

Netzwerkmanagement

1 Aufgaben des Netzwerkmanagements	1
1.1 Gegenstand und Einordnung des Netzwerkmanagements	1
1.2 Aufgaben des Netzwerkmanagements (FCAPS)	2
1.2.1 Fehlermanagement (Fault Management).....	5
1.2.1.1 Vorgehen bei der Fehlerbehebung	7
1.2.1.2 Informationssammlung / Problemdefinition	7
1.2.1.3 Auswahl und Einsatz von Messtools.....	7
1.2.1.4 Problemlösung	8
1.2.1.5 Eskalation	8
1.2.2 Konfigurationsmanagement (Configuration Management).....	9
1.2.3 Abrechnungsmanagement.....	11
1.2.4 Leistungsmanagement (Performance Management).....	12
1.2.5 Sicherheitsmanagement (Security Management)	13
1.3 Managementsysteme	14
1.3.1 Management Domains.....	15
1.3.2 Topological Framework.....	18
1.3.3 Management Application Domains	20
1.4 Überblick über Netzwerkmanagementmodelle	20
1.5 Relevante Links	21

1 Aufgaben des Netzwerkmanagements

1.1 Gegenstand und Einordnung des Netzwerkmanagements

In der Vergangenheit konnten die homogenen Büronetze, die mit Komponenten eines Herstellers aufgebaut wurden, auch durch die vom Hersteller angebotenen proprietären Managementsysteme gepflegt und administriert werden. Auf Grund stetig anwachsender Netze und das Zusammenwachsen unterschiedlichster Netztypen zu einem Netzverbund (z.B. Intranet) stießen diese proprietären Managementsysteme häufig an ihre Grenzen.

Ebenso ist bereits seit einiger Zeit die Entwicklung der industriellen Netze zu immer größeren Netzstrukturen zu beobachten. Die vertikale Integration, wie das Zusammenwachsen von Industrienetz und Büronetz auch genannt wird, bringt einerseits transparenten Durchgriff auf alle Daten, braucht aber andererseits eine ebenso durchgängige Diagnosemöglichkeit.

Gelöst wurden diese beispielhaft angeführten Probleme, als in den 80er Jahren von der Internet Activities Board (IAB) das Simple Network Management Protocol (SNMP)

eingeführt wurde. Mit diesem Standard, der von der Netzwerkindustrie sehr schnell akzeptiert wurde, werden die grundlegenden Aufgaben eines Netzwerkmanagements erfüllt.

Das **Netzwerkmanagement hat die Aufgabe**, den ordnungsgemäßen Betrieb eines Netzwerks zu gewährleisten. Der Betrieb eines Netzwerks ist das Zusammenspiel der Funktionen der eingesetzten Netzwerkkomponenten mit dem Verhalten der Endgeräte und deren Installationen.

Die IT Infrastruktur eines Unternehmens besteht aus:

- Einer Vielzahl von Klienten- und Server Rechnern, die über Netzelemente miteinander verbunden sind,
- Prozessen und Verfahren, die im Normal- und im Störfall einen reibungslosen Betrieb ermöglichen,
- Einrichtungen, die eine zentrale oder hierarchische Verwaltung der Infrastruktur, sowie ihre Anpassung an sich ständig ändernde Verhältnisse, mit einem Minimum an menschlichen Ressourcen ermöglichen.

Definition:

Die Summe der Einrichtungen, die zur Steuerung, Verwaltung und Anpassung der IT Infrastruktur dienen, werden als Netzwerk- und System Management (NSM) bezeichnet.

Gegenstand des Netzwerkmanagement sind vor allem Vermittlungs- und Weiterleitungssysteme, wie z. B.: Router, Bridges, Hubs, Endsysteme (hosts).

1.2 Aufgaben des Netzwerkmanagements (FCAPS)

Die funktionale Bereiche des Netzwerkmanagements betreffen das Fault-, Configuration-, Accounting-, Performance- und Securitymanagement, die auch mit dem Akronym FCAPS bezeichnet werden.

