Dr. Suppan International Institute

Der Netzwerk Insider

November 2002

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

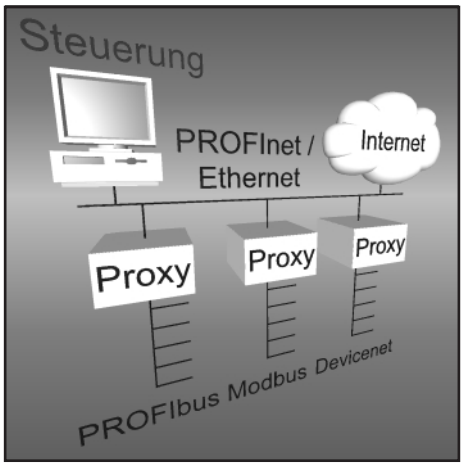
Schwerpunktthema

Ethernet im industriellen Einsatz

von Dipl.-Ing. Roland Moos

Intelligenz, Zeit und vor allem Kosten sind auch in der Fertigungsindustrie zum entscheidenden Produktionsfaktor geworden, so dass es in der Industrie mittlerweile einen unaufhaltsamen Trend zu einer einheitlichen und standardisierten Kommunikation vom Bürobereich bis hin zum Produktionsbereich (-maschine) gibt und damit Medienbrüche nicht mehr bestehen.

Dies ermöglicht einen durchgängigen Datenfluss vom administrativen (Büro-) Arbeitsplatz bis zur produzierenden Maschine, um beispielsweise wichtige Prozessdaten aufzeichnen, organisieren und weiterverarbeiten zu können. Diesen Trend belegt das Kommunikationsnetz der Volkswagen AG am Standort Zwickau, das neben dem administrativen Bereich (Büros) auch einige Produktionsbereiche in ein durchgängiges Datennetz integriert hat.



Industrial Ethernet

In der Büro-Welt hat sich anerkannterweise Ethernet durchgesetzt, so dass hier eine Industrieversion nahe liegt. "Industrial Ethernet" lautet das Schlagwort.

- Doch herrschen in Büro- und Produktionswelt die gleichen Bedingungen?
- Sind Produkt- oder Design-Entscheidungen Eins-zu-Eins in die Fertigung übertragbar?
- Wenn nicht, wo bestehen gegenwärtig Probleme und was sagt die Normung dazu?

Ethernet-Netzwerke sind heute grundsätzlich für Industrieanwendungen bzw. für Vernetzungen in Produktionsstätten tauglich, aber nicht ohne komplexere Fragen zuvor beantworten zu können, was wir im Folgenden weiter erläutern möchten.

weiter Seite 6

Zum Geleit

Voice-over-IP jetzt einsetzen!

Fast jedes Unternehmen, das zur Zeit mit der Beschaffung einer neuen TK-Anlage befasst ist, wird dabei auch den denkbaren Einsatz einer VoIP-Lösung prüfen. Die Gründe dafür sind sicher abhängig vom Einzelfall, jedoch gibt es mittlerweile gute Argumente, VoIP als seriöse Alternative anzusehen:

- die Produkte haben einen akzeptablen Reifegrad erreicht
- alle Hersteller stehen mittlerweile hinter VoIP, auch die traditionellen TK-Hersteller haben entsprechende Lösungen in ihr Angebot aufgenommen
- VoIP beinhaltet eine Reihe ernstzunehmender Vorteile
- das traditionelle Corporate Network mit Remote Access auf der Basis von Dial-In Verbindungen ist viel zu teuer und unflexibel gegenüber einer Internet-basierten VPN-Lösung, dementsprechend entsteht mit der Nutzung des Internets als neues Corporate Network aber damit auch gleichzeitig eine ideale Infrastruktur für eine interne VoIP-Lösung zwischen den Standorten
- ein Wechsel zu VoIP wird im Markt in den nächsten Jahren auf jeden Fall erfolgen, so dass bei der Neubeschaffung einer Anlage mit einer vorgesehenen Nutzungszeit von mehrere Jahren auf jeden Fall eine VoIP-Integration Gegenstand der Entscheidung sein muss

Bedauerlicherweise gibt es aber immer auch noch massive Probleme, die die VoIP-Nutzung erschweren bzw. einzelne Vorteile wieder in Frage stellen:

weiter Seite 2

MPLS-Serie

Multiprotokoll Label Switching – Teil 5

Petra Borowka hat für den Insider unter dem Titel "Multiprotokoll Label Switching " eine umfangreiche Abhandlung verfasst, die wir Ihnen mit diesem Heft als Abschluss in fünf leicht verdaulichen Portionen serviert haben.

Letzter Teil ab Seite 18

Voice over IP jetzt einsetzen!

Fortsetzung von Seite 1

- die VoIP-Hersteller werben in ihren Unterlagen gerne vollmundig mit dem Abschied von der proprietären TK-Lösung und der Einführung einer TK-Lösung auf international genormter Basis mit damit verbundenen massiven Kosten-Vorteilen. Dies entspricht definitiv nicht der Realität. Zum einen werben die meisten Hersteller zwar mit dem Bezug auf Standards, bei näherer Betrachtung benutzen sie aber selber eine nicht standardisierte Lösung. Entsprechend teuer sind in der Regel die Telefon-Apparate, ein absolut unakzeptabler Zustand, der auch die Wirtschaftlichkeit einer VoIP-Lösung massiv gefährdet. Zum anderen ist nach wie vor unklar, welcher Standard sich in Zukunft durchsetzen wird. Nach wie vor kämpfen die Standards der ITU (H.323) und der IETF (SIP) gegeneinander. Vieles spricht dafür, dass sich SIP durchsetzt, die Produkt-Realität ist aber an H.323 ausgerichtet. Wenn man überhaupt eine Chance hat, ein preiswerte VoIP-Telefon zu erwerben, dann basiert dies in der Regel noch auf H.323

- Anforderungen an hohe Verfügbarkeit können die Lösung stark verteuern
- die Integration wichtiger Applikationen wie Unified Messaging, ACD und CTI hat bei vielen Anbietern längst nicht das Niveau erreicht, das man sich wünschen würde

Trotz dieser Nachteile macht die Evaluierung von VoIP auf jeden Fall für die meisten Unternehmen mittlerweile Sinn. Einer der Gründe dafür sind die völlig verschiedenen Nutzungsvarianten von VoIP, die unter anderem eine stufenweise Umsetzung ermöglichen und so dem Kunden die Möglichkeit geben, die Vorteile, die gerade für ihn Sinn machen, zu nutzen und auf andere Varianten später umzusteigen. So können wir heute folgende Nutzungs-Varianten unterscheiden:

- die reine VoIP-Lösung als Komplettersatz der traditionellen TK-Anlage (typisch CISCO)
- die hybride Lösung in einer Mischung aus TK-Anlage mit VoIP-Integration (typisch: Alcatel, Nortel und Siemens), wobei die Integration auch aus einer eigenständigen VoIP-Unteranlage bestehen kann (siehe aktuelle Ankündigungen von Siemens)
- die Kombination einer klassischen TK-Anlage mit einer VoIP-Anlage eines anderen Herstellers über QSIG
- die Nutzung von VoIP-Trunk-Verbindungen zwischen TK-Anlagen
- die Home-Office oder Filial-Integration
- Einsatz von Softphones (siehe Innovaphone, SWYX)
- Einsatz von XML-Applikationen im Telefon-Apparat (siehe CISCO)

Schon diese Auflistung macht deutlich, dass eine pauschale Bewertung denkbarer Vor- oder Nachteile von VoIP-Lösung schwierig ist, zu vielfältig sind die denkbaren Einsatz-Szenarien und zu groß werden die Unterschiede in den Anforderungen der Unternehmen sein. Entsprechend schwierig und umgebungsabhängig ist die häufig zitierte Betriebskosten-Bewertung.

Dies macht für jeden, der eine neue TK-Lösung sucht, eine VoIP-Evaluierung notwendig. Diese ist allein bei Betrachtung der genannten Szenarien sehr aufwändig.

Hier setzt unsere diesjährige Winterschule an, die sich in 5 Tagen intensiv nur dem Thema VoIP widmet. Dabei werden nicht nur die technischen Grundlagen besprochen sondern insbesondere die möglichen Einsatzvarianten vorgestellt und eine Auswahl der führenden VoIP-Produkte besprochen. Ebenso kommen Referenz-Anwender zu Wort, die über ihre Einsatzerfahrung ungeschönt berichten. Dementsprechend werden ausgewählte Hersteller Stellung beziehen und ihre Sichtweise vorstellen, sich aber auch der Diskussion zum Thema Einsatz-Erfahrungen und Anforderungen bzw. Kritik des Marktes stellen.

In dieser Form kann die Winterschule ihre VoIP-Evaluierung massiv unterstützen und ihnen viel Zeit und Geld ersparen. Sie erfahren in 5 Tagen-Intensiv wo der Markt steht und ob und in welcher Form sich die weitere Evaluierung für sie lohnt.

Ich würde mich freuen, Sie dort zu treffen, um gemeinsam mit Ihnen den Stand der Technik und die Marktsituation von VoIP zu diskutieren.

Ihr
Dr. Jürgen Suppan

(drsuppan@comconsult-akademie.de)

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

Nachdruck,
auch auszugsweise
nur mit Genehmigung
des Verlages

© Dr. Suppan International Institute b.v.

Winterschule der ComConsult-Akademie

Voice over IP Intensiv Evaluierung

Vom 2. - 6. Dezember 2002 veranstaltet die ComConsult Akademie im Hilton Hotel in Bonn ihre diesjährige Winterschule ganz im Zeichen von Voice over IP.

Die Moderation der Winterschule hat Petra Borowka von der UBN, sie wird tatkräftig unterstützt von der ComConsult Firmengruppe. Spezialisten von Avaya, Alcatel, CISCO, Nortel und Siemens stellen sich in ihren Vorträgen der Diskussion und der Bewertung.

Die Winterschule 2002 der ComConsult Akademie bringt den Teilnehmern die 5-Tage-Intensiv-Evaluierung:

- wo steht VoIP?
- welche Vorteile entstehen wann und für wen?
- welche Erfahrungen wurden in den bisherigen Projekten gemacht?
- was leistet die aktuelle Standardisierung? Ist das Ende der Hersteller-spezifischen Lösungen nahe? Setzt sich ITU oder IETF durch?
- was bieten die großen Hersteller? Wie sind die aktuellen Produktlinien zu bewerten? Wer hat die Nase vorne?
- wie entwickeln sich Preise und Leistungen, sind weitere dramatische Preisveränderungen zu erwarten?
- was ist beim Betrieb einer VoIP-Lösung zu beachten?
- macht ein traditionelles Corporate Netzwerk noch Sinn?

Die Winterschule 2002 beleuchtet alle Vorteile, die eine VoIP-Lösung bringen kann:

- geringere Investitionskosten
- geringere Betriebskosten inkl. Gebühren und Arbeitsaufwand
- wesentlich vereinfachter Betrieb

- wesentlich flexiblere TK Archktektur bei verteilten Lösungen
- geringerer Aufwand zur Umsetzung von ACD und UM in kleinen Umgebungen
- Nutzung neuer Kommunikations-Funktionen

Dabei geht die Winterschule ein auf

- die technologische Basis von VoIP, insbesondere die Kernfrage der Erreichbarkeit einer standardisierten Telefonie-Lösung und einer Loslösung von den bisherigen Hersteller-spezifischen Lösungen
- die verschiedenen Einsatzszenarien von VoIP
- die bisherigen Einsatz-Erfahrungen
- die Zusatzfunktionen einer VoIP-Lösung: ACD, Unified Messaging, das Telefon als multifunktionales Endgerät, Internet-basierte Telefonie, Einsatz einer Softphone-Lösung und Video-Integration
- die Markt- und Produktrealität sowie die Wettbewerbssituation zwischen Alcatel, Avaya, CISCO, Nortel und Siemens
- den Betrieb einer VoIP-Lösung mit den Aspekten: Netzwerk-Architektur für VoIP, Überwachung und Analyse, Fehlersuche, Abrechnung von VoIP-Telefonaten, Kombination mit VPN im Internet, Verfügbarkeit und Stabilität und Stromversorgung: wie sieht die optimale Lösung aus?
- relevante verfügbare Analyse-Tools: Finisar, NetIQ, Network Associates und RADcom

Allerdings sind die Vorteile einer eine VoIP-Lösung sehr Situations-, Umgebungs- und Produkt-abhängig und erfordern eine genaue Markt- und Technologie-Kenntnis. So kann der Bedarf nach vielen Telefonen und gleichzeitig hoher Verfügbarkeit beispielsweise den Investbedarf massiv und unrentabel erhöhen. Deshalb müssen völlig verschiedene Einsatz-Aspekte einer Voice-over-IP-Lösung betrachtet werden, um für die jeweilige Situation das Optimum zu erreichen:

- die reine Voice-over-IP-Lösung
- die Hybridlösung mit einer traditionellen TK-Anlage
- die Anlagenkopplung über einen VOIP-Tunnel
- die Integration von Home-Offices und kleinen Büros
- neue Konzepte für Arbeitsabläufe, Büronutzung und Kundenkontakt
- der Einsatz der Add-on-Funktionalität ACD/UM
- neue Konzepte der Telefon-Endgerätetechnik
- die Integration mit Video

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Winterschule 2002

Ich melde mich an für die

Winterschule 2002
Voice over IP Intensiv Evaluierung

zum Preis von € 2.290,-- zzgl. MwSt.

☐ vom 02.12. - 6.12.02 in Bonn

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Name, Vorname _____ Vorname _____

Firma _____ PLZ, Ort _____

Straße _____ eMail _____

Telefon, Fax _____ Unterschrift _____

Winterschule der ComConsult-Akademie 2002 – Die Inhalte

Marktsituation und Trends
- Was treibt den Einsatz von IP Telefonie?
- Was verhindert den Einsatz von IP Telefonie?

Dipl.-Inform. Petra Borowka

Einführung in IP Telefonie
- Paketierung von Voice
- Codecs
- Komponenten: Telefone, Telefonserver, Gateways

Dipl.-Inform. Petra Borowka

Einsatz von Hardphones und "Power über LAN"
- Lösungen
- LWL zum Endgerät
- Typ 1
- Standardisierung 802.3af

Markus Schaub

Standards – ITU vs. IETF
- H.323 v1, v2, v3
- H.248 / MeGaCo • SIP
- Wichtigkeit der einzelnen Standards, Marktbedeutung
- Ersetzen Standards die Herstellerlösungen?

Dipl.-Inform. Petra Borowka

Architektur von VoIP-Anlagen und Funktionen
- Zentrale Architektur
- Dezentrale Architektur
- Basisfunktionen
- Erweiterte Funktionen
- Unified Messaging
- Call Center / ACD
- CTI

Dipl.-Inform. Petra Borowka

Softphones: Stand der Technik, Einsatzszenarien

Dr. Jürgen Suppan

Einheitliche Handhabung aller Nachrichten durch Unified Messaging
- Voice-mail, Email, Fax...
- Einsatzszenarios: Speech to Text, Text to Speech

N.N.

Voice über Internet, VoIP für SOHO, VoIP und VPN
- Technische Probleme bei Einrichtung von VoIP über Internet
- Sicherheitsaspekte
- Sichere Lösungs-Szenarien durch Einsatz von VPN für IP Telefonie

Dr. Behrooz Moayeri

Hat das Corporate Netzwerk ausgedient? VoIP in öffentlichen Netzen
- CN-Möglichkeiten
- Angebote der Carrier
- Übergang vom Enterprise zum öffentlichen Netz
- Centrex-Dienste in der BRD?

Dr. Behrooz Moayeri

Kombination von Voice und Video über IP im Netz
- Technische Anforderungen
- Streaming Video
- Desktop Video
- Raumkonferenz-Systeme

Dipl.-Inform. Petra Borowka

Architektur und Lösungsmöglichkeiten für VoIP mit Alcatel
- Sanfte Migration
- Aktueller zentraler Ansatz: OmniPCX 4400, Enterprise 4400
- Neuer dezentraler Ansatz: Linux Server und PCX Office
- Einsatz-Szenarios von TK-Servern und Media-Gateways

Architektur und Lösungsmöglichkeiten für VoIP mit Avaya
- ScreenPhone: Der neue VIP Arbeitsplatz
- Die neue MultiVantage Architektur: Media Server und Cajun P330 als dezentrale Media Gateways
- Migration mit vorhandenen Avaya Produkten

Architektur und Lösungsmöglichkeiten für VoIP mit Cisco
- ScreenPhone: Der neue VIP Arbeitsplatz
- Flexible Anwendungen in einem Tag mit XML
- Das dezentrale Konzept des Call Managers
- Voice und Video Integration

Einsatz des Cisco Call Managers beim Rechenzentrum der Finanzverwaltung NRW
- Anforderungen
- Erforderliche Komponenten
- Leistungsmerkmale
- Ausfallsicherheit, Backup
- Wirtschaftliche Vorteile?

Karl-Heinz Hommen-Menz (RZF)

Architektur und Lösungsmöglichkeiten für VoIP mit Nortel
- Migration mit vorhandenen Nortel Komponenten
- Die neue VoIP Lösung mit Succession
- Die Small Office Lösung BCM

Architektur und Lösungsmöglichkeiten für VoIP mit Siemens
- KMU: HiPath 5000
- Von der Hicom 150 zur HiPath 300
- Von der Hicom 300 zur HiPath 4000

Realisierung einer IP Telefonie-Lösung mit Alcatel / Siemens – Anwenderbericht
- Entscheidungsgründe • Funktionen
- Projektdauer • Aufgetretene Probleme
- Vorteile

Kostenabrechnungs-Lösungen und ihre Anwendung bei IP
- Zielgruppen, Einsatz-Szenarien
- Besonderheiten bei VoIP-Lösungen

York Hauser (Aurenz Ingenieurbüro)

Monitoring und Analyse von Voice im Netzwerk
- Monitoring in geswitchten Netzen
- Messgrößen
- Überwachungs-Punkte
- Einsatzbeispiele
- Markt, Tools

Dipl.-Inform. Petra Borowka

Voice-Monitoring und Qualitätstests
- Tool-Einsatz im Betrieb: VoipPerformer von RADcom
- Tool-Einsatz vor der Voice-Implementierung: NetAlly

Karl Schuicki (Datakom)

Überwachung von VoIP Netzen
- VoiP Manager von Chariot/ NetIQ
- VoIP Assessor von Net IQ

N.N. (Netcor)

Voice Monitoring mit dem Sniffer

Thomas Hemker (Network Associates)

Design von Voice-Lösungen und erforderliches Netzwerkdesign
- Voice: Einstandort-, Zentrales und Dezentrales Mehrstandort-Konzept
- IP-Netz: Verfügbarkeit, Delay
- Enterprise Design-Beispiele

Dipl.-Inform. Petra Borowka

Quality of Service: Mit welchen Verfahren und wann sollte man QoS einsetzen?
- Diff Serv, 802.1D/p, 802.1Q Tagging
- RSVP
- Wie ist QoS für Voice-Lösungen einsetzbar?
- Wann und wo sollte QoS für Voice-Lösungen implementiert werden?

Dipl.-Inform. Petra Borowka

Der Veranstalter behält sich Änderungen im Programm vor.

Neuer Technologie Report

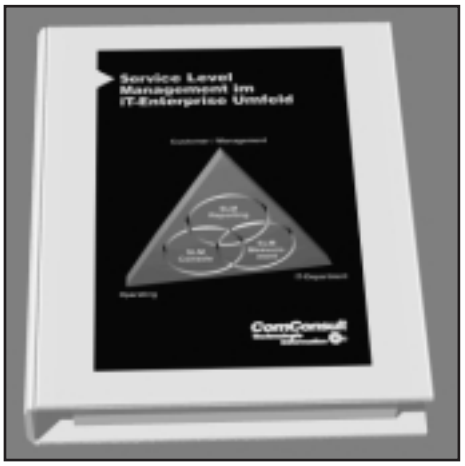
Service-Level-Management im IT-Enterprise Umfeld: Grundlagen, Auswahlkriterien, Kriterienkataloge

Produkte für Service-Level-Management unterscheiden sich erheblich. Gute und erfolgreiche Lösungen für Service-Level-Management setzen dementsprechend voraus, dass die Eigenschaften der auf dem Markt angebotenen Produkte mit allen Vor- und Nachteilen bekannt sind. Die Anforderungen an den Funktionsumfang von Service-Level-Management-Lösungen schwanken zwischen den Projekten erheblich, so dass in jedem Fall ein Mix aus geeigneten Produkten benötigt wird.

In der Regel kann kein einzelnes Produkt die bestehenden Anforderungen komplett erfüllen. Viel gute und erfolgreiche Lösungen entstehen, wenn gerade eine optimierte Kombination aus wenigen, aber sich gut ergänzenden Produkten zum Einsatz kommt.

Eine Evaluierung der angebotenen Produkte erfordert in der Regel mehrere Monate an Arbeit. Hier setzt dieser hochaktuelle Service Level Management Technologie Report an.

Der Autor hat eine Auswahl der bekanntesten SLM-Produkte der aktuellen Generation analysiert. Aufbauend auf den Anforderungen einer Reihe von Kundenprojekten wurde ein detaillierter Kriterienkatalog erarbeitet. Dieser dient unter Berücksichtigung von Hersteller- und Produktneutralität



als Entscheidungshilfe für die Auswahl derartiger Tools für den individuellen Kunden. Aufgrund der unterschiedlichen Ausrichtung der am Markt befindlichen Produkte haben wir bei der Erarbeitung des Kataloges in Kauf genommen, dass kein Produkt alle Kriterien hundertprozentig erfüllt. Mithilfe des Katalogs können aber seine aktuellen Fähigkeiten festgestellt und die jeweilige Produktausrichtung eingeschätzt werden.

Dieser Report beleuchtet die Grundlagen und Strukturen des Themas Service Level Management und ermöglicht im Folgenden eine Einschätzung der evaluierten elf Service Level Management Produkte.

Folgende Produkte wurden untersucht:

- Patrol for Service Level Management von BMC
- VitalSuite von Lucent
- Provisio von Quallaby
- Info Vista von InfoVista
- eHealth von Concord
- IBM-Tivoli Service Level Advisor
- Unicenter Service Level Management von CA
- HP OpenView Operations von HP
- Netcool von Micromuse
- Proxima Centauri Business Manager von Proxima Technology
- Formula von ManagedObjects
- IBM-Tivoli Business Systems Manager

Der Autor Dipl.-Ing. Markus Pütz ist bei der ComConsult Kommunikationstechnik GmbH im Bereich IT Enterprise Management beschäftigt. Er verfügt über langjährige Erfahrung in den Bereichen Konzeptionierung, Aufbau und Betrieb von Windows- und Unix-Netzwerken, aktive Komponenten sowie IT-Sicherheit und Service Level Management.

Der Service Level Management Report "Service-Level-Management im IT-Enterprise Umfeld: Grundlagen, Auswahlkriterien, Kriterienkataloge" ist zu beziehen über den Verlag, die ComConsult Technologie Information.

Fax-Antwort an ComConsult 02408/955-399

Reportbestellung

Ich bestelle den Technologie Report

☐ **Service Level Management**
zum Preis von € 398,--
zzgl. MwSt. und Versandkosten

_____
Unterschrift

_____
Name, Vorname

_____
Firma, Abteilung

_____
Straße

_____
PLZ, Ort

Bedingungen:

Die Ware kann nicht umgetauscht oder zurückgegeben werden. Bei Versand berechnen wir eine Gebühr von € 5,-- zzgl. MwSt. für Porto und Verpackung, bei 2 und mehr Reports € 10,-- zzgl. MwSt. (Bei Versendungen ins Ausland € 25,-- bzw. bei 2 oder mehr Reports € 30,-- zzgl. MwSt.)

Ethernet im industriellen Einsatz

Fortsetzung von Seite 1

1. Einleitung

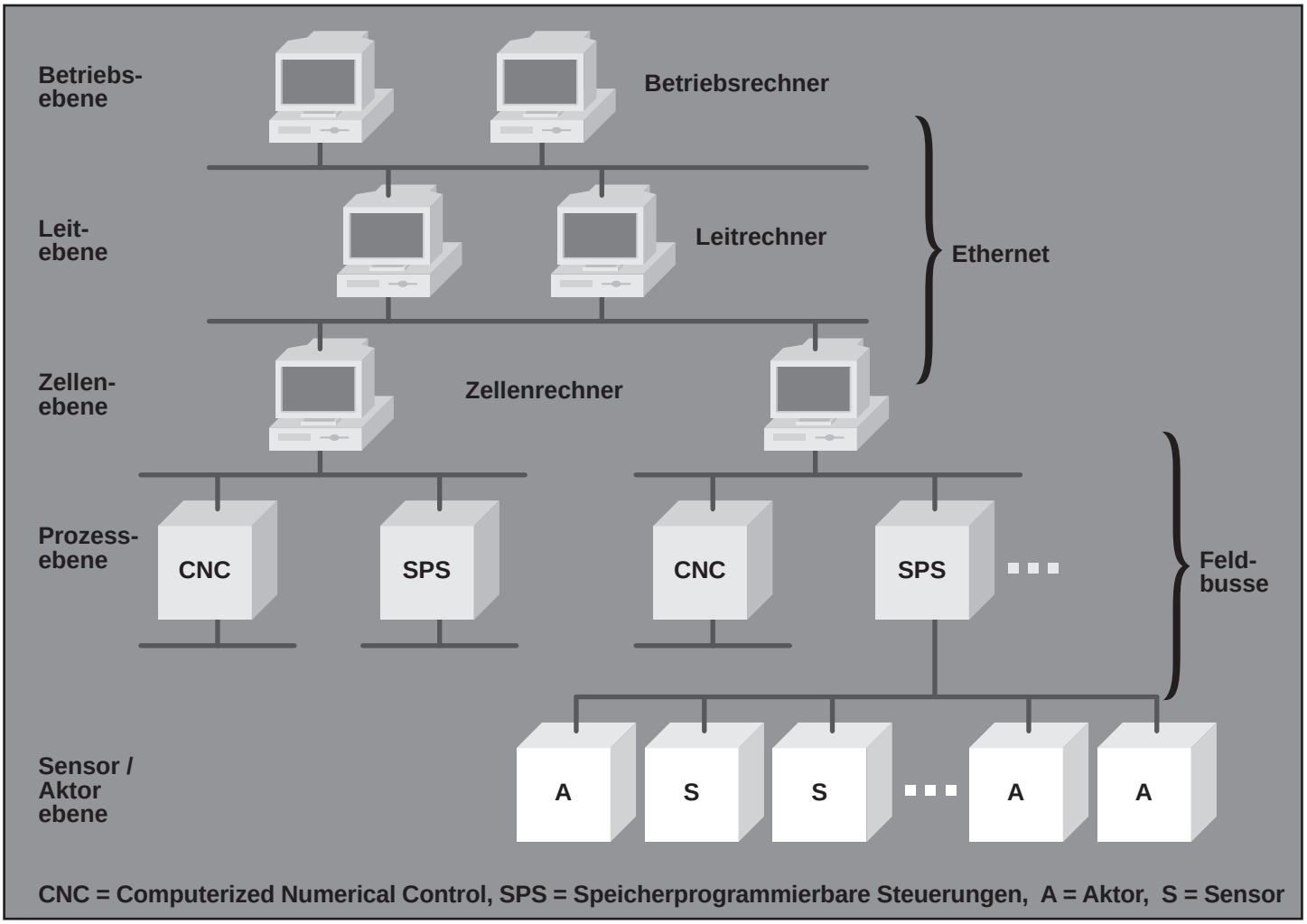
Die industrielle Kommunikation unterliegt typischerweise einer hierarchischen Vernetzung, die die so genannte Betriebs-, Leit- und Systemebenen miteinander verbindet (Bild 1). Zur Vernetzung der Rechner aus den oberen beiden Ebenen werden heute schon längst Ethernet-Netzwerke standardmäßig genutzt.

Die Systemebene gliedert sich in der Fertigung weiter in eine so genannte Prozess- und Sensor-/Aktor-Ebene. Hier befinden sich zum Beispiel rechnergesteuerte Werkzeugmaschinen (CNC), Handhabungsgeräte mit ihren Steuerungen (RC), Speicherprogrammierbare Steuerungen (SPS), die dezentral angeordnete Sensoren oder Aktoren aus den technischen Prozessen seriell anbinden, oder auch Einheiten für Betriebsdatenerfassungen (BDE). Die Vernetzung dieser Systeme erfolgt heute weitestgehend noch über die Feldbus-Technologie. Allerdings befindet sich dieser Markt stark im Umbruch, erhält nun auch Ethernet massiv den Einzug in den bisherigen Feldbus-Bereich.

Der Autor

Dipl.-Ing. Roland Moos
hat in über 10 Jahren Berufspraxis bei verschiedenen Carriern umfassende Kenntnisse in der Sprach- und Datenkommunikation erworben. Heute arbeitet er als Senior-Trainer bei der ComConsult Akademie und im Produktforschungsbereich der ComConsult Technologie Information.

Bild 1 Kommunikationshierarchie in der Fertigung



Die Feldbus-Technik brachte im Vergleich zur konventionellen 4...20 mA - Technik und deren Einzelverdrahtung (Bild 2) zwischen den Anschlusskomponenten und den Feldgeräten (sowie der Vielzahl an Anschlusskomponenten selbst) durch ihre linienförmige Verkabelung die Einsparung vieler getrennter und paralleler Punkt-zu-Punkt-Verbindungen und I/O-Komponenten mit sich, so dass im Wesentlichen geringere Hardwarekosten zum Erfolg dieser Technik beitrugen[1].

Heute sehen sich die Anwender im industriellen Umfeld aber immer noch mit einer größeren Menge herstellerspezifischer und vor allem untereinander inkompatibler Lösungen bzw. Feldbusse konfrontiert, die sich trotz Normungsaktivitäten, beispielsweise des DKE oder auch IEC, bis heute nicht völlig offen gestaltet. Somit existieren in den Produktionsstätten eher autarke (Fertigungs-)Inseln als ein einziges oder gar durchgängiges Kommunikationsnetz. Zudem ist in vielen Unternehmen wenig Wissen über solche Feldbusse vorhanden, was zu weiteren Kosten führt. Hier zu Lande besitzt sicherlich der PROFIbus von Siemens einen gewichtigen Stellenwert, es stehen aber mit Interbus, DeviceNet, Modbus, CAN, ControlNet und wie sie alle heißen mögen weitere Lösungen zur Auswahl.

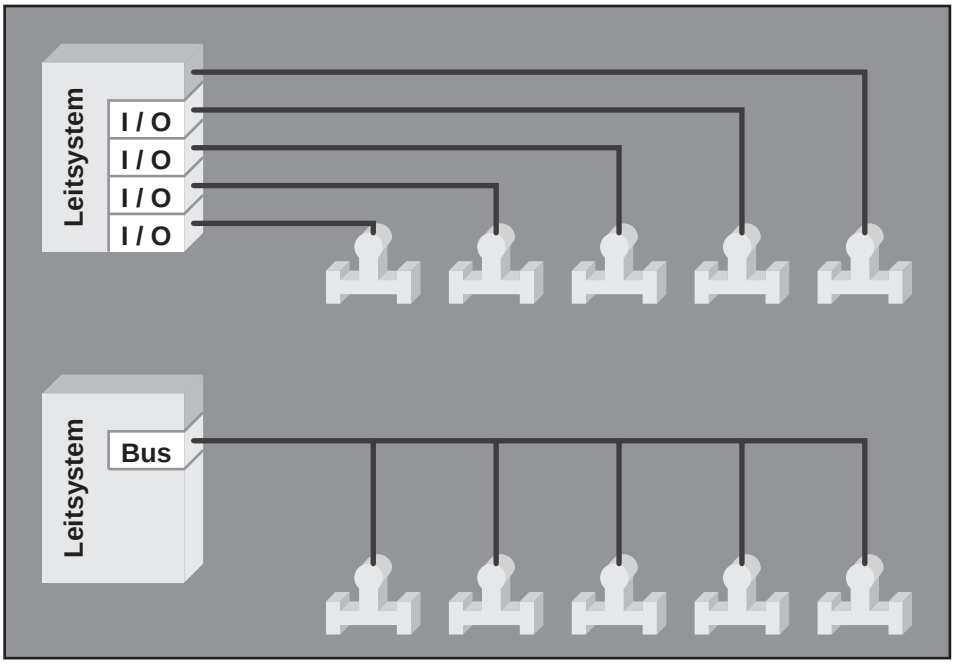
2. Warum auf einmal Ethernet in der Industrie?

Diese Frage ist so eigentlich gar nicht richtig, denn einerseits gibt es (wie zuvor beschrieben) in den Betriebs- und Leitebenen der Fertigungsindustrie heute schon Ethernet, zum anderen wird über Ethernet für den industriellen Einsatz – also in den Produktionshallen bzw. an den -maschinen – schon seit etwa Mitte der 80er Jahre diskutiert. Damals beginnend mit Untersuchungen über die prinzipielle Tauglichkeit des CSMA/CD-Verfahrens für die Automatisierung. War doch die Dominanz von IBM mit ihrem Token Ring recht groß. Schrittweise entwickelte sich Ethernet in der Industrie weiter, von redundanten Busstrukturen (um 1989) über Lichtwellenleiter in EMV-gefährdeten Umgebungen (um 1992) bis hin zum geswitchten Fast Ethernet (um 1998). Heute stellt sich diese Frage in den verschiedenen Normungsgremien oder bei den unterschiedlichen Herstellern gar nicht mehr, denn die letzten Entwicklungsschritte von Ethernet, wie die Vollduplex-Fähigkeit mit IEEE 802.3xy3 (siehe auch "Der Netzwerk Insider" Ausgabe April 2002) seit etwa fünf Jahren, die Verschiebung von "Shared Networks" hin zu "Switched Networks" über das letzte Jahrzehnt, die Erhöhung der Übertragungsrate auf 1 Gigabit und mehr sowie damit verbunden (und aus Sicht der Datennetze) auch die sehr geringe Netzverzögerung (IEEE 802.3ab & z, um 1999) wie auch die Einführung von Classes of Service (CoS) – sprich Priorisierung – führten dazu, dass auch die letzten Zweifel den Kritikern genommen und damit neue Einsatzfelder für Ethernet zugänglich wurden. Allerdings eben nur unter Beachtung neuer Regeln (später mehr).

Nicht nur die technischen Weiterentwicklungen des Ethernets selbst waren entscheidend für seinen Durchbruch, vielmehr sind es die Einsparungspotenziale, die gegenüber der Feldbus-Technik mit dem Faktor fünf bis zehn angegeben werden können. Die Gründe liegen in der seit über 20 Jahren etablierten Technik in Büroumgebungen und den damit verbunden günstigen (Port-)Kosten wie auch in der Verwendung hochgradig standardisierter Komponenten und Schnittstellen, die eine breitere Herstellerwahl nun ermöglicht. Der zeitgleich erfolgende Wechsel von Hersteller-spezifischen hin zu standardisierten Netzwerken führt weiter zu einer Integration des Netzwerk-Zugangs auf Chip-Basis und damit wiederum zu geringeren Kosten. Darüber hinaus sind die verschiedenenn Industrieunternehmen damit in der Lage variantenreichere Netzwerk-Strukturen aufzubauen und das bereits vorhandene Know How über Ethernet zu nutzen, wie auch die vielfältigen Management-Möglichkeiten der "neuen" Geräte über HTTP / Web-Browser oder SNMP. Hierüber wurden auch die Vorzüge für Diagnose, Instandsetzung, Überwachung und Reporting entdeckt. Diese Vorteile treffen alle Anbieter. Die Hersteller der Feldbusse, die damit ihre Entwicklungskosten senken können und die Hersteller kleiner Steuerungen und Anlagenlösungen, die jetzt auf preiswerte Chip-Technik aufsetzen können. Für den Anwender – also die Industrie – entstehen Vorteile durch die Nutzung einer einheitlichen und vor allem herstellerübergreifenden Kommunikationsinfrastruktur in der Fertigung.

Bedenkt man weiter, dass PCs in nahezu allen Industrieunternehmen heute zur Standardeinrichtung zählen sowie auch den hohen Verbreitungsgrad von Windows-Anwendungen, werden auch diese Standards zunehmend in der Industrie genutzt.

Bild 2 Konventionelle und Feldbus-Technik



[1] Einer NAMUR-Studie zufolge wurde die Einsparung mit rund 40 Prozent beziffert.

[2] Die Erweiterungen von Ethernet über die Zeit sind in die neueste Ausgabe der Standards IEEE 802.3 aus 2002 alle integriert worden, so dass korrekter Weise eigentlich nur noch von IEEE 802.3 gesprochen werden muss.

Ethernet allein stellt "nur" eine einheitliche und kostengünstige Übertragungstechnik bereit. Mitentscheidend ist auch die Verwendung geeigneter Kommunikationsprotokolle, wie es heute de-facto nur die TCP/IP-Protokolle in der Büro-Welt darstellen sowie geeignete Anwendungsprotokolle. Ethernet und TCP/IP läuten den Umbruch in der industriellen Kommunikation ein. Getrieben durch die Anwender sieht sich auch die Normung gezwungen, schnell zu reagieren und geeignete Vorschläge zu erarbeiten.

3.
Die Varianten

Ein einheitliches Standard-Anwendungsprotokoll unter dem Namen "Industrial Ethernet" gibt es heute noch nicht. Getrieben aus der Feldbus-Ecke existieren auch für die "Ethernet-Variante" eine Vielzahl verschiedener Ansätze, die wiederum alle untereinander inkompatibel sind. Das ist auch der Grund, weshalb sich beispielsweise gegen Ende 1999 die IAONA Europe (heute IAONA e.V.) gegründet hat. Sie sieht sich heute selbst als Dachorganisation für industrielle Kommunikation speziell in den Bereichen Fabrikautomation, Prozessautomation und Gebäudeautomation und verfügt mit den Organisation IDA-Group und ODVA (Open DeviceNet Vendor Association) über ein "Memorandum of Understanding", um gemeinsam Strategien für die weitere Entwicklung von Ethernet-basierten Automatisierungsprodukten voranzutreiben. Allerdings werden deren Bemühungen von der Profibus Nutzerorganisation e.V. (PNO) etwas kritisch betrachtet, denn weder Siemens noch die PNO selbst zählen zu deren Mitgliedern.

Auf dem "Industrial Ethernet"-Markt tummeln sich derzeit im Wesentlichen die Ansätze PROFInet (Siemens), Ethernet/IP (ODVA, CI, IEA), Modbus/TCP (Schneider Electric), IDA (IDA-Group) oder Ethernet Powerlink (B&R Automation), wobei es mit Interbus on Ethernet, CANopen, HSE (Foundation Fieldbus), SafeEthernet usw. ein schier unerschöpfliche Liste weiterer Lösungen gibt.

Allen gemeinsam ist zunächst nur die Tatsache, dass sie alle Protokolle auf Anwendungsebene darstellen, bezogen auf das OSI-Referenzmodell eben den Schichten 5 bis 7 zugeordnet werden können. Außerdem setzen sie alle auf das Standard-Ethernet nach IEEE 802.3 auf. Neben den Protokollspezifika unterschieden sich die Ansätze aber auch bei den Kommunikationsprotokollen. Hier setzen sie entweder auf die Standard-Protokolle TCP, UDP und IP auf, wie z.B. PROFInet, Modbus/TCP oder Ethernet/IP oder definieren eigene Stacks, wie es bei Ethernet Powerlink beispielsweise der Fall ist (und für Echtzeit-Kommunikation auch notwendig erscheint).

PROFInet

PROFInet stellt gegenwärtig sicherlich noch kein "PROFIbus on Ethernet" dar, da Feldgeräte weiterhin am PROFIbus angeschlossen und derzeit lediglich über eine Ethernet-Schnittstelle angesprochen werden. Allerdings definiert PROFInet einen Standard zur herstellerneutralen Integration verschiedener Automatisierungssysteme. Für zeitunkritische Kommunikation stützt sich PROFInet auf das Industrial Ethernet. Dabei werden die Remote Procedure Calls (RPC) über TCP/IP übertragen. Für zeitkritische Kommunikation (Echtzeit-Anwendungen) werden PROFIbus Segmente (Feldbusse) weiterhin eingesetzt. Über so genannte Proxies lassen sich dann aber auch Feldbusse anderer Hersteller in das Gesamtsystem integrieren.

Ethernet/IP

Im Gegensatz zu PROFInet werden bei diesem Ansatz tatsächlich die Feldbus-Komponenten von DeviceNet bzw. der Schwester ControlNet durch Ethernet ersetzt. "IP" steht hier nicht für "Internet Protocol", sondern für "Industrial Protocol". Im Vergleich zu anderen Ansätzen wird Ethernet/IP von drei Organisationen unterstützt, nämlich ControlNet International (CI), der Industrial Ethernet Association (IEA) sowie der Open DiveNet Vendor Association (ODVA).

Bild 3 Schematische Zuordnung verschiedener Ansätze

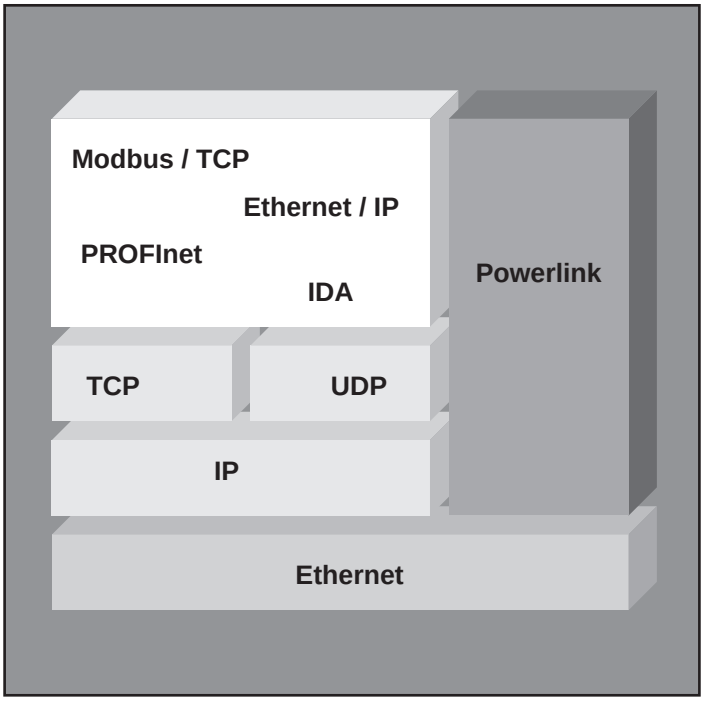
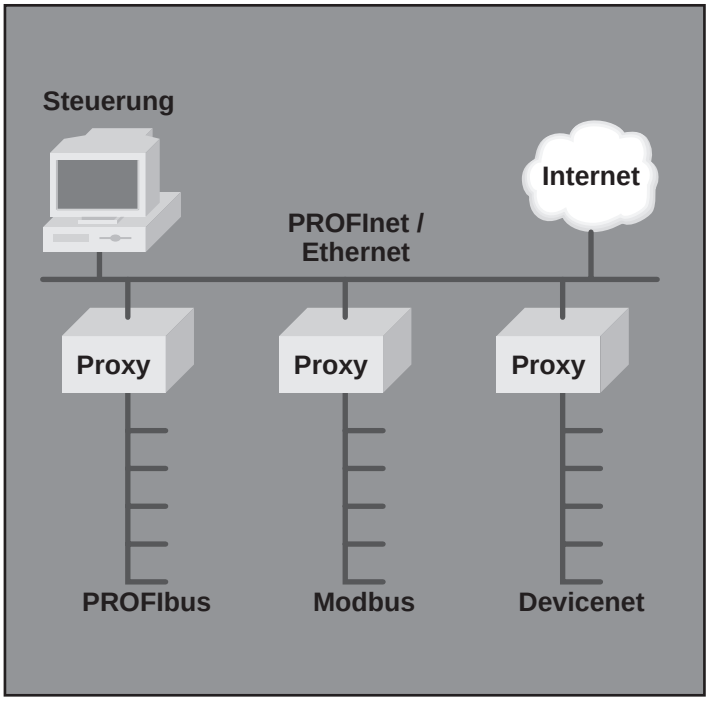


Bild 4 PROFInet



Zu letzterer Organisation hat sich kürzlich auch CISCO System angeschlossen, was das zunehmende Interesse auch der klassischen Netzwerkspezialisten an Industrial Ethernet unterstreicht (geht es doch hier um einen nicht gerade kleinen Markt)[3]. Auch bei Ethernet/IP lässt sich eine gewisse Form von "Investitionsschutz" erkennen. Es wird nämlich das Control and Information Protocol (kurz CIP) aus DeviceNet bzw. ControlNet in die neue "Ethernet-Welt" überführt. Damit wurden das gesamte Objektmodell wie auch die Gerätefiles übernommen (Bild 5). Somit sind die Protokollprinzipien bei Ethernet/IP, DeviceNet und ControlNet identisch. So genannte Explicit Messages enthalten bei CIP die Instruktionen. Geräte müssen diese Nachrichten interpretieren, ausführen und Antworten generieren. Dieser Nachrichtentyp dient der Gerätekonfiguration sowie der Diagnose und wird gesichert in TCP übertragen. Der zweite Nachrichtentyp sind die so genannten Implicit Messages, welche wegen ihrer Echtzeit-Anforderung über UDP übertragen werden. Im Datenfeld gibt es dabei keine Protokollinformation, lediglich I/O Daten. Zur letztlichen Übertragung über ein Ethernet-Netzwerk werden von Ethernet/IP die herkömmlichen Standard-Chipsätze verwendet. Dadurch, dass die Anwendungsschicht mit ihren Geräteprofilen wie auch dem Objektmodell sowohl bei den Feldbussen DeviceNet bzw. ControlNet als auch bei der Ethernet-Variante identisch sind, wurde bei diesem Ansatz die Interoperabilität angestrebt.

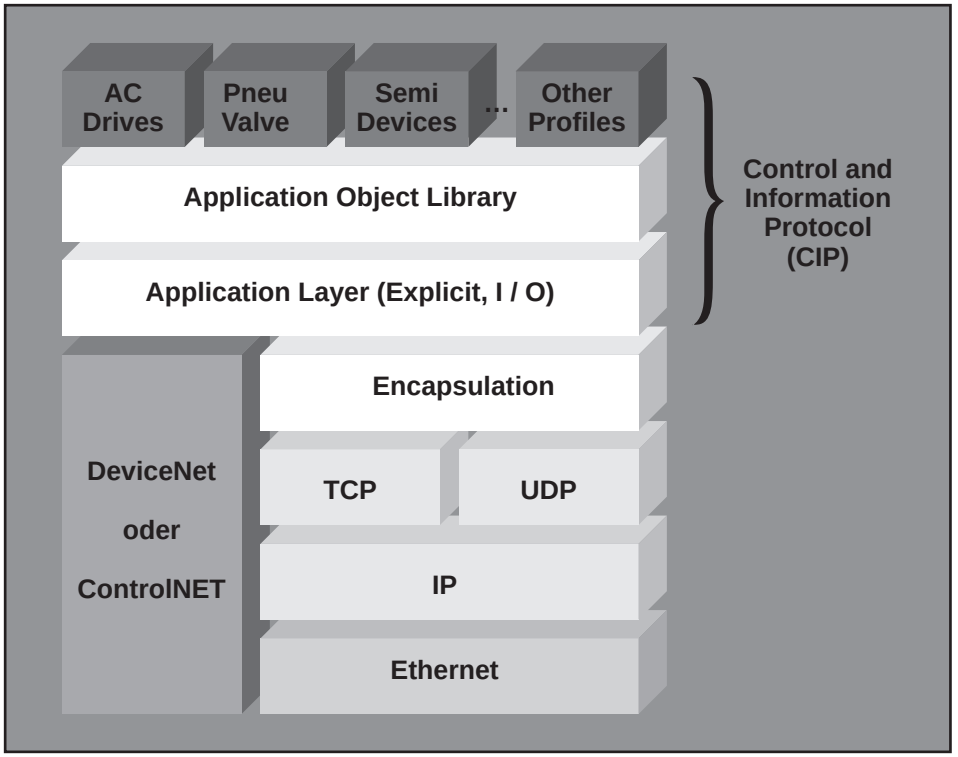
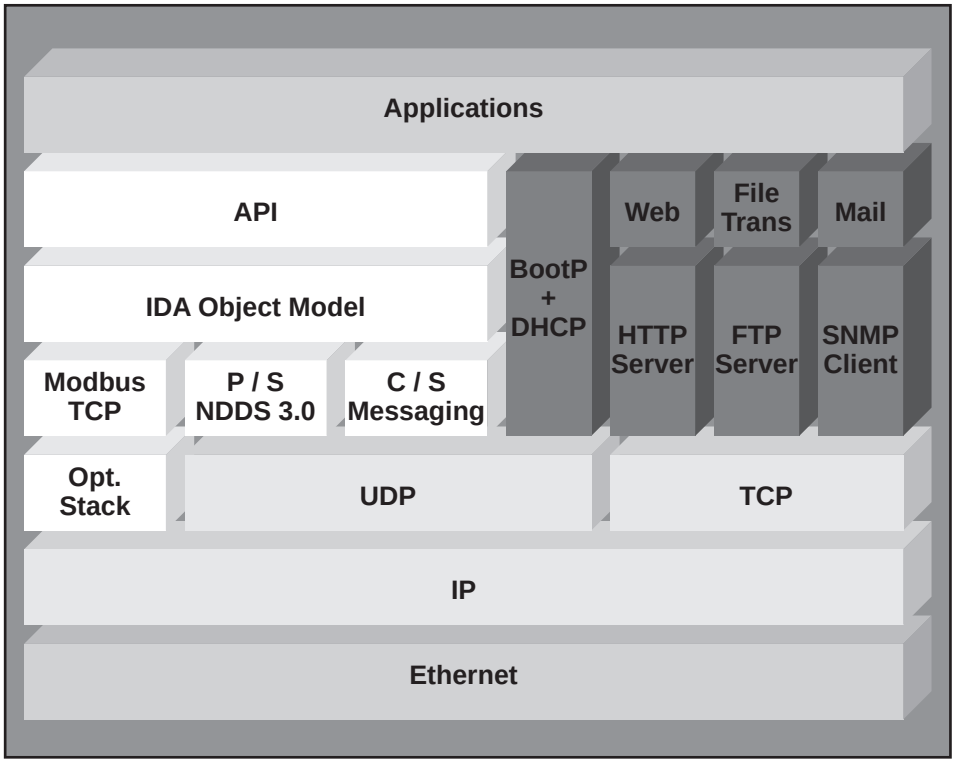


Bild 5 Architektur Ethernet/IP (Quelle: ODVA)

Bild 6 IDA und Modbus / TCP (http://ethernet.industrial-networking.com)



Modbus/TCP

Dieser Ansatz (ursprünglich von Schneider Electric spezifiziert) stellt wohl das einfachste auf Ethernet-basierende Protokoll dar, weil es das bekannte Modbus-Protokoll lediglich in TCP/IP Paketen überträgt und daher weit verbreitet ist. Dies hat übrigens auch die IDA-Group erkannt, so dass Modbus TCP nach einer Zusammenarbeit mit der Modbus User Group als Teil des IDA Standards unterstützt wird. Im Gegensatz zu anderen Lösungen handelt es sich hier nicht um einen objekt-orientierten Ansatz, sondern um das Master/Slave- Prinzip. Der Master sendet beispielsweise seine Ausgangsdaten, der Slave antwortet mit seinen Eingangsdaten. Das ganze ist – wie schon gesagt – recht einfach und verwendet dabei die Protokollmechanismen von TCP, wie Flusskontrolle, Quittierung und Retransmission.

[3] Den Beitritt von CISCO Systems sieht man innerhalb der ODVA mit gemischten Gefühlen. Bisher wurde DeviceNet von Rockwell Automation (einer der drei großen Player neben Siemens und Schneider Electric) dominiert und mit CISCO wir hier ein Gegenpol erwartet, andererseits besteht die Sorge, dass die ODVA künftig "CODVA" heißen könnte.

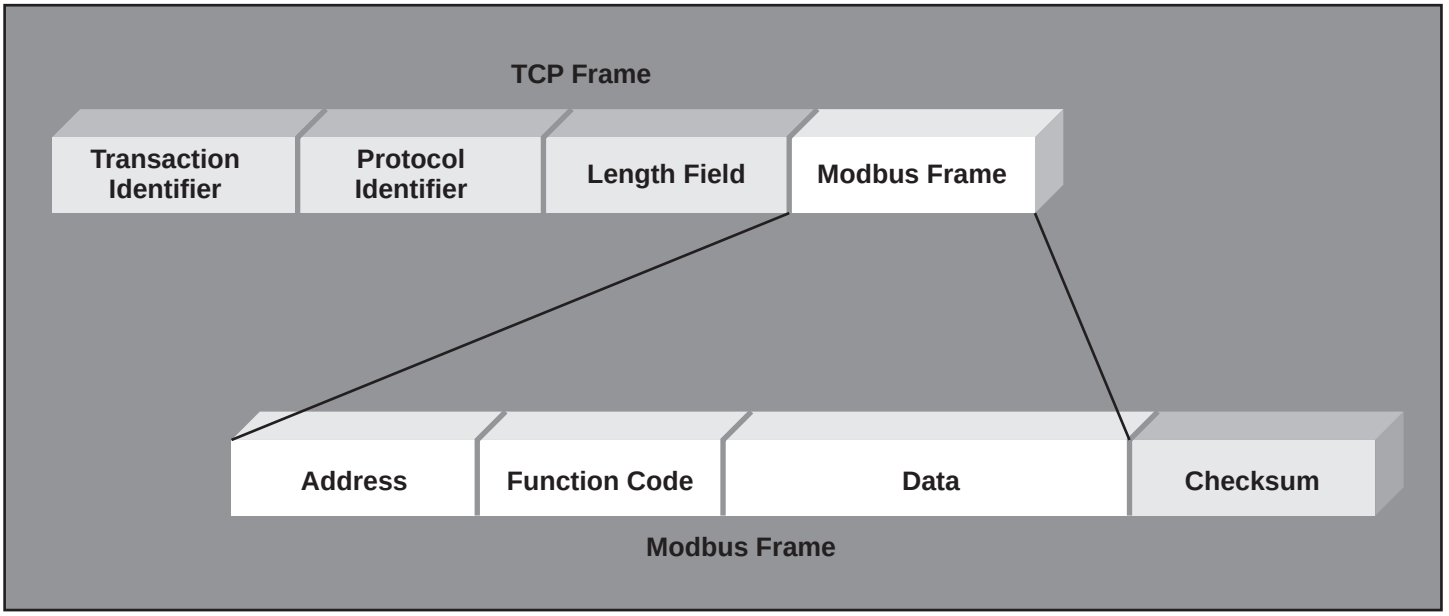


Bild 7 Encapsulation bei Modbus/TCP

Eine Modbus/TCP Nachricht enthält die Adresse des Slave, ein Kommando (z.B. lese Register) sowie Daten und eine Checksumme (LRC oder CSC). Weil das Modbus-Protokoll eine reine Messaging Struktur hat, ist es eigentlich unabhängig von der Übertragungstechnik, so dass es traditionell über serielle Schnittstellen, wie RS 232, RS 422 oder RS 485 und über verschiedene Kabeltypen übertragen werden konnte.

Die Modbus/TCP Spezifikation kann frei unter http://www.modbus.org geladen werden.

IDA

Die Spezifikationen zu dieser Variante sind bei der IDA ebenfalls frei zugänglich und befinden sich seit kurzem auch auf dem Server der ComConsult-Akademie im Network Professional Club unter www.comconsult-akademie.de.

Hinter diesem Ansatz steht eine so genannte verteilte Intelligenz für die Industrie-Automation basierend auf Ethernet- und Web-Technologien. Verteilt deshalb, weil man entsprechend der IT-Welt verteilte Geräte, Tools und Applikationen so "unter einen Hut" bringt, dass sie wie eine einzige zentrale Anwendung agieren. Dabei kann jedes Gerät im System auf alle Objekte (auch Software) zugreifen (Horizontale Integration) wie auch alle Geräte, Tools oder Applikationen in beiden Richtungen mit einem Intranet oder dem Internet kommunizieren (Vertikale Integration). Letzteres bedeutet die Schnittstelle zwischen Produktions- und IT-Welt. Ethernet und TCP/IP bilden dabei "lediglich" die Kommunikationsplattform, denn IDA ist weit mehr als ein "Protocol on Ethernet".

Dieser Anspruch wurde zunächst auf eine zentrale Schnittstelle gestützt, derer sich alle Hersteller bedienen können. Darauf basierend spezifizierte die IDA verschiedene Modelle (Architektur-, Kommunikations-, Web-Technologien oder Safety-Modell), so dass sich Software und Komponenten verschiedener Hersteller in einem gemeinsamen Netzwerk betreiben lassen. Auf Anwendungsebene befindet sich ein Objektmodell, durch das die gesamte Anlage beschrieben wird.

Wo immer möglich setzt IDA auf bereits existierende Standards, wie eben IP, UDP, oder TCP, aber auch HTTP, FTP oder SNMP. Die Echtzeit-Kommunikation geschieht mittels einer Middleware und dem User Datagram Protocol (UDP).

4. Anforderungen an industrielle Netzwerke

Um die zuvor angesprochenen Anwendungen der Feldbus-Ebene auf einem Industrie-tauglichen Netzwerk verfügbar zu machen, stellen die neuen Anforderungen der Automation eine große Herausforderung für die klassischen Netzwerk-Hersteller dar.

Im Wesentlichen sind dies die Anpassungen an die rauen Betriebsbedingungen unter Staub, Schmutz (z.B. Öle), Vibrationen oder höheren Temperaturen (auch Temperaturschwankungen) und vor allem der Aspekt der Verfügbarkeit, denn Ausfälle bedeuten in der Produktion enorme Verluste.

Verkabelung

Zunächst einmal stellt sich für die Fertigungsbereiche (Produktionshallen und -maschinen) die Frage, welche Normen der Industrieverkabelung zugrunde gelegt werden sollen. In Büroumgebungen hat sich die europäische Norm EN 50173 (hier zu Lande DIN EN 50173) für strukturierte Verkabelungen etabliert, die eine anwendungsneutrale Verkabelung baumartig in drei Hierarchiestufen (Primär-, Sekundär- und Tertiärbereich) definiert.

Neben der Topologie wird darin aber auch die Leistungsfähigkeit der Kabelstrecken sowie Stecker selbst beschrieben. Diese Norm beschränkt allerdings selbst ihren Gültigkeitsbereich auf Büroumgebungen und ist in ihrer heutigen Ausprägung nicht einfach auf Industrieumgebungen übertragbar; macht teilweise sogar gar keinen Sinn.

So geht die Norm beispielweise von einer rein hierarchisch-sternförmigen Struktur aus, dabei sind Etagenverteiler für jede Etage und einer Versorgungsfläche von 1.000 qm einzuplanen.

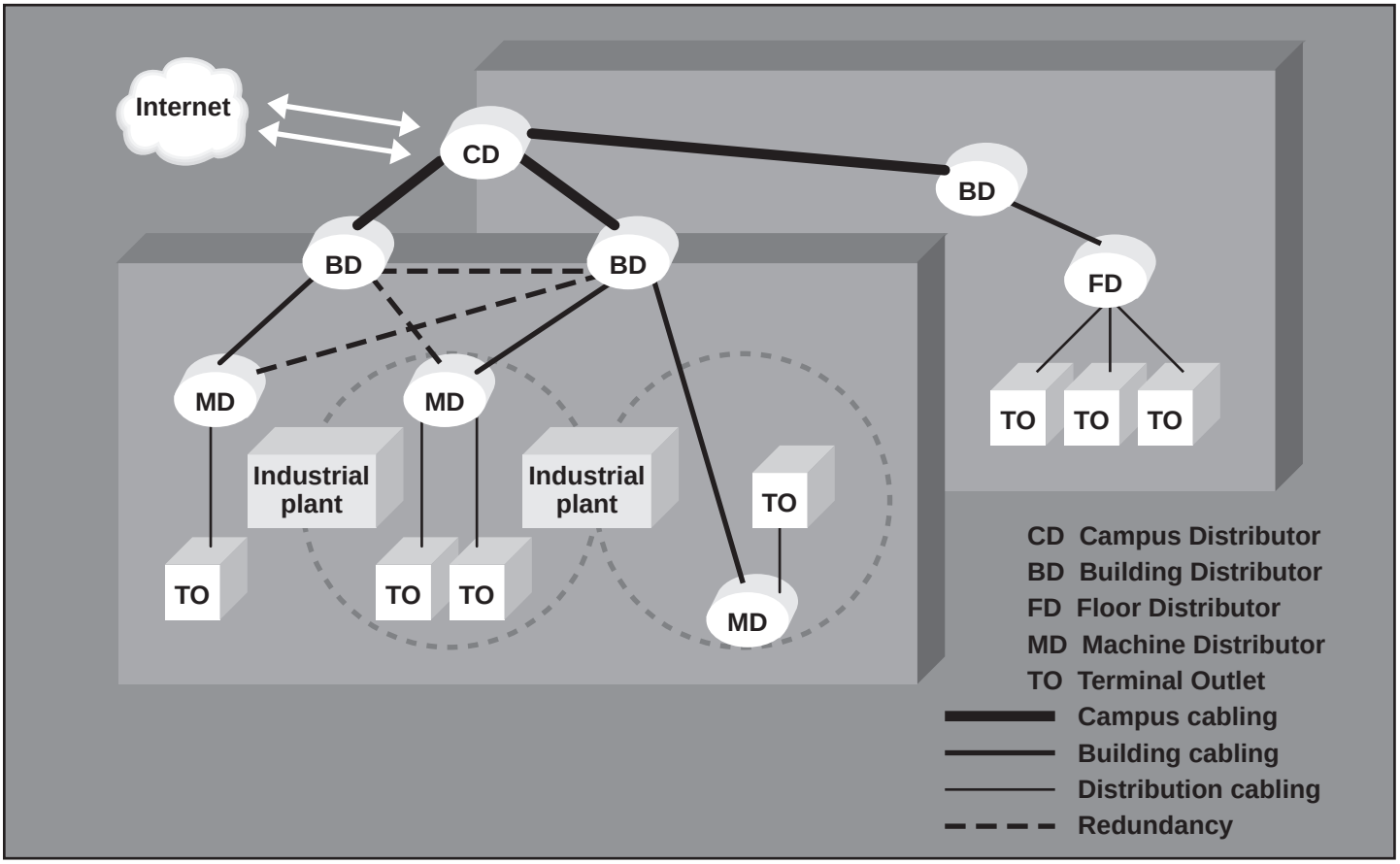


Bild 8 Industrielle Verkabelungsstruktur (Quelle: IAONA Draft)

In den Fertigungsumgebungen (in der Regel Hallen) gibt es aber auf der einen Seite keine Etagen. Auf der anderen Seite sind die zu versorgenden Flächen viel größer, so dass andere Distanzen zu überbrücken sind, was heute in den Fertigungsbereichen durch linienförmige Strukturen gelöst wird. Zudem sind geringere Anschlussdichten vorhanden, die einen klassischen Verteiler gar nicht erfordern. Deshalb müssen neue Spezifikationen für die Industrieanwendung her, die sich aber auf die vorhandene EN 50173 stützen.

So hat die IAONA am 8. November 2001 einen "Planning and Installation Guide" der Öffentlichkeit als Draft[4] vorgestellt, der die EN 50173 auf die Industrie quasi "umsetzt" (Bild 8) und dieses Jahr sogar der IEC zur Normung eingereicht wurde.

Demnach sind prinzipiell die seit 1995 eingeführten Strukturen (Primär-, Sekundär- und Tertiärbereich) für die Industrie verwendbar, allerdings musste der Tertiärbereich und insbesondere der "Etagenverteiler" neu definiert werden. Damit werden in den Produktionshallen auch linienförmige Strukturen möglich, ja sogar unter Verwendung von Hubs und Switches in Beispielen beschrieben.

Daneben ist der Planungshorizont für Büroverkabelungen ein anderer: Verkabelungen werden hier auf eine Nutzungsdauer von mindestens 10 Jahren ausgelegt, was eine hohe Qualität der Kabel und vor allem Leistungsreserven voraussetzt. Demnach wird eine Büroverkabelung zukunftsorientiert geplant, man denke beispielsweise an Gigabit am Arbeitsplatz oder Multimedia-Anwendungen, wie Business-TV/CATV.

Leistungsreserven und eine gut durchdachte Vorverkabelung (denn nichts ist teurer als nachträglich Kabel einzuziehen) spielen in der Fertigung weniger eine Rolle. Hier wird bedarfsgerecht geplant, da Produktionshallen nicht selten umgestaltet werden. Also wo sollte man Dosen (TOs in Bild 8 genannt) fest vorplanen? Außerdem kann eine Fertigungshalle als eher "schwach besiedelt" (geringe Anschlussdichte) beschrieben werden und die zu übertragenden Datenmengen sind bei weitem nicht so hoch (geringer Kapazitätsbedarf). Modulare Switches mit über 300 Ports sind hier also kein Thema, ebenso wenig Übertragungsraten von 10 Gigabit, wozu heute in der IEEE die Standards gerade verabschiedet werden.

Die Spezifikationen zu den Übertragungseigenschaften der Kabel unterschieden sich zwischen Büro- und Industrieanwendung kaum. Allerdings bedeutet eine Industrieverkabelung heute den Einsatz symmetrischer Kupferkabel (Twisted Pair), und genau hier entsteht dann ein Problem durch die Beschränkung der Kabellänge auf 100 Meter. Führt man sich wiederum die Ausdehnung einer Produktionshalle vor Augen, so wird erneut klar, dass nur Linienstrukturen in Frage kommen. Von daher ist das ein weiterer Grund, warum Industrie-taugliche Switches nur mit einer geringen Portzahl benötigt werden.

[4] Am 28. 10. 2002 wurde aus dem Draft ein Release 1.0, der in der nächsten Sitzung am 7. 10. 2002 verabschiedet werden soll

	Schutz gegen Berührung	Schutz gegen Fremdkörper
0	kein Schutz	kein Schutz
1	großflächigen Körperteile (z.B. Handrücken)	große Fremdkörper (Durchmesser > 50 mm)
2	Finger	mittelgroße Fremdkörper (Durchmesser > 12 mm)
3	Werkzeuge und Drähte (Durchmesser > 2,5 mm)	kleine Fremdkörper (Durchmesser > 2,5 mm)
4	Werkzeuge und Drähte (Durchmesser > 1 mm)	kornförmige Fremdkörper (Durchmesser > 1 mm)
5	vollständiger Berührungsschutz	Staubablagerung
6	vollständiger Berührungsschutz	Staubeintritt

Tabellen 1 (oben) und 2 (Mitte) IP Schutzklassen

0	kein Schutz
1	Schutz gegen senkrecht fallendes Tropfwasser
2	Schutz gegen schräg (bis 15°) fallendes Tropfwasser
3	Schutz gegen Sprühwasser (bis 60°) gegen die Senkrechte
4	Schutz gegen allseitiges Spritzwasser
5	Schutz gegen Strahlwasser
6	Schutz gegen starkes Strahlwasser
7	Schutz gegen zeitweiliges Untertauchen
8	Schutz gegen dauerndes Untertauchen

Nicht die altherbekannten Übertragungseigenschaften der Kabel sind als kritisch zu bewerten, es sind vielmehr die physikalischen Eigenschaften, denn in der Fertigung gibt es je nach Industriezweig stärkere Temperaturschwankungen, aggressive Stoffe in der Umgebung oder eine hohe Feuchtigkeit, die dementsprechende Anforderungen an den Außenmantel der Kabel (und auch der Stecker) stellen. In der Nähe von Maschinen wird zudem eine Schleppkettenfähigkeit vorausgesetzt, was heute noch mit vieradrigen Kupferkabeln gelöst wird. Vier Kabeladern bzw. zwei Leitungspaare bedeuten aber eine Begrenzung der Übertragungsrate auf 100 Mbit/s, denn Kupfer-basiertes Gigabit Ethernet benötigt heute acht Kabeladern bzw. 4 Leitungen. Dementsprechend sind die heute entwickelten vierpoligen Stecker als bedenklich einzustufen, wird damit ein späteres "Upgrade" auf Gigabit Ethernet nicht ohne weiteres möglich (man denke an die Verfügbarkeit geeigneter Chips!). Ferner stellen sich heute Kategorie 5-Kabel für die Fertigung (noch) als ausreichend dar, denn wie gesagt, höhere Übertragungsraten werden aufgrund der geringen Datenmengen gar nicht benötigt. Allerdings stellt dieser Zustand ein Problem für das Thema "Echtzeit-Anforderungen" (siehe später) dar, denn je höher die Sendegeschwindigkeit (und das wäre bei Gigabit um den Faktor 10 der Fall), desto schneller gelangen die Daten auf ein Kabel und desto geringer wird die (Netz-)Verzögerung.

Besonderes Augenmerk muss bei der Planung von Industrie-tauglichen Netzwerken auf die elektromagnetische Verträglichkeit (EMV) und das Erdungskonzept gelegt werden, denn die Störfelder durch die Stromversorgung der Anlagen sind nicht zu vernachlässigen. Gut geschirmte Kupferkabel stellen hier ein Muss dar, wobei das Problem der Erdung vielfach besteht, denn überwiegend werden unterschiedliche Potenziale in einer Fertigungshalle vorgefunden.

Bei den Steckern zu einer Industrietauglichen Verkabelung gibt es heute - neben der Poligkeit - noch eine weitere Unsicherheit. Entweder erfüllen die Stecker nicht einmal die Kategorie 5, wenn sie von ihrer Konstruktion her für die Industrieumgebung geeignet erscheinen (z.B. M12), oder sie sind eben nicht in der rauen Umgebung einer Maschine einsetzbar (Stichwort Schmutz und Korrosion). Der allseits bekannte RJ45-Stecker (IEC 60603-7) spielt auch hier wieder eine wichtige Rolle, denn heute werden meist Standardkabel und -komponenten eingesetzt. Die Firma Phoenix Contact beispielsweise bietet hier ein Schutzgehäuse für einen herkömmlichen RJ45-Stecker. Eine endgültige Festlegung gibt es aber derzeit nicht.

In geeigneten Schaltschränken ist dieses Manko nicht so problematisch, direkt an Maschinen aber ist die Schutzklasse IP67 (Tabellen 1 und 2) zu erfüllen. Und hierin liegt eben das Problem.

Es liegt also auf der Hand, nicht für jede Umgebung einen neuen Stecker zu entwerfen. Von daher konzentrieren sich auch die Normungsbestrebungen auf derzeit zwei Kategorien für elektrische Stecker: Schutzklasse IP20 plus Vibrations- und Schockbelastungen für Schaltschrankanwendungen und Schutzklasse IP67 mit zusätzlichen Forderungen für stark verschmutzte Bereiche.

Aktive Komponenten

In den Produktionshallen werden heute überwiegend noch "Büro-Produkte" à la CISCO, Nortel oder Enterasys usw. eingesetzt. Um den Umgebungsbedingungen gerechter zu werden, werden zudem diese Switches einfach in Verteilerschränke entsprechender Schutzklassen (siehe oben) gepackt. Gründe liegen zur Zeit in der fehlenden Verfügbarkeit Industrie-tauglicher Produkte, wie beispielsweise von Hirschmann Electronics. Denn müssen aktive Komponenten gar in die Nähe von Maschinen aufgestellt werden, kommt hier die Schutzklasse IP 67 zum Tragen, wofür Büro-Produkte heute nicht gebaut sind.

	Büro-Welt	Produktions-Welt
Temperatur	5 - 40°	0 - 55°
Stromversorgung	230 V Wechselstrom	24 V Gleichstrom
Montage	19" Schrank	Hutschiene, Wand
Kühlung	Lüfter	Kühlkörper
Schutzlasten	IP 20	IP 20 / IP 67
Beständigkeit	Staub	Öl, Staub, Schmutz ...
Nutzungsdauer	> 3 Jahre	> 6 Jahre
Rekonfigurationszeit	< 1 Sekunde	< 30 Sekunden

Tabelle 3 Vergleich Büro-Welt mit Produktions-Welt

Auch lässt sich der zuvor beschriebene Aspekte "Linienstruktur" hier wieder aufgreifen, denn genau eben diese Linienstruktur erfordert Switches mit wenigen Ports. Da diese dann auf Hutschienen montierbar sein müssen und zudem in der Industrie gängigerweise mit 24 Volt Gleichspannung versorgt werden, ist mit dem Einsatz von Büro-Produkten Schluss. Industrie-taugliche Switches sind daher "im Kommen" und werden zunehmend eingesetzt.

Die Tabelle 3 verdeutlicht noch einmal die Unterschiede zwischen Büro- und Industrie-Switches; geeignete Produkte befinden sich (von Ausnahmen abgesehen) noch in den Roadmaps der Hersteller für 2003 oder gar später.

Das Thema "Verfügbarkeit"

Neben den Umgebungsbedingungen (Schmutz, Temperatur, Schock, Vibration, Feuchtigkeit) stellt die Ausfallsicherheit des Netzwerkes die offensichtlichsten Unterschiede zwischen Büro und Industrie dar.

Hier besteht das Ziel einerseits in einer einfachen Lösung à la Plug-and-Play, die andererseits äußerst stabil sein muss, denn die Anwender möchten produzieren und sich weniger über die Administration oder gar ein proaktives Management ihres Netzwerkes Gedanken machen müssen. Kommen in Datennetzen Informationen nicht an, werden sie einfach wiederholt. Geschieht dies in Industrienetzwerken, kann zum Beispiel ein Schweißroboter die erforderliche Information nicht erhalten und dies kann Auswirkungen auf die gesamte Fertigungsstraße haben.

Beides scheint zunächst einen Widerspruch darzustellen, denn die klassischen Redundanzverfahren auf OSI-Ebene 2 (Spanning Tree) setzen nicht nur Bridging bzw. Switching voraus, sondern wollen auch gemanagt werden. Redundanzmechanismen ohne Überwachung sind kaum sinnvoll, denn hat beispielsweise ein Komponentenausfall stattgefunden und sich auch ordnungsgemäß das Netzwerk rekonfiguriert, besteht durch den Gebrauch der Backup-Wege jetzt zum einen keine Redundanz mehr und zum anderen würde der Anwender es nicht einmal merken.

Industrie-taugliche Switches realisieren hierfür Meldekontakte, worüber auf einfache Weise dem Anwender ein Fehlerzustand angezeigt werden kann (und sei es auch nur durch das "Aufleuchten einer Lampe").

Der Aspekt der Stabilität ist momentan noch der Grund, warum sich ein "drahtloses Ethernet" (WLANs nach IEEE 802.11b) "nur" in den Evaluierungen vieler Anwender befindet. Trotzdem deuten die Bestrebungen auch in diese Richtung, konzentriert sich die Normung mittlerweile nicht mehr ausschließlich auf das "drahtgebundene Ethernet" nach IEEE 802.3.

Zurück zum eigentlichen Thema: bei Betrachtung der Ausfallsicherheit eines Ethernet-Netzwerkes kommt den Redundanzverfahren eine große Bedeutung zu, wie auch vorausgehend der Abbildung redundanter Strukturen bei der Verkabelung.

Verfahren wie OSPF oder VRRP/HSRP spielen heute in Industrienetzwerken (noch?) keine Rolle, basieren doch die heutigen Industrienetzwerke auf so genannten "flachen" 10 Mbit/s-Strukturen, also rein auf Layer 2-Techniken (mit Switches). Würden Layer-3 fähige Geräte eingesetzt, wäre wiederum der Komplexitätsgrad für die Fertigung zu hoch, folgt man dem vorhergehenden Argument des "Plug-and-Play".

Also kommt zunächst nur Spanning Tree (STP) nach IEEE 802.1D in Frage, das aber in seinen Umschaltzeiten – je nach Einstellung der Parameter – kaum unter 30 Sekunden reicht, sieht man von herstellerspezifischen Lösungen, wie beispielsweise Resilient Link von 3Com, einmal ab. Umschaltzeiten in dieser Größenordnung gelten im Produktionsprozess als völlig inakzeptabel. Hier liegt die obere Grenze bei etwa einer Sekunde. Folglich kommt die neueste IEEE-Variante mit dem Rapid Spanning Tree (IEEE 802.1w) zunächst nur in Betracht. Mit seinen Änderungen und Erweiterungen gegenüber dem Classical Spanning Tree kann hier diese Industrie-Forderung grundsätzlich erfüllt werden, vorausgesetzt die eingesetzten Switches unterstützen diesen.

Aufgrund dieser Schwierigkeiten haben die Firmen Siemens und Hirschmann gemeinsam den so genannten HIPER-Ring entwickelt, für den beide Firmen sogar ein Patent halten und damit auf dem Markt für ihre Lösungen quasi ein Alleinstellungsmerkmal genießen. Dieser unterstützt einerseits die bestehende linienförmige Verkabelung (ergänzt um eine zusätzliche Leitung) in der Fertigung (denn eine hierarchische und baumartige Verkabelung ist der Industrie noch neu) und andererseits die Anforderungen bzgl. der Umschaltzeiten, welche maximal 500 ms beträgt. Jedoch handelt es sich hier um eine proprietäre Lösung und damit um keinen Standard.

Der HIPER-Ring wird in den Fertigungsbereichen mit Hilfe von RS2- oder MICE-Geräten zu je einem Ring aufgebaut. Mehrere Fertigungs(teil)bereiche können über einen HIPER-Ring Backbone miteinander verbunden werden. Gigabit Ethernet wird (im Backbone) ebenso untertsützt wie die Möglichkeit zum weiteren Ausbau der Verfügbarkeit etwa durch Dual-Homing (Anbindung über zwei verschiedene Geräte an die nächst höhere Netzwerkebene) oder Doppelringe.

Die maximale Umschaltzeit beträgt – laut Herstellerangabe – dabei maximal 500 ms, wobei diese (wie beim Spanning Tree Algorithmus) unabhängig der angeschlossenen Gerätezahl (maximal 50) erfolgt.

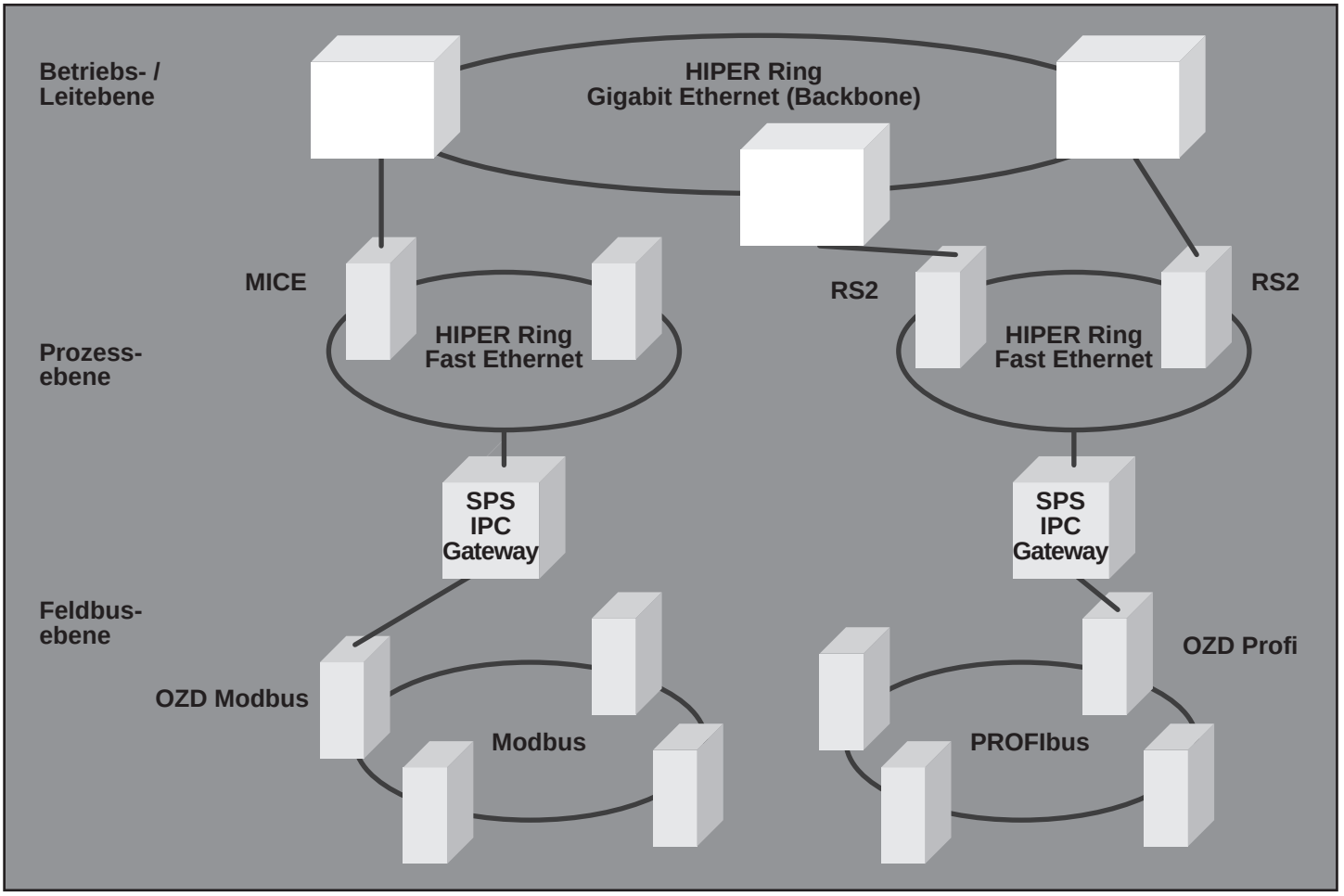


Bild 9 Kommunikationshierarchie in der Fertigung Quelle: Hirschmann

Das Thema "Echtzeit"

Als kritisch ist allerdings das Echtzeit-Verhalten zu beurteilen, zumindest was die Industrie für bestimmte Anwendungen darunter versteht. Denn im Gegensatz zu Sprach- und Datenanwendungen in herkömmlichen Datennetzen erreicht diese Anforderung Dimensionen, vor denen sich Netzwerker heute nicht einmal bei Cluster-Lösungen konfrontiert sehen[5]. Treffen in der Fertigung Echtzeit-sensitive Daten später ein als erwartet, kann dies einen gesamten Prozess zum Stillstand bringen, was naturgemäß zum Ausfall der Produktion oder der Beschädigung von Gütern oder Geräten führt. Das ist auch der Grund, warum sich Ethernet bei seinem Echtzeitverhalten an den bisher im Sensor-/Aktor-Bereich dominierenden Feldbussen messen lassen muss.

"Echtzeit" in der Fertigung wird je nach Anwendung (und auch Hersteller) unterschiedlich interpretiert. So erfordern Anwendungen, wie beispielsweise Motion Control bei CNC oder Bestückungsrobotern Antwortzeiten im unteren Mikrosekundenbereich. Andere Anwendungen, wie beispielsweise einfache Band- oder Transportsteuerungen "begnügen" sich dagegen mit etwa 20 Millisekunden und gelten in der Industrie als "weniger kritisch". Deshalb unterscheidet man "Echtzeit" durch die beiden Begriffe: weiche Echtzeit (soft real-time) und harte Echtzeit (hard real-time). Dabei versteht man gänigerweise unter harter Echtzeitanforderung solche Forderungen, die bei Verletzung eine Fehlfunktion in der Anwendung hervorrufen. Dagegen führen weiche Echtzeitanforderungen bei Verletzung "lediglich" zu Performance-Verlusten. Aber wie gesagt, wir reden hier von Antwortzeiten im Bereich 20 Millisekunden bis wenige Mikrosekunden und genau hier liegt derzeit ein "Schwachpunkt" industrieller Ethernet-Lösungen.

Da sich bisher die Quantifizierung von "Echtzeit" schwierig gestaltet, hat die IAONA (zusammen mit der ODVA und IDA Grou) zunächst den Weg eingeschlagen, das Thema in vier Klassen zu strukturieren. Diese reichen von 0,5 bis 15 Mikrosekunden (Klasse 4) bis hin zu "größer 1 Millisekunde" (Klasse 1). Aber unabhängig von der letztlichen Quantifizierung lässt sich heute feststellen, dass keine dieser Anforderungen (auch in Form von Klassen ausgedrückt) auch nur annähernd von den

[5] In Datennetzen wurde das Thema "Echtzeit" mit Aufkommen von Voice over IP forciert. Von der absoluten Netzwerkverzögerung her gesehen stellt sich die Sprache in Datennetzen nicht als kritisch dar, denn Netzverzögerungen um 40 ms reichen aus, um eine Ende-zu-Ende-Verzögerung unter 150 ms zu erzielen. Filetransfer, Datenbanken oder Cluster stellen hier strengere Anforderungen. Kritisch ist aber ein so genannter Jitter, sprich die Varianz der Verzögerung, was nicht nur verstärkt zu Switched-Networks führte, sondern auch zur Diskussion von Priorisierungsmaßnahmen.

heutigen LAN-Redundanzverfahren erfüllt werden kann. Deshalb werden harte Echtzeitanforderungen wohl auch weiterhin auf Feldbussystemen aufsetzen und weiche Echtzeitanforderungen von den bisherigen Verfahren der engeren Wahl (Rapid Spanning Tree, HIPER Ring, siehe oben) auch nur dann unterstützt, wenn sie in den Millisekunden-Bereich reichen.

Doch nicht nur die Umschaltzeiten redundanter Strukturen stehen für diese Bereiche auf dem Prüfstand, auch sind es die Kommunikationsstacks selbst. Insbesondere für die harten Echtzeitanforderungen können die Kriterien wohl nur dadurch erreicht werden, dass Eingriffe vor allem auf den OSI-Ebenen 3 und 4 erfolgen. Dies wurde bisher bei den oben dargestellten Industrial-Ethernet Varianten weitestgehend vermieden, steht aber gegenwärtig durch "neue" Stacks in der Diskussion. Ob hierfür jeder Hersteller seinen eigenen Stack entwickelt oder was letztlich die Normung erreicht, darauf darf man gespannt sein.

Links

http://www.odva.org
http://www.industrialethernet.com
http://www.ida-group.org
http://www.modbus.org
http://www.iaona-eu.com

CAN	Controller Area Network
CbA	Component-based Automation
CI	ControlNet International
CIP	Control and Information Protocol
CoS	Class of Service
DCOM	Distributed Component Object Model
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Norm
HSE	Highspeed Ethernet
I/O	Input / Output
IAONA	Industrial Automation Open Networking Alliance
IDA	Interface for Distributed Automation
IEA	Industrial Ethernet Association
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol / Industrial Protocol / International Protection
MES	Manufacturing Execution Systems
ODVA	Open DeviceNet Vendor Association
PLS	Prozessleitsysteme
PNO	Profibus Nutzerorganisation e.V.
RPC	Remote Procedure Call
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Dokumente

[1] IAONA: "Industrial Ethernet Planning and Installation Guide", IAONA Draft, 8. November 2001, http://www.iaona-eu.com
[2] IDA Group: "Intelligence for Distrubuted Automation" IDA White Paper, Rev. 1.0, April 2001, http://www.ida-group.org
[3] Rockwell Automation: "Ethernet/IP Performance and Application Guide", Allen-Bradley, ENET-AP001B-EN-P, Juni 2001

Das Seminar zum Thema: Ethernet in der Industrie, 25. -29.11.02 in Aachen

Das Seminar vermittelt das notwendige Wissen, um Ethernet-Netzwerke in industriellen Umgebungen planen und einsetzen zu können. Bisherige "Industrial Ethernet"-Lösungsansätze werden mit herstellerspezifischen (Feld-)Bussystemen verglichen.
Referenten: Dipl.-Ing. Roland Moos, Dipl.-Ing. Hartmut Kell Preis: € 1.990,-- zzgl. MwSt.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Ethernet in der Industrie

Ich melde mich an für das Seminar

Ethernet in der Industrie

zum Preis von € 1.990,-- zzgl. MwSt.

☐ vom 25.11. - 29.11.02 in Aachen

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Name, Vorname _____ Vorname _____

Firma _____ PLZ, Ort _____

Straße _____ eMail _____

Telefon, Fax _____ Unterschrift _____

Neues Seminar

Microsoft's Windows .Net & PKI – die richtige Kombination?

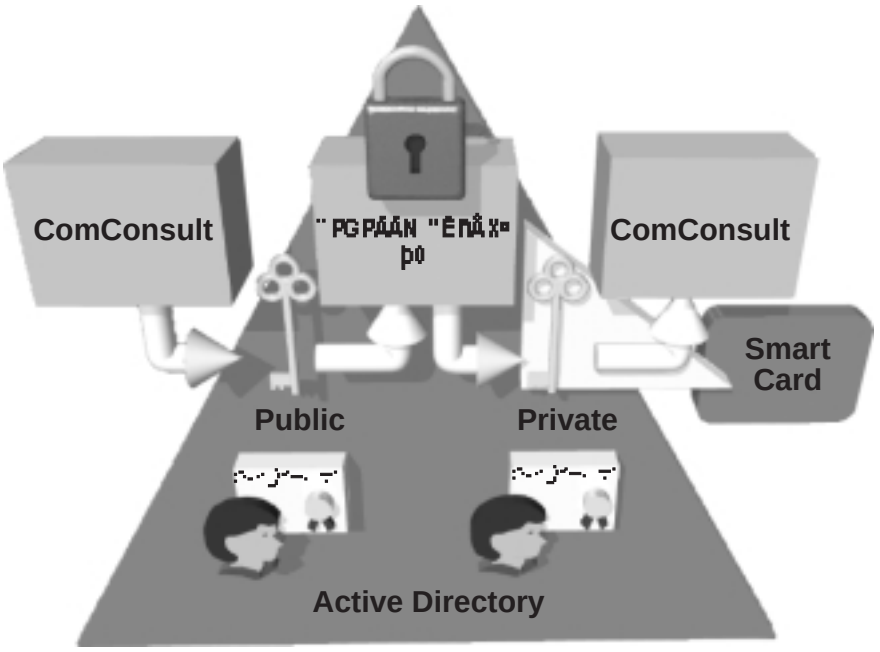
Am 9. und 10. Dezember 2002 veranstaltet die ComConsult Akademie im Arabella Sheraton Hotel in München zum ersten Mal ihr neues Seminar "Microsoft's Windows .Net & PKI – die richtige Kombination?"

Zum Thema

Mit Windows XP und der Windows .Net-Serverfamilie und der zunehmenden Marktbedeutung Microsoft-basierter Sicherheits-und VPN-Lösungen gewinnen die Themen PKI und Smartcard immer mehr an Bedeutung. Eine Evaluierung der damit verbundenen Möglichkeiten, aber auch der Schwachstellen ist für jedes VPN und Sicherheitsprojekt unvermeidbar, das folgende Themen umfasst:

- Gesicherte Authentifizierung im Rahmen einer VPN-Lösung
- E-Mail Verschlüsselung und Digitale Signierung (S/Mime)
- Verschlüsselter Zugriff auf Web Seiten über https (SSL)
- Authentisierung von Benutzern über das Web
- Verschlüsselung von Dateien und Verzeichnissen (EFS)

In diesem Umfeld läuft Microsoft zunehmend den Spezialanbietern den Rang ab, da die Infrastruktur öffentlicher Schlüssel (PKI) unter Windows 2000 sowie unter Windows .Net eine "built in" Funktionalität ist. Vorbei sind augenscheinlich die Zeiten proprietärer Software-Implementationen und der damit verbundene Integrationsaufwand und die möglichen Inkompatibilitäten. Windows 2000- und Windows .Net-Server verfügen über alle benötigten Komponenten, um eine Infrastruktur öffentlicher Schlüssel (PKI) zu etablieren. Durch eine hohe Integration der PKI in das Betriebssystem und in BackOffice-Komponenten können Lösungen zügig und technisch weitestgehend konfliktfrei umgesetzt werden.



Das Seminar richtet sich an IT-Entscheider, Systemverantwortliche und Projektleiter, die diese Sicherheitstechnologie kennen- und einschätzen lernen wollen. Hinzu kommen wichtige Update-Informationen zu Microsoft's jüngster Servergeneration, die mit der Bezeichnung "Windows .Net Server" im Frühjahr 2003 offiziell released werden soll.

In dem Seminar erfahren dieTeilnehmer nicht nur die theoretischen Grundlagen einer PKI, sondern Sie werden auch mit der grundsätzlichen Installation, Konfiguration, Administration und dem Betrieb einer Windows 2000 / .Net PKI im Rahmen von Live-Präsentationen vertraut gemacht. Die Verwendungszwecke einer PKI werden erläutert und in der Praxis gezeigt. Im Seminar wird auf Zusatzprodukte und Lösungserweiterungen anderer Hersteller eingegangen, die sich in die Windows 2000 PKI Infrastruktur integrieren. Ein expliziter Vergleich aller Hersteller und Anbieter würde jedoch den Rahmen dieser Veranstaltung sprengen.

Dieses Seminar bearbeitet folgende Fragen, die sich im Rahmen der Einführung von PKI/Smart-Card stellen:

- Welche Vorteile bietet die PKI unter Windows 2000/.Net?
- Wie sehen typische Nutzungs-Szenarien aus?
- Ist die SmartCard-Technologie ausgereift?
- Welche Vorteile und Nachteile hat die PKI "built in" Funktionalität unter Windows im Vergleich zu Mitbewerbsprodukten?
- Lohnt es sich auf die Windows .Net-Serverfamilie zu warten oder kann Windows2000 eine geeignete Basis sein?
- Welche wesentlichen Verbesserungen beinhaltet Windows .Net?
- Ist es ratsam, von Windows 2000 auf Windows .net upzugraden?

Microsoft's Windows .Net & PKI – die richtige Kombination?

Microsoft's Windows .Net & PKI – Die Inhalte

Dieses zweitägige Seminar liefert einen Überblick über wesentliche Neuerungen am Verzeichnisdienst Active Directory (AD) speziell im Bereich der Infrastruktur öffentlicher Schlüssel (PKI) in Verbindung mit der SmartCard-Technologie.

Der erste Seminartag schlüsselt die Unterschiede bzw. die Zusammenhänge zwischen der.Net Initiative (Microsoft Web Services) und .Net Serverfamilie auf. Zudem werden die Neuerungen und Änderungen der .Net Serverfamilie gegenüber den bisherigen Windows 2000 Komponenten eingehend behandelt.

Windows .Net Server
- .Net Server und .Net Technology
- Die .Net Server Familie
- Vergleich zu Windows 2000

Änderungen und Neuerungen im Detail
- Active Directory
- Administration
- Netzwerkdienste
- Serverfeatures
- Public Key Infrastructure

PKI Grundlagen
- Verschlüsselung
- Authentifizierung
- Zertifikate (X.509)
- Sperrlisten
- Windows 2000 Zertifizierungsstellen
- Zertifikathierarchien

Der zweite Seminartag konzentriert sich auf das Thema Infrastruktur öffentlicher Schlüssel (PKI) unter Verwendung von SmartCard Technologien verschiedener Hersteller. Neben der allgemeinen Grundfunktionalität und dem Betrieb einer PKI werden die Verbesserungen im .Net Server erläutert und an praktischen Beispielen demonstriert.

Windows 2000 /.Net PKI - Planung
- Planen von Zertifikat Server Strukturen
- Planen von Zertifikat Verteilung und Verwaltung
- Planen einer Zertifikatserneuerung
- Planen von Zertifikatsperrlisten
- Definition und Veröffentlichung der Betriebsweise einer PKI
- Intranetszenarien
- Extranetszenarien
- Zertifikatshandling für Benutzer

Realisierung
- Installation einer Beispiel Zertifikat Server Struktur
- Konfiguration der Zertifikat Server

Demonstration einiger Anwendungszwecke
- SmartCard Login
- Encrypted File System (EFS)
- VPN (PPTP,L2TP/IPSec)
- IPSec
- Kerberos(PKINIT)
- Einbindung Exchange Server 5.5/2000 (S/Mime)

Der Veranstalter behält sich Änderungen im Programm vor

Unter der Leitung von Dipl.-Ing. Martin Barbian sowie dem Fachgruppenleiter "IT Infrastructure" Jörg Stangl (W2k MCSE) werden die Veränderungen der Windows Leistungsmerkmale, Features und Funktionen vorgestellt. Dabei werden viele Bestandteile live demonstriert und Bezüge zu bestehenden PKI-Infrastrukturen hergestellt. Zudem werden die Vorzüge und Mehrwerte, aber auch die Defizite und Grenzbereiche genannt.

Dipl.-Ing. Martin Barbian von der ITC GmbH mit den Standorten Detmold, Düsseldorf, Frankfurt und Hamburg zählt mit seinem Team zu den führenden deutschen SMS-Experten. Darüber hinaus befasst sich das anerkannte Beratungshaus neben dem Desktopmanagement mit anderen aktuellen Themen, die einer betriebswirtschaftlichen Optimierung der IT-Landschaft Rechnung tragen. Dazu zählen das Netz- und Systemmanagement sowie eMail- und Informationssysteme, User Help Desk Lösungen und Multiuser Systeme (Windows Terminal Server) unter Windows NT / 2000. Im Zuge der Weiterentwicklung der Windows Betriebssystemfamilie und der BackOffice Suite gewinnt die 2000er Generation zunehmend Akzeptanz in bundesdeutschen Unternehmen. Die ITC GmbH blickt bereits auf einige Windows 2000 Projekte mit unterschiedlichsten Schwerpunkten zurück - u.a. inkl. PKI-Infrastrukturen. Insofern kann die Praxisnähe eingehend vermittelt werden. Aufgrund der kurzen Innovationszyklen des Herstellers Microsoft befasste sich die ITC als "Microsoft Beta Program Partner" unter anderem sehr frühzeitig mit der nächsten Servergeneration: "Windows .Net Server Family" sowie "SMS 2003."

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Windows .Net & PKI

Ich melde mich an für das Seminar

Microsoft's Windows .Net & PKI – die richtige Kombination?

zum Preis von € 1.290,-- zzgl. MwSt.

☐ vom 09.12. - 10.12.02 in München

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Name, Vorname _____ Vorname _____

Firma _____ PLZ, Ort _____

Straße _____ eMail _____

Telefon, Fax _____ Unterschrift _____

MPLS-Serie – Teil 5

Sollten Sie die zuvor veröffentlichten Teile ("Der neue Star für Qualität und Verkehrssteuerung?" aus dem Insider vom Februar, "Paketbildung und Paketbearbeitung" im April, "Verkehrssteuerung" im Juli und "MPLS-TE Signalisierung" im September) nicht erhalten haben, schicken wir sie Ihnen gerne zu. Senden Sie uns einfach eine formlose E-Mail an mail@comconsult-akademie.de

Zum Thema

MPLS hat sich in den letzten Jahren zu einer ganzen Suite von Protokollen und Standards entwickelt und erhebt den Anspruch, im MAN / WAN / Provider-Bereich als ATM-Ablösung für Quality of Service und effiziente Verkehrsflusssteuerung zu sorgen. Welche Konzepte MPLS liegen zugrunde? Wie sind die Marktchancen? Wie passt MPLS zu der neuen Generation optischer Netze?

Die Autorin

Dipl.-Inform. Petra Borowka leitet das Planungsbüro UBN; langjährige Projekterfahrung mit herstellerunabhängiger standardbasierter Netzwerk-Planung in Beratungsprojekten für verschiedenste Industrie- und Dienstleistungsunternehmen; Schulungen, Veröffentlichungen

Da MPLS mit Tunnels arbeitet, eignet es sich für VPN Technik. Ob ein Tunnel definiert wird, um bestimmte Dienstgüte-Anforderungen sicherzustellen oder um einen Datenstrom vom Rest der Welt zu isolieren, ist lediglich ein anwendungstechnischer Unterschied: VPN-Implementierung ist eine weitere Anwendung für MPLS. Da Label-Technik, insbesondere Label Stacking, größere Flexibilität besitzt als eine IP Adresse, lassen sich auch ineinandergeschachtelte VPNs oder VPNs über mehrere Providernetze hinweg aufbauen.

Allerdings leistet MPLS ähnlich wie Frame Relay oder ATM lediglich Isolierung der Datenströme, keine Verschlüsselung, wie es der landläufige VPN-Begriff meistens unterstellt. Ist Verschlüsselung gefordert, so muss sie durch andere zusätzliche Protokolle wie IPsec implementiert werden. Es gibt mehrere Vorschläge, MPLS VPNs zu betreiben:

- Virtueller Router
- BGP Erweiterungen (RFC 2547)
- Draft-Rosen-RFC2547
- Martini-Draft, PWE3

Virtueller Router

Das Konzept "Virtueller Router" separiert VPNs, indem je VPN separate Routing Tabellen aufgebaut werden und der physikalische Router intern gleichsam in mehrere "virtuelle" Router aufgesplittet ist (unterstützt z.B. von Extreme Networks). Zwischen den einzelnen Routing Tabellen werden keine Verbindungen geschaltet oder gelernt.

BGP Erweiterungen, RFC 2547

RFC 2547 beschreibt BGP/MPLS VPN's, bei denen die einzelnen VPN's überlappende IP Adressräume nutzen, wie es in Provider-Umgebungen mit mehreren Kunden der Fall sein könnte, die den privaten Adressraum nutzen. Hier werden MPLS VPNs auf Layer-3 IP Strukturen aufgesetzt. Die "BGP Multiprotocol Extensions" (MP-BGP) definieren, wie BGP in den so genannten Reachability Nachrichten erweiterte VPN-IPv4 Adressen zwischen Label Edge Routern so propagiert, dass Informationen über ein bestimmtes VPN nur anderen Mitgliedern dieses VPN's bekannt gegeben werden. Ein gültiger Empfänger, d.h. Mitglied des VPNs, wird über die Multiprotokoll-Erweiterungen von BGP erkannt und identifiziert. Alle Mitglieder eines VPN's lernen so die Routen zu den anderen VPN-Mitgliedern.

Eine VPN-IPv4 Adresse ist 12 Byte lang, 8 Byte RD (Route Distinguisher) und die 4 Byte klassische IP Adresse. Durch den 8 Byte RD werden VPN's, die denselben IP Adressraum nutzen, unterscheidbar, und das in einer hohen Anzahl, also mit ausreichender Skalierbarkeit.

Draft-Rosen-RFC2547

Draft-Rosen-RFC2547 ist der Nachfolge-Draft für RFC 2547. So genannte Provider Edge (PE) Router können mehrere VPNs mit überlappenden IP Adressen unterstützen, wenn sie je VPN eine separate VPN Routing und Forwarding Tabelle, kurz VRF, führen. Die VRF Tabellen werden über zwei Mechanismen aufgebaut und aktualisiert: Erstens: ein PE Router lernt Routen von einem direkt angebundenen Customer Edge (CE) Router, der Mitglied des VPNs ist. Zweitens: der PE empfängt Routen über BGP Reachability Informationen. Routen, die über einen CE Router erreichbar sind, können mittels manueller Konfiguration oder über dynamische Routing Protokolle zwischen PE Router und Kunden-Router gelernt werden. Der Draft beschreibt Konfigurationen, bei denen PE und CE Router RIP, OSPF oder BGP Peers sind. VPN-spezifische Routen werden durch die IP Adressen zweier Peers in Kombination mit unterschiedlichen MPLS Labels je VPN codiert. Je VPN wird ein eigener LSP zwischen Peer Routern eingerichtet.

Anders als bei RFC 2547 werden RDs nicht für Informationen über das VPN-Set verwendet, dem eine Route bekannt gegeben werden soll. Zur besseren Skalierbarkeit werden hierfür so genannte Route Target Attribute genutzt. Ein Route Target identifiziert einen Satz von VRFs, jeder VRF sind ein oder mehrere Route Target Attribute zugeordnet. Export Targets sind die Route Targets, die der PE Router einer Route zuordnet, die er von einem CE Router gelernt hat. Import Targets sind die Route Targets, die benutzt werden, um zu entscheiden, ob eine von einem anderen PE Router gelernte Route in eine bestimmte VRF aufgenommen werden darf. Somit sind Route Targets der Mechanismus, der die PE Router in die Lage versetzt, ausschließlich die Routen-Informationen für VPNs zu handhaben, die er bedient.

MPLS Label bei BGP/MPLS VPNs bilden einen 2-Level Label Stack. Der äußere MPLS Label regelt den Transport über den MPLS Backbone, wird vom Backbone IGP mitgeteilt und ist mit der besten Route zur BGP Next Hop Adresse desjenigen PE Routers

MPLS-Serie – Teil 5

assoziiert, der die entsprechende VPN Route bekannt gegeben hat. Der innere MPLS Label wird vom BGP mitgeteilt und ist mit der besten Route zur VPN Zieladresse assoziiert. Mindestens gibt dieser Labes die VRF an, die der Egress PE Router benutzen wird, um ein Paket zum CE Router weiterzuleiten, möglicherweise gibt er auch noch das Ausgangs-Interface an.

Martini Draft, PWE3

Der Draft von Luca Martini und mehreren anderen spezifiziert, wie MPLS eingesetzt wird, um Layer-2 VPN-Dienste über Ethernet, Frame Relay oder ATM für Anwender zu unterstützen, die non-IP Applikationen betreiben. Unter Pseudo Wire Emulation Edge-to-Edge (PWE3) werden aktuell weitere Standards für Layer-2 VPNs definiert. Vielfach werden sie als "Any Transport / Any Protocol over MPLS", AToM / APoM oder AP/ToM bezeichnet.

Da MPLS keine Verschlüsselung vorschreibt, argumentieren Kritiker, MPLS VPNs seien nicht sicher. In der Tat ist MPLS ohne Zusatz-Verschlüsselung nicht sicherer als Frame Relay oder ATM. MPLS verhindert aber auch keine Sicherheit. Wenn Verschlüsselung unverzichtbar ist, kann MPLS zusammen mit IPsec oder SSL betrieben werden.

Fazit

Aktuell sind MPLS VPNs nach RFC 2547 die einzigen produktiv implementierten Lösungen, forciert von AT&T, Cisco und Juniper. Kritiker von RFC 2547 - unter ihnen so bekannte Personen wie Steve Bellovin und Randy Bush - bemängeln, dass sich durch die fehlende Verschlüsselung scheunentor-große Sicherheitslücken öffnen und dass RFC 2547 aufgrund der sehr hohen Prozessorbelastung im Internet nicht skaliert.

Das Gegenlager favorisiert Layer-2 MPLS VPN's mit dem Argument besserer Skalierbarkeit und dem Argument, dass viele Kunden mit der Sicherheit von Frame Relay und ATM zufrieden sind - diese könnten mit Layer-2 MPLS VPN's gleichwertig bedient werden. Hierbei wird der Konfigurations-Aufwand auf den Edge-Bereich ausgelagert und muss ggf. vom Kunden bewältigt werden.

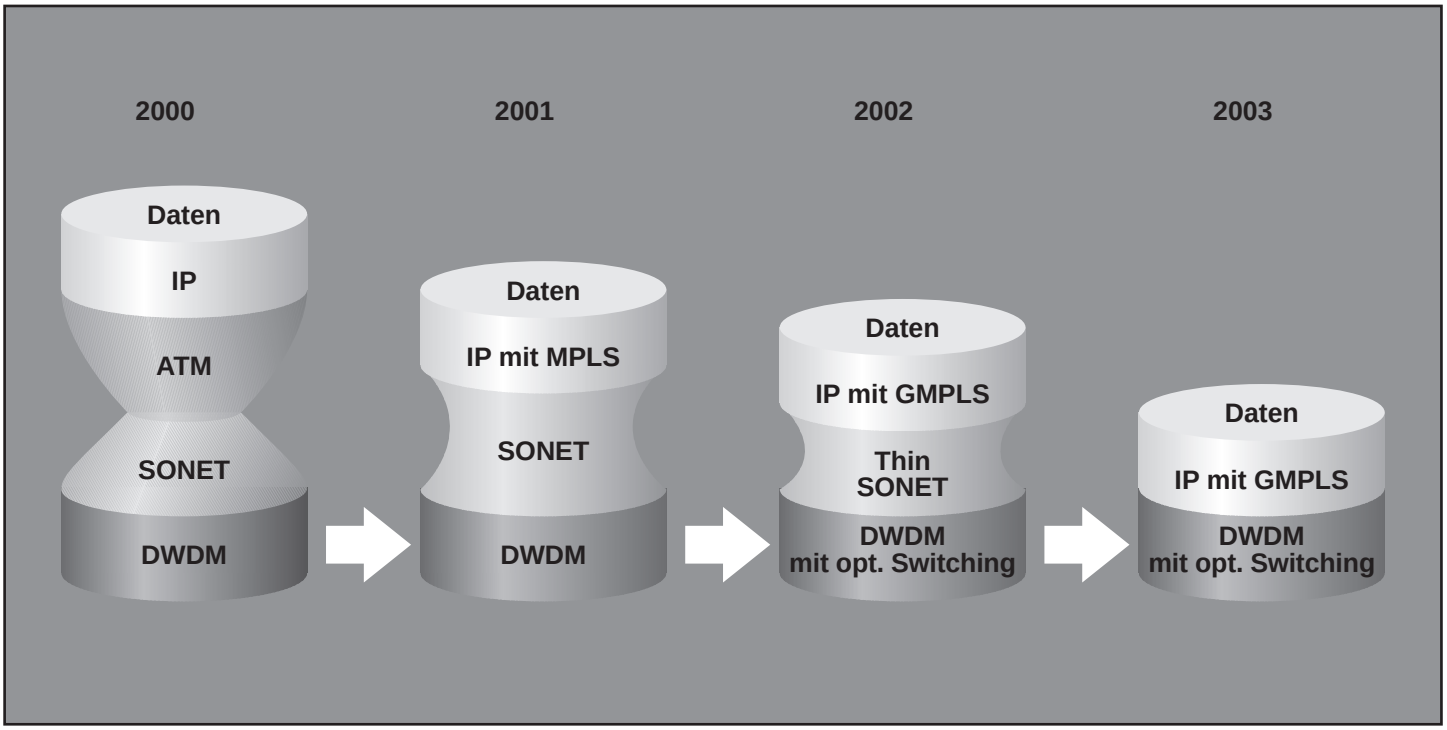
MPLS für Traffic Engineering ist komplex. VPN-Technik ist komplex. MPLS kombiniert mit VPNs ist sehr komplex und erzeugt CPU-Hochlasten. MPLS VPNs mit zusätzlicher Verschlüsselung ist sehr komplex, ein Leistungs-Killer, undurchschaubar und erschwert die Störfalldiagnose. Hier muss eindeutig eine schlankere, intelligentere Lösung her.

8
Neue Entwicklung: GMPLS, MPλS

Heutige Provider Netze haben typischerweise vier Ebenen: IP für beliebige Applikationen, ATM für eine Vermittlungsstruktur, die VPN- und QoS-Bedarfen gerecht wird, Sonet/SDH als Layer-1 Transport und DWDM, um die notwendige Kapazität bereitzustellen. Diese Architektur kann nicht schnell genug an die stark wachsenden Skalierungswünsche angepasst werden und ist gleichzeitig ziemlich kostenintensiv. Neue OXC-Komponenten (Optical Cross-Connect) werden die Sonet ADMs ersetzen und entwickeln sich zur bevorzugten Alternative, um Terabit Datenströme zu switchen, da eine elektronische Bearbeitung je Paket vermieden wird.

Es wird allgemein akzeptiert, dass IP weiterhin erhalten bleibt, also ist die Entwicklung schneller Routertechnologien ganz wesentlich, um langsamere Datenströme so zu aggregieren, dass sie für schnelle OXCs geeignet sind. Mit der hohen Kapazitätssteigerung von optischen Routern und OXCs ist ein Trend erkennbar, die ATM und Sonet/SDH Ebenen einfach auszulassen und deren Funktionen gleich in Router, OXCs und DWDM einzubauen. Damit vereinfacht sich die Netzstruktur auf zwei bis zweieinhalb Ebenen: IP, GMPLS als Zwischenebene und DWDM. Die Entwicklung zeigt Bild 35.

Bild 35 Evolution von ATM/SDH-Netzen zu DWDM-Netzen



MPLS-Serie – Teil 5

In optischen Netzen wird also nicht nur über Paketvermittlung (Packet Switching) nachgedacht sondern auch über andere Vermittlungs-Verfahren wie

- TDM: Zeitmultiplex mit Sonet ADMs
- Spatial Switching: Vermittlung von optischem Eingangsport auf optischen Ausgangsport
- Lambda Switching: In DWDM Netzen, Vermittlung einer Eingangs-Wellenlänge als Kanal, kurz (oder "Farbe" genannt, auf eine Ausgangs-Wellenlänge

Nicht nur paketvermittelte Routen, sondern auch andere Vermittlungsschemata sollen mit Label-Technik kontrollierbar werden. Die Loslösung der Forwarding Information vom IP Header erlaubt es, MPLS auch für optische Komponenten wie OXCs zu nutzen, die kein IP verstehen. Beispielsweise könnte eine Wellenlänge (Farbe) als impliziter Label behandelt werden. Das hierarchische Label Stacking Konzept ermöglicht die Interaktion mit Geräten, die nur einen sehr begrenzten Label-Adressraum unterstützen können. Beide genannten MPLS-Eigenschaften sind im OXC und DWDM Kontext sehr wichtig.

Zielsetzung von GMPLS, dem erweiterten "Generalized" MPLS ist es, prinzipiell beliebige Transportnetze über alle Layer-1 und Layer-2 hinweg mit einem gemeinsamen Verfahren provisionieren zu können, das heißt insbesondere, einheitliche Verfahren einzusetzen für

- Forwarding
- Signalisierung

und

- Routing

Die MPLS Weiterentwicklungen für GMPLS haben Synergien im Auge, z.B. zwischen Label Switch Routern und photonischen Switches oder zwischen einem LSP und einem optischen Trail. Ein optischer Trail ist eine Ende-zu-Ende Verbindung, die ausschließlich aus optischen Komponenten besteht und keinerlei optisch-elektrische Wandlung mehr beinhaltet. Analog zu einem LSR schaltet ein photonischer Switch Wellenlängen vom Eingangs- zum Ausgangsport. Während der LSR Eingangs- und Ausgangs-Label aufeinander mappt, mappt der photonische Switch Eingangs-Lambdas und -Ports auf Ausgangs-Lambdas und -Ports. Genau wie LSR's brauchen optische Switches Routing Protokolle, um Topologie-Informationen auszutauschen und dynamisch anzupassen. Ein vereinfachtes Beispiel für kombinierte Label zwischen LSRs und optischen Switches zeigt Bild 36.

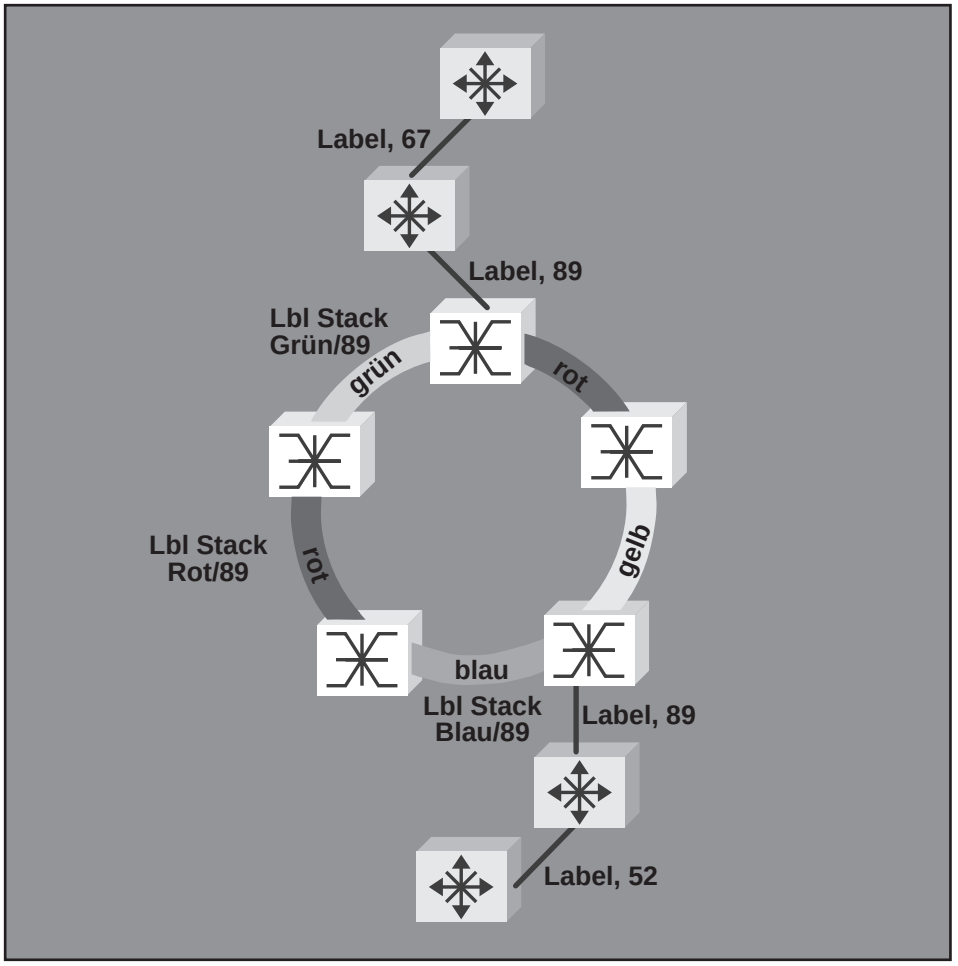


Bild 36 Label Stacking mit GMPLS (vereinfacht)

Wichtige Funktionselemente von GMPLS sind:

- Routing Erweiterungen
  - Link Bündelung
  - LSP Hierarchie
  - Unnumbered Links
  - Link Management Protokoll
- Signalisierungs-Erweiterungen
  - Hierarchisches LSP Setup
  - Labelvorschläge
  - Bidirektionales LSP Setup
  - Notify Nachrichten

Wir werden auf diese Funktionen später näher eingehen.

GMPLS unterstützt zwei Netzmodelle:

- Peer Modell: Alle Komponenten in einer Domäne haben dieselbe Kontroll-Ebene (Control Plane, Management Logik)
- Overlay Modell: Die optische und logische (Layer-3) Kontroll-Ebene sind voneinander getrennt. Dieses Modell ist weidlich von Overlay-Netzen wie IP over PPP over Frame Relay over ATM over Sonet oder ähnlichen Missgeburten bekannt.

Auch das OIF (Optical Internetworking Forum) hat sich für GMPLS engagiert und das OIF UNI (User to Network Interface) in der Version 1 verabschiedet.

Es spezifiziert wesentliche Verbindungsfunktionen wie

- Einrichtung eines optischen Paths
- Änderung
- Löschen
- Statusabfragen und Statusantworten

MPLS-Serie – Teil 5

Overlay Modell

Das Overlay Modell verbirgt die Details der unteren Schichten, indem es zwei separate Kontrollebenen mit minimaler Interaktion implementiert, eine eigene Kontrollebene für das optische Kern-Netzwerk und eine für das logische Netzwerk inklusive des optischen Zugangs (Optical Edge). Die Edge Geräte fordern LWL-Kanäle, die entweder dynamisch über den optischen Core Backbone hinweg signalisiert oder statisch provisioniert werden. Durch die Trennung in optische und logische Kontrollebene lässt sich beim Overlay Modell eine administrative "Grenzkontrolle" zwischen optischem Kernnetz und logischem Zugangspunkt (Edge) einrichten. Dies ermöglicht separate Fehler-Isolierung und unterschiedliche Kontrollverfahren für physikalische und logische Netzebenen, was einigen Netzwerk-Betreibern attraktiv erscheint.

Das Overlay Modell wird vielfach von optischen Herstellern bevorzugt, erfordert aber für beliebige Konnektivität eine vollständig definierte Punkt-zu-Punkt Vermaschung der Edge Komponenten (analog dem BGP Problem bei MPLS) für Datenkommunikation und Routing. Dies bedeutet einen hohen Overhead Protokollaufwand, der quadratisch mit Anzahl der Edge Komponenten steigt und skaliert daher schlecht; die Anzahl sinnvoll betreibbarer Edge Komponenten ist limitiert. Dafür kann eine größere Vielfalt an Edge Komponenten mit dem optischen Core kommunizieren und nach allgemeiner Einschätzung sind Overlay Netze in ihren Einzelebenen leichter zu implementieren als das Peer Modell.

Peer Modell

Da das Peer Modell eine gemeinsame Kontroll-Ebene nutzt, fasst eine einzelne administrative Domäne das optische Kernnetz (optical Core) und die angebundenen Edge Komponenten zusammen. So lassen sich z.B. optische Switches und Router durchgängig integrieren, da die Router die optische Topologie kennen und die Switches ihre benachbarten Router kennen. Zwar werden noch Punkt-zu-Punkt Verbindungen definiert, jedoch nur noch für Datenverkehr, was den Overhead erheblich reduziert. Routing Informationen werden nicht mehr zwischen Edge Routern, sondern zwischen "benachbarten" Komponenten ausgetauscht, also vom Edge Router zu seinem über- oder untergeordneten optischen Switch.

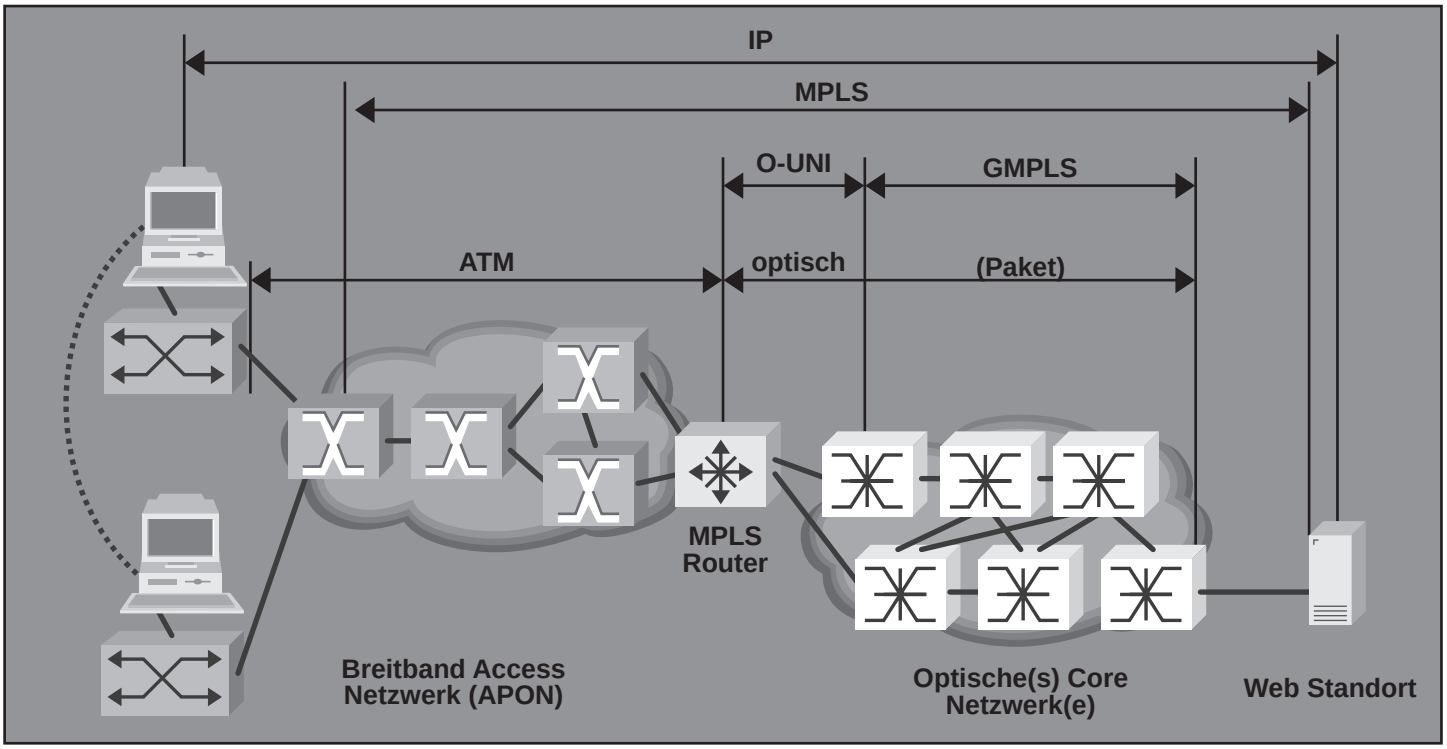
Das Peer Modell ist erkennbar übersichtlicher und skaliert besser, dafür ist Fehler-Isolierung schwieriger und die Kontrollverfahren können nicht spezifisch auf Layer-1, Layer-2 und Layer-3 Komponenten angepasst werden.

Da zur Zeit in beiden Richtungen Entwicklungen laufen, wird sich möglicherweise ein hybrider Ansatz etablieren. Da die Funktionen, die im Peer Modell implementiert werden müssen, netterweise eine Obermenge des Overlay Modells darstellen, kann ein Carrier mit dem Peer Modell beginnen und es dann in Richtung Overlay Modell ausbauen. Das Overlay Modell kann aus dem Peer Modell abgeleitet werden, indem administrativ das Topologie Sharing deaktiviert wird, während die Signalisierungs-Funktionen beibehalten werden.

8.1 Die optische Kontroll-Ebene

Techniken wie PON (Passive Optical Networking) bringen optische Netze näher an den Endanwender heran. Daraus könnte ein Trend entstehen, Netzwerk-Intelligenz auf der optischen Ebene zu implementieren. Aktuell sieht es noch so aus, als ob PON als Zugangstechnik ATM nutzen wird. Das verhindert den Einsatz von MPLS jedoch nicht, in diesem Fall wird es als Overlay zu ATM eingesetzt, um später die ATM Signalisierung abzulösen, wenn auf der optischen Ebene kein Cell-Transport mehr genutzt wird. Für die Anfangszeit ist MPLS, ob nun für IP oder für optische Netze jedoch eher im Core als im Access-Bereich zu sehen, wie in Bild 37 zu sehen ist.

Bild 37 Im Aufbau befindliche Struktur von PON und optischen Core Netzen



Die neuen optischen Core Netze bzw. die hierfür entwickelten neuen optischen Komponenten benötigen eine detailliert ausgearbeitete Kontroll-Ebene, da die Implementierung von aktuell nur für Paketvermittlung (oder Cell-Vermittlung) eingesetzten Funktionen wie Routing und Signalisierung, zukünftig auch für optische Netze erforderlich werden. Dies schafft die Perspektive, für beide Bereiche einheitliche Routing- und Signalisierungs-Verfahren zu betreiben, um Synergie-Effekte zu nutzen. Entsprechend bemüht sich die IETF, mit ihren GMPLS Standards existierende Verfahren wie OSPF und MPLS so anzupassen, dass eine Nutzung durch die optische Kontroll-Ebene möglich wird.

Aktuelle Entwicklungen

Klassisches IP geht von der Annahme aus, dass Kontroll-Verkehr und Datenverkehr zwischen Nachbarroutern ausgetauscht wird. Für optische Technik ist diese Annahme aber weit weg von der Realität: Dies würde bedeuten, dass jedes optische Interface einen Kontroll-Kanal betreiben würde, der an jeder Komponente decodiert wird. Für rein optische Geräte wäre dies ausgesprochen lästig, für Sonet/SDH Komponenten und OEO Switches würde es gravierende Einschränkungen bedeuten. Daher wird die Lösung angestrebt, einen Out-of-Band Kontroll-Kanal zu betreiben. Dieser muss bidirektional sein und wirft das Problem auf, Connectivity zwischen zwei benachbarten Komponenten festzustellen, wie Bild 38 zeigt. OSPF oder IS-IS leisten dies nicht mehr, es wird ein Protokoll erforderlich, das näher an der physikalischen Ebene arbeitet. Dieser Bedarf führte zur Spezifikation des Link Management Protokolls (LMP), das generisch dafür ausgelegt wurde, typische Layer-1 Funktionen wie Fehlererkennung und Fehler-Isolierung umzusetzen.

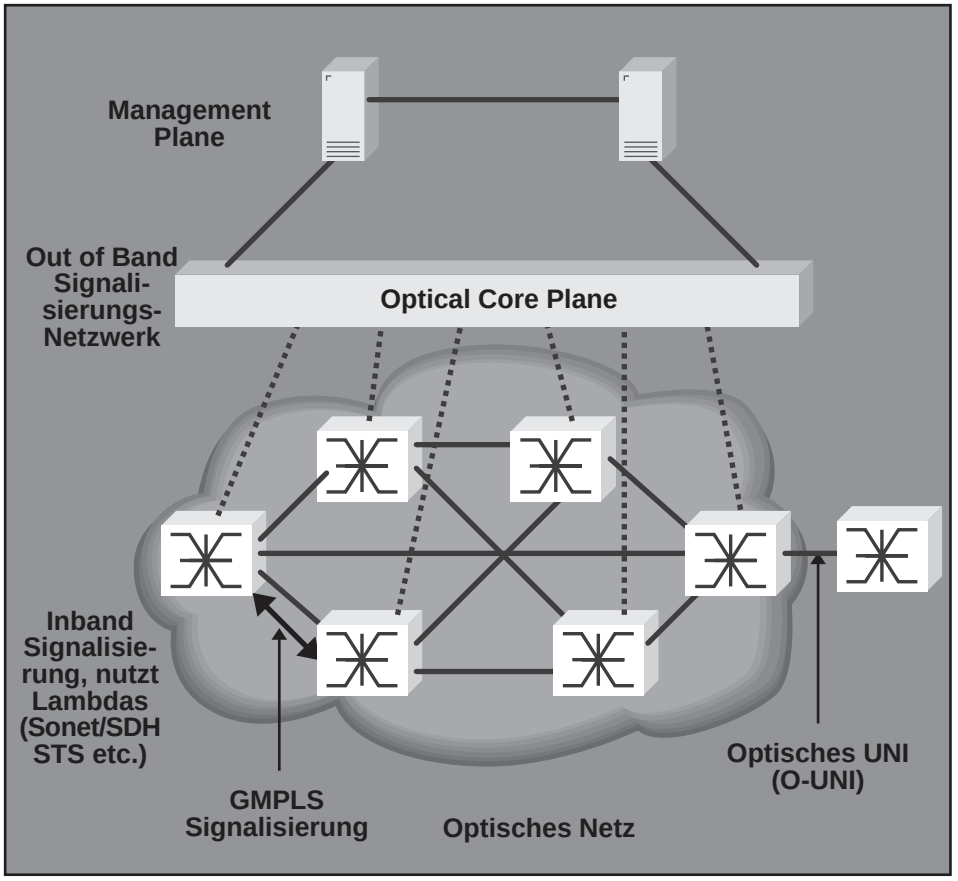
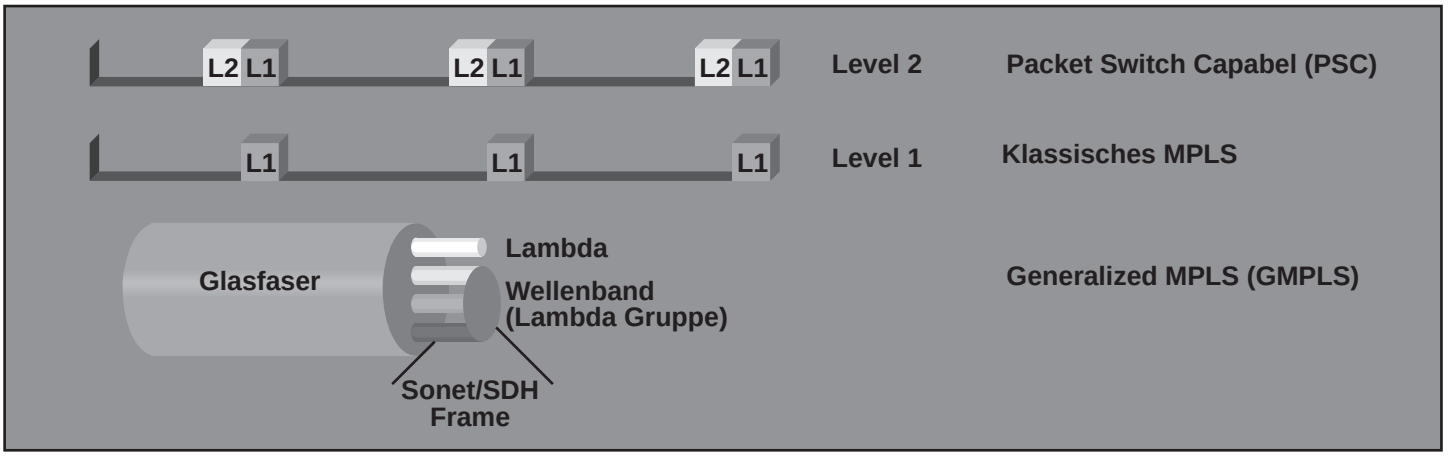


Bild 38 Optionen für den Aufbau einer optischen Kontroll Ebene

Optische Netze nutzen verschiedene Technologien, mindestens Sonet/SDH TDM und LWL-Verbindungen, die mit DWDM gefahren werden. Diese Technologien können hierarchisch betrachtet werden, so dass jeweils Verbindungen auf einer unteren Ebene als Verbindungsweg (Path) genutzt werden können, um auf der nächsthöheren Ebene Ende-zu-Ende Verbindungen herzustellen. Dies ist im Kern eine radikale Abkehr vom klassischen IP Routing, das eine völlig "flache" Layer-2 Transportstruktur unterstellt. Die Hierarchische Struktur erfordert Routing und Signalisierung auf mehreren Ebenen, wie Bild 39 verdeutlicht: Für einzelne λ, λ-Gruppen, LWL-Fasern und die Paketvermittlung sind jeweils eigenständige Ebenen.

Bild 39 MPLS Struktur auf optischer und Paket-Ebene



MPLS-Serie – Teil 5

8.2
GMPLS Routing Erweiterungen

Die Haupt-Anforderungen an MPLS für optische und Sonet/SDH TDM Netze sind:

1. Der MPLS Label-Adressraum ist sehr groß (1 Mio pro Port), wogegen die genutzten Lambdas und TDM Kanäle sich selbst in den nächsten Jahren erst auf einige Tausend hocharbeiten werden.

2. MPLS stellt Bandbreite kontinuierlich zur Verfügung, während optische und TDM Netze Erhöhungen mit einem begrenzten Satz diskreter Werte durchführen.

3. Heute gibt es selten mehr als 10 parallele Verbindungen zwischen zwei Knoten. Zukünftige optische Netze handhaben Hunderte paralleler Glasfasern mit jeweils Hunderten von Lambda-Kanälen. Das bedeutet, in optischen Netzen gibt es eine um mehrere Größenordnungen höhere Anzahl Verbindungen. Diese alle mit IP Adressen auszustatten stellt selbst mit IPv6 rein technisch und administrativ ein gravierendes Problem dar. Außerdem ist es sehr fehleranfällig und aufwändig festzustellen, welcher Port einer optischen Komponente mit welchem Port einer benachbarten optischen Komponente verbunden ist.

4. Extrem schnelle Fehlererkennung und -Behebung sind notwendig.

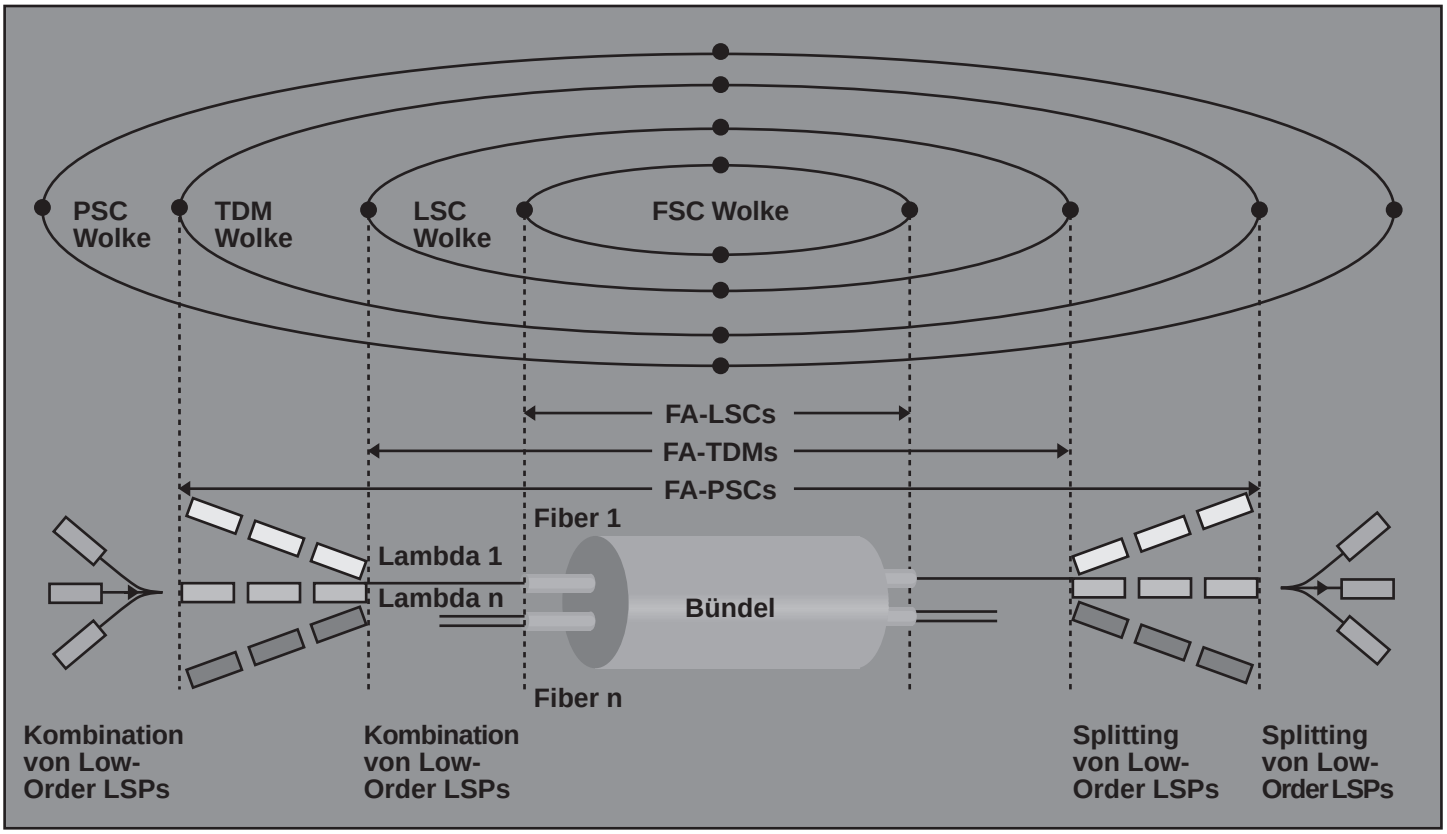
5. Die Daten, die optisch übertragen werden, werden transparent übertragen, um die Effizienz zu erhöhen. Daher muss eine Kontroll-Ebene eingerichtet werden, die von der Dateninterpretation – und sei es auch nur ein Layer-3 IP Header – losgelöst ist.

Nachfolgend werden Lösungsansätze für diese Anforderungen beschrieben sowie die resultierenden MPLS-Erweiterungen bei GMPLS.

LSP Hierarchie

Label Switch Path Hierarchie bedeutet, dass ein LSP in einen anderen LSP eingebettet sein kann. Bei mehrfacher Anwendung dieses Prinzips entsteht eine LSP Hierarchie von LSP's. Dies bringt eine Antwort auf Anforderung 1 und 2: (1) Ein LSP wird wie die Link State Datenbank eines OSPF oder IS-IS Routers behandelt. MPLS LSPs, die an einem gemeinsamen Knotenpunkt in das optische Netz hinein- und an einem anderen gemeinsamen Knotenpunkt hinauslaufen, können aggregiert und innerhalb eines einzelnen LSP getunnelt werden. (2) Wenn ein optischer LSP aufgebaut wird, erhält er eine diskrete Bandbreite, z.B. 2,488 Gbit/s. Wenn er jedoch als Link behandelt wird, ist seine Bandbreite nicht länger diskret. Ein 100 Mbit/s MPLS LSP, das durch den optischen LSP getunnelt wird, lässt 2,388 Gbit/s für andere LSPs ungenutzt. So entsteht eine natürliche Hierarchie, wie LSPs ineinander geschachtelt werden können, die auf der Multiplex-Fähigkeit der LSP Typen basiert. Beachten Sie hierbei, dass LSPs immer an gleichen Komponententypen starten und terminieren. Die oberste Hierarchie-Ebene bilden daher Komponenten mit Schnittstellen, die Glasfasern verschalten, genannt Fiber-Switch-Capable (FSC). Die nächste Hierarchie-Ebene bilden Komponenten mit Schnittstellen, die Lambdas verschalten, genannt Lambda-Switch-Capable (LSC). Weiter geht es mit TDM-fähigen Interfaces und die unterste oder innerste Hierarchiestufe sind Schnittstellen, die Pakete vermitteln, genannt Packet-Switch-Capable (PSC). Die resultierende Hierarchie ist in Bild 40 gezeigt.

Bild 40 LSP Hierarchie bei GMPLS



MPLS-Serie – Teil 5

Die FSC-Wolke wird mit einer (größeren) LSC-Wolke verbunden, d.h. eine FSC-Verbindung transportiert viele LSC-Verbindungen. Die LSC-Wolke wird wiederum mit einer (größeren) TDM-Wolke verbunden und so weiter. Innerhalb jeder Wolke verläuft der Informations-Austausch für Kontroll-Informationen automatisch.

Es ergeben sich aktuell vier Typen von LSPs:

- FSC-LSP (Glasfasern)
- LSC-LSP (Lambdas)
- TDM-LSP (Sonet/SDH)
- PSC-LSP (IP Pakete)

Andersherum:

Ein LSP, der an einem PSC Interface startet und endet, kann zusammen mit vielen anderen PSC-LSP's in einen TDM-LSP geschachtelt werden. Der TDM-LSP kann zusammen mit vielen anderen TDM-LSPs in einen LSC-LSP geschachtelt werden. Der LSC-LSP kann zusammen mit vielen anderen LSC-LSPs in einen FSC-LSP geschachtelt werden. Und viele FSC-LSPs werden weltweit in der Erde verbuddelt.

Und wenn sie nicht gestorben sind, dann leben sie noch heute...

Schwierig?

Nein!

Die verschiedenen LSP-Typen werden einfach als separate Link-Typen in der OSPF Datenbank gehandhabt. So lassen sich alle bisherigen Methoden der Informations-Verteilung (Information Flooding) beibehalten. Wenn ein Router Path Constraints berechnet, berücksichtigt er dafür eben nicht mehr nur IP Constraints sondern auf andere LSP-Typen angepasste Constraints, z.B.:

Für rein optisches Routing ohne OEO-Wandlung (Optisch-Elektrisch-Optisch) gibt es spezifische Einschränkungen. Optische Geräte sind grundsätzlich unfähig, die Wellenlänge oder "Farbe" zwischen Eingangs- und Ausgangs-Port zu ändern. Wenn also ein "Ultraviolett" von einem Interface genutzt wird, müssen die anderen Interfaces durch Signalisierung und Routing daran gehindert werden diese Farbe zu nutzen; Signalisierung und Routing müssen "Ultraviolett" für alle anderen Interfaces dieser Komponente blockieren. Solche Einschränkungen müssen als Constraints in den Dijkstra CR-SPF Algorithmus eingebracht werden.

Link Bündelung

Traditionelles IP Routing schreibt vor, dass die Discovery über jeden Link abläuft und Topologie-Informationen über alle diese Links ausgetauscht werden. Dies erzeugt massenhaft redundante Information und beeinträchtigt die Skalierbarkeit eines Routing Protokolls. Die Link State Datenbank eines optischen Netzes wäre um mehrere Größenordnungen voller als die eines MPLS Netzwerks.

Um dieses als Anforderung (3) genannte Problem zu entschärfen, führt GMPLS das Konzept der Link Bündelung (Bundling) ein, bei dem mehrere physikalische Verbindungen zu einer logischen Verbindung zusammengefasst und dem Routing Protokoll als eine einzelne Verbindung bekannt gegeben werden (bei Ethernet als Link Aggregierung nach IEEE 802.3ad bekannt). Wenn die Attribute mehrerer Links zusammengefasst werden, können leider einzelne Informationen verloren gehen.

Beispiel: Ein Sonet Link Bündel mit OC-12, OC-48 und OC-192 flutet die Gesamtkapazität, aber nicht mehr die Anzahl der Links und die exakten Timeslots.

Der Nutzen der Link Bündelung ist jedoch so hoch, dass dieser Nachteil in Kauf genommen wird.

Unnumbered Links

Dies betrifft Anforderung (3). Vielleicht der offensichtlichste Unterschied zwischen optischen und Layer-3 Netzen ist der: Optische Netze kennen kein IP Adress-Konzept. Routing und Signalisierung müssen also für IP-technisch nicht-nummerierte Verbindungen ebenfalls funktionieren. Gebraucht wird ein eindeutiges Verfahren, Verbindungen innerhalb eines Netzwerks zu identifizieren.

Das lässt sich in zwei Schritten erreichen:

Erstens wird jede Komponente innerhalb eines Netzes identifiziert, danach wird jeder Link identifiziert, der von diesem Knoten ausgeht. Die Knoten lassen sich mittels eindeutiger Router ID kennzeichnen. Jeder Knoten nummeriert seine Links lokal, dann ist das 2-Tupel (Router ID, Linknummer) netzweit eindeutig. Das bedeutet, dass die Signalisierungsverfahren wie OSPF, IS-IS, CR-LDP und RSVP-TE darauf angepasst werden, mit 2-Tupel Kennungen anstelle der IP Adressen zu arbeiten.

GMPLS Label Format

Bei GMPLS ist der Label 32 Bit lang statt nur 20 Bit (plus TTL, TOS etc. insgesamt ebenfalls 32 Bit). Dadurch können auch Lambda-Typen und SDH Frame Strukturen auf den Label gemappt werden, um spezielle Bandbreiten-Bereitstellungen zu kennzeichnen.

Link Management Protokoll (LMP)

Als Konsequenz der MPLS Erweiterungen ist ein Label nicht länger eine abstrakte Kennung sondern muss z.B. Zeitslots, Lambdas und physische Ressourcen wie Switchports abbilden. Das bedeutet: Irgend jemand muss die Labelzuweisung zwischen benachbarten Knoten generieren.

Hierfür wird ein neues Protokoll spezifiziert, das LMP, Link Management Protocol. Es läuft zwischen benachbarten Knoten und handhabt die Einrichtung von Kontroll-Kanälen, Fehlererkennung, Korrelation von Link Eigenschaften und Prüfung der Connectivity. Eine Schlüsselfunktion von LMP ist, zwischen benachbarten Knoten solche Link ID's zuzuweisen, die anschließend als Label für physische Ressourcen genutzt werden können. Somit müssen die Zuweisungen nicht mehr manuell konfiguriert werden, was wiederum Anforderung (3) erfüllt.

Korrelation von Link Eigenschaften bezieht sich auf z.B. Link ID, Protection Verfahren und Priorität zwischen benachbarten Knoten. Sie erfolgt, wenn der Link anfänglich aufgebaut wird und kann intervallgesteuert wiederholt werden. LMP ist so in der Lage, Link Fehler und Kanalfehler in transparenten (rein optischen) und opaquen (optoelektrischen) Netzen unabhängig vom dort verwendeten Datenformat zu isolieren. Dies erfüllt Anforderung (4).

LMP erlaubt die Trennung von Kontroll-Ebene und Komponenten-Verbindungen zur Lösung von Anforderung (5). Beispielsweise kann der Kontroll-Kanal über eine spezielle Wellenlänge (Lambda), eine spezielle Glasfaser oder eine separate Ethernet Verbindung gesendet werden. Mit dem netten Nebeneffekt, dass eine Störung der Datenwege nicht notwendig den Kontroll-Kanal betrifft. Sie kennen die Vorteile dieser Taktik vom Thema Outband Management.

Zusätzlich zu LMP erarbeitet die IETF Arbeitsgruppe CCAMP (Common Control and Measurement Plane) Erweiterungen für IGP Protokolle wie OSPF und IS-IS, um GMPLS zu unterstützen.

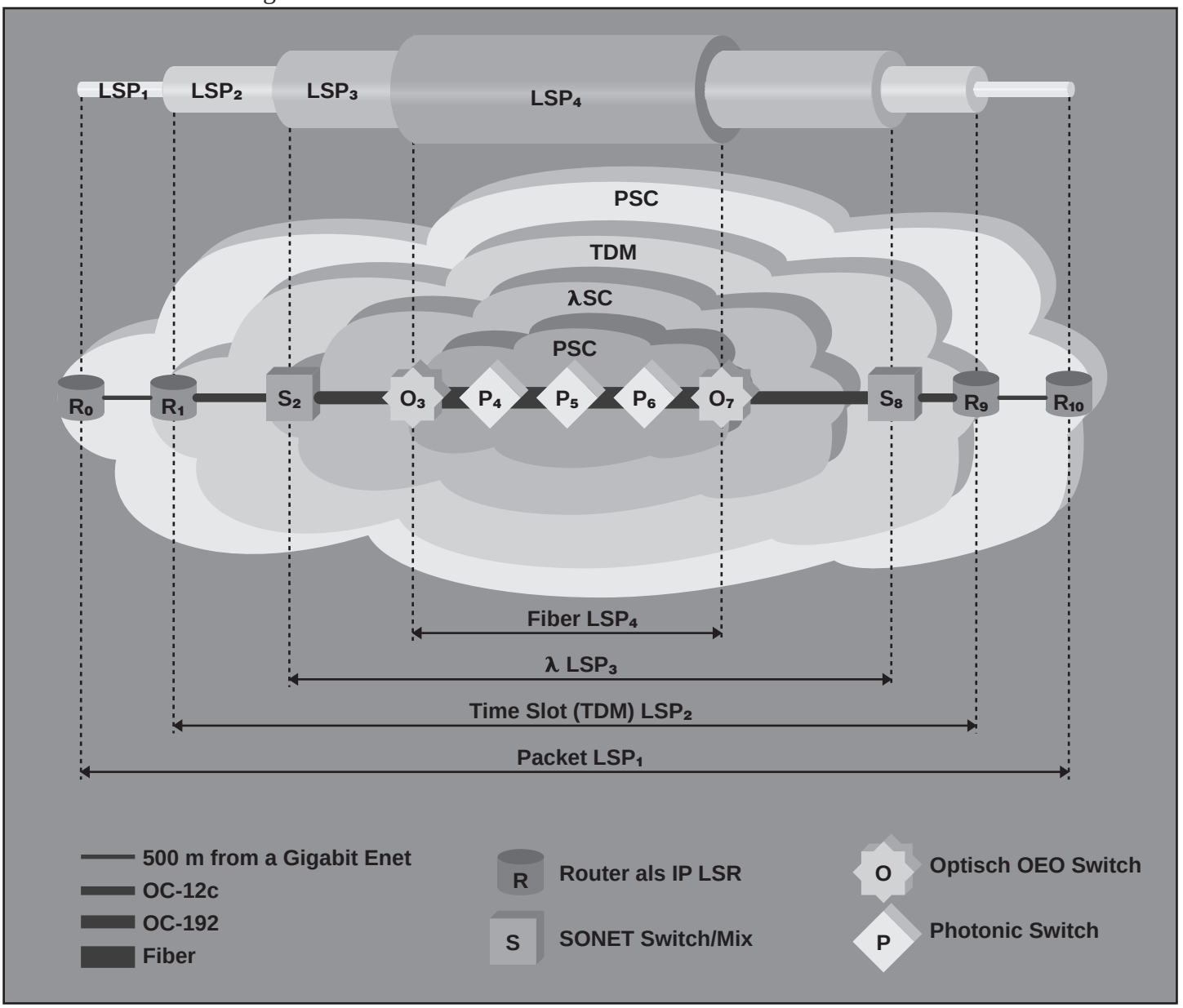
8.3 GMPLS Signalisierungs-Erweiterungen

Hierarchische Signalisierung von LSPs

Klassisches MPLS setzt voraus, dass ein LSP an einem LER anfängt und an einem anderen LER aufhört. Dieses Konzept wird bei GMPLS hierarchisch erweitert, LSPs können auf jeder Hierarchie-Ebene betrieben werden. Es gilt lediglich die Regel, dass ein Path auf gleichen Komponenten oder auf derselben Hierarchie-Ebene anfangen und enden muss: Ein Ethernet Path muss mit Ethernet starten und terminieren, ein Lambda Path muss auf einem WDM-Gerät starten und terminieren. Ein Lambda LSP kann dabei über mehrere physikalische Geräte hinweg verlaufen, was nicht mehr der klassischen Definition von Nachbarbeziehung (Adjacency) entspricht.

Wir betrachten nun, wie LSPs einer niedrigeren Ebene die Bildung höherwertiger LSPs anstoßen. Betrachten Sie hierfür das Beispiel in Bild 41. Die Bandbreite, die für LSP1 signalisiert wird, beträgt 500 Mbit/s Bandbreite. Alle Links, die dieser LSP durchläuft, müssen die 500 Mbit/s unterstützen können. R0 klassifiziert und mappt Pakete auf LSP1 und drosselt die Last auf 500 Mbit/s, falls notwendig (Shaping). Die 500 Mbit/s von LSP1 werden von LSP2 provisioniert, der auf dem nächsthöheren SDH Inkrement läuft, also OC-12c. Der Switch S2 packt OC-12c in LSP3, der ein OC-192 zwischen S2 und O3 ist. Der optische Switch O3 schnappt sich diesen für ihn leichten OC-192 und schleppt ihn durch LSP4, einen WDM-Kanal nach P4. Die OC-192 (zugehörig zu LSP3) werden durch P4, P5 und P6 nach O7 geschleift. O7 macht weiter, sucht das passende Lambda aus und schickt das Signal zum Nachbarport S8. S8 sucht einen passenden OC-12c aus den OC-192 und sendet diesen an R9 weiter. Schließlich und endlich nimmt der Router R9 dem OC-12 die Pakete ab und leitet sie an R10 weiter.

Bild 41 Aufbau geschachtelter LSPs von den unteren zu oberen Hierarchie-Ebenen



MPLS-Serie – Teil 5

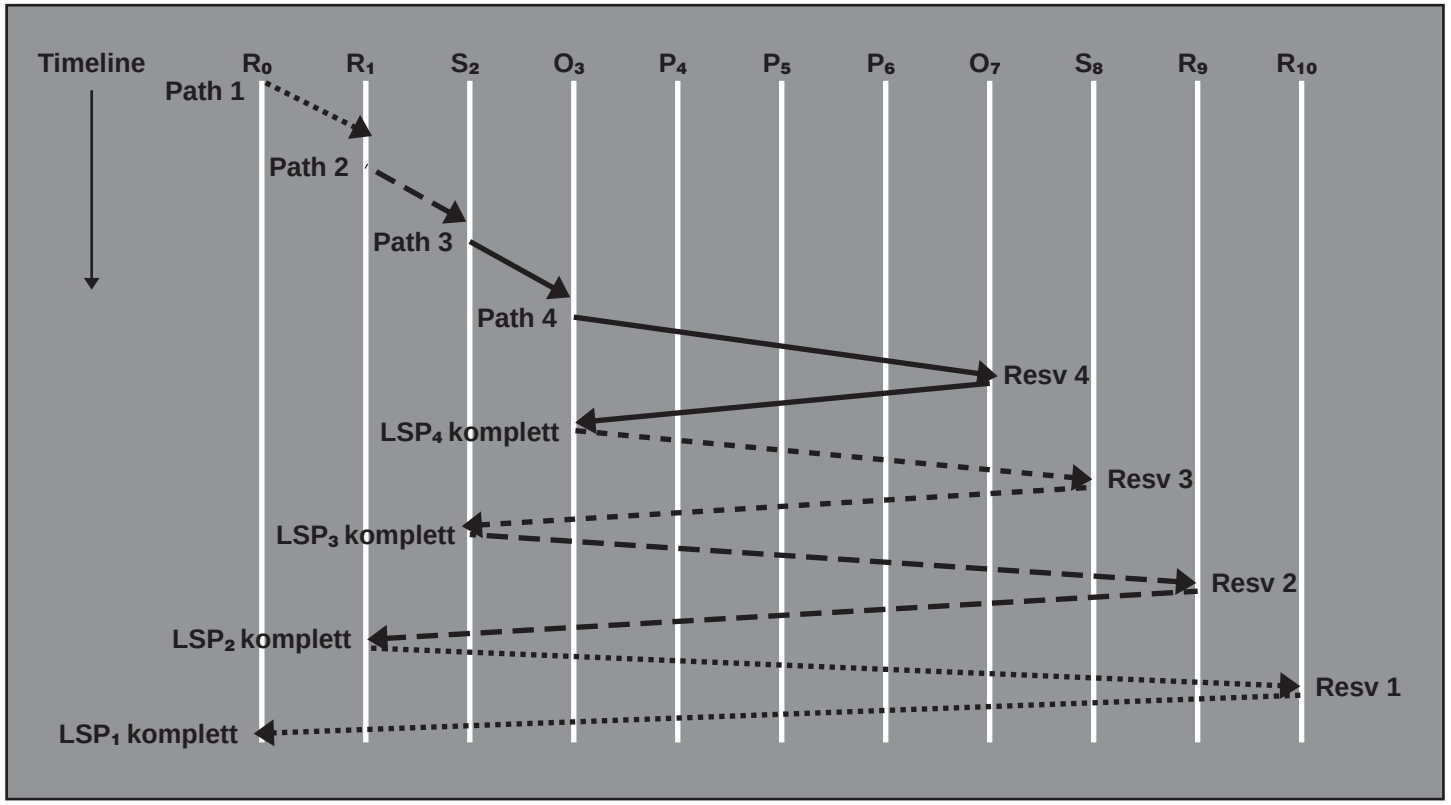


Bild 42 Path Request mit RSVP-TE und entsprechenden GMPLS-Erweiterungen

Ausgeschlossen, so etwas manuell zu konfigurieren. Betrachten wir also am Beispiel von Bild 41 und 42, wie eine RSVP-TE Signalisierung für diesen Fall aussieht, wenn die für GMPLS definierten Erweiterungen genutzt werden. Nehmen wir hierfür an, die angefragten Bandbreiten wären auf allen Verbindungen noch frei. Die Einrichtung von LSP1 triggert folgendes: LSP2, eine STS-12c Verbindung zwischen R1 und R9; LSP3, eine OC-192 Verbindung zwischen S2 und S8; und LSP4, WDM-Kanäle zwischen O3 und O7. Dabei ist anzumerken, dass die verfügbare Bandbreite in der LSP Hierarchie von dem genutzten IGP bekannt gegeben wird wie folgt:

- Knoten R1 gibt einen Packet-Switch-Capable (PSC) "Link" von R1 nach R9 bekannt mit einer Bandbreite, die gleich der Differenz zwischen der STS-12c (622 Mbit/s) Kapazität und den in LSP1 bereitgestellten 500 Mbit/s ist.
- Knoten S2 verkündet den Gegenwert für 180 STS-1 Kanälen als TDM "Link".
- Knoten O3 gibt 15 Lambdas an, von denen jedes OC-192 Bandbreite für einen Lambda-Switch-Capable (LSC) "Link" hat.

O-UNI zur Vereinfachung

Anhand der beschriebenen Funktionen wird klar, dass Signalisierung und Routing für GMPLS Netzwerke eine komplexe Kontroll-Ebene erfordern, die die Hersteller möglicherweise gar nicht in jeder Komponente implementieren wollen. Für Komponenten mit eingeschränkter GMPLS-Fähigkeit hat das OIF die O-UNI Schnittstelle in Abstimmung mit den GMPLS-Spezifikationen der IETF entwickelt.

Labelvorschlag und Bidirektionale Signalisierung

Klassische MPLS LSP's sind unidirektional. Protokoll-Änderungen für optische LSP's müssen daher sowohl die typischerweise bidirektionale Natur von optischen LSP's berücksichtigen als auch die Tatsache, dass einige optische Komponenten wie z.B. MEMS (Micro Electrical Mechanical Systems) eine bestimmte Umschalt-Zeit benötigen, um die Änderungen zu aktivieren. GMPLS erlaubt daher, Labels in Downstream Richtung vorzuschlagen (Ingress nach Egress, also auf dem "Rückweg" der Signalisierung) um Latenzzeit zu reduzieren. Allerdings entsteht dabei das Risiko, dass der LSP-Aufbau scheitern kann, wenn der vorgeschlagene Label beim Downstream Router nicht frei ist.

Der Label-Vorschlag ist eine Optimierung, die von einem Downstream Router überschrieben werden kann, was jedoch meistens zu einer höheren LSP Aufbauzeit und möglicherweise nicht-optimaler Ressourcen-Bereitstellung führt. Der Label-Vorschlag ist besonders hilfreich, wenn ein bidirektionaler LSP aufgebaut werden soll, der Sende- und Empfangs-Paar zum selben physikalischen Port hat. Auch für das Setup eines LSP, der mehrere optische Switchkomponenten durchläuft, bei denen jeweils Latenzzeit für die Konfiguration der Switching Fabric anfällt, z.B. müssen Mikrospiegel in einem MEMS-Switch positioniert werden, und die physikalische Bewegung und anschließendes Fixieren kostet Zeit. Wenn der Upstream Knoten den Label vorschlägt, kann er seine eigene Konfiguration schon durchführen, anstatt auf die Downstream Signalisierung zu warten.

Auch für optische Subnetze mit limitierter Konvertierungs-Fähigkeit für Wellenlängen ist der Label-Vorschlag ein hilfreiches Konzept. In rein optischen Umgebungen, wo zusätzlich noch dieselbe Eingangs- und Ausgangsfarbe Ende-zu-Ende genutzt werden muss, wird das Ganze nochmals schwieriger.

MPLS-Serie – Teil 5

Bidirektionale LSP's oder Lichtverbindungen sind eine Anforderung für viele optische Service Provider. GMPLS unterstützt dies unter der Annahme, dass beide Richtungen dieselben Traffic Engineering Anforderungen für Sharing, Fehlerbehandlung und Ressourcen wie Bandbreite, Antwortzeit und Jitter haben. Der Knoten, der den LSP-Aufbau beginnt, wird Initiator genannt, der Ziel-Knoten wird Terminator genannt, obwohl der Standard nicht von Arnold Schwarzenegger gesponsert wurde.

Unidirektionale LSPs wie bei klassischem MLSP hätten folgende Nachteile:

- Die Latenzzeit wird um ein Round-Trip-Delay vergrößert.
- Der Kontroll-Overhead ist doppelt so hoch.
- Da die Ressourcen in unterschiedlichen Segmenten bereitgestellt werden, kann die Routenauswahl sehr komplex werden (z.B. können Tx und Rx separaten Transpondern in einer WDM-Komponente zugewiesen werden).
- Eine saubere Schnittstelle zu Sonet/SDH wird schwieriger, da Sonet für Protection Switching bidirektionale Hop-by-Hop Paths benötigt.

Notify Nachrichten

Nur schnelle Reaktionen auf Fehler und intelligente Entscheidungen als Folge führen zu einer angemessenen Verfügbarkeit. Wenn ein Fehler auftritt, sollte daher auch ein Transit-Knoten (an dem eine bestimmte Verbindung weder beginnt noch endet), der den Fehler bemerkt, in der Lage sein, nicht-benachbarte Knoten zu informieren, die dafür verantwortlich sind, den Path zu reparieren. Die Information sollte nicht von weiteren zwischengeschalteten Knoten interpretiert, kommentiert, modifiziert, kurz: bearbeitet werden. Also sendet der Transit-Knoten das Notify direkt an Start oder Ziel des betroffenen LSP, oder theoretisch auch an einen in der Mitte liegenden Knoten, wenn er erkennen kann, dass dieser in der Lage ist, den Fehler zu reparieren. Die Erweiterungen in RSVP-TE gehen eher von Start oder Ziel aus. Für CR-LDP wurden keine vergleichbaren Erweiterungen definiert. Zu beachten ist, dass die NOTIFY Message die bisherigen ERROR Messages nicht ersetzt. Sie unterscheidet sich von ihnen aber darin, dass ein Zielknoten angegeben wird, der kein Upstream oder Downstream Knoten des sendenden Routers ist.

8.4 Fehlertoleranz

Fehlerbehandlung auf Verbindungs-Ebene besteht in GMPLS aus vier hauptsächlichen Schritten:

- Erkennung (Detection)
- Lokalisierung (Localization)
- Benachrichtigung (Notification)
- Umgehung (Mitigation)

Fehlererkennung sollte auf der Ebene passieren, die dem Fehler am nächsten ist: dem physikalischen d.h. optischen Layer. Sie erfordert die Kommunikation von Komponenten, um festzustellen, wo der Fehler aufgetreten ist. Angewandte Techniken sind LOL (Loss of Light), zukünftige Techniken OSNR (Optical Signal to Noise Ratio), optisch gemessene BER (Bit Error Rate), Dispersion, Nebensprechen (Crosstalk) und Signalverzögerung. Ein interessanter Effekt beim Einsatz von LOL zur Fehlererkennung ist die Downstream Propagierung, daher können alle Downstream Knoten Kenntnis von dem Fehler erhalten. Das LMP beinhaltet Fehlerlokalisierungs-Prozeduren, die dafür ausgelegt sind, Fehler sowohl in transparenten (rein optischen) als auch in opaquen (optoelektrischen) Netzen zu lokalisieren. Hierfür werden so genannte Channel Fail Nachrichten zwischen benachbarten Knoten gesendet. Das Senden erfolgt outband über einen Kontroll-Kanal, der von den Datenkanälen getrennt ist. Die Trennung von Daten- und Kontroll-Kanal erlaubt es, für Fehler-Lokalisierung einen einzelnen für alle Komponenten gemeinsamen Satz von Nachrichten zu verwenden, ohne Rücksicht auf das Codierungsschema der verschiedenen Datenübertragungs-Ebenen. Ist der Fehler erkannt und lokalisiert, werden wie bei MPLS Protection und Restoration Verfahren eingesetzt, um ihn zu umgehen. Protection und Restauration unterscheiden sich hauptsächlich in der Umschaltzeit, wie an anderer Stelle erklärt wurde. Sie verwenden im Regelfall Path Switching und Line-Switching. Bei Path Switching werden die Endpunkte (Ingress, Egress) des Paths angesprochen, bei Leitungs-Switching der Knoten, an dem der Fehler lokalisiert wurde. Path Switching wird unterteilt in Path Protection und Path Restoration wie unter MPLS erklärt. Line Switching wird unterteilt in Span Protection und Line Restoration. Span Protection schaltet auf einen anderen parallelen Kanal oder Link um, der die beiden betroffenen Komponenten verbindet. Line Restauration schaltet auf eine andere Route zwischen den beiden betroffenen Komponenten um, wobei zwingend andere zwischengeschaltete Komponenten durchlaufen werden. Bei GMPLS Signalisierung wird Span Protection und Path Protection verwendet.

9 Fazit

"Die Konzepte sind modern, intelligent und flexibel. Die Umsetzung allerdings verläuft eher schleppend". Warum trifft das sowohl für MPLS als auch für GMPLS zu?

MPLS

Zur Zeit hat MPLS noch nicht in wesentlichem Umfang zu ROI geführt, da die meisten MPLS Implementierungen entweder auf Quality of Service im WAN abzielten, wofür derzeit noch keine "Killerapplikationen" existieren, oder aber VPN Lösungen waren, die nicht allzu gut skalierten. Trotzdem ist ein Trend erkennbar, von "leitungsvermittelten" / circuit-basierten Netzen auf paketvermittelte Netze zu migrieren, da dies zur Zeit die höheren Übertragungsraten erlaubt. Möglicherweise wird mit Etablierung der DWDM-Technik hier wieder ein Gegentrend einsetzen.

GMPLS

Vorteile von GMPLS sind in der größeren Kontrolle und Flexibilität für Bandbreiten-Provisionierung zu sehen. Ändert sich das Lastprofil, wird die Bandbreiten-Zuordnung dynamisch geändert. Die Einsparung von Protokoll-Ebenen (aus vier mach zwei) vereinfacht die Kommunikation. Dagegen spricht, dass das komplette Switching und Traffic Engineering auf WDM-Ebene geleistet wird, das heißt alle wesentlichen Funktionen für Monitoring, Leistungsüberwachung, Fehlererkennung, Fehlerlokalisierung und Fehlerbehebung müssen für GMPLS "neu erfunden" oder mindestens vorhandene Verfahren dort neu integriert werden.

Die Entwicklung hin zu GMPLS wird sehr langsam und in mehreren Schritten vonstatten gehen. Eine spannende Frage hierbei ist, wie schnell und ob überhaupt DWDM, GMPLS und optische Switches die Sonet Netze in nennenswertem Umfang ablösen werden. Rein optische Netze müssen erst noch den "Proof of Concept erbringen".

GMPLS ist definitiv noch weiter von der Profitabilität entfernt als MPLS. Ein Urteil, ob GMPLS sich wirtschaftlich entwickeln und betreiben lässt, muss der Markt noch fällen.

Tom Nolle (CIMI Corp.) meint dazu: "Sie brauchen keine Standards, wenn Sie gar nicht genug Dienste verkaufen können, die Ihre Investition in diese Standards rechtfertigen".

Anzeige

Ausbildung zum ComConsult Certified Network Engineer

Mit den neuen Terminen für 2003:

Nutzen Sie unsere Paketpreise!

3er Paket: Buchen Sie drei beliebige Seminare unserer Ausbildung zum ComConsult Certified Network Engineer und Sie zahlen statt € 5.970,-- nur den Paketpreis von € 5.190,-- zzgl. MwSt.

Komplett-Paket: Für die komplette Ausbildung mit allen vier Seminaren zum ComConsult Certified Network Engineer zahlen Sie statt € 7.960,-- nur den Paketpreis von € 6.690,-- zzgl. MwSt.

Das CCNE-Praxis-Seminar:

LAN-Praxis-Intensiv-Seminar:
Praktischer Aufbau von lokalen Netzen und Umsetzung typischer Netzwerk-Konfigurationen
Einzelpreis: € 2.290,-- zzgl. MwSt.
Zusätzlich zum Komplett-Paket: € 1.890,-- zzgl. MwSt.

- **20.01. - 24.01.03 in Aachen**
- **05.05. - 09.05.03 in Aachen**

ComConsult Akademie

Lokale Netze
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **09.12. - 13.12.02 in Aachen**
- **27.01. - 31.01.03 in Aachen**
- **17.03. - 21.03.03 in Aachen**
- **19.05. - 23.05.03 in Aachen**
- **21.07. - 25.07.03 in Aachen**
- **15.09. - 19.09.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**
- **10.11. - 14.11.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

Internetworking
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **18.11. - 22.11.02 in Aachen**
- **09.12. - 13.12.02 in Aachen**
- **20.01. - 24.01.03 in Aachen**
- **10.03. - 14.03.03 in Aachen**
- **05.05. - 09.05.03 in Aachen**
- **30.06. - 04.07.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

Neue Ethernet Technologien
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **09.12. - 13.12.02 in Aachen**
- **27.01. - 31.01.03 in Aachen**
- **17.03. - 21.03.03 in Aachen**
- **12.05. - 16.05.03 in Aachen**
- **30.06. - 04.07.03 in Aachen**
- **15.09. - 19.09.03 in Aachen**
- **13.10. - 17.10.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

TCP/IP und SNMP
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **02.12. - 06.12.02 in Berlin**
- **27.01. - 31.01.03 in Bonn**
- **17.03. - 21.03.03 in Berlin**
- **05.05. - 09.05.03 in Bonn**
- **21.07. - 25.07.03 in Berlin**
- **22.09. - 26.09.03 in Berlin**
- **13.10. - 17.10.03 in Berlin**
- **08.12. - 12.12.03 in Berlin**

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Schirmung, Erdung, Potentialausgleich..., 09. - 10.12.02 in Bonn

Das Seminar behandelt die scheinbar unerklärbaren Störerscheinungen in Netzwerken und im Betrieb elektronischer Geräte, die durch Wechselwirkungen mit der Elektroinstallation entstehen.
Referenten: Dipl.-Ing. Karl-Heinz Otto und Hans-Günter Hergesell — Preis: € 990,-- zzgl. MwSt.

Microsofts Windows .Net & PKI, 09. - 10.12.02 in München

Das Seminar macht die Teilnehmer neben den theoretischen Grundlagen einer PKI auch mit der grundsätzlichen Installation, Konfiguration, Administration und dem Betrieb einer Windows 2000 / .Net PKI im Rahmen von Live-Präsentationen vertraut.
Referent: Dipl.-Ing. Martin Barbian (ITC GmbH) — Preis: € 1.290,-- zzgl. MwSt.

Optische Netze und 10 Gbit Ethernet, 09. - 11.12.02 in München

Das Seminar führt in die faszinierende Welt der 0ptischen Netze, die ausgehend von den Aufrüstungen der Carrier auch für die Bereiche SAN, LAN-Backbone, MAN und Access eine bisher ungeahnte Leistungsdimension erschließen.
Referent: Dr. Franz-Joachim Kauffels — Preis: € 1.590,-- zzgl. MwSt.

Integrierte Lösungen ... 09. - 11.12.02 in Bonn

Das Seminar beschäftigt sich mit der Voraussetzung für die Sicherstellung der Verfügbarkeit und der Performance der Unternehmenswichtigen Applikationen am Arbeitsplatz: eine funktionale und datentechnische Integration der einzelnen Management-Lösungen für Netzwerke, Server, Clienten und Applikationen.
Referenten: Dipl.-Verwaltungswirt Jürgen Dierlamm, Dr. Jürgen Suppan — Preis: € 1.590,-- zzgl. MwSt.

Cisco-Router erfolgreich einsetzen, 09. - 13.12.02 in Aachen

Das Seminar lehrt den Aufbau und die Arbeitsweise von Cisco-Routern an Cisco 2600 Routern, an denen die Teilnehmer aktiv arbeiten können. Referent: Markus Schaub — Preis: € 2.590,-- zzgl. MwSt.

Lokale Netze für Einsteiger, 09. - 13.12.02 in Aachen

Das Intensiv-Seminar vermittelt die grundsätzliche Funktionsweise, das Leistungsspektrum, aber auch die Defizitbereiche Lokaler Netze. Es bietet ein solides Fundament für den erfolgreichen Einstieg in den Netzwerk-Alltag.
Referenten: Dipl.-Ing. Roland Moos und Dr. Jürgen Suppan, ComConsult Akademie — Preis: € 1.990,-- zzgl. MwSt.

Internetworking, 09. - 13.12.02 in Aachen

Das Seminar vermittelt die technischen und methodischen Kenntnisse zur erfolgreichen Strukturierung von Netzwerken mit Switching und Routing wobei Grundlagen-Kenntnisse Lokaler Netzwerk-Technologien erforderlich sind.
Referentin: Dipl.-Inform. Petra Borowka — Preis: € 1.990,-- zzgl. MwSt.

Neue Ethernet-Technologien, 09. - 13.12.02 in 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.
8 Referenten der ComConsult Beratung und Planung GmbH — Preis: € 1.990,--zzgl. MwSt.

ComConsult Akademie – Telefax: 02408/955-399

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 **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**	Telefon	Fax
	eMail	Unterschrift

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerkkomponenten

Die Spielregeln

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen. Die Spielregeln: Sie melden uns ihr Angebot oder Gesuch per Mail, mit dem Fax-Formular (unten) oder über den Web-Server. Wir veröffent-lichen es unter einer Anzeigen-Nr. im Netzwerk Insider und auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de. 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.

Gebote

Adapter

Allied Telesyn Modell: MX40F/ST, MX26F/ST, Anzahl 60, Preis VB, Bemerkung: als Gesamtpaket Anzeigen-Nr. B20908

Madge Modell: MKII/BM2, Anzahl 100, Preis VB, Bemerkung: Win9x,NT,W2K,XP, Anzeigen-Nr. B21003

Madge Smart LAM STP & UTP, Anzahl 10, Preis VB Anzeigen-Nr. B21002

3Com Accessbuilder 4000, Anzahl 1, Preis VB, Bemerkung: ohne Handbücher, Anzeigen-Nr. B20906

Hub

10Base-T Hub, Anzahl 1, Preis VB Anzeigen-Nr. B21016

Net Worth 16 Port 10Base-T RJ45, Anzahl 3, Preis VB, Anzeigen-Nr. B21013

Netgear 10Mbit Hub Model EN516, Anzahl 1, Preis VB, Anzeigen-Nr. B21011

Hirschmann Modell: ASGE 1 RE, Anzahl 20, Preis 80 Euro, Bemerkung: Hubs sind sehr gut einsetzbar in der Industriellen Ethernet Kommunikation (Automatisierungstechnik) für Twisted-Pair und Fiberoptische Übertragungsstrecken mit 10 Mbit zB. als Siemens OLM Diverse Interfacekarten wie OYDE, UYDE, CYDE. Anzeigen-Nr. B20901

IBM Modell: 8230-013, Anzahl 15, Preis 175 Euro, Bemerkung: Alle Geräte sind geprüft und in sehr gutem Zustand. Anzeigen-Nr. B20903

Gebote

Ringleitungsverteiler

Madge Smart CAU & RAM, Anzahl 15, Preis VB, Anzeigen-Nr. B21001

BinTec MPR Router X4000, Anzahl 1, Preis VB, Anzeigen-Nr. B21008

Sternkoppler

Hirschmann ASGE, Anzahl 24, Preis VB, Anzeigen-Nr. B21006

Switch/Brücke

IBM Modell: 8229 TR/TR, Anzahl 20, Preis 80 Euro, Bemerkung: Die IBM Brücken 8229 Tokenring/Tokenring sind geprüft und in gutem Zustand Brücke kann umgerüstet werden zu Tokenring/Ethernet, Umrüstkosten: Auf Anfrage, Anzeigen-Nr. B20902

Madge Ringswitch Plus, Anzahl 2, Preis VB, Bemerkung: diverse Module vorhanden, auch einzeln abzugeben Anzeigen-Nr. B21005

Madge Deskstream, Anzahl 2, Preis VB, Bemerkung: Stacking und HSTR Module vorhanden, Anzeigen-Nr. B21004

Hirschmann Gigabit Routing Switch GRS 1403, Anzahl 1, Preis VB Anzeigen-Nr. B21010

DEC FDDI Gigaswitch, Anzahl 2, Preis sehr, sehr günstig, VB, Bemerkung: je Switch mit folgenden Linecards bestückt: 3x DEFGL-AA (Rev. F) FDDI Linecard, dual 4x DEFGL-AB (Rev. A, F) FDDI Linecard,single als Reservematerial einsetzbar, anstelle teurer Wartung! Anzeigen-Nr. B20905

Intel 8 Port 10/100 RJ45, Anzahl 27, Preis VB, Anzeigen-Nr. B21009

Sonstiges

W&T ComServer, Anzahl 1, Preis VB, Anzeigen-Nr. B21014

CentreCom MR 128FT Mediakonverter, Anzahl 1, Preis VB, Anzeigen-Nr. B21015

Hirschmann Media Converter ASGE 230VAC, Anzahl 1, Preis VB, Anzeigen-Nr. B21012

IBM LANROVER 8235-022, Anzahl 1, Preis VB, Anzeigen-Nr. B20907

IBM 3174-13R mit TR-Adapter, Anzahl 1, Preis VB, Anzeigen-Nr. B20415

3Com Core Builder 5000, Anzahl 4, Preis VB, Anzeigen-Nr. B21007

Gesuch

Router

BinTec Modell: Brick-XM, Anzahl 1, Preis VB, Anzeigen-Nr. S20904

Fax an ComConsult
02408/955-399

☐ **Ich suche**

☐ **Ich biete**

☐ **Antwort auf Anzeigen-Nr.** ☐ ☐☐☐☐

Produkt/Komponente/Release/Software

_____

_____

_____

_____

_____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon

_____

Fax

_____

eMail

Weitere Anzeigen finden Sie auf dem Web-Server der ComConsult Akademie

www.comconsult-akademie.de