Zeitschrift: Technische Mitteilungen / Schweizerische Post-, Telefon- und Telegrafenbetriebe = Bulletin technique / Entreprise des postes, téléphones et télégraphes suisses = Bollettino tecnico / Azienda delle poste, dei telefoni e dei telegrafi svizzeri

Herausgeber: Schweizerische Post-, Telefon- und Telegrafenbetriebe

Band: 68 (1990)

Heft: 2

Artikel: Gestion des réseaux informatiques selon OSI

Autor: Pitteloud, Joseph

DOI: https://doi.org/10.5169/seals-876193

Gestion des réseaux informatiques selon OSI

Joseph PITTELOUD, Berne

Systemverwaltung der Informatiknetze nach OSI

Zusammenfassung. *Die Verwaltung der Informatiknetze ist aktuell geworden, da die Verwaltungskosten immer höher werden, obschon die Beschaffungskosten von Hard- und Software für die Übermittlung eher sinken. Deshalb haben sich die Normierungsinstitute die Aufgabe gestellt, einige Aspekte dieser Verwaltung zu standardisieren. Den Anstoss haben ISO und die Systemhersteller gegeben. CCITT, einige PTT-Betriebe und weitere Netzbetreiber haben sich angeschlossen. Ein beachtlicher Konsens wurde bereits erreicht. Der Autor versucht, eine Standortbestimmung zu machen, die allen Informatikern und Ingenieuren, die sich mit dem Bau und der Verwaltung der verschiedensten Informatiknetze (LAN, WAN, X.25, Meldungsvermittlungsnetze usw.) befassen, sicher nützlich sein wird.*

Résumé. *La gestion des réseaux informatiques est devenu un sujet à la mode, car les coûts de gestion sont de plus en plus élevés, même si les coûts d'acquisition du matériel et du logiciel de communication ont tendance à baisser. C'est pourquoi les organismes de normalisation se sont attachés à la tâche de standardiser certains aspects de cette gestion. Tout a commencé avec l'ISO et les constructeurs de systèmes informatiques. Le CCITT, différentes entreprises des PTT et d'autres opérateurs de réseaux ont suivi. Un consensus remarquable a déjà été obtenu. L'auteur tente de présenter une synthèse de l'état de l'art, qui sera certainement utile à tout informaticien ou ingénieur confronté à la conception de la gestion des réseaux informatiques les plus divers (LAN, WAN, X.25, réseaux de messagerie, etc.).*

Gestione delle reti informatiche secondo le norme OSI

Riassunto. *La gestione delle reti informatiche è un argomento attuale: infatti, anche se i costi di acquisto di hardware e software di comunicazione tendono a diminuire, le spese di gestione continuano ad aumentare. Per questo motivo gli istituti di normalizzazione si sono prefissi di standardizzare alcuni aspetti di questa gestione. Hanno cominciato l'ISO e i produttori di sistemi, seguiti dal CCITT, da alcune amministrazioni PTT e da altri gestori di reti, ottenendo un consenso notevole. Il punto della situazione fatto dall'autore potrà tornare utile agli informatici e agli ingegneri addetti alla costruzione e alla gestione delle diverse reti informatiche (LAN, WAN, X.25, reti di messaggeria, ecc.).*

Préambule

Ce préambule donne un aperçu de l'évolution dans le domaine d'interconnexion des systèmes ouverts utilisés en informatique et de l'importance de la gestion de tels systèmes.

OSI

Depuis une dizaine d'années, les organismes de normalisation se sont attelés à l'interconnexion d'ordinateurs de fabricants hétérogènes, selon un modèle en sept couches appelé *OSI* (Open System Interconnection). A l'aide de ce modèle, on a défini, non seulement l'interfonctionnement des basses couches de transport de l'information (par exemple la norme CCITT X.25), mais aussi celui des hautes couches, comprenant l'application répartie entre les deux systèmes impliqués. Ainsi, les applications de transfert de fichiers (FTAM, File Transfer Access and Management) ou de messagerie électronique (MHS, Message Handling System, norme X.400) sont actuellement une réalité. L'Entreprise des PTT suisses a, par exemple, ouvert, le 1er janvier 1990, un service commercial de transfert de messages arCom 400, pouvant s'interconnecter à tout système ouvert au sens OSI, ayant implémenté les normes d'application de messagerie.

Gestion OSI de systèmes

Tous les aspects de gestion entre systèmes ouverts qu'il n'était pas possible de définir pour chaque couche en particulier furent englobés sous le titre de «Gestion OSI de systèmes» (OSI Systems Management), dès le début de la normalisation du modèle OSI. Il fallut beaucoup de temps et plusieurs expérimentations pour que ce domaine prenne forme. Aujourd'hui, on comprend mieux ce qu'est l'application «OSI Systems Management» qui permet à un ordinateur ou à un groupe d'ordinateurs formant un centre de gestion de contrôler et d'administrer un autre groupe d'ordinateurs constituant un système ouvert géré, tel un réseau LAN ou WAN, un réseau à commutation par paquets ou un réseau applicatif (plusieurs centraux Vidéotex ou plusieurs agents de transfert de messages électronique selon la norme CCITT X.400, par exemple).

Importance de la gestion OSI de systèmes

Actuellement, lorsqu'une administration de télécommunications ou une firme acquiert un réseau, elle doit presque toujours prendre le système de gestion tel qu'il a été défini par le concepteur de ce réseau, sans avoir beaucoup de marge de manœuvre pour opérer son choix. L'un des éléments classiques du chemin critique, lors de l'introduction d'un nouveau réseau, est l'adaptation à l'environnement de l'acheteur du centre de gestion fourni par le fabricant du réseau. L'introduction de normes de gestion devrait permettre de créer un environnement hétérogène entre systèmes gestionnaires et systèmes gérés, c'est-à-dire assurer l'utilisation de produits de différents constructeurs. Il en résulterait un accroissement de la flexibilité pour l'organisation de la gestion et une simplification de l'introduction de nouveaux réseaux.

Certains grands constructeurs de systèmes informatiques ont très tôt compris les enjeux d'une telle évolution et ont vu en elle une possibilité de s'introduire discrètement, par le biais des systèmes de gestion, dans les domaines actuellement encore bien protégés des fournisseurs des télécommunications, et de se créer une niche de marché intéressante.