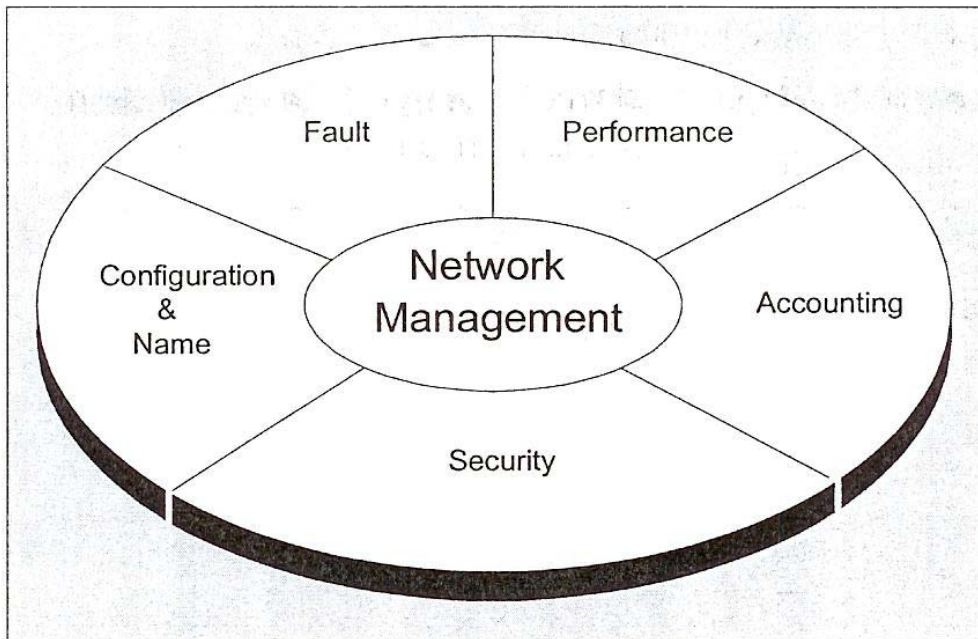


Bild: OSI-Funktionen des Netzwerkmanagements

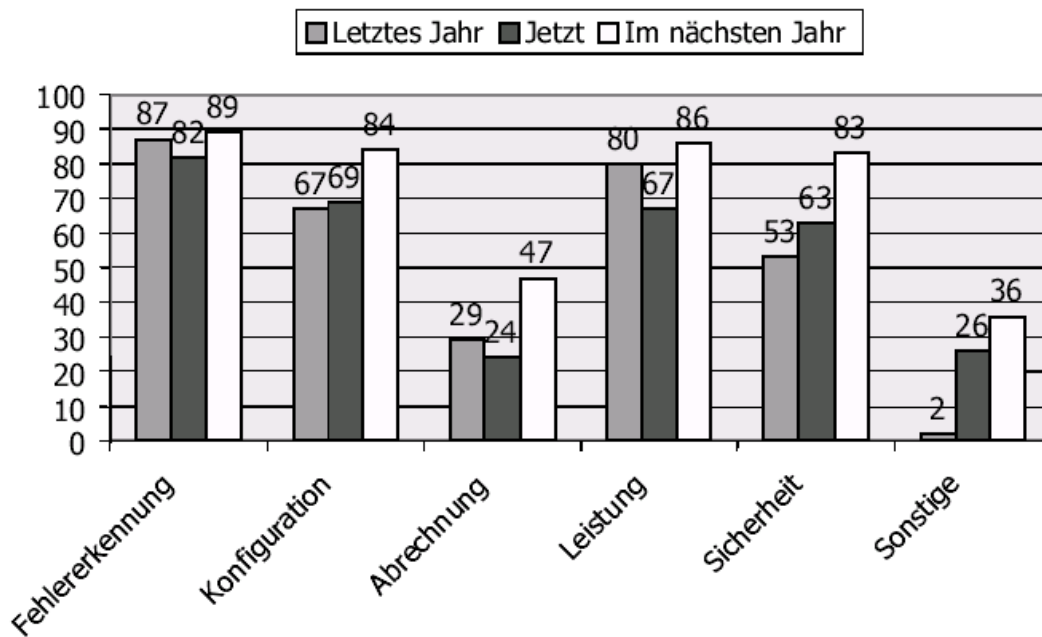


Bild: Einsatz von Managementwerkzeugen

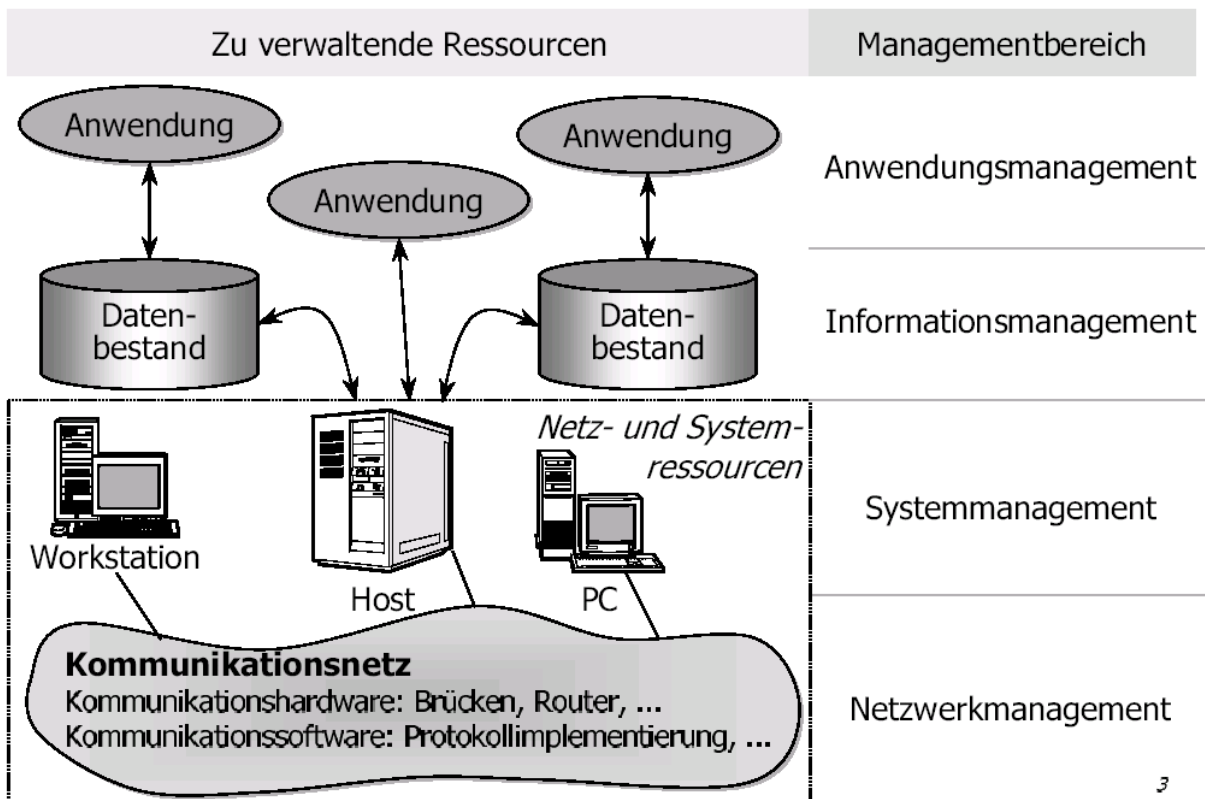
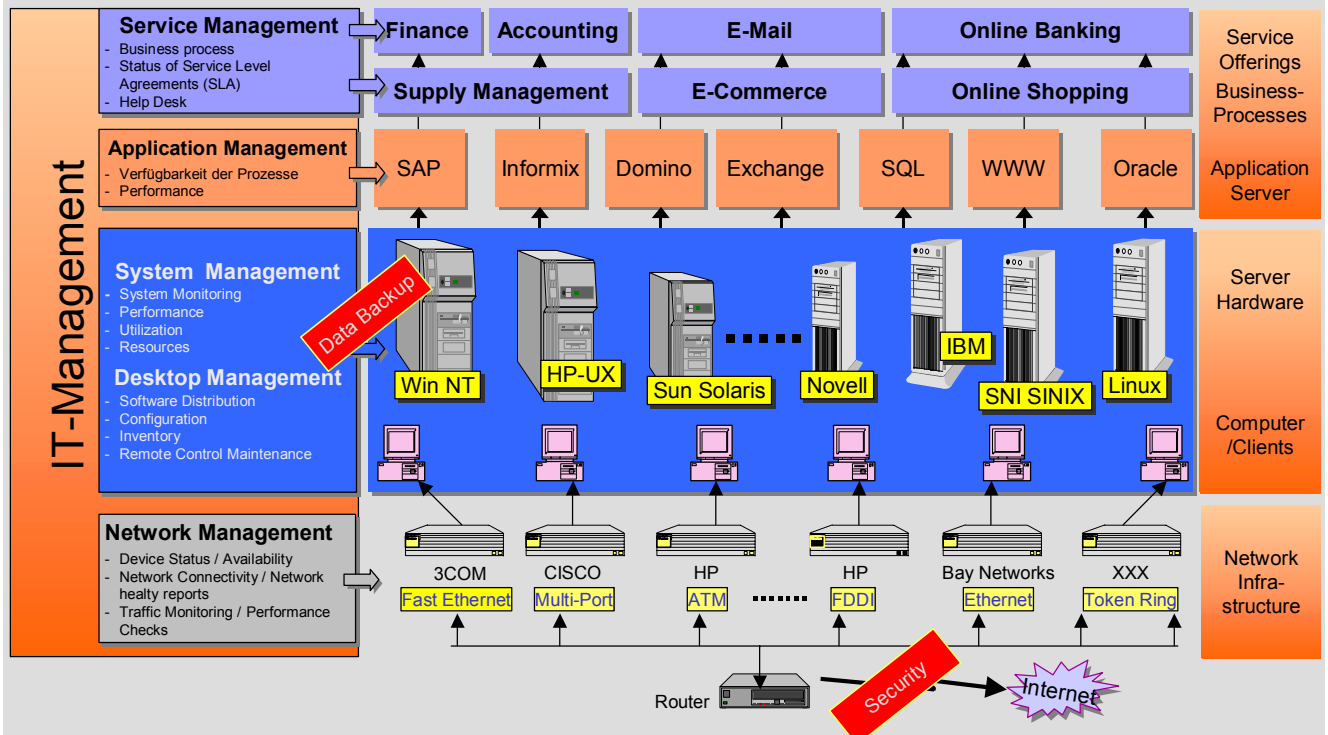


Bild: Managementbereiche

Trend: Wachsende Kundenwünsche...



Dr. Ludwig Eckert

Page 5

Hauptvortrag NM ppt 05/2000

Bild: Anwendungen und Managementbereiche

Netzwerkmanagement

- ❑ Gegenstand des Netzwerkmanagements:
 - ↳ Systeme: vor allem Vermittlungs- und Weiterleitungssysteme
 - Router, Bridges, Hubs, aber natürlich auch die Endsysteme (hosts)
- ❑ Aufgaben
 - ↳ ISO Network Management Model: FCAPS
 - ↳ Fault Management
 - ↳ Configuration Management
 - ↳ Accounting Management
 - ↳ Performance Management
 - ↳ Security Management
- ❑ Oft unterschiedliche Systeme und Programme für unterschiedliche Aufgaben

Darüber umfasst das Netzwerkmanagement weitere Aufgaben, wie z. B. das Report Management, Inventory Management, Service Management (SLA), Policy Management.

Die einzelnen Managementbereiche (siehe Bild Anwendungen und Managementbereiche) sind nicht strikt voneinander getrennt. Vielmehr können einzelne Funktionen mehreren Managementbereichen zugeordnet werden. Allgemein gilt jedoch, dass Funktionen eines Bereiches die Grundlage für die Funktionen des nächst- höheren Bereiches darstellen.

1.2.1 Fehlermanagement (Fault Management)

Um einen einwandfreien, ununterbrochenen Netzwerkbetrieb gewährleisten zu können, muss auf die Funktionalität des Netzes als Ganzes, aber auch jeder einzelnen Komponente geachtet werden. Das Fault Management will die Verfügbarkeit des Netzwerkes erhöhen. Die Dienste des Fault Managements umfassen Tests zur Überprüfung von Netzkomponenten bzw. zur Lokalisierung, es können aber auch Fehlermeldungen ausgetauscht oder Fehlerstatistiken

Die Funktionen des Fehler-Managements befassen sich mit abnormen Zuständen im Netzbetrieb und beinhalten drei Aufgabenbereiche:

- Erkennen (Fehlerdetektion),
- Diagnostizieren (Fehleridentifikation, Fehleranalyse),

- Beheben (Fehlerbeseitigung).

Fehlererkennung: Dazu werden in Intervallen Diagnosetests durchgeführt (Polling), oder es wird, sofern möglich, eine Fehlermeldung von einem Managed Object an den Manager gesendet (Trapping).

Tritt ein Fehler auf, so ist es wichtig, folgende Schritte möglichst schnell auszuführen:

- a) Exakt feststellen, woran der Fehler liegt.
- b) Isolation des restlichen Netzwerkes von der Störungsstelle, so dass es ohne Unterbrechung weiter verwendet werden kann.
- c) Modifikation oder Rekonfiguration des Netzwerkes, um eine Verwendung der fehlerhaften Komponente(n) zu minimieren oder Umschalten auf redundante Netzkomponenten.(z. B. Umleiten des Datenverkehrs über einen anderen Router durch entsprechenden Eintrag in der Routingtabelle oder der Access Liste)
- d) Reparatur oder Austausch der fehlerhaften Komponenten, um das Netzwerk wieder in seinen ursprünglichen Zustand zu bringen.

Fehlerdiagnose: um die Art und die Ursache des Fehlers zu erforschen, müssen die Aktivitäten der Objekte aus den Ereignis- und Fehler-Reports analysiert und ggf. Diagnoseprogramme gestartet werden.

Zur **Fehlerbehebung** bedient sich das Fault Management der Dienste des Configuration Managements, startet passende Fehlerbehebungs-Programme oder fordert einen aktiven Eingriff des Administrators.

Wenn der Fehler korrigiert wurde und das System sich wieder in seinem ursprünglichen Zustand befindet, muss der Administrator sicherstellen, dass das Problem auch tatsächlich beseitigt wurde und dabei keine neuen Probleme entstanden sind.

Fault Management (1)

- ❑ Management von im Netz auftretenden Fehlfunktionen
- ❑ Ziel: Aufrechterhaltung oder schnellstmögliche Wiederherstellung des Netzbetriebs beim Eintritt von Fehlfunktionen
 - ↳ Erkennung von Fehlfunktionen
 - ↳ Protokollierung von Fehlfunktionen,
 - ↳ Benachrichtigung der Betroffenen Benutzer und Betreuer über erkannte Fehlfunktionen
 - ↳ Behebung der Fehlfunktionen
- ❑ Motivation: Ausfall von Netzdiensten kann zu hohen unerwartete Kosten und anderen Nachteilen für Betreiber und Benutzer führen

Benutzer erwarten schnelle und zuverlässige Problemlösungen. Durch die Verwendung von schnellen und zuverlässigen Fehlerverwaltungstechniken. Die Verwendung systematischer Vorgehensweisen bei der Fehlersuche.

1.2.1.1 Vorgehen bei der Fehlerbehebung

Um einen Fehler schnell zu analysieren und zu beheben, ist es wichtig systematisch an das Problem heranzugehen. Nach einer ausführlichen Informationssammlung kommen evtl. Messtools für die zusätzliche Informationsgewinnung zum Einsatz.

Nach der Problemidentifikation folgt die Lösung. Evtl. ist es notwendig an einer bestimmten Stelle im Problemlösungs-Prozess zu eskalieren.

1.2.1.2 Informationssammlung / Problemdefinition

Zu Beginn ist es wichtig, das Problem wirklich richtig einzuordnen. Nur wenn man den wahren Fehler gefunden hat, sollte man handeln. Folgende Fragestellungen können hier weiterhelfen:

- Wobei tritt der Fehler auf? - während der Datensicherung, immer beim Drucken etc.
- Welche Systeme sind betroffen? – das gesamte Netzwerk, nur ein Gebäude, nur eine Etage, ein Endgerät, alle Windows-Rechner etc.
- Wann tritt der Fehler auf? - ständig, zu einer bestimmten Zeit
- Welche Netzkomponenten sind betroffen? - alle, eine bestimmte Bauart etc.
- Welche Anwendungen sind betroffen? - alle, SAP, Oracle etc.
- Wie sieht mein Netzwerk aus? - Netzwerkdokumentation
- Wurde am Netzwerk etwas geändert? - Software-Upgrade, Hardware-Tausch etc.
- Ist das Problem reproduzierbar?
- Gab es schon einmal ähnliche Probleme?

Für den Fall, dass das so ermittelte Wissen nicht ausreicht, muss man sich weitere Informationen verschaffen. Dies geschieht oft mit Hilfe von Netzmessungen.

1.2.1.3 Auswahl und Einsatz von Messtools

Das Ziel dieser Stufe ist die Fehlereingrenzung. An dieser Stelle gilt es, bestimmte Fehlermöglichkeiten auszuschließen.

Für die Entscheidung über den Einsatz der Mess-Werkzeuge können folgende Fragestellungen weiterhelfen:

- Welche Informationen liegen bereits vor?
- Welches Tool kann was?

Bei Problemen im Netzwerk können natürlich auch Messungen im Netzwerk erschwert, verfälscht oder unmöglich gemacht werden.

1.2.1.4 Problemlösung

In diesem Schritt wird nun das Problem gelöst, in dem die Fehlerquelle/Ursache beseitigt wird. Ist dies geschehen, findet eine Prüfung statt um sicherzugehen, dass der Fehler nicht mehr vorhanden ist.

Nachdem das Problem gelöst ist, sollte eine genaue Dokumentation von Ursache, Auswirkungen und Lösung vorgenommen werden. Bei neuen Problemen kann man dann auf diese Erfahrungen zurückgreifen. Natürlich sollten auch die Veränderungen in einem Logbuch festgehalten werden.

1.2.1.5 Eskalation

Ist es notwendig mehr Ressourcen für die Problemfindung /-lösung einzubinden, wird das Problem eskaliert. Dies geschieht meist über den Vorgesetzten.

Folgende Informationen müssen bei einer Eskalation zur Verfügung stehen:

- Beschreibung der Fehlersituation
- Netzwerkdokumentation
- Zugang zu Messtools
- Konfigurationen der Netzwerkkomponenten
- Physikalischer Zugang zu den Netzwerkschränken/-komponenten
- Passwörter für den Zugriff
- Was wurde bereits geprüft? Was hat es gebracht?

Fault Management (2)

- ❑ Vorwiegende Aktionen
 - ↳ Bearbeitung eingehender Meldungen aus dem Netz (traps)
 - ↳ Durchführung von “health checks” für Systeme und Netzwerke (polling)
- ❑ Bewältigung mit vielfältigen Systemlösungen, Anwendungen und Modulen
- ❑ Behebung von Fehlern nur begrenzt automatisiert.
 - ↳ Bestimmung der Symptome
 - ↳ Isolation des Fehlers
 - ↳ Behebung des Fehlers
 - ↳ Test der Fehlerbehebungsmaßnahme
 - ↳ Dokumentation der Fehlerinstanz, der Umstände und der Behebungsmaßnahme

Isolation eines Fehlers

- ❑ Typische Situation:
 - ↳ Ein Fehler in einer unteren Netzwerkschicht tritt auf.
 - ↳ Aufgrund der Schichtstruktur treten in den höheren Schichten große Mengen von Fehlern auf.
 - ↳ Beim Fault Management-System geht eine Flut von Fehlermeldungen ein.
- ❑ Vorgehensweise:
 - ↳ Automatische Filter für eingehende Fehlermeldungen, die auf der Korrelationen von Ereignissen beruhen
 - ↳ Automatische Filter, die auf dem Prinzip des Verursachers in der untersten Schicht arbeiten.
 - ↳ Der Erfahrene Blick des Betreuers
- ❑ Einige Softwarelösungen schlagen sogar nach der Isolation Fehlerbehebungsmaßnahmen vor.

1.2.2 Konfigurationsmanagement (Configuration Management)

Das Konfigurationsmanagement bietet dem Netzwerkadministrator die Möglichkeit, Kontrolle über das System bzw. Netz auszuüben.

Das Konfigurationsmanagement will die im Netz vorhandenen Komponenten überwachen, deren Bestandteile und Einstellungen kontrollieren und ggf. verändern. Die Konfiguration von bestimmten Netzkomponenten bestimmt das Verhalten des Datennetzwerkes.

Deswegen umfasst das Configuration Management alle Funktionen, die im Zusammenhang mit Konfigurationsdaten stehen: Sammeln und Darstellen, Kontrollieren und Aktualisieren von bestimmten Konfigurationsparametern.

Folgende Aspekte zählen ebenso zum Konfigurationsmanagement:

- Existenz und Namen von Netzkomponenten
- Technische Daten von Netzkomponenten
- Beziehungen zwischen Netzkomponenten
- Status (aktiv/inaktiv) von Netzkomponenten
- Adressierungen
- Routing-Kontrolle

Spezielle Softwaretools sind in der Lage (teil-)automatisiert die Konfiguration eines Netzwerkes, der Rechnersysteme und der darauf applizierten Anwendungen zu erfassen, zu protokollieren und zu archivieren (Inventory Management).

Configuration Management

- ❑ Die Konfiguration ist die wichtigste Aufgabe des Netzwerkmanagements.
- ❑ (Fast) alle Vorgänge beim Management der Netzwerkkonfiguration müssen mit den anderen Managementsystemen (und den Betreuern) koordiniert werden.
- ❑ Aufgaben
 - ↳ Installation neuer Systeme
 - ↳ Installation von Software-Updates
 - ↳ Installation neuer Module
 - ↳ Installation neuer Anwendungen und Dienste
 - ↳ Regelmäßiger Abgleich (ist - soll) der Konfiguration

Configuration Management: Inventory Management

- ❑ Inventarisierung aller Geräte
 - ↳ Router, Switches, Bridges, Hubs
 - ↳ Leitungen, Netzanschlüsse
 - ↳ Zugangsgeräte (Modems, Gateways, ...)
- ❑ Grundlage für die Planung von Optimierungen und Erweiterungen
- ❑ Übliche Softwarelösungen sind Datenbanken, die das Inventar selektiv darstellen können.

Configuration Management: Traffic Management

- ❑ Konfiguration von Parametern für die Verkehrssteuerung
- ❑ Ziele:
 - ↳ Vermeidung von Stauungen im Datenfluss
 - ↳ Minimierung von Intensität, Ausdehnung und Dauer von Stauungen
- ❑ Bereiche des traffic management:
 - ↳ Provisioning: Konfiguration von Verbindungen und Übertragungstrecken
 - ↳ Connection Admission Control (CAC): Zulassungskontrolle von Benutzern zu Diensten
 - ↳ Usage Parameter Control: Überprüfung der Einhaltung eines Service Level Agreement (SLA) durch den Benutzer
 - ↳ Priority Control: Welche Pakete oder andere Daten werden bei Überlast zuerst gelöscht?
 - ↳ Traffic Shaping

1.2.3 Abrechnungsmanagement

Die Funktionen des **Accounting Management** möchten die Nutzung von Netzwerkressourcen quantifizieren bzw. die mit dem Netzwerk erbrachten Leistungen benutzerbezogen identifizieren und abrechnen (Gebührenverwaltung). Um die Kosten, die durch das Netzwerk entstehen zu decken, muss dessen Verwendung berechnet und bezahlt werden.

Die Zuteilung von benötigten Ressourcen erfolgt durch die Vergabe von Prioritäten und Benutzerrechten. Eventuell sind Limits zu setzen, nach deren Überschreitungen der Zugang zum Netz eingeschränkt wird. Die Funktionen beinhalten auch den Austausch von Kosteninformationen.

Der Netzwerkadministrator sollte zu jedem Zeitpunkt feststellen können, welche Anwendungssoftware, welcher Benutzer oder welche Benutzergruppe das Netzwerk verwendet, und zwar aus folgenden Gründen:

- Ein Benutzer oder eine Benutzergruppe missbraucht Zugriffsprivilegien und belastet das Netzwerk unnötig auf Kosten der anderen Benutzer. (z. B. Web-Radio, Video-Onlinestreaming etc.)
- Benutzer können das Netzwerk ineffizient verwenden, so dass der Netzwerkadministrator sie dabei unterstützen kann, einzelne Prozeduren zu verändern, um die Leistung zu verbessern.
- Der Netzwerkmanager kann die Erweiterung des Netzwerkes besser planen, wenn er die Benutzeraktivitäten und die Netzwerkverwendung in ausreichendem Maße kennt.

Accounting Management

- ❑ Erfassung der Benutzung des Netzwerks, so dass Personen, Gruppen, oder Unternehmen die Benutzung in Rechnung gestellt werden kann.
- ❑ Je nach Netzwerk kann Erfassung und Rechnungsstellung die primäre geschäftlich Grundlage für den Betrieb des Netzes sein.
- ❑ Abrechnungsmodelle schwanken stark abhängig von der Art des Netzwerks und dem Betriebsort.

1.2.4 Leistungsmanagement (Performance Management)

Das Performance Management überwacht die Leistungsfähigkeit der einzelnen Systeme und des gesamten Netzes. Moderne Datenkommunikationsnetzwerke bestehen aus vielen und unterschiedlichen Komponenten, die miteinander kommunizieren und Daten sowie Ressourcen teilen müssen. Falsche Konfigurationen der Netzkomponenten sowie eine ungünstige Wegewahl des Datenverkehrs können zu Datenengpässe (sog. bottle necks) führen. Solche Engpässe müssen frühzeitig festgestellt und beseitigt werden. Aus diesem Grund und um die Leistungsfähigkeit zu verbessern, enthält das Performance Management Funktionen, die die statistischen Informationen bzgl. der Leistungsfähigkeit des Systems abrufen können und die Konfiguration von Netzkomponenten modifizieren (-> Konfigurationsmanagement).

Insbesondere moderne Anwendungen wie Netmeeting, Voice-over-IP oder Multimedia-Streaming-Anwendungen stellen hohe Anforderungen an die Performance eines Netzwerkes und der entsprechenden Server und Applikationen. Genaue Informationen über die durchschnittliche und schlechteste Verzögerungszeit, die Antwortzeit, der minimale und maximale Durchsatz sowie die Zuverlässigkeit von Netzwerkdiensten sind hier wichtige Kriterien, die letztlich die Qualität des Dienstes bestimmen.

Netzwerkadministratoren benötigen Durchsatzstatistiken zur Planung, zur Fehlersuche und zur Verwaltung von großen Netzwerken. Ebenso dienen sie auch dazu, potentielle Engpässe zu entdecken und geeignete Verbesserungsmaßnahmen anzuwenden, noch bevor sie den Endbenutzern Probleme bereiten.

Der Bereich des **Performance Management** beinhaltet somit Funktionen zur quantitativen Analyse und Bewertung relevanter Kommunikationsprozesse. Die Funktionen sammeln ständig die über Polling oder Trapping erhaltenen Informationen und ermöglichen eine benutzerdefinierte Anzeige und Auswertung.

Dazu muss der Administrator in der Lage sein,

- selbständig Grenzwerte und Pollingfrequenzen zu bestimmen,
- Leistungsreports über alle wichtigen Variablen zu generieren und dazu den

- Zeitraum zu bestimmen, über den sich diese Reports erstrecken sollen.

Für das Performance Management werden typischerweise Echtzeitstatistiken, historische Statistiken (über ein längeren Zeitraum gesammelt) und Gauges (Pegelanzeiger mit Schwellwerten für die automatische Alarmierung) benötigt.

Um bei abnormen Leistungsdaten das Netz-System besser abstimmen zu können, werden Funktionen des Konfigurationsmanagements benötigt.

Performance Management

- ❑ Leistungsoptimierung auf der Grundlage von quantitativer Erfassung mehrerer Aspekte der Leistung des Netzes
 - ↳ Netzwerkdurchsatz
 - ↳ Antwortzeiten
 - ↳ Ausnutzung der Kapazitäten
- ❑ Arbeitsschritte:
 - ↳ Sammeln von Leistungsdaten
 - ↳ Aufstellen von Basisleistungswerten als Maßstab
 - ↳ Festlegung von Grenzwerten für Leistungsparameter, bei deren Überschreitung Maßnahmen zur Optimierung eingeleitet werden sollen.
- ❑ Auch pro-aktive Methoden werden angewendet.

1.2.5 Sicherheitsmanagement (Security Management)

Als Security Management wird der Prozess bezeichnet, der die Zugriffsberechtigung auf Netzwerkdaten kontrolliert und schützt. Damit verbunden ist die Generierung, Verteilung und Speicherung von Kodier- und Zugriffsschlüsseln zum Zwecke der Autorisierung und Authentifizierung. Dadurch wird sichergestellt, dass nur autorisierte Benutzer auf die Daten zugreifen können.

Im Falle eines unerlaubten Zugriffs besteht die Möglichkeit, diese Zugriffe aufzuzeichnen und dadurch die Herkunft der Security-Verletzungen festzustellen und u. U. die entsprechende Person festzustellen.

Weiterhin besteht die Möglichkeit, bei unbefugtem Zugriff Alarme automatisiert auszulösen.

Die Funktionen des **Security Management** beziehen sich nur auf die Sicherheit von Diensten und Protokollmechanismen der sieben OSI-Ebenen. Sie sollen vor unberechtigtem Zugriff auf Datennetze und deren Ressourcen schützen.

Dazu gehören Strategien

- gegen nichtautorisierten Datenempfang,
- gegen Datenverfälschung bei der Übertragung
- und Zugriffsberechtigungen bei der peer-to-peer Kommunikation.

Der Begriff "Sicherheit" hat viele Aspekte, die nicht von einer Management-Norm abgedeckt werden können. In der Praxis überschneiden sich die Aufgaben der vorgenannten fünf Bereiche.

Security Management

- Kontrolle des Zugangs zu Netzwerkbetriebsmitteln
 - ↳ entsprechend vorgegebener Richtlinien
 - ↳ so dass der Netzwerkbetrieb nicht gefährdet wird (absichtlich oder unabsichtlich)
 - ↳ so dass Benutzer nicht ohne entsprechende Autorisierung auf vertrauliche Informationen zugreifen können

- Arbeitsschritte:
 - ↳ Identifikation schützenswerter Betriebsmittel
 - ↳ Vergabe von Zugangsrechten
 - ↳ Überwachung von Zugangspunkten zu schützenswerten Betriebsmitteln
 - ↳ Protokollierung von Übertretungen der Zugangsrechte

1.3 Managementsysteme

1. Der Bedarf für das Netzwerkmanagement

Um die gewaltige Anzahl von Kommunikationsressourcen verwalten zu können, wurde das Netz in geographische und administrative Regionen aufgeteilt, um für den normalen Informationsfluss zwischen den einzelnen Netzwerkeinheiten definieren zu können. Wie auch immer diese Aufteilung der Netze geschieht, braucht es Managementsysteme, die für die Überwachung und Kontrolle von Netzwerkressourcen zuständig sind. Neben diesen zwei wesentlichen Funktionen findet man andere Merkmalen wie das Fault-, Configuration-, Accounting-, Performance- und Securitymanagement, auch FCAPS genannt.

Managementsysteme sind nicht nur Werkzeuge und Technologien, die erlauben, verschiedene Netzwerke und Ressourcen zu verwalten. Sie beinhalten auch standardisierte Prozeduren und Protokolle darüber, wie Managementinformationen gesammelt

und ausgewertet werden. Das gewaltige Wachstum von Netzwerken hat die Rolle von Managementsystemen verändert. Sie sind jetzt Bestandteil der meisten Kommunikationstechnologien.

Die reelle Komplexität und Größe von Managementsysteme wird in Umgebungen mit mehreren Protokollen, Geräten unterschiedlicher Hersteller und verschiedenen Technologien spürbar. Managementsysteme sollen eine wachsende Anzahl von physischen und logischen Ressourcen verwalten. Das Vorhandensein von verschiedenen (proprietären und standardisierten) Architekturen, Betriebssystemen und Kommunikationsparadigmen (manager/agent, RPC, distributed management interfaces) sind nur ein Teil des Problems. Mit der Migration von zentralisierten Systemen zu verteilten Client/Server Umgebungen wird die Komplexität der Netzwerkverwaltung ebenfalls erhöht. Eine zusätzliche Komplexitätssteigerung ergibt sich, wenn größere Konzerne die Integration ihrer Netzwerke und lokalen Managementsysteme verfolgen.

Managementsysteme sind Hardware-Komponenten, Software-Applikationen und Prozeduren, die folgende Funktionalitäten erbringen: Überwachung, Steuerung, Betrieb, Koordination, Planung, Administration, Verkehrserfassung und Verrechnung im Netzwerk und der Systemressourcen, die eine Kommunikation ermöglichen.

Man kann davon ableiten, dass Managementsysteme nicht nur für die Überwachung und das Controlling geeignet sind, sondern dass sie ebenso komplexe administrative und reporting Funktionen beinhalten.

Es existieren verschiedene Merkmale eines Managementsystems. Diese sind verschieden wichtig, da der Betrachtungswinkel des Benutzers anders als der des Entwicklers ist.

Es werden im Wesentlichen folgende Merkmale unterschieden:

- Management Domains,
- Topological Framework,
- Management Application Domains.

1.3.1 Management Domains

Es gibt fünf große Bereiche: Netzwerk Management, Computing System Management, Applikationsmanagement, Datenbankmanagement und Servicemanagement.

Jede dieser Bereiche verwaltet verschiedene Ressourcen. Die Integration dieser Domänen ist sehr wichtig, um Managementsysteme zu schaffen und zu benutzen.

Netzwerk-Managements - Network-Maintenance

Die unterste Ebene des Netzwerk-Managements ist die **Network-Maintenance**. Um diese physische Grundlage des LANs zu legen, nutzen Techniker Werkzeuge wie Seitenschneider, Abmantelmesser, digitale Multimeter und Netzwerk-Prüfgeräte.

Der nächste Level wird **Configuration-Management** genannt. Hier gilt es, die physische und logische Anordnung des lokalen Netzwerks zu planen: welche Geräte in

einem Netz arbeiten, wie die Komponenten angeschlossen werden und welche Ressourcen freigegeben sein müssen. Der Administrator entscheidet, wie Router einzusetzen sind, ob feste IP-Adressen vergeben werden oder ob ein DHCP-Server zum Einsatz kommt.

Auf der nächsthöheren Stufe befinden sich die Network-Administrators. Diese verwalten das Netzwerk, damit es stabil läuft. Die Aufgabe der Administratoren ist, logische Konfigurationen und Service-Operationen auszuführen und zu verbessern. Darüber hinaus bestimmen die Netzwerk-Administratoren die Anzahl der erreichbaren Ports an Switches und Routern und verwalten Clients und Server.

Auf der höchsten Ebene finden sich die Network-User. Für diese bedeutet Management, sich in das LAN ein- oder auszuloggen und Daten zu bearbeiten.

System-Management

Eng mit dem Netzwerk- ist das **System-Management** verknüpft. Die Bedeutungen dieser Begriffe überschneiden sich teilweise. Beide Arten des Managements beinhalten das Sammeln von Daten über Geräte wie Router, Server und Workstations. Beide kümmern sich um Überwachung und Pflege dieser Geräte. Der Unterschied: System-Management betrachtet jedes Gerät als unabhängige Einheit oder als Mitglied in einer logischen Gruppe von Systemen. LAN-Management sieht die einzelnen Geräte als einen Teil des Netzwerks.

System-Management konzentriert sich also auf die Überwachung und Wartung einzelner Geräte. Dazu gehören das Installieren und Aktualisieren von Software, Backups, Überwachen der System-Ressourcen, Einrichten von User-Accounts und das (De-)Installieren von Systemdiensten.

Netzwerk-Management schließt alle Funktionen auf Geräte-Ebene ein, die die Funktionalität eines Netzes überwachen und steuern. Komponenten, die keinen Einfluss auf die LAN-Performance haben, fallen in den Bereich des System-Managements. Ein Beispiel hierfür ist ein Drucker, der an einer Workstation angeschlossen ist und nur von dieser benutzt wird.

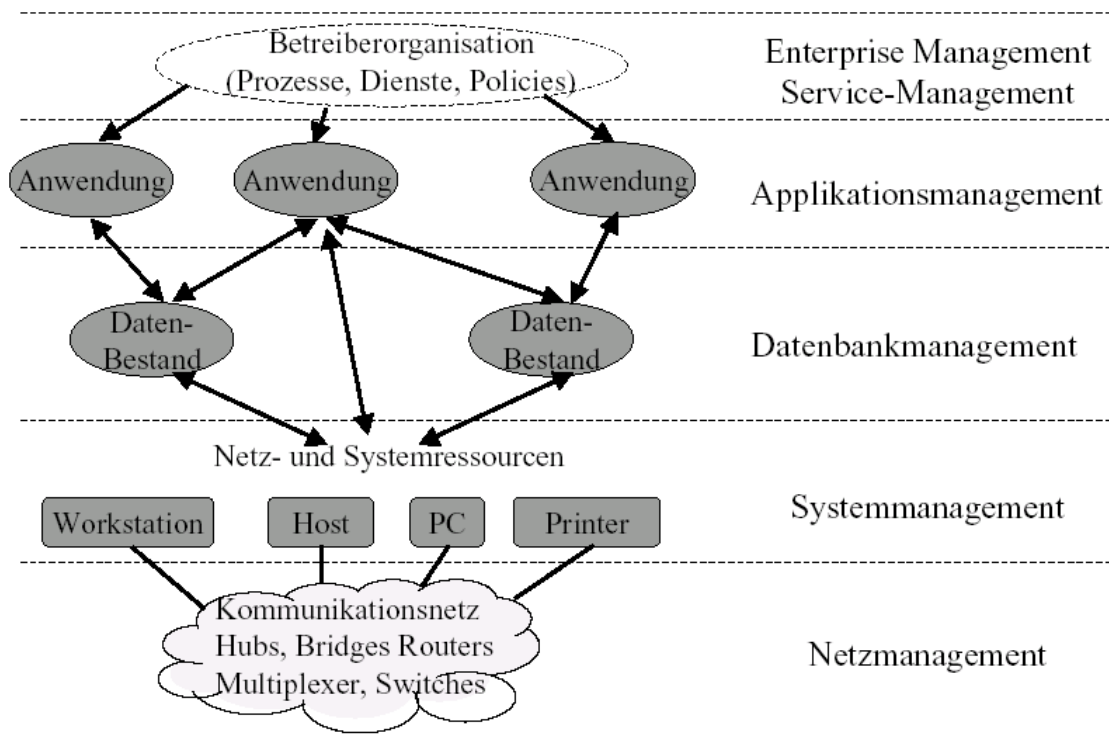


Bild: Management von verteilten Systemen

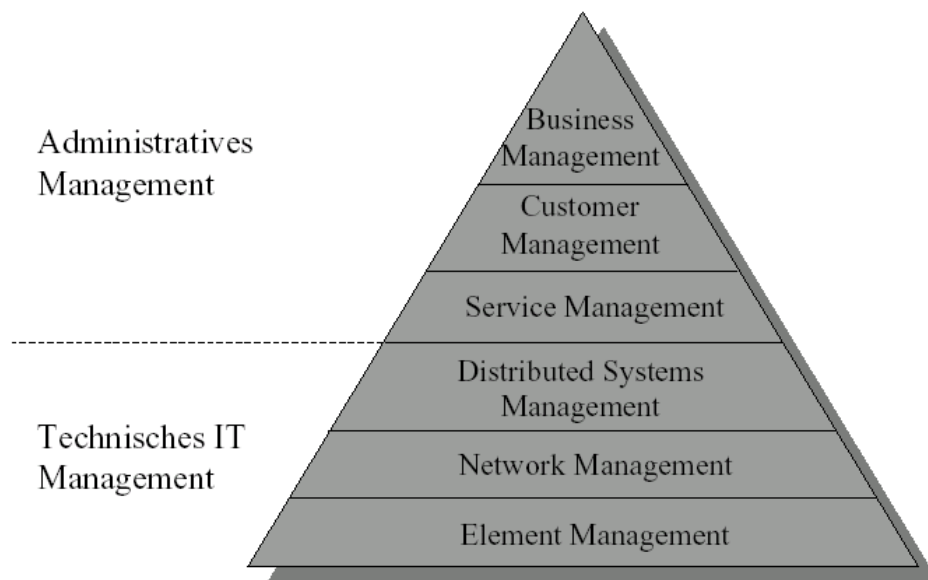


Bild: Managementpyramide eines Unternehmens

1.3.2 Topological Framework

Wenn man die hierarchische Beziehung zwischen den verschiedenen Komponenten analysiert, lassen sich im Wesentlichen drei Typen von Managementsysteme erkennen:

- vollständig zentralisiert (single point management),
- logisch zentralisiert und physisch verteilt (manager of manager) und
- vollständig verteiltes System (peer-to-peer oder client/server management).

Der erste Frameworktyp weist einen einschichtige Architektur auf und wird somit als "single point management"-Framework bezeichnet.

