement for total service integration with voice, data, video, ... in one network. Chances are increasing that traditional leased lines get replaced by IP-VPNs within few years. Concepts, technology and implementation problems are discussed in this article which bases on tests performed during a half a year stay at "tesion" Telekommunikation, a former 50% Swisscom daughter in Stuttgart, Germany.

Plant Transmeta einen Alleingang?

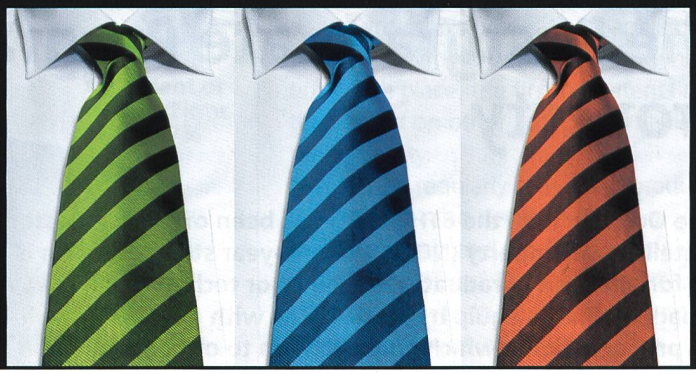
Als Transmeta mit seinen «Crusoe»-Prozessor Anfang des Jahres an den Markt ging, da machte das Start-up-Unternehmen Schlagzeilen in allen Ländern. Die leistungsfähige Prozessorarchitektur ist auf Energie sparen ausgelegt und das genau ist im Zeitalter des mobilen Internet-Computings gefragt. Als erstes Unternehmen baut Hitachi den «Crusoe» in ein Notebook ein. Lizenzen für die Prozessorarchitektur waren seitens der Halbleiterindustrie gefragt. Klammheimlich hat jetzt Transmeta von IBM und Toshiba die erteilten Lizenzen zurückgekauft: Nun rätseln die Mitbewerber, was denn Transmeta damit bezweckt. Vermutungen gehen dahin, dass das Unternehmen in das grösste Marktsegment für Mikroprozessoren – immer noch die x86-kompatiblen Industrieprozessoren – mit Eigenentwicklungen einsteigen will, um auf eine kostengünstigere Volumenfertigung in der Produktion zu kommen. Der Einstieg von Intel in den Markt für Energie sparende Mikroprozessoren könnte eine solche Entscheidung mit beeinflusst haben: Gegen Intel ist es eben schwer mit Neuentwicklungen anzukommen.

Transmeta Corp., 3940 Freedom Circle
Santa Clara CA 95054, USA
Tel. +1-408-919 3000
Fax +1-408-919 6540

R&M

Convincing cabling solutions

Welche steht Ihnen am besten?



Gebäudeverkabelungs-Lösungen für Ihre Bedürfnisse

Das R&M freenet LAN-Verkabelungssystem für Sprach-, Daten- und Videoanwendungen erfüllt höchste Ansprüche. Es ist in drei verschiedene Lösungen unterteilt, die jeweils für das entsprechende Kundenbedürfnis das optimale Angebot darstellen. Das R&M CLASSIC*system* erfüllt alle heutigen Standards auf Basis Kat. 5e und bietet ein optimales Preis-Leistungs-Verhältnis. Das R&M STAR*system* basiert auf dem Kat. 6 Standard und ist für anspruchsvolle Kundensegmente interessant, die höchsten Wert auf die Zukunftssicherheit ihrer IT-Infrastruktur legen. Mit dem R&M VISION*system* gehen wir absolut neue Wege. Als Alternative zur klassischen universellen Gebäudeverkabelung bieten wir eine «Single Point of Administration»-Infrastruktur, die Platz sparend auf Etagenverteiler verzichtet und alle Daten mit Glasfaser- oder Kupferleiter von einem zentralen Punkt im LAN direkt an jeden Arbeitsplatz bringt. Interessiert? Dann rufen Sie uns doch einfach an!

Info 01 931 97 77

R&M *freenet*

The LAN solution

Reichle & De-Massari AG
Binzstrasse 31
CH-8622 Wetzikon
Telefon +41 1 931 97 77
Telefax +41 1 931 93 29
www.rdm.ch