Constructeurs et opérateurs de réseaux

Les constructeurs de systèmes informatiques qui ont clairement défini leurs intentions quant à la gestion des réseaux sont entre autres:

- *International Business Machines* (IBM) avec l'architecture de gestion «SNA/NetView»

- *Digital Equipment Corporation* (DEC) avec son «Entreprise Management Architecture» (EMA)
- *Hewlett Packard* (HP) avec son architecture «OpenView».

Il est plus que probable que ces architectures utiliseront d'une manière ou d'une autre des interfaces aux normes de gestion OSI de systèmes.

En ce qui concerne les opérateurs de réseaux (carriers), deux d'entre eux sont vraiment en avance avec leur concept d'utilisation des normes OSI dans la gestion de leurs réseaux:

- *American Telegraph and Telephone* (ATT), qui utilise son «Unified Network Management Architecture» (UNMA) et
- *British Telecom* (BT, UK), avec son «Open Network Architecture» (ONA).

L'Entreprise des PTT suisses étudie également l'introduction de ces normes de gestion pour rationaliser les opérations et diminuer les coûts d'exploitation de ses réseaux, en particulier dans le domaine de la télématique (Télépac, Vidéotex, arCom 400, etc.).

Eléments normalisés

Dans le domaine de la gestion OSI de systèmes, un certain nombre d'outils de gestion sont en cours de standardisation, dont un modèle de données de gestion ainsi qu'un protocole d'application pour l'échange d'informations de gestion. L'état actuel de ces projets de normes et de ces outils est présenté dans l'article qui suit. Tout informaticien et tout ingénieur des télécommunications confronté à la gestion de réseaux devraient en saisir au plus tôt les éléments essentiels.

Par souci de ne pas trahir le sens de la terminologie anglaise utilisée dans les textes originaux, l'auteur a volontairement conservé certaines expressions dans leur langue originale (en particulier en ce qui concerne les figures).

1 Introduction

Cet article est un reflet fidèle de l'état de la normalisation, selon les documents utilisés comme base de travail à la réunion ISO/IEC JTC/SC 21/WG4 qui s'est tenue du 31 octobre au 9 novembre 1989 à Florence.

La normalisation de la gestion OSI de systèmes (OSI Systems Management) a essentiellement été étudiée par l'ISO (International Standard Organisation), sous l'impulsion des grands constructeurs d'ordinateurs (IBM, DEC, etc.). Ce n'est que récemment que les opérateurs de réseaux (PTT et autres «carriers»), dont le métier fut de tout temps de gérer les réseaux, se sont intéressés à ces travaux par le biais de leur organisme de normalisation, le CCITT (Comité consultatif international télégraphique et téléphonique). La responsabilité d'assurer la liaison entre les différentes activités de gestion du CCITT et les travaux de l'ISO concernant la gestion OSI de systèmes a été confiée récemment au sous-groupe VII/Q.24 du CCITT.

Bien que les travaux de l'ISO datent déjà de plusieurs années, certains documents sont encore peu stables et peu cohérents entre eux. Il est tenté, dans cet article, de donner une vue didactique des travaux, sans changer l'esprit des textes originaux.

2 Architecture de la gestion OSI de systèmes

21 Cadre de la gestion OSI de systèmes

211 But de la gestion OSI

Selon [1], la gestion OSI est la faculté de contrôler, de coordonner et de surveiller les ressources qui permettent à une communication d'exister dans un environnement OSI. Dans cet environnement de systèmes ouverts, certains systèmes peuvent avoir la responsabilité de se gérer eux-mêmes et/ou de gérer d'autres systèmes ouverts. Dans ce dernier cas, il y a échange d'informations de gestion entre les systèmes ouverts pour assurer les activités indispensables de gestion coordonnée.

Il faut donc clairement comprendre que, dans le cadre de la gestion OSI de systèmes, le mot «management» est limité aux systèmes et non au personnel de gestion, qui ne peut, heureusement, faire l'objet de mesures de normalisation.

212 Relations de gestion entre systèmes ouverts

Dans les relations de gestion entre deux systèmes ouverts, l'un prend le rôle de système gestionnaire (manager) et l'autre celui de système géré (managed, *fig. 1)*. Le rôle joué par un système donné peut être statique, varier au cours du temps ou selon la communication de gestion en cours.

213 Objets gérés

Selon [1] et [3], les objets gérés (managed objects) sont les abstractions des ressources réelles de traitement ou de communication de données, telles que les voit la gestion. Ces ressources réelles peuvent être des machines

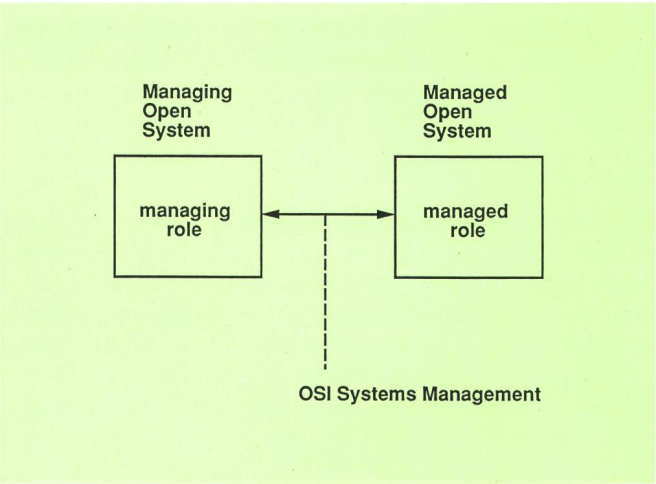
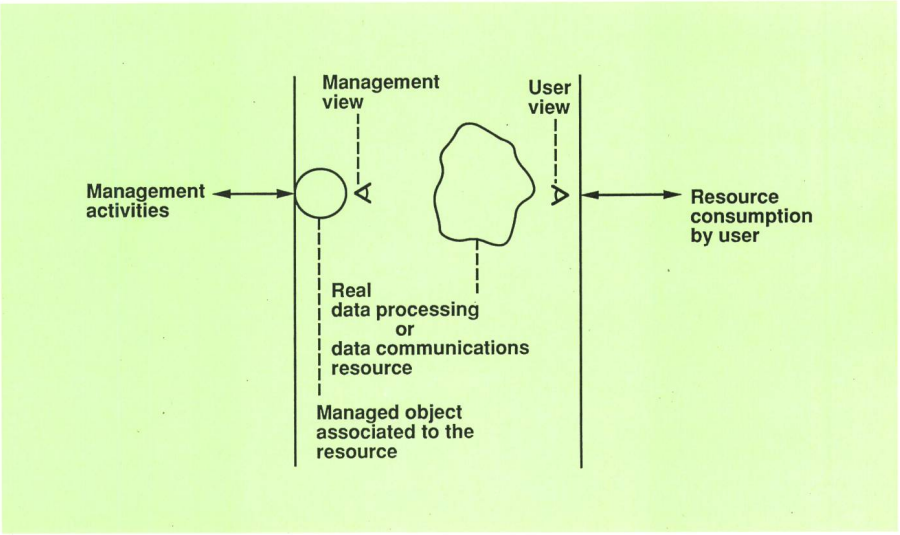


Fig. 1
Relations de gestion entre systèmes ouverts

Fig. 2
Objets gérés



protocolaires, des connexions, des ressources physiques (modem, etc.).