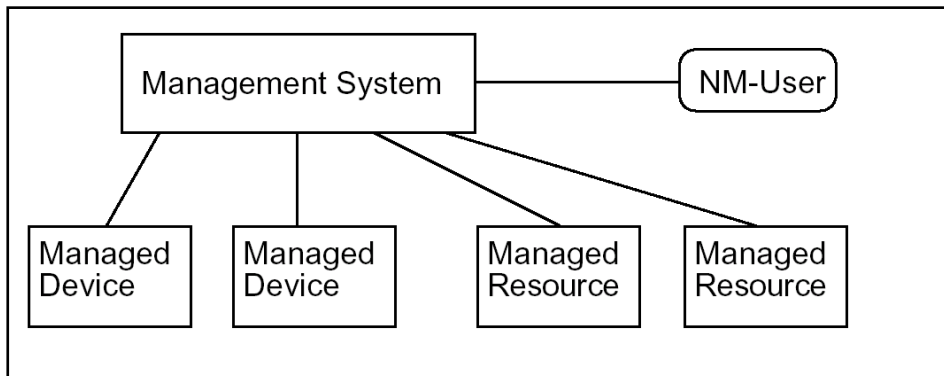
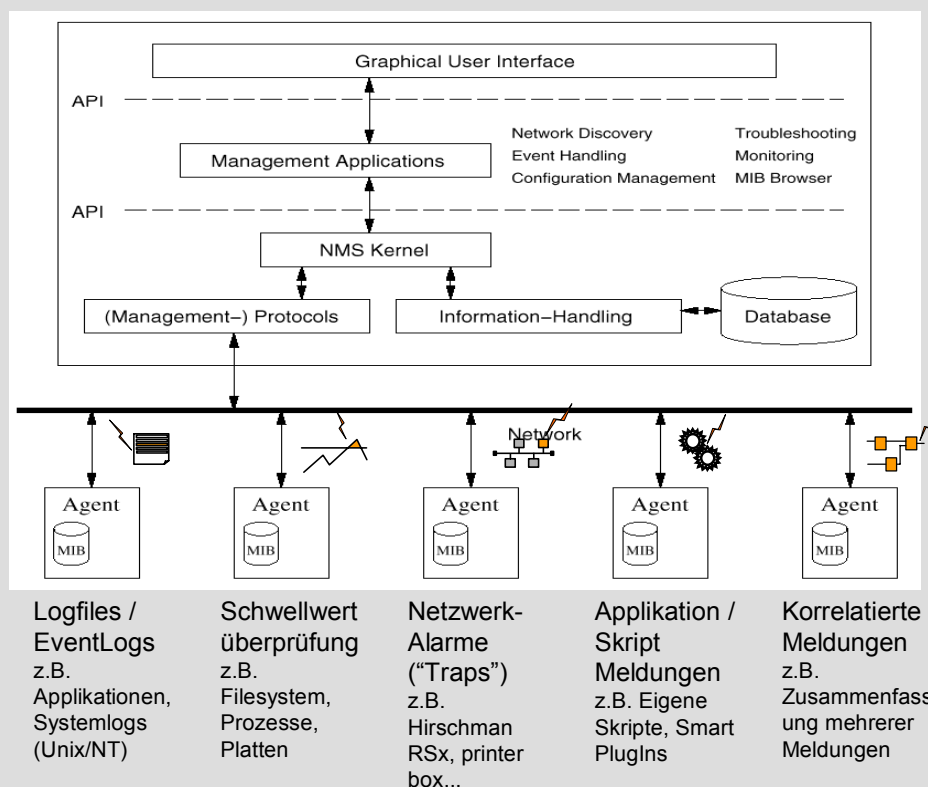


Bild: "Single Manager" , Quelle [Ghe97]

Architecture of local System/Network Management Platforms



Dr. Ludwig Eckert

Page 19
HauptvortragNM.ppt 05/2000

Bild: Architektur des "Single Manager"

Die zweite Netzwerk Management Architektur weist zwei oder mehr hierarchische Schichten. Die einzelnen lokalen Element Management Systeme managen dabei einen topologisch abgegrenzten Bereich der IT-Infrastruktur. Die einzelnen Bereiche können sich dabei überlappen (z.B. Redundanz-Strategie).

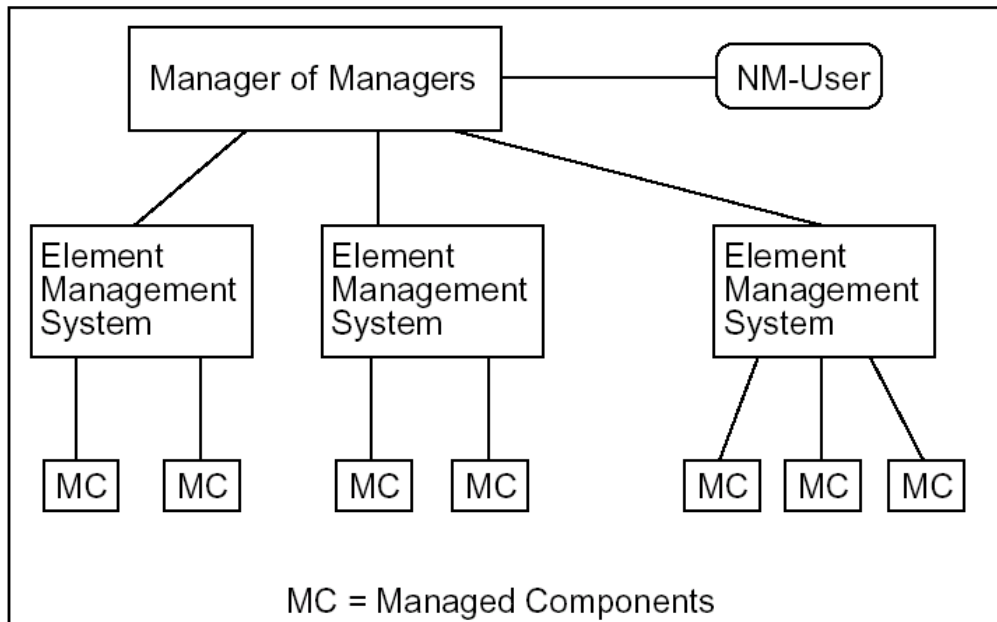
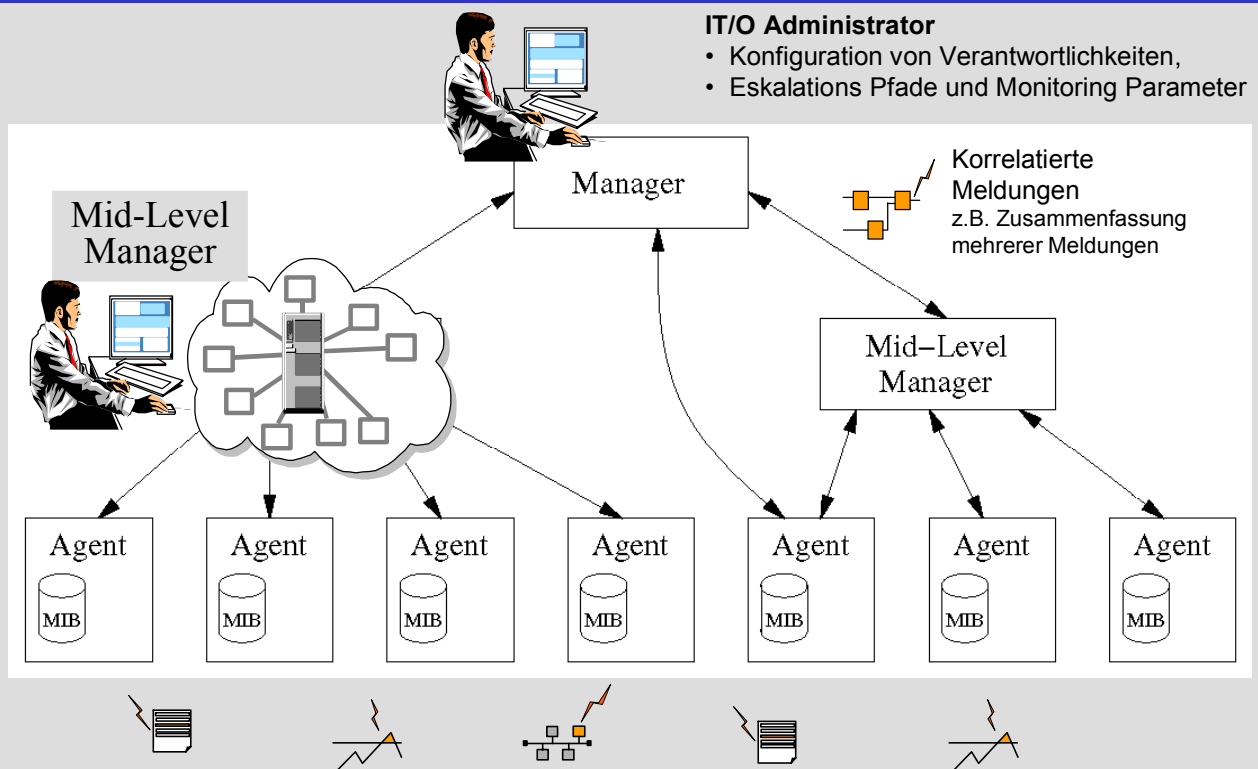


Bild: "Manager of Managers", Quelle [Ghe97]

Hierarchical Network-/System Management Structure



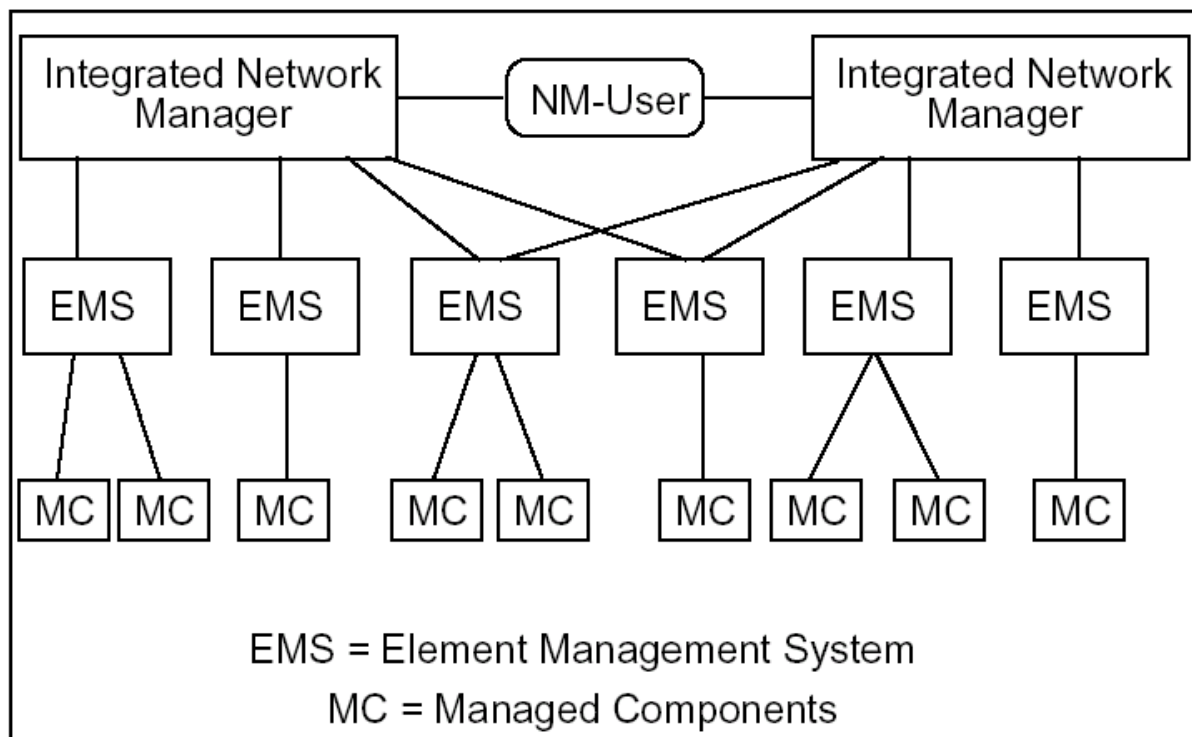
Dr. Ludwig Eckert

Page 20

HauptvortragNM.ppt 05/2000

Bild: Hierarchische Struktur von "Manager of Managers" (MOMs)

Der dritte Typ hat die Eigenschaft von eine peer-to-peer Beziehung zwischen benachbarten Managementsystemen.



Figur 1-4 "Network of Managers", Quelle [Ghe97]

1.3.3 Management Application Domains

Man gliedert normalerweise die Managementfunktionen und Managementapplikationen in fünf Kategorien: Fehler-, Konfigurations-, Abrechnungs-, Leistungs- und Sicherheitsmanagement.

1.4 Überblick über Netzwerkmanagementmodelle

Als das Internet Mitte der 80er Jahren begann wichtig zu werden, erhöhte sich die Notwendigkeit für standardisierte Netzwerkmanagementsysteme.

Common Management Information Protocol (CMIP)

1987 schlug OSI sein Common Management Information Protocol (CMIP) vor, als Lösung für das Netzwerkmanagement. Das CMIP war schon für das Management von OSI-Netzwerke zuständig. Das Protokoll lautet CMOT (CMIP Over TCP). Die Entwickler, die an diesem Protokoll arbeiteten, hatten den Wunsch, alle mögliche Aspekte um ein Netzwerk zu verwalten, abzudecken. Das war wahrscheinlich den Grund für den Misserfolg dieses Protokolles.

Simple Gateway Monitoring Protocol (SGMP).

Als die Entwickler nach einigen Monaten an den hohen Ansprüchen zu verzweifeln drohten, begannen einige von ihnen im März 1987 an einer neuen, einfacheren Lösung zu arbeiten: so entstand das Simple Gateway Monitoring Protocol (SGMP).

Im August 1987 wurde SGMP veröffentlicht und wurde sofort wegen seiner Einfachheit übernommen.

Im Februar 1988 entschied die Internet Activities Board (IAB), dass das CMOT zwar in die richtige Richtung wies, dass aber vorläufig SGMP wegen seiner hohen Akzeptanz verwendet werden sollte, bis dass das CMOT vollständig entwickelt sein würde.

SNMP-Modell

Um die Transition von SGMP auf CMOT zu ermöglichen, wurde das SNMP-Modell entwickelt und noch 1988 vorgestellt. Ein Jahr später wurde es von der IAB für die Verwendung in TCP/IP-Netzwerken empfohlen ("recommended status").

Als es zwischen den Entwicklern von CMOT und SNMP zu Schwierigkeiten kam, wurde deutlich, daß die Entwicklung eines gemeinsamen Modells nicht mehr möglich war. Die IAB entschied darauf im März 1989, die beiden Gruppen ihre Arbeit unabhängig fortführen zu lassen.

1.5 Relevante Links

- Institute of Electrical and Electronics Engineers (IEEE)
<http://www.ietf.org/>
- International Telecommunication Union (ITU)
<http://www.itu.int/>
- Warriors of the Net
<http://www.warriorsofthe.net/>
- Internet Mapping Project
<http://research.lumeta.com/ches/map/>
- Cooperative Association for Internet Data Analysis (CAIDA)
<http://www.caida.org/>
- The Internet Protocol Journal
<http://www.cisco.com/ipj/>