**Zeitschrift:** Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses

**Band:** 85 (1994)

**Heft:** 17

**Artikel:** Management von Netzwerken : 2. Teil : Managementumgebung von Kommunikationsnetzen und TCP/IP-Umgebung

**Autor:** Bjenscu, Titu I.

**DOI:** https://doi.org/10.5169/seals-902590

Im ersten Teil dieses Artikels (Bulletin 11/94) wurden die Problematik und die Aufgaben des Netzwerkmanagements vorgestellt. Im vorliegenden zweiten Teil werden die Managementumgebung von Kommunikationsnetzen (das Konfigurations-, Fehler-, Leistungs-, Sicherheits-, OSI-Sicherheits- und Abrechnungsmanagement) und die TCP/IP-Umgebung näher beschrieben. Die wichtigsten Funktionen (Facilities) werden kurz erläutert.

# Management von Netzwerken

## 2. Teil: Managementumgebung von Kommunikationsnetzen und TCP/IP-Umgebung

■ Titu I. Băjenescu

## OSI-Netzwerkmanagement

### Managementumgebung der Kommunikationsnetze

Die OSI-Protokollumgebung (Bild 1) ermöglicht unmittelbare Kommunikation, unterstützt aber auch verteilte Ausführungsumgebungen [1;2]. Jede Protokollschicht ist in der Lage, eine einzelne Instanz einer Kommunikationsverbindung (das Zusammenwirken der an der logischen Verbindung beteiligten Arbeitseinheiten) zu überwachen und zu kontrollieren. Dadurch wird ein ergänzender Mechanismus erforderlich, der in der Lage ist, die Gesamtheit der OSI-Ressourcen (Bild 2) zu beobachten, zu kontrollieren und zu überwachen.

Die Umgebung für eine OSI-Protokollwelt (und somit für das notwendige Management) konkretisiert sich immer mehr; beide Anwendungsservice-Elemente, das *Common Application Service Element* (CASE) und das *Specific Application Service Element* (SASE), unterstützen eine verteilte Systemumgebung. Sie nutzen dabei die Protokoll- und Service-Elemente der Schichten *1–6*. Auf den unteren Schichten steht eine grosse Auswahl an übertragungstechnischen Alternativen bereit, aus denen Subnetze unterschiedlichster Qualität, Geschwindigkeit und Kosten kreiert werden können.

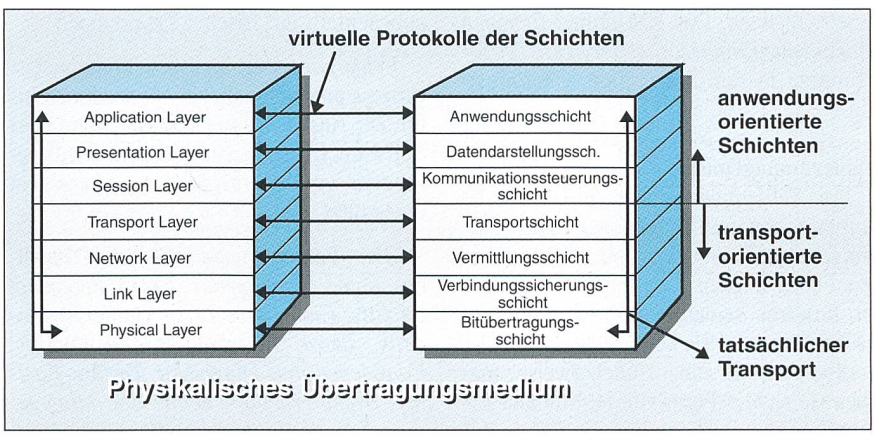



Bild 1 Das ISO/OSI-Referenzmodell

**Adresse des Autors:**
*Titu I. Băjenescu*, M. Sc., Consultant,
13, Chemin de Riant-Coin,
1093 La Conversion/Lutry.

Das OSI Management Framework[1] ist ein ISO-Standardisierungsdokument (DIS 7498-4), welches Richtlinien für die Koordination der Weiterentwicklung bestehender OSI-Managementstandards angibt [1; 3; 4]. Es definiert die Terminologie und beschreibt seine grundsätzlichen Konzepte. Dazu wird ein abstraktes Modell erstellt, welches Ziele und Möglichkeiten des OSI-Netzmanagements aufzeigt. Schliesslich beschreibt es die OSI-Managementaktivitäten.

Die Möglichkeiten des Netzwerkmanagements (NM) in der OSI-NM-Umgebung werden in den fünf Funktionskategorien *Konfigurationsmanagement* (KM), *Fehlermanagement* (FM), *Leistungsmanagement* (LM), *Sicherheitsmanagement* (SM) und *Abrechnungsmanagement* (AM) beschrieben. Für jede der eingeteilten Kommunikationsnetzklassen gibt es spezifische Managementanforderungen; andererseits lassen sich zwischen den Klassen auch Parallelen ziehen. In einer realen Umgebung wird mit grosser Wahrscheinlichkeit ein Netz aus einer Mischung von Subnetzen der angegebenen Klassen bestehen.

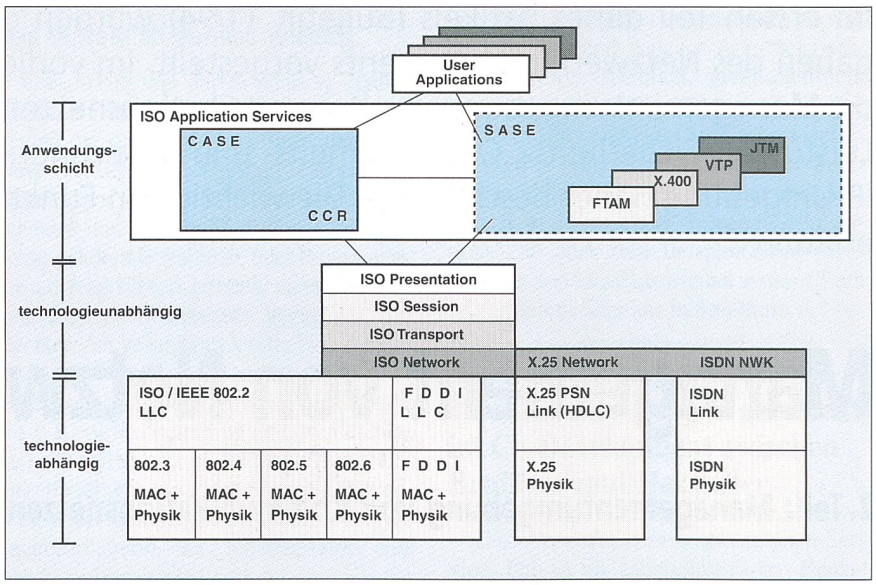



Bild 2 OSI-Gesamtszenario

## Konfigurationsmanagement

Konfigurationsmanagement (KM) ist die Überwachung und Kontrolle herkömmlicher, normaler Operationen in einem offenen System oder Netz. Die Konfigurationsmanagement-SMFA (*Specific Management Functional Area*) versetzt das Netzwerkpersonal in die Lage, operationelle Parameter und Bedingungen, die die laufende Arbeitsweise von Verbindungen im offenen System überwachen, zu erstellen, zu beachten und zu ändern.

Das KM umfasst Definition, Sammlung, Beobachtung, Kontrolle und Benutzung von Konfigurationsdaten[2]. Das KM stellt anderen Specific Management Functional Areas Funktionen zur Verfügung und benutzt auch solche aus anderen Bereichen. Das KM überwacht und kontrolliert ein *Managed Object* über dessen Existenz, Attribute, Zustände und Beziehungen zu anderen Objekten. Das KM ordnet *Common Management Information Services*(CMIS)-Primitive in fünf Kategorien (*Facilities*)[3] ein.

## Fehlermanagement

Das Fehlermanagement (FM)[4] hat die Aufgabe, abnorme Operationen in der OSI-Umgebung zu entdecken und zu identifizieren. Fehler können ein offenes System daran hindern, seinen regulären Aufgaben nachzukommen. Sie können dauerhaft oder vorübergehend sein. Üblicherweise machen sie sich in Form von bestimmten Ereignissen bemerkbar. Die Facilities des Fehlermanagements führen über die Fehler Buch. Sie verarbeiten Nachrichten der Fehlererkennung und handeln danach. Schliesslich helfen sie dabei, Diagnoseroutinen laufenzulassen.

Netzwerk-Administratoren, -Operatoren und -Repairmen können die Elemente des FM dazu benutzen, abnorme Systemoperationen zu erkennen und korrigierend einzugreifen. Dabei gibt es drei prinzipielle Bereiche:

*Fehlererkennung*: Diese läuft prinzipiell auf drei Wegen. Zunächst einmal können Benutzer Fehler während des Ablaufs normaler Operationen feststellen, zum Beispiel durch mitlaufende Überwachungsprozeduren oder durch die Generierung eines Error Reports. Weiter können sich Fehler beim Durchlauf von Zuverlässigkeitstests herausstellen. Schliesslich können sich Fehler durch die Überschreitung voreingestellter Schwellwerte äussern.

*Fehlerdiagnose*: Sie umfasst die Analyse von Error und Event Reports über Managed Objects und den Lauf von Diagnoseprogrammen, die ein Managed Object gegebenenfalls auf frischer Tat ertappen.

*Fehlerkorrektur*: Sie ist ein kombinierter Prozess unterschiedlicher Massnahmen bis hin zur Auswechslung von Hardware oder Software. In den meisten Fällen wird dieser Prozess vom Konfigurationsmanagement unterstützt.

Die Fehlermanagement-SMFA-Facilities sind: *Spontaneous Error Reporting Facility*, *Cumulative Error Gathering Facility*, *Error Threshold Alarm Facility*, *Confidence and Diagnostic Testing Facility*, *Event Tracing Facility* und *Management Service Control Facility* (siehe Facilities-Glossar).

## Leistungsmanagement

Das Leistungsmanagement (LM) dient dazu, das Verhalten von Managed Objects und die Effektivität von Kommunikationsaktivitäten zu bewerten. Seine Funktion ist letztlich die mittel- bis langfristige Bewertung von OSI-Systemen. Dieser Managementbereich muss mit regelmässig gesammelten statistischen Daten versorgt werden, um Trends in der Kommunikation zwischen offenen Systemen zu analysieren oder vorherzusagen. Damit unterstützt er im wesentlichen die mittel- und langfristige Sicherung der Funktionalität durch Vorhersehen und Eingrenzen von Engpässen und die Erweiterung des Netzes durch analytisches Durchspielen von Szenarien.

Das *OSI Performance Management* enthält die Funktionen, Parameter und Nach-

[1] Das OSI Management Framework gilt in der OSI-Managementumgebung, die als Teil der gesamten OSI-Umgebung aufgefasst wird. Die Managementumgebung beinhaltet alle Werkzeuge und Dienste, die für die Kontrolle und Überwachung von Verbindungsaktivitäten und *Managed Objects* gebraucht werden. Die Managementumgebung erlaubt Managern, Daten zu sammeln, Kontrolle auszuüben, das Vorhandensein der Managed Objects zu prüfen und sich über deren Status berichten zu lassen.

[2] Konfigurationsdaten enthalten jede Information über OSI-Betriebsmittel, die zum Management des Systems gebraucht werden. Konfigurationsdaten repräsentieren sowohl statische als auch dynamische Gegebenheiten. Systemadministratoren können diese Konfigurationsdaten auch zu weitergehenden Zwecken wie der Inventur, der Konfigurations- und Erweiterungsplanung, der Netzwerkkonfiguration, dem Netzwerkentwurf, der Systemgenerierung, dem Operator-Support usw. benutzen.

[3] Der Begriff *Facility* für ein Konglomerat von Funktionen, Prozeduren, Parametern und Daten ist bei OSI nicht streng definiert und schwierig zu übersetzen.

[4] Das Fehlermanagement definiert eine Anzahl von Facilities und zu diesen gehörige Prozeduren zur Fehlererkennung und Diagnose. Der Standard legt des weiteren die CMIS-Dienste fest, die diese Facilities unterstützen, und die Klassen von *Managed Objects*, die von den Facilities behandelt werden. Der Standard spezifiziert weiterhin eine Untermenge von Fehlererkennungs- und Diagnose-Facilities zur Bildung realistischer Conformance-Klassen.

richtensätze zur Überwachung von Leistungsdaten, Sammlung und Analyse von Systemstatistiken, Tuning und Kontrolle aufgrund der statistischen Analysen sowie Erstellung von Reports über die Netzleistung. Um effizient zu arbeiten, muss es Leistungsdaten spezieller Betriebsmittel anhand spezifischer Ereignisse und Messergebnisse bestimmen[5]. Dies bedingt, dass die Benutzer Ereignisse, Schwellwerte, Beobachtungsintervalle und Beobachtungszeiträume festlegen können.

Ein Netzmanagementsystem muss in der Lage sein, seinen Benutzern Berichte über die Leistungsfähigkeit des Systems und seine aktuellen (und in der Vergangenheit erbrachten) Leistungen zu geben. Diese Berichte können sich auf ein einzelnes System im Verbund (aber auch auf den gesamten OSI-Bereich, einschliesslich Netz oder beliebige Teilmengen hiervon) erstrecken. Zur Dokumentation des Gesamtbetriebes sind Reports auf täglicher, wöchentlicher, monatlicher oder jährlicher Basis erforderlich. Bei den Facilities[6] ist generell zwischen Funktionen für die Überwachung von irgendwelchen Ereignissen oder Betriebsmitteln und Funktionen zur Auswertung der Ergebnisse der überwachenden Funktionen zu unterscheiden.

### Sicherheitsmanagement

Beim Sicherheitsmanagement (SM) geht es um ein breites Spektrum von Aufgaben, von einfachen Dingen (wie dem Schutz vor zufälligem, unberechtigtem Zugriff durch reguläre Benutzer) bis hin zur Absicherung militärischer oder anderer hochsensitiver Systeme gegen hochspezialisierte Eindringlinge. Ein gegen alle Angriffe völlig sicheres System kann es heute nicht geben [2;5]. Die vorhandenen Klassifikationen definieren Sicherheitsklassen, die den Grad der Sicherheit eines Systems beschreiben. Diesen Klassen ist generell zweierlei vorzuwerfen:

- Der von diesen Klassen generierte Sicherheitsbegriff bezieht sich primär auf militärische Systeme und die in diesen abgespeicherten Daten. Dies führt aber zu einer relativ statischen Perspektive, da dynamische Änderungen und die Behandlung der Daten ausserhalb der Intervalle, in denen sie im Speicher liegen (funktionelle Integrität), weitgehend ausser acht gelassen werden.
- Ausserhalb des militärischen Bereiches gibt es noch andere Anforderungen, die die Sicherheit im weiteren Sinne betreffen und die mit der Zuverlässigkeit und der Ausfallsicherheit zusammenhängen. Die Unsicherheit, die bereits bei der Betrachtung isolierter Systeme besteht, setzt sich im Netzbereich potenziert fort.

Zurzeit gibt es bei ISO mehrere Arbeitsgruppen, die sich im Rahmen des Netzwerkmanagements und des Security Framework mit Sicherheit befassen.

### OSI-Sicherheitsmanagement

Auch für das OSI-System [6;7] gibt es eine Sicherheitspolitik, die durch das *OSI Security Framework* beschrieben wird. Das OSI-Sicherheitsmanagement unterstützt die Funktionen dieses Frameworks insbesondere durch die Realisierung von Sicherheitsaspekten in den einzelnen Schichten (Bild 3), Schnittstellen, Protokollen und Diensten. Die Beachtung dieser Sicherheitsaspekte unterliegt wiederum den Aspekten des Security Framework und liegt vielfach im Sichtbereich der einzelnen Schichten. So bleibt für das Sicherheitsmanagement SMFA lediglich die Realisierung von Hilfsfunktionen und Schnittstellen, die die Sicherheitsfunktionen der einzelnen Schichten benutzbar machen und koordinieren. Das Standardisierungsgebäude ist momentan in diesem Bereich noch ziemlich wackelig.

Kernelemente des OSI-Sicherheitsmanagements sind die Sicherheitspolitik und Sicherheitsobjekte. Sie werden durch OSI-Sicherheitsmanagementdienste und -mechanismen beschrieben. Wir unterscheiden drei Bereiche:

*Security Related Object Management*: Es benutzt die gleichen Facilities wie die Konfigurationsmanagement-SMFA und verwaltet damit sicherheitsbezogene Objekte, Attribute, Zustände und Beziehungen.

*Security Related Event and Audit Trail Management*: Dieses arbeitet mit Facilities, die denen des Fehlermanagements entsprechen, und ermöglicht vor allem die Erstellung, Pflege und Weitergabe von Audit Trails.

*Security Management*: Es ist ein Platzhalter für den noch undefinierten Rest.

### Abrechnungsmanagement

Das Abrechnungsmanagement (AM)[7] umfasst Mechanismen zur Überwachung und Kontrolle von Informationen und Betriebsmitteln, die individuelle Nutzer der OSI-Umgebung betreffen. Es gibt zwei grundsätzliche Aspekte: Kosten für ein Kommunikationsmedium und Übertragungssystem sowie Kosten für Betriebsmittel in den Endsystemen. Die Endsysteme und das Kommunikationssystem können dabei zu unterschiedlichen Abrechnungsdomänen gehören. Jede Domäne kann eigene Festlegungen über Kosten und deren Behandlung haben. Also ist der Austausch von Kosteninformationen zwischen den Domänen erforderlich[8].

Vor allem in der Anwendungs- und in der Vermittlungsschicht gibt es eine Reihe

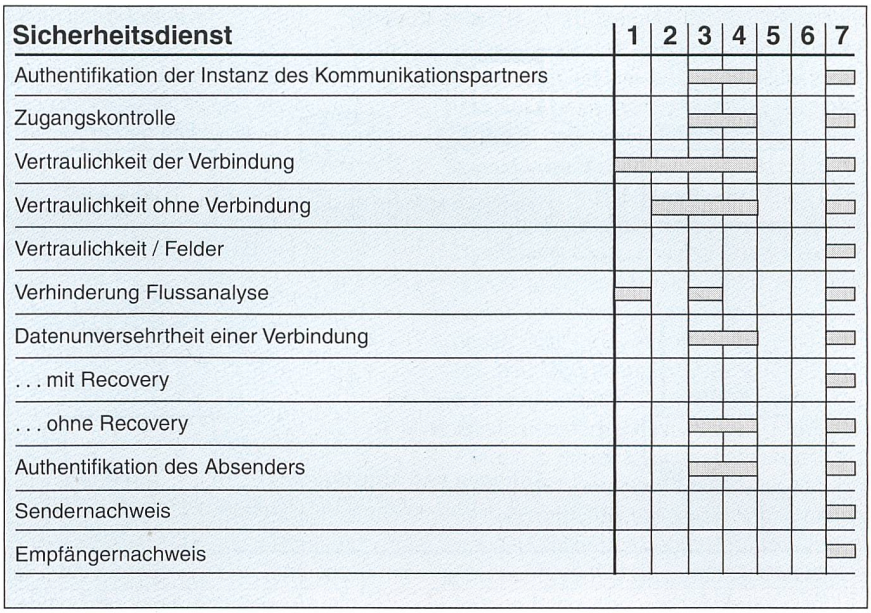



**Bild 3** Sicherheit in ISO/OSI

[5] Gibt es Anhaltspunkte dafür, dass bei den Leistungseckdaten eines offenen Systems etwas nicht stimmt, so müssen die Benutzer in die Lage versetzt werden, das System für eine bessere Leistung abzustimmen. Dazu müssen sie in der Lage sein, Betriebsmittel-Zuordnungen, -Parameter und -Attributwerte zu verändern. Derartige Funktionen greifen jedoch auch wieder in das Konfigurationsmanagement hinein, und die Beibehaltung der strikten Trennung der einzelnen Bereiche ist wiederum fraglich.

[6] In diesem Bereich ist die Standardisierung noch nicht besonders weit vorgedrungen.

[7] Ein System, welches Daten für Abrechnungszwecke erzeugt, heisst *Accounting Management Agent*. *Accounting Manager* sind dann solche Systeme, die Abrechnungsmanagementdaten abfragen oder auf andere Weise erhalten. Ein System kann auf diese Weise beide Rollen spielen.

[8] Der Standard spezifiziert, wie CMIS und CMIP für das Abrechnungsmanagement benutzt werden können, und definiert daher eine Menge von Facilities und Prozeduren zur Unterstützung des Abrechnungsmanagements, die Art und Weise der Benutzung von CMIS-Diensten, die betreffenden Klassen von Managed Objects und Untermengen für Conformance-Zwecke.

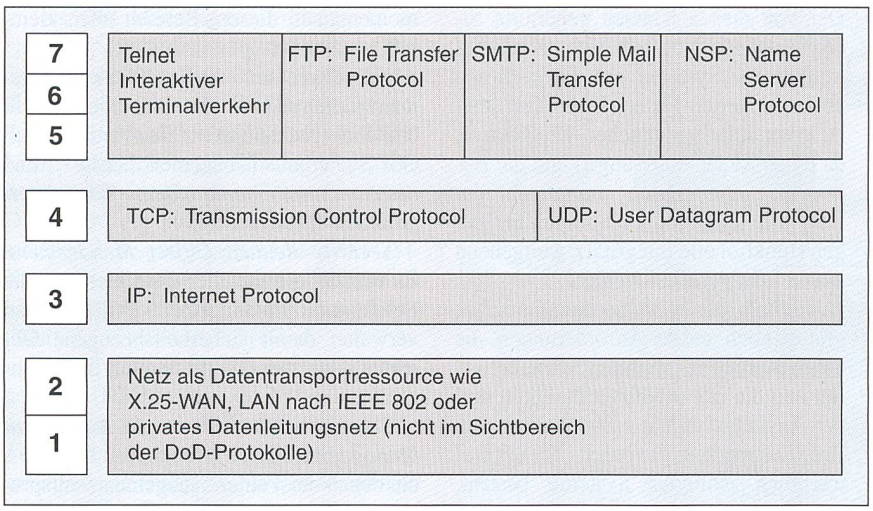



Bild 4 DoD-Protokollfamilie

von Abrechnungsprozeduren, die dienst- oder verbindungs(netzwerk)spezifisch sind und es den Benutzern erlauben, Abrechnungen zu aktivieren, Abrechnungsinformationen zu sammeln, diese aufzulisten und auszuwerten sowie um Abrechnungen zu verhandeln. Die Abrechnungs-SMFA überdeckt diejenigen Managementaktivitäten innerhalb eines offenen Systems, die den tatsächlichen Austausch von Abrechnungsinformationen betreffen.

Wenn das Abrechnungsmanagement über verschiedene Systeme verteilt wird, kann verlangt werden, dass alle Systeme ihren Bereich zunächst eigenständig kontrollieren. Weiterhin kann ein System von den anderen Systemen entsprechende Informationen zu eigenen Abgleichungszwecken verlangen. Die SMFA legt hier praktisch keine Beschränkungen auf.

Obwohl das Abrechnungsmanagement eine sehr handfeste Angelegenheit ist, ist auch dieser Standard noch nicht sehr weit gediehen.

## Die TCP/IP-Umgebung

Die TCP/IP-Protokollfamilie ist nicht für ein spezielles Nachrichtensystem (wie zum Beispiel ein LAN) konzipiert, sondern auf verschiedenen Übertragungsmedien, -systemen und -netzen und auf verschiedenen Rechnern einsetzbar. Somit realisiert die DoD-Protokollfamilie (Bild 4) bereits heute Zielsetzungen des ISO/OSI-Modells, entspricht jedoch nicht den internationalen Standards. Der eigentliche Vorteil der DoD-Standards ist, dass sich die Standardisierung nicht nur auf die unteren Schichten beschränkt hat, sondern dass auch für die oberen Schichten *5–7* Standards und Anwendungen definiert wurden, die inzwischen auf fast allen Datenverarbeitungssystemen implementiert worden sind.

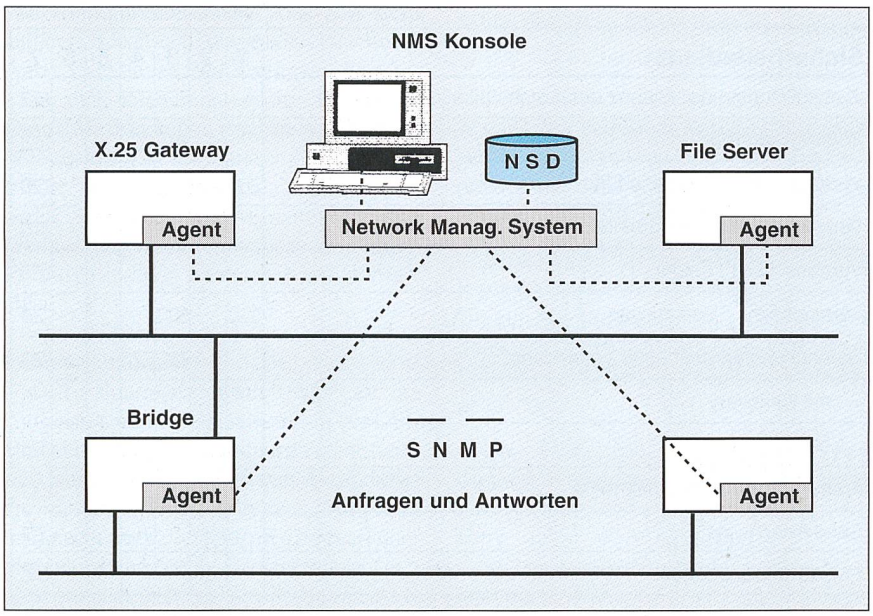



Bild 5 SNMP: das zentrale Management-Modell

### SNMP: Simple Network Management Protocol für TCP/IP-Umgebungen

Ein Netzwerk-Management-System ist um so nützlicher, je weiter es reicht. SNMP wurde als Internet-Managementsystem entworfen; ein Endpunkt im Internet ist heute jedoch immer seltener eine individuelle Station und immer häufiger ein LAN. SNMP hat das Ziel, Netzwerkmanagern einen zentralen Punkt zur Beobachtung, Kontrolle und Verwaltung ihrer Installationen – völlig unabhängig von herstellergebundenen Konzepten – zu geben [8;9]. Die TCP/IP-Familie[9] besteht aus einer Reihe von Protokollen für die Schichten *3–7* und wurde für den Verbund heterogener Systeme und zur Vereinheitlichung der Computer-Kommunikation im Rahmen des Arpanet entwickelt.

Auf SNMP basierende Produkte ermöglichen die Pflege von komplexen Internets und die Rekonfiguration eines weiten Spektrums von Geräten im Netz vom Router bis zur Workstation (WS) in Abhängigkeit vom aktuellen Bedarf. Diese Produkte basieren auf leistungsfähigen WS mit graphischem Benutzerinterface. So kann der Netzwerkmanager bequem, nur mit Hilfe einer zentralen WS, durch das Netz «reisen» und sich die Schwachstellen ansehen – im Idealfall, bevor es zu Fehlern kommt. SNMP wurde auch um Steuerungsfähigkeiten für Nicht-TCP/IP-Geräte wie IEEE 802.1-Bridges erweitert; es enthält auch andere Teile wie die *Management Informations Basis* (MIB) und die *Structure of Management Information* (SMI)[10]. Die *Netzwerk Management Station* (NMS) ist eine zentrale Komponente (WS), die dem Administrator einen Überblick über den Zustand des Netzes verschafft und ihm Möglichkeiten zum Eingriff gibt. In den einzelnen Netzwerkgeräten residieren sogenannte Agents, das heisst kleine Pro-

[9] TCP/IP (*Transport Control Protocol / Internet Protocol*) stellt einen sicheren Process-to-process-Kommunikationsdienst der Schichten *3* und *4* in einer Multinetwork-Umgebung zur Verfügung. Es ist ein Host-zu-Host-Transportprotokoll unter Benutzung mehrerer Netzwerke. Wichtige Stärke: hervorragende Sicherungsmechanismen; Schwäche: aufwendiger Routing-Mechanismus. Das *User Datagram Protocol* (UDP) erlaubt Anwendungsprozessen – ohne Aufbau einer virtuellen Verbindung – Datagramme auszutauschen. TCP und UDP setzen auf IP auf. IP ermöglicht den Austausch der Daten über mehrere Netze hinweg, garantiert aber weder eine Ablieferung der Datagramme beim Empfänger noch eine Einhaltung der Reihenfolge der Datagramme. Er ist in der Lage, eine entsprechende Fragmentierung bei unterschiedlichen zulässigen Nachrichtenlängen auf den verschiedenen Netzen durchzuführen. Telnet, SMTP (*Simple Mail Transfer Protocol*) und FTP (*File Transfer Protocol*) sind für den Benutzer direkt verfügbare Anwendungen, die TCP sowie IP benutzen.

[10] MIB ist eine Ansammlung von Objekten, die Geräte im Netz und deren interne Komponenten abstrakt repräsentieren. SMI ist eine Menge von Regeln zur Definition der Charakteristika von Netzwerkobjekten und ein Regelwerk darüber, wie Managementprotokolle Informationen über diese Objekte beschaffen.

gramme für die Ausführung der wichtigsten Managementfunktionen wie die Aufnahme von Zustandswerten vor Ort (Bild 5).

### SNMP-Struktur und -Funktionen

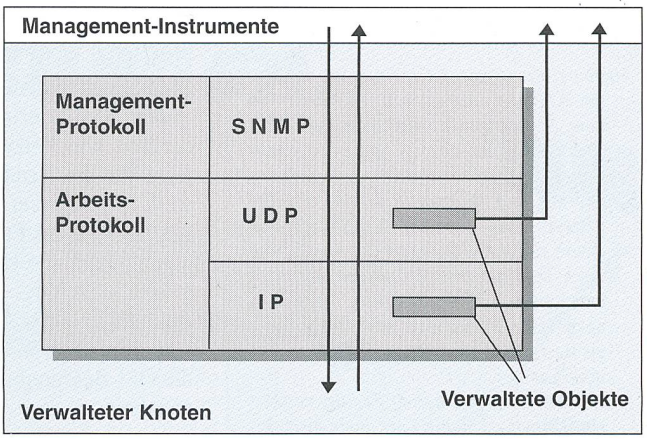
SNMP [3;9] basiert auf der TCP/IP-Protokollfamilie und ist für den Einsatz im Rahmen der verteilten Datenverarbeitung mit PCs, WS, Minis und Grossrechnern in der kommerziellen Büroumgebung und Verwaltung gedacht. Im engeren Sinne ist SNMP das Protokoll zur Zusammenarbeit zwischen Agents und NMS; alle SNMP-Systeme benutzen dabei sowohl das verbindungslose UDP-Protokoll als auch das verbindungsorientierte TCP für den Nachrichtenaustausch (Bild 6). Die Management-Software in der NMS überwacht und kontrolliert Geräte durch Abfrage von Werten, die die Agents zusammenstellen[11].

Ein SNMP-System unterstützt drei wichtige Typen von Kommandos: GET, SET und EVENT. Eine weitere SNMP-Funktion ist ein Proxy Agent, der es einer Managementstation ermöglicht, Netzwerkelemente zu überwachen und zu kontrollieren, die die SNMP-Spezifikationen nicht implementieren. Der Proxy kann dazu Protokolle konvertieren und verschafft der NMS ein einheitliches Bild.

### SNMP MIB

SNMP MIB ist eine datenbankartige Ansammlung von Objekten[12] in den Agents, die von der Management-Workstation aus beobachtet und kontrolliert werden kann. Das Ziel der verteilten MIB ist die Schaffung eines einheitlichen, protokollunabhängigen Datenraums. Jedes Gerät im Sichtbereich des SNMP heisst *verwalteter Knoten* und hat drei Softwarekomponenten: Übertragungsprotokolle wie TCP/IP oder UDP, die die eigentliche Arbeit verrichten, ein Managementprotokoll (SNMP), welches die Fernüberwachung und Kontrolle der verschiedenen Übertragungsprotokolle ermöglicht, und Managementinstrumente, die mit den Übertragungsprotokollen[13] zusammenwirken, um die Überwachung und die Kontrolle zu implementieren.

Bild 6 SNMP: verwalteter Knoten




Die MIB definiert 126 hierarchisch organisierte Objektgruppen, die zum Teil permanent oder temporär obligatorisch sind. Die höchste Stufe sind Tafeln, die aus Einträgen zusammengesetzt sind. Die zwei wichtigsten Operationen, die die Management-Software auf der MIB ausführt, sind SET- und GET-Funktionen. Die Information betreffend zum Beispiel die Adresse der nächsten Hops in einer IP-Routing (die in den seltensten Fällen explizit ausgefürt wird) kann der Manager über das GET bekommen.

### Kontrollfunktionen

Vom zentralen Punkt der Workstation aus vollziehen die Administratoren und Netzwerkmanager ihre Beobachtungs-[14], Überwachungs-, Steuerungs- und Installationsfunktionen. Wenn ein Gerät nicht mehr funktioniert, tritt eine Alarmbedingung oder *Trap* auf. Es gibt fünf wichtige Ereignisse, die zu einer Trap führen[15]:

- Niedergang einer Verbindung
- Neustart einer Verbindung
- Initialisierung eines Agent
- Neustart eines Agent
- Fehler bei der Authentifikation, wenn ein unberechtigter Benutzer ohne entsprechende Autorisierung versucht, Zugang zu einem Agent zu bekommen.

Parameteränderungen werden prinzipiell auf der Basis des SET-Kommandos ausgeführt, die es in Analogie zu den GET-Kommandos ermöglichen, Variablen in den Tabellen zu setzen. Die gesammelten Daten können des weiteren dazu verwendet werden, langfristige Planungsaufgaben zu unterstützen. Letztlich sind auch Künstliche-Intelligenz-(KI-)Programme denkbar, die auf der Basis der NSD-Daten oder von Erfahrungen und Regeln dem Netzwerkmanager (besonders im Falle von grösseren Netzen) Vorschläge für seine weitere Arbeit unterbreiten.

### SNMP-Grenzen, -Probleme und -Zukunft

SNMP ist eine zentral orientierte, taktische Lösung für die heutigen Probleme der Netzmanager und wurde auf Einfachheit optimiert [9]. Auch wenn SNMP in der jüngsten Vergangenheit mit vielen verschiedenen Erweiterungen ausgestattet wurde, kann es seine Herkunft – die TCP/IP-Internetzwerk-Umgebung – nicht verleugnen. Es war nie dazu gedacht, beispielsweise Konfigurationsmanagement auf hohem Niveau zu realisieren, und seine Fähigkeiten sind auf die Überwachung von Netzen und die Isolation von Fehlern beschränkt. SNMP ist vielmehr ein dringend benötigtes Hilfsmittel für die Integration unterschiedlicher Teilnetze und diese verbindender Geräte wie Bridges und Router.

SNMP ist primär im Hinblick auf Funktionalität (und weniger im Hinblick auf Sicherheit) konstruiert worden; zwischen den Kommunikationspartnern besteht keine Session. Eine totale Kontrolle ist hier sicherlich unangebracht und auch wirtschaftlich nicht vertretbar. Der Schutz der Daten und Anwendungen muss im Netz «weit oben» oder «weit aussen» liegen, nämlich bei den Anwendungen selbst und im Rahmen der sie unterstützenden anwendungsorientierten Grunddienste wie FTAM oder FT, da ja in den meisten Fällen nicht bekannt ist, über welche Wege Anwendungen in einer verteilten Umgebung kommunizieren. Die Zukunft von SNMP sieht äussert gut aus [10–12], da die wichtigsten Hersteller von Rechnern, von LAN- und TCP/IP-Software, von Internet-Umgebungen sowie

[11] Die wichtigste Aufgabe eines Agent-Programms ist das Bereithalten von Informationen über die Objekte, die den kritischen Teilen und Aktionen des vom Agent betreuten Gerätes entsprechen. Die Agents speichern diese Informationen und geben sie auf Anfrage an ein Managementprogramm ab. Unaufgeforderte Meldungen (Alarme) werden von den Agents nur im Rahmen kritischer Bedingungen, aussergewöhnlicher Fehler und bei Stromversorgungsausfällen erzeugt.

[12] Diese Objekte sind meist statistischer Natur wie Zähler für gesendete Pakete, benutzte Verbindungen, Versuche des Verbindungsaufbaus, Anzahl fehlerhafter Pakete, Anzahl von Kollisionen in einem LAN-Segment.

[13] Die Übertragungsprotokolle heissen *Useful Protocols* und enthalten Objekte, die unabhängig vom SNMP-Managementprotokoll definiert sind und die verwaltet werden müssen (wie Routing-Tafeln, Informationen über physikalische Schnittstellen, Zähler, Parameter), ohne die Useful Protocols oder die Software für die Managementinstrumente ändern zu müssen.

[14] Die Beobachtung des Netzes geschieht bei SNMP durch Anpollen der Geräte, wobei kontinuierlich aus den Agents Informationen geholt und in der NSD-Datenbank zu Korrelations- und Planungszwecken gesammelt werden. Der Netzadministrator kann die Polling-Rate bestimmen; die Agents antworten auf die Polling-Anfragen und verbrauchen dabei auch unmittelbar ihre gesammelten Daten, so dass der durch sie in den Geräten belegte Speicherplatz gering bleibt.

[15] SNMP erlaubt den Herstellern, weitere Trap-Bedingungen zu definieren wie zum Beispiel Ereignisse im Rahmen der Benutzung von X.25, Decnet oder 802.1-Protokollen. Polling mit Traps ist die Methode von SNMP, sehr effektiv und schnell Fehlerquellen zu isolieren.

**Facilities-Glossar**

*Attribute Management Facility* wird benutzt, um Attribute anzuschauen, zu setzen und über Änderungen zu berichten. An CMIS Services werden get, set und event report benutzt.

*Confidence and Diagnostic Testing Facility* versetzt einen Benutzer in die Lage, von einem entfernten Benutzer die Ausführung eines Tests auf einem Managed Object zu bekommen, um festzustellen, ob dieses noch seine Funktionen zuverlässig (oder als Bestandteil einer Diagnoseroutine) ausüben kann.

*Cumulative Error Gathering Facility* versetzt einen Benutzer in die Lage, periodisch Informationen aus Fehlerzählern eines anderen Benutzers mittels des CMIS-GET-Dienstes abzurufen. Damit kann man die Fehlerzähler in anderen, gleichberechtigten Systemen pollen, um Fehlerbedingungen zu entdecken.

*Error Threshold Alarm Facility* versorgt den Benutzer mit verschiedenen Schwellwertfunktionen. Er kann Schwellwerte setzen, überwachen, Schwellwertreporte versenden und Schwellwerte auf einer gleichberechtigten Stelle abfragen. Ein Schwellwertalarm wird ausgelöst, wenn ein vorher eingestellter Schwellwert erreicht, über- oder unterschritten wird (je nach Festlegung).

*Event Tracing Facility* ermöglicht das Buchführen über Ereignisse (Events).

*Management Services Control Facility* enthält Profile für Management Services und versetzt den Benutzer in die Lage, diese Profile zu aktivieren, zu benutzen und zu desaktivieren. Es wird allerdings überlegt, ob diese eher allgemeine Facility nicht in einen anderen Bereich eingeordnet werden sollte.

*Object Configuration Facility* wird benutzt, um Managed Objects zu erzeugen, zu benennen und zu löschen. Diese Facility benutzt vier CMIS-Dienste: create, delete, get und event report.

*Relationship Management Facility* wird benutzt, Beziehungen zwischen Managed Objects zu prüfen, zu setzen und über Änderungen in solchen Beziehungen zu berichten. Dies erfordert die vier CMIS-Dienste create, delete, get und event report.

*Software Distribution Facility* ist eine noch nicht ganz definierte Facility zur Verteilung von Software in der offenen Systemumgebung. Sie wird dazu benutzt werden, eine Konfiguration an einen anderen, gleichberechtigten Benutzer weiterzugeben, Softwarekomponenten an einer entfernten, gleichberechtigten Stelle zu prüfen, upzudaten oder zu warten sowie Fernladen und Fernstart im Netz durchzuführen. Sie braucht dazu sowohl Dienste von CMIS/CMIP als auch von FTAM.

*Spontaneous Error Reporting Facility* versetzt einen Nutzer in die Lage, anderen Nutzern Error Reports zuzusenden.

*State Management Facility* wird benutzt, um den Zustand von Managed Objects zu beobachten und über Änderungen zu berichten. Auch hier werden get, set und event report benutzt.

einige Hersteller von LAN-Hardware SNMP kräftig unterstützen.

### SMI-Spezifikationen

Die SMI-Spezifikationen sind Regeln darüber, wie Netzwerkvariablen oder Objekte für die Benutzung durch das Netzwerk-Management-Protokoll definiert sein müssen, wie das Protokoll auf die Objekte zugreift und wie Objekte in die MIB eingebracht werden. Zur Beschreibung der Datenformate für Objekte, die einem *Objektinformationsmodell* entsprechen, wird die OSI-Beschreibungssprache ASN.1 verwendet[16].

Wenn man heute einen Router installiert, wird er für einige Zeit an seinem Platz bleiben; in seiner Lebenszeit werden weitere Router installiert, die anderen Versionen entsprechen und möglicherweise auch andere MIB-Objekte unterstützen. Um zukünftige Erweiterungen neben bestehenden Objekten und Funktionen zu ermöglichen, gibt es in der SMI vier Objektklassen: Verzeichnisobjekte, Managementobjekte, experimentelle Objekte und private Objekte[17]. Im Rahmen dieser Objektklassen kann SNMP stufenweise sinnvoll erweitert werden, wobei Erweiterungen gründlich erprobt werden können, bevor sie Aufnahme in die vorgeschriebene Objektklasse finden.

## Schlussfolgerung

Das Netzwerkmanagement ist in eine wachsende Komplexitätsspirale geraten, genauso wie das gesetzliche, organisatorische, wirtschaftliche und technische Umfeld des Netzmanagements. Wenn in erster Linie ökonomische Gründe von den Telekombetreibern und -unternehmen beim Netzwerkmanagement eine neue Dynamik verlangen, so darf Netzwerkmanagement nicht nur aus diesem Winkel betrachtet werden. Netzwerkmanagement ist heute ein wichtiger Wirtschaftsfaktor, welcher Beschäftigung bringt und der Öffentlichkeit leistungsfähige und nutzbringende neue Dienste anbietet.

## Literatur


[1] *J.A. Huntington*: OSI-based Net Management: It is too early, or too late? Data Communications 3(1989).

[2] *T.I. Băjenescu*: Datenkommunikationsnetzwerke heute und morgen. Expert Verlag, Renningen, 1994.

[3] *F.-J. Kauffels*: Netzwerk-Management. Datacom-Verlag, 1992.

[4] *Arpège*: Gestion de réseaux. Masson, Paris, 1992.

[5] *C. Ruland*: Datensicherheit in lokalen Netzen. Datacom 12(1989); 1(1990).

[6] *F. Rose*: OSI-Netzwerk-Management. Datacom 4(1990).

[7] *J. Pitteloud*: OSI Systems Management – Les derniers développements. Bulletin technique des PTT Suisses, avril 1991.

[8] *J. Benett*: The Simple Network Management Protocol. Telecommunications 2(1990).

[9] *J. Krall*: SNMP Opens New Lines. Data Communications 3(1990).

[10] Les réseaux de gestion des télécommunications. Communication et Transmission, numéro spécial, 1991.

[11] *J. Cohen*: Network Management in the 1990s. Telecommunications, internat. edition, vol. 24, no. 10, Oct. 1990.

[12] *B. Basset* et al.: Customer network management: a service provider's view. IEEE Communications Magazine, March 1990.


[16] ASN.1 erlaubt die systemunabhängige Definition von Objekten. Unter ASN.1 erhalten die SMI-Objekte Nummern, die *Objekt-Identifier* genannt werden. Die Philosophie hinter SMI ist die *Modularität* und *Erweiterbarkeit* innerhalb des Protokolls. SNMP behandelt nur einfache Datentypen. Die Erzeugung, Behandlung und Pflege komplexer zusammengesetzter Datentypen bleibt OSI-NM-Implementierungen vorbehalten.

[17] *Managementobjekte* sind die, die zwingend in jeder SNMP-Implementierung vorzusehen sind; *experimentelle Objekte* wurden in Internet-Experimenten als Kandidaten für zukünftige Erweiterungen benutzt; *private Objekte* werden einseitig definiert.

# La gestion de réseaux

## 2e partie: réseaux de communications et l'environnement TCP/IP

Dans la première partie de cet article (Bulletin 11/94) nous avons présenté la problématique et les tâches de la gestion des réseaux. Dans cette seconde partie est décrit plus en détail l'environnement des réseaux de communications (gestion de la configuration, des anomalies, des performances, de la sécurité – également pour les systèmes ouverts – ainsi que des informations comptables) et l'environnement TCP/IP. A la fin de l'article on donne un glossaire des facilités de service.

La gestion de réseaux est entraînée dans une spirale de complexité croissante, tout comme l'est l'environnement réglementaire, organisationnel, économique et technique de la gestion de réseaux. Si des impératifs économiques impliquent un nouveau dynamisme des opérateurs et des entreprises pour la gestion des réseaux, elle n'est pas à appréhender uniquement sous son angle économique; elle intègre des aspects industriels, soutenant ainsi l'industrie et l'emploi, mais aussi des aspects politiques – car les enjeux sociaux de la gestion de réseaux sont aussi ceux de la mise à disposition de nouveaux services pertinents, performants et diversifiés au public.

# Starke Produkte für starke LAN-Lösungen.


**An der Orbit: Halle 224, Stand D70**
**Basel Mustermesse, 6. – 10.9.1994**

*Wir bauen LANs und WANs für allerhöchste Ansprüche, ... für Kunden mit internationalem Rang und Klang. Unsere Referenzliste ist lang, die Erfahrung gross. Welchen Grund gibt es, um als ebenso erfolgreicher LAN-Anbieter unbedingt beim Mitbewerber einzukaufen? Ganz klar: Das Know-how von LAN-Com, die Hard- und Software von Partnerfirmen, die im internationalen LAN-Markt seit Jahren Bestmarken setzen. Festgefahrene Strukturen existieren nicht. Jede Netzwerklösung hat ihre eigenen Gesetze, ... jede individuelle Netzwerklösung bedarf der sorgfältigen Auswahl ihrer LAN-Komponenten. Nicht starre Verbindungen, sondern die ideale Lösung kommt zum Tragen. Wir vernetzen und wissen darum aus eigener Erfahrung, wovon wir sprechen. Deshalb ist unser Angebot komplett und unsere Beratung kompetent. Ein wichtiger Faktor ist der Handel geprüfter, qualitativ hochwertiger LAN-Komponenten (LANConnect, LANOptinet, LAN-Cabinet, LANConnect-Ware, LANConnectivity, LANBroadband) zu marktgerechten Preisen, mit hoher Lieferbereitschaft und mit dem nötigen technischen Support. Bei uns ist auch Erfahrung aus der Praxis im Preis inbegriffen. Nicht nur Produkte, sondern auch Support aus erster Hand.*

NETWORKS
for the future

***Das Netzwerk im Griff!*** *Bitte senden Sie uns kostenlos und unverbindlich Ihre Dokumentation:*

*Firma:*

*Sachbearbeiter/in:*

*Strasse:*

*PLZ/Ort:*

*Telefon:*

*Einsenden an: LAN-Com Kabelkommunikations AG, Luzernerstrasse 145, Postfach 165, 6014 Littau, oder rufen Sie uns doch einfach an: 041 57 83 57*

# LAN-Com

*LAN-Com Kabelkommunikations AG*
*6014 Littau/Luzern, Luzernerstrasse 145, Telefon 041 57 83 57*
*3014 Bern, Stauffacherstrasse 77, Telefon 031 331 82 92*
*8048 Zürich, Buckhauserstrasse 24, Telefon 01 492 02 22*
*1214 Vernier, 28, rue du Village, téléphone 022 341 50 34*

*Ein Unternehmen der Fischer-Gruppe*

# Das geographische Informations-System ARGIS 4GE setzt sich durch: Kommunal, kantonal und international.

Nyon Fribourg London

Unisys ist der weltweit führende Anbieter von Informatik-Lösungen im Land- und Infrastruktur-Management:
Methoden der Ersterfassung von raumbezogenen und attributiven Daten sowie deren Nachführung. Verwaltung von komplexen und grossen Datenbeständen. Vernetzte Systeme und Datenbanken. Vermessungstechnische EDV-Praxis nach AV 93. Aufgaben der Energie- und Wasserversorgung sowie der Abwasserentsorgung. Schnelle und zuverlässige Reaktion im Schadenfall. Optimierung der Planung und Wartung. Rasche und umfassende Auskunft über verschiedene Datenbestände. Sowie der Weg vom handgeschriebenen zum vollständig mit Computer geführten Grundbuch.
Schon heute arbeiten namhafte Ingenieurbüros, Hochschul-Institute, städtische, kommunale und kantonale Behörden wie z.B. die PTT-Kommunikationsmodellgemeinde Nyon, die Kantone Fribourg, Genf, Neuenburg und Waadt, mit ARGIS 4GE. Das bedeutet, dass bereits rund 20% des Schweizer Territoriums mit ARGIS 4GE bewirtschaftet werden. Wenn Sie sich jetzt fragen, wie Ihnen ARGIS 4GE nützen kann: Rufen Sie uns an.

**ARGIS 4GE:**
- **Geographisches Informations-System (GIS)**
- **Land-Informations-System (LIS)**

mit:
- *ARGIS*NIS:* Netzinformations-System für Versorgungs- und Entsorgungswerke (SIA 405)
- *ARGIS*KISS:* Kataster-Informations-System Schweiz für das Amtliche Vermessungswesen (AV 93)

UNISYS
We make it happen.

Unisys (Schweiz) AG
Zürcherstrasse 59 – 61, 8800 Thalwil
Telefon 01/723 33 33, Fax 01/720 37 37

Niederlassungen in Basel, Bern, Lausanne

Szombath & Zürrer