Les usagers de cet environnement OSI utilisent ces ressources selon leur point de vue, c'est-à-dire selon le service qu'offre la ressource en question. Pour une couche 3/X.25, par exemple, la ressource est une machine protocolaire de paquets dans un nœud de commutation X.25, géré selon OSI *(fig. 2)*.

214 Aires fonctionnelles

Cinq aires fonctionnelles ont été identifiées pour la gestion OSI *(fig. 3)*.

- *«Fault Management, FM»,* pour la détection, l'isolation et la correction de fautes
- *«Accounting Management, AM»,* pour la taxation de l'utilisation de ressources par l'usager
- *«Configuration Management, CM»,* pour la configuration des objets gérés en vue de l'offre de services de communication
- *«Performance Management, PM»,* pour l'évaluation du comportement des ressources sous charge
- *«Security Management, SM»,* pour la gestion des mécanismes de sécurité mis en place pour contrôler l'utilisation des ressources par l'usager.

Ces aires ne sont pas indépendantes les unes des autres: Ainsi une alarme (FM) peut concerner une atteinte à la sécurité du système (SM).

215 Distinction entre gestion par protocoles de gestion et gestion par d'autres protocoles

Il y a différentes manières d'échanger des informations de gestion entre deux systèmes ouverts [1]. Deux d'entre elles sont présentées aux *figures 4* et *5*.

La forme préférée est l'échange selon le protocole de gestion de la figure 4, c'est-à-dire à travers une application de gestion entre un système gestionnaire et un système géré (objet de cet article).

Une autre forme plus limitée d'échange d'informations de gestion est celle utilisant comme véhicule de transport les protocoles normaux de communication. La figure 5 représente l'échange, entre deux réseaux, d'informations de gestion par le biais de la norme X.75 (par exemple, pour les codes de libération/clear codes). Chacun de ces réseaux est supposé être géré en interne par un protocole d'application de gestion OSI et former un domaine administratif de gestion propre.

22 Gestion de systèmes ouverts

221 Gestionnaires et agents

La *figure 6* illustre le principe de la gestion de systèmes ouverts [2]: Dans le système gestionnaire, un processus d'application – *manager process* – a la responsabilité de la gestion et envoie des opérations de gestion au système géré. Celui-ci possède un processus d'application

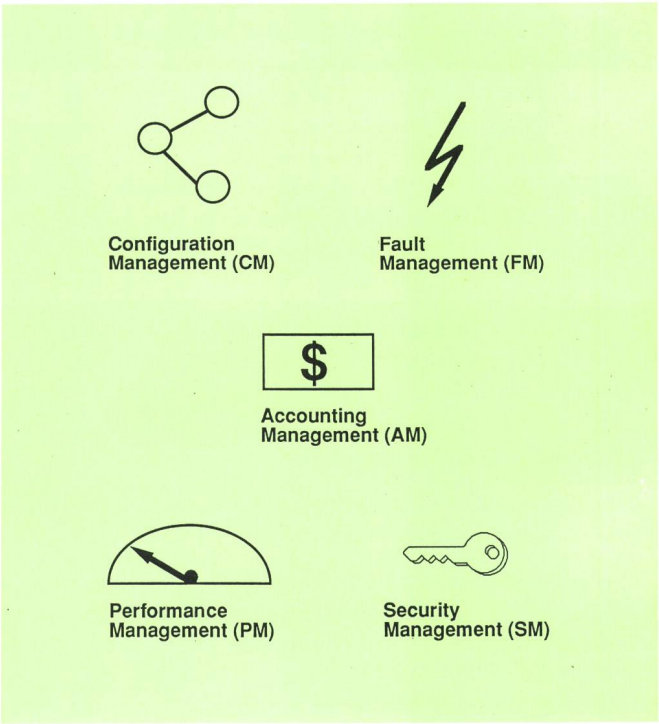


Fig. 3
Aires fonctionnelles de la gestion OSI

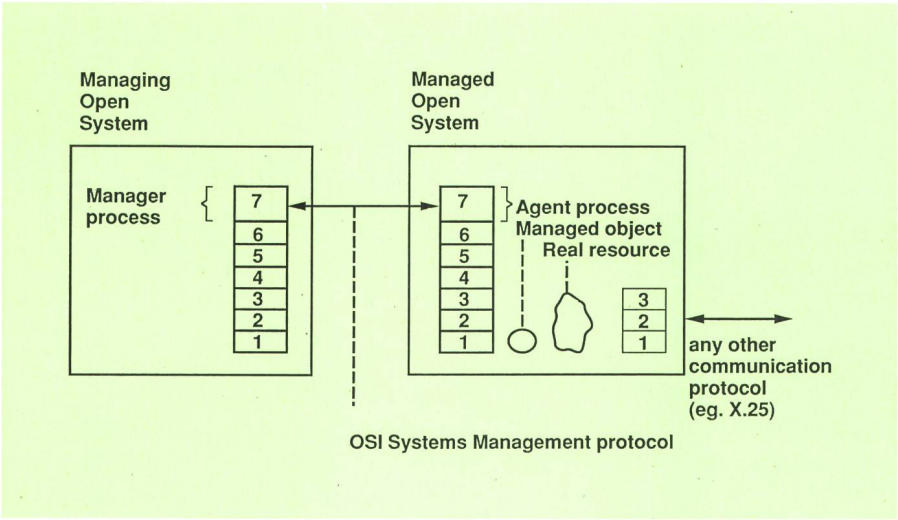


Fig. 4
Protocole de gestion de systèmes

appelé agent – *agent process* – chargé d'exécuter ces opérations de gestion sur les objets placés sous son contrôle – *managed objects.* Ces objets peuvent, suivant les événements qui se produisent dans la ressource dont ils sont l'abstraction, émettre des rapports (notifications) qui sont rassemblés et éventuellement filtrés dans le processus d'agent par des discriminateurs (eux-mêmes étant une classe spéciale parmi les objets gérés). Après filtrage, ces rapports sont retransmis par le processus d'agent au processus de gestion. Seuls les rapports entre «manager process» et «agent process» sont normalisés dans un protocole.

222 Couche d'application de gestion

L'une des méthodes recommandées [2] pour l'infrastructure du protocole de gestion en couche d'application est celle indiquée à la *figure 7.* Aux deux briques de fondation des applications OSI («Association Control Service Element», ACSE et «Remote Operation Service Element», ROSE), on rajoute deux couches de processus. Le premier élément est constitué par le *«Common Management Information Service Element»,* CMISE qui assure l'échange des opérations de gestion et des notifications de gestion de manière commune. Le second élément, le *«Systems Management Application Service Element»,* SMASE, permet de spécifier ces activités de gestion selon les aires fonctionnelles désirées (FM, AM, CM, PM, SM), par exemple.

D'autres moyens d'infrastructure pour les protocoles de gestion sont suggérés dans [2].

223 Domaines de gestion

La notion de domaine de gestion est encore bien peu étudiée: Deux types ont été définis [2]:

- Le *domaine de gestion fonctionnel,* qui définit des règles «policies» applicables à un certain nombre de systèmes ouverts, gestionnaires ou gérés, telles qu'une directive de sécurité, de taxation, etc. Il est possible que ces domaines s'entrecoupent (overlap).
- Le *domaine de gestion administratif,* qui fixe la barrière de responsabilité d'une autorité de gestion (personne ou organisation, telle qu'une administration ou une entreprise privée).

224 Conformité

Pour qu'un fournisseur puisse utiliser la gestion OSI de systèmes, il faut qu'il justifie la conformité de ses équipements aux standards et que celle-ci puisse être testée [2].

Deux écoles s'opposent encore à ce sujet: L'une prétend que la conformité est limitée au protocole de gestion et qu'un testeur A dans le système gestionnaire peut examiner la visibilité de l'objet géré, sans juger de son comportement et de son action réelle sur la res-

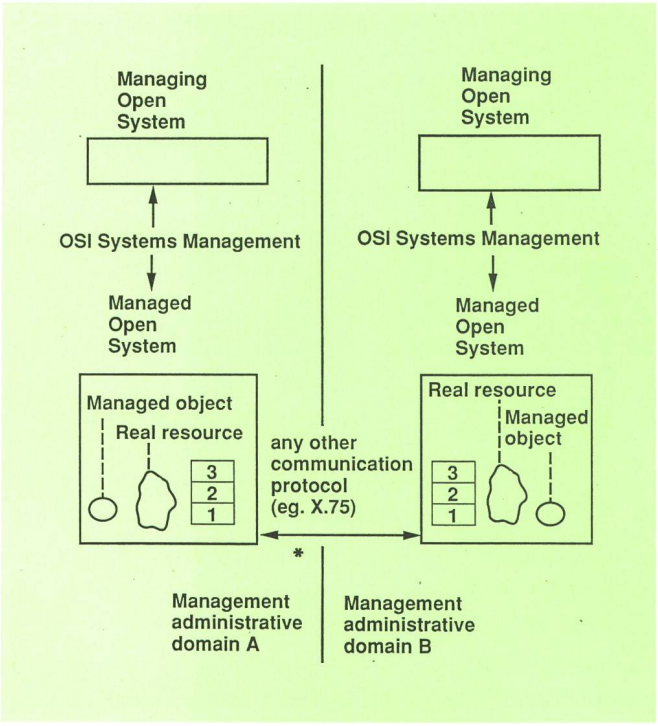
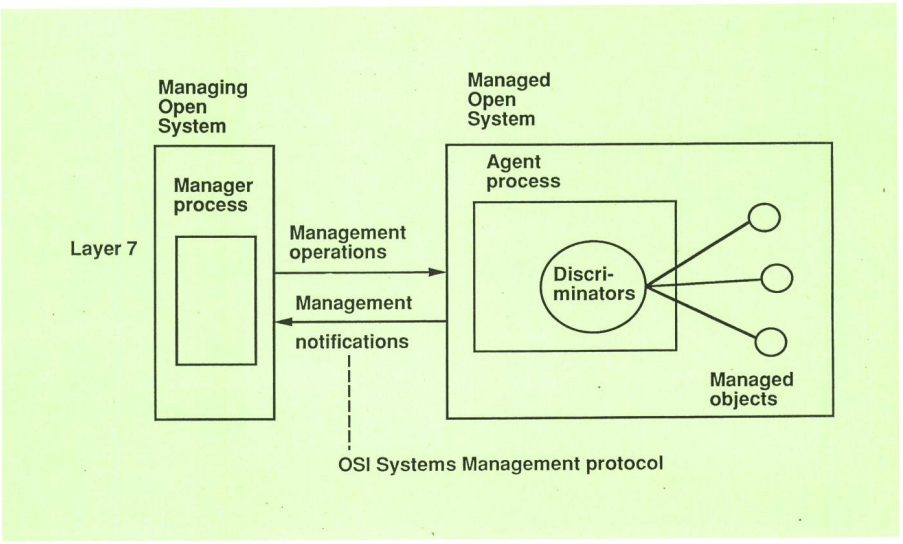


Fig. 5
Opération de la couche de niveau N
* Information de gestion transportée par les protocoles de communication (par exemple les codes de libération dans les paquets X.75 de libéralisation)

Fig. 6
Interactions entre le système gestionnaire (manager), le système géré (agent) et les objets



source à gérer. L'autre école est d'avis que la conformité exige également l'examen de l'action sur la ressource, par l'utilisation d'un deuxième testeur B du côté de l'usager et par le contrôle de la corrélation des événements aux deux testeurs. Ainsi, dans le cas de la saisie du nombre de segments X.25 taxés (accounting meter of accounting management), le testeur B générerait un nombre prédéterminé de paquets, donc de segments, tandis que le testeur A lirait, par le biais du protocole de gestion, la valeur du compteur de segments et en vérifierait l'exactitude.

3 Service et protocole communs de gestion

A ce jour, le service commun de gestion entre deux systèmes ouverts et son protocole correspondant [7 et 8] ont été définis. Ils portent la désignation de:

- CMIS Common Management Information Service
- CMIP Common Management Information Protocol.

Le service de ce protocole commun peut être décomposé en trois parties:

A. Les services d'association de gestion

- M-INITIALISE, pour établir une association d'applications entre les deux systèmes ouverts
- M-TERMINATE, pour conclure une telle association
- M-ABORT, pour libérer l'association de manière abrupte.

B. Les services de notification de gestion

- M-EVENT-REPORT, pour rapporter un événement relatif à un objet géré au système gestionnaire.

C. Les services d'opération de gestion

- M-GET, pour aller chercher une information de gestion
- M-SET, pour modifier la valeur d'une information de gestion
- M-ACTION, pour exécuter une action
- M-CREATE, pour créer un nouvel objet géré
- M-DELETE, pour supprimer un objet géré
- M-CANCEL-GET, pour effacer une requête antérieure de M-GET, non encore exécutée.

4 Structure de l'information de gestion

41 Modèle d'information de gestion

Chaque objet géré possède un certain nombre d'attributs, définissant ses propriétés *(fig. 8)*. Ces attributs ont des valeurs généralement observables à la limite visible pour la gestion des objets gérés. L'ensemble des objets gérés d'un système ouvert et de leurs attributs forme la base de l'information de gestion («Management Information Base», MIB) [3].

42 Opérations de gestion

421 Opérations orientées «attributs»

Les opérations orientées vers la gestion des attributs d'un objet géré sont [3]:

– «Get attribute value»
– «Replace attribute value»

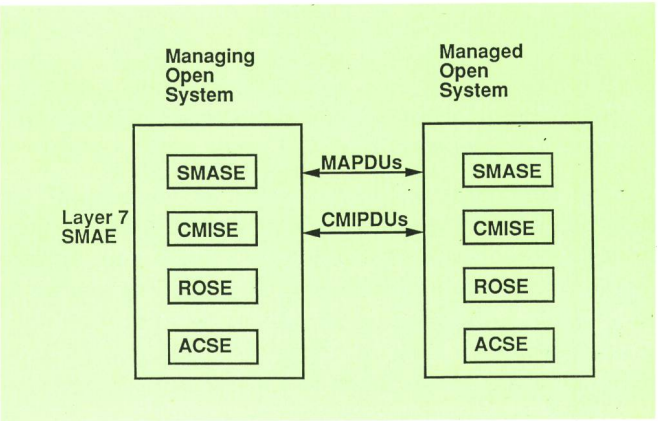


Fig. 7
Gestion des systèmes et la couche d'application
ACSE Association Control Service Element
ROSE Remote Operation Service Element
CMISE Common Management Information Service Element
SMASE Systems Management Application Service Element
SMAE Systems Management Application Entity
MAPDU Management Application Protocol Data Unit
CMIPDU Common Management Information Protocol Data Units

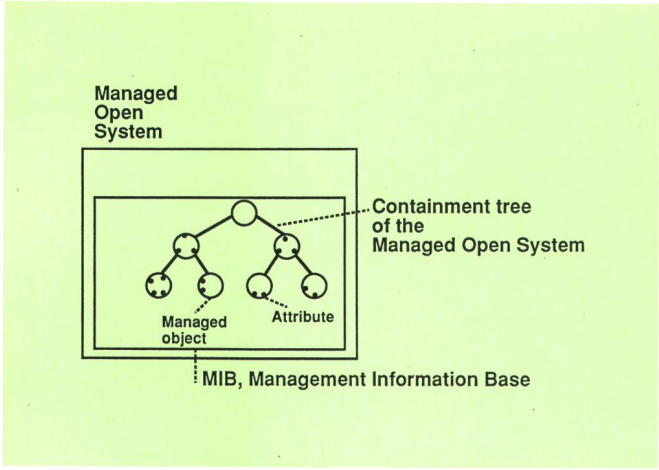


Fig. 8
Base de données d'information de gestion et gestion des objets

- «Add attribute value» (lorsque l'attribut peut avoir plusieurs valeurs en même temps)
- «Remove attribute value».

422 Opérations orientées «objets gérés»

Les opérations qui gèrent l'objet dans son ensemble sont [3]:

- «Create a managed objet»
- «Delete a managed objet»
- «Action» (requête à l'objet d'exécuter une action et d'en indiquer le résultat).

43 Filtres

Les filtres sont encore une notion mal précisée. Ils semblent être les attributs des discriminateurs (fig. 6) permettant [3]:

- pour les opérations, de filtrer si une application déterminée doit être exécutée ou non sur un objet géré
- pour les notifications, de filtrer les événements qui doivent être remontés au système gestionnaire.

44 Classes d'objets gérés et hiérarchie inhérente dans une classe

Les objets gérés ayant les mêmes opérations, les mêmes notifications et les mêmes attributs appartiennent à la même classe *(fig. 9)* [3]. Une classe peut être l'extension d'une autre classe par un raffinement de la première, en rajoutant de nouvelles opérations, de nouvelles notifications ou de nouveaux attributs. La classe supérieure est définie comme «superclass», tandis que la classe dérivée est la «subclass». Celle-ci hérite les opérations, les notifications, les attributs et le comportement de la classe supérieure. L'ensemble forme une hiérarchie inhérente (inheritance hierarchy) dans une classe, avec à sa tête la classe supérieure, ancêtre formant le sommet (top) de cette hiérarchie. Ce mécanisme est puissant, mais il y a lieu de craindre une prolifération de sous-classes!

45 Désignation des objets gérés et hiérarchie englobante

Un objet géré d'une classe donnée peut être le supérieur (superior) d'un objet géré d'une même classe ou d'une classe différente (subordinate, *fig. 10)* [3]. Il est aussi dit que le supérieur (container) contient le subordonné (contained). Le subordonné a *un* supérieur. La hiérarchie des objets supérieurs/subordonnés forme l'arbre englobant (containment tree) dont le supérieur général forme la racine (root). Cette racine est définie comme un objet nul qui existe en tous les cas (cette définition n'a bien sûr aucun rapport avec la position hiérarchique d'un PDG!).

Le subordonné ne peut exister sans que son supérieur existe aussi: Le nom du subordonné est dérivé du nom du supérieur, par adjonction d'un attribut d'identification unique. La relation entre supérieur et subordonné est donc contenue implicitement dans le nom du subordonné.

Grâce à cette conception de la hiérarchie, on dispose d'un outil puissant. La gestion d'un réseau X.25 pourrait faire appel, par exemple, à une hiérarchie englobante de la forme suivante, définissant la «Management Information Base» MIB:

- *X.25 Network*
  - Services
  - Network Elements
    - Measurement ...
    - Test
      - Hardware ...
      - Software ...
    - Layer Entity
      - Layer 1 ...
      - Layer 2 ...
      - Layer 3 ...

Il est évident que la création concrète de cette hiérarchie englobante pour un réseau réel sera la partie la plus importante de toute la conception, car elle rendra la

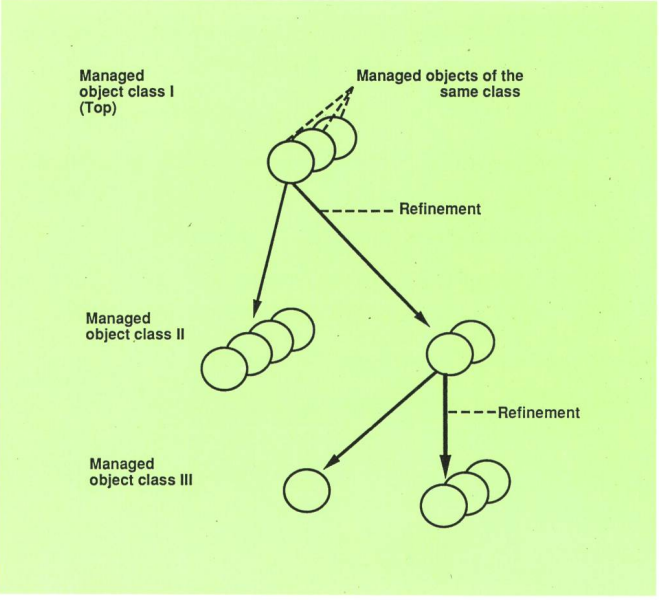


Fig. 9
Classes d'objets gérés et hiérarchie inhérente

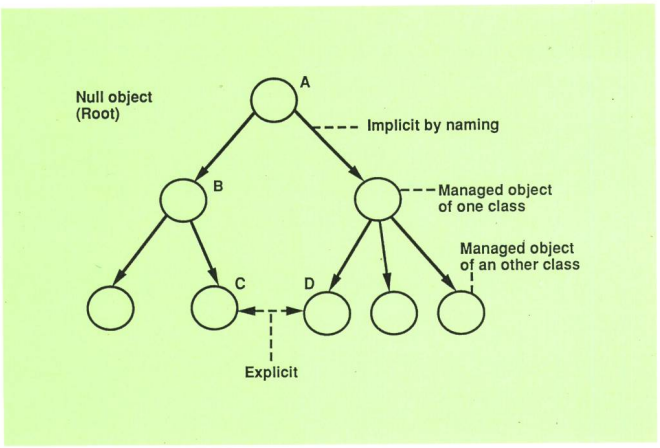


Fig. 10
Désignation des objets gérés et hiérarchie englobante (containment hierarchy)
B Objet géré subordonné à l'objet A (contenant), supérieur à l'objet géré C (contenu)
Chaque subordonné n'a qu'un et un seul supérieur
C Le nom de C est le nom de B additionné d'un attribut d'identification unique. C ne peut exister que si B existe

gestion conviviale et aisée ou compliquée et inutilisable. Les objets normés ne constituent que les «blocs de construction» de la gestion: Seule l'implantation concrète de ces éléments dans les réseaux réels sera, soit intelligente, soit stupide. Dans les deux cas, le constructeur peut prétendre être conforme aux standards.

46 Quelques attributs

Quelques attributs sont décrits ci-après [6]:

- le *compteur,* qui, associé à un événement interne de l'objet géré, augmente d'une unité à chaque événement. Il peut être remis à zéro ou pas par le système gestionnaire
- le *seuil du compteur* (threshold); une notification est générée dès qu'il est atteint
- la *jauge* qui représente une variable dynamique, susceptible de changer dans les deux directions
- le *seuil supérieur* de la jauge, qui génère une notification au moment où il est atteint
- le *seuil inférieur* de la jauge; une notification est générée dès que ce seuil est dépassé
- le *«tide-mark»* qui est la valeur extrême atteinte par la jauge lors d'une période de mesure. On définit soit une valeur maximale, soit une valeur minimale. Dans le premier cas, la «tide-mark» ne se déplace que vers le haut, et dans l'autre cas, vers le bas.

Les seuils de la jauge permettent de générer une seule notification, même en cas d'oscillations de la valeur de la jauge vers l'un des seuils: En effet, une fois la notification supérieure émise, par exemple, il n'y aura plus d'autre notification supérieure émise, même si le seuil haut est traversé plusieurs fois par la jauge, cela aussi longtemps que la jauge ne sera pas descendue au niveau du seuil inférieur. La distance entre le seuil supérieur et le seuil inférieur est appelée intervalle d'hystérèse.

47 Directives pour la définition d'objets gérés

Une directive, donnant une définition générique en «ASN.1» (Abstract Syntax Notation one) des objets gérés a été fixée [6]. Ce «patron» (template) peut être utilisé pour la définition d'objets gérés spécifiques et assure la description cohérente des différents objets de gestion par tous les implémenteurs.

5 Gestion de la configuration

51 Configuration des objets gérés

Selon [9], les objets gérés peuvent générer un certain nombre de notifications liées à la configuration. Ce sont:

- «Objet Creation Notification» (soit le résultat de M-CREATE, soit une initiative locale du système géré)
- «Objet Deletion Notification»
- «Objet Name Change Notification»
- «Attribute Change Notification».

Les opérations sur les objets et leurs attributs ont été décrites au chapitre 42.

52 Gestion de l'état des objets gérés

Selon [10], on distingue deux sortes d'états: les états opérationnels et les états administratifs d'un objet.

Les états opérationnels sont (fig. 11):

- «Disabled» — l'objet géré n'est pas exploitable
- «Enabled» — l'objet géré est exploitable et non utilisé
- «Active» — l'objet supporte plusieurs usagers, et est utilisé par un nombre d'usagers inférieur au maximum
- «Busy» — l'objet est exploité au maximum de sa capacité.

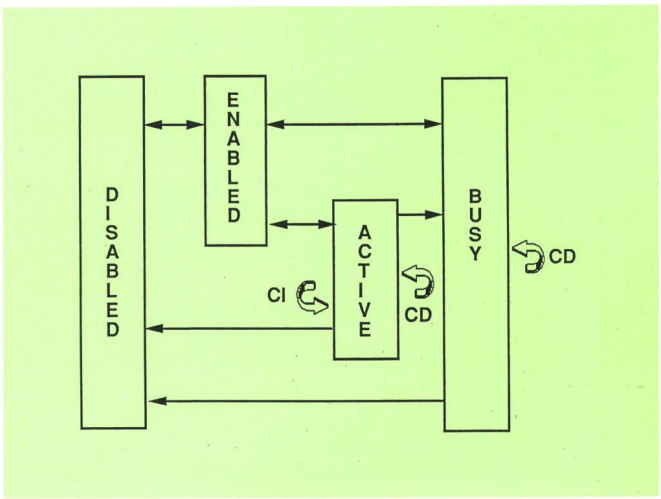


Fig. 11
Etats opérationnels d'objets gérés (CM)
CI Accroissement de capacité
CD Diminution de capacité

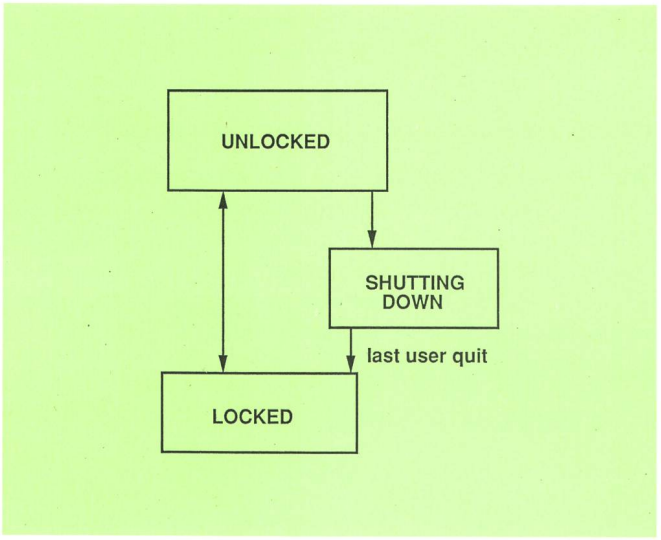


Fig. 12
Etats administratifs d'objets gérés (CM)
Suspendre une action: mettre l'état administratif sur verrouillé (locked)
Reprendre une action: mettre l'état administratif sur déverrouillé (unlocked)

Les états administratifs sont (fig. 12):

- «Unlocked» l'usage normal de l'objet est autorisé administrativement
- «Locked» l'usage de l'objet est prohibé
- «Shutting Down» l'utilisation normale de l'objet n'est autorisé qu'aux usagers déjà en train d'utiliser l'objet.

Lorsqu'on suspend une action, on met l'objet concerné à l'état verrouillé «locked». Lorsqu'on reprend une action, on met l'objet à l'état déverrouillé «unlocked».

53 Gestion des relations entre objets gérés

Une relation, selon [11], est un ensemble de règles qui décrit comment le fonctionnement d'un objet géré d'un système ouvert agit sur le fonctionnement d'un autre objet de ce même système.

On distingue:

- une *relation directe,* quand les informations de gestion d'un des objets identifient expressément l'autre objet dans ses relations
- une *relation indirecte,* quand on peut déduire une relation par enchaînement de plusieurs relations directes
- une *relation symétrique,* quand l'ensemble des règles gérant l'objet X par rapport à l'objet Y est identique à l'ensemble des règles gérant l'objet Y par rapport à l'objet X
- une *relation asymétrique,* dans le cas inverse.

On distingue, en outre, deux catégories de relations (fig. 10):

- *Containment relationship*
  Dans ce cas de relation englobante, l'un des objets C est la possession exclusive d'un autre objet B, qui en est le contenant (container). L'identité de l'objet possédant est implicitée dans le nom de l'objet possédé. Une telle relation englobante apparaît automatiquement à la création de l'objet possédé et ne peut être modifiée. Elle persiste jusqu'à la destruction de l'objet possédé.
- *Explicit relationship*
  Dans le cas de relation explicite, certains attributs de chacun des objets liés (C et D) contiennent le nom (pointeurs) des autres objets auxquels ils sont liés (D et C respectivement).

Les relations explicites peuvent représenter des relations du type:

- «one-to-one»
- «many-to-one»
- «one-to-many»
- «many-to-many».

Les relations explicites peuvent être modifiées par la gestion (création, destruction, modification). On distingue dans les relations explicites les types de relations suivants:

- *Peer relationship:* relation entre deux objets similaires
- *Service relationship:* relation entre un premier objet qui est le fournisseur d'un service «service provider» pour le second, lequel est l'utilisateur d'un service «service user» (exemple: relation de l'objet responsable de la couche 4 avec celui responsable de la couche 3)
- *Backup relationship:* relation décrivant que le second objet d'une paire joue le rôle de «backup»
- *Group relationship:* relation entre un objet membre d'un groupe et un autre, représentant le groupe dans son ensemble.

Les opérations suivantes sur les relations explicites sont identifiées:

- «Creation» la création d'une relation
- «Deletion» sa suppression d'une relation
- «Changing» la modification des valeurs des attributs associés à la relation
- «Listing» la liste des relations entre objets.

Les notifications sont définies:

- «Relationship creation reporting»
- «Relationship deletion reporting»
- «Relationship change reporting».

La notion de relation «one-way explicit» est à l'étude.

6 Fault management (FM)

61 Rapport d'erreurs

Selon [12], on définit les notions suivantes pour les rapports d'erreurs *(fig. 13):*

- Fault: Cause physique ou algorithmique (software) d'un mauvais fonctionnement
- Error: Manifestation de fautes sous forme de déviation d'un objet par rapport à son fonctionnement normal
- Alarm: Notification d'un événement. Une alarme peut représenter une erreur ou non (situation anormale possible).

Différents niveaux de sévérité ont été définis pour les alarmes:

- «Cleared» la situation anormale a disparu
- «Indeterminate» situation indéterminée

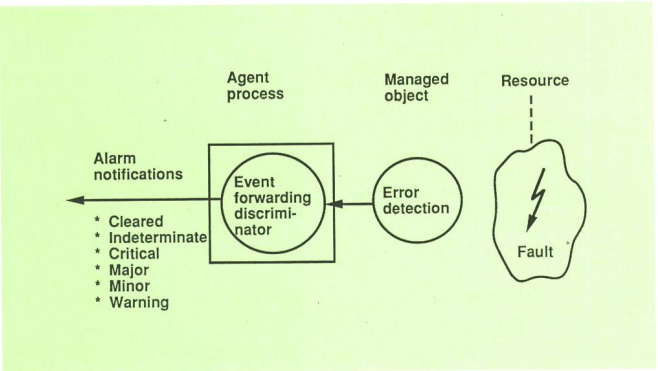


Fig. 13
Rapport d'erreur et filtre de transfert d'événements (event forwarding discriminator, FM et SM)

- «Critical» situation critique
- «Major» alarme majeure
- «Minor» alarme mineure
- «Warning» mise en garde.

Le niveau de sévérité peut être différent selon l'endroit d'où est vue la faute. Ainsi, une faute dans les couches basses d'OSI peut être considérée comme majeure par ces couches, alors qu'elle peut être mineure ou ne pas apparaître du tout dans les couches supérieures, à cause des processus de retransmission.

Cinq notifications d'alarmes génériques ont été définies (fig. 13):

- «Communication alarm»
- «Quality of service alarm» (temps de réponse, débits, etc.)
- «Processing alarm» (capacité de mémoire, logiciel, etc.)
- «Equipment alarm» (alimentation, matériel)
- «Environmental alarm» (fumée, humidité, température, intrusion détectée, etc.).

Des informations concernant entre autres:

- la tendance générale («more severe», «no change», «less severe») en relation avec les autres alarmes actives
- les informations de niveaux («triggered thresholds»)
- les corrélations avec les alarmes précédentes
- etc.

sont également envoyées, en relation avec les notifications génériques.

62 Discriminateur d'annonce d'événements

Pour contrôler le service de gestion, la notion de discriminateurs a été définie. Un seul d'entre eux est fixé en détail à ce jour, dans le cadre de la gestion des fautes: Il s'agit du filtre de transfert d'événements *«Event forwarding discriminator»* [4 et 13]. C'est un objet géré servant à filtrer les événements qui sont annoncés au système ouvert gestionnaire.

Les opérations sur cet objet sont les suivantes:

- «Initiation of Event Forwarding»
- «Termination»
- «Suspension and Resumption»
- «Modification of Event Forwarding Conditions»
- «Retrieval of Event Forwarding Conditions».

Les notifications d'événements peuvent être adressées *(fig. 14):*

- au système ouvert local
- au système gestionnaire ou
- à un système tiers.

Ce dernier aspect permet d'imaginer des fonctions de contrôle très sophistiquées.

63 Tests de diagnostic

Pour la gestion des fautes et de la performance (FM et PM), il est nécessaire que le système de gestion puisse procéder à des tests [14]. Les classes de tests suivantes ont été définies:

- *Connectivity tests:* possibilité de deux ressources à s'interconnecter
- *Data Integrity test:* échange de données entre deux ressources, sans corruption
- *Protocol Integrity tests:* échange de PDU spécifiques (Protocol Data Units) et contrôle des réponses (mécanismes de «self-test» ou de «loop-back»)
- *Data Saturation test:* transmission au débit maximal de PDU de données
- *Connection Saturation test:* test du nombre maximal de connexions possibles
- *Response time test:* délai de réponse entre deux ressources (round trip delay)
- *Imaging Loopback test:* écho de données reçues, généralement renvoyées à la source
- *Function test:* test de fonctionnement d'une ressource («self-test», par exemple)
- *Diagnostic test:* essais pour localiser une faute.

Le modèle de test suivant est mis en place *(fig. 15* et *16):* Un système ouvert, responsable du test *(test conductor)* est en relation avec un certain nombre de systèmes ouverts à tester, soit de manière directe (primary test performer), soit de manière indirecte *(secondary test performer).* Un système ouvert exécutant un test pos-

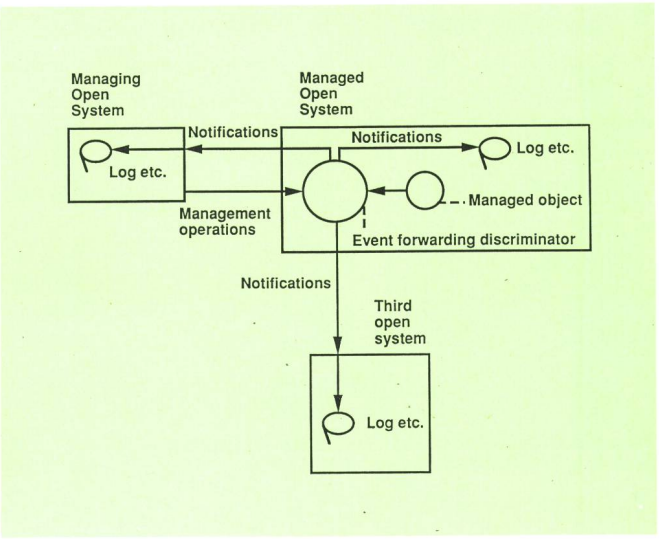


Fig. 14
Contrôle du transfert d'événements
Destination des notifications
- le système ouvert local
- le système ouvert gestionnaire
- un système ouvert tiers

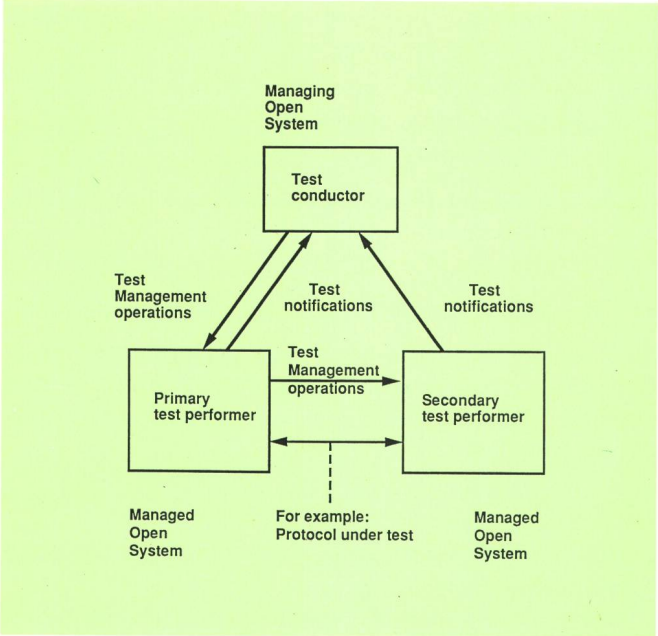


Fig. 15
Modèle de test (FM et PM)

sède un objet géré recevant les requêtes de test *(Test Request Receiver)*. Il peut, pour le test, générer des objets spécifiques *(Test object)*. Ceux-ci existent au moins pour la durée du test et contiennent l'état du test en cours et les résultats intermédiaires des tests. Ces objets agissent sur les ressources réelles à tester (Resource Under Test).

Un objet (Test object) peut avoir les états suivants pour les tests:

- «Initiation» (démarrage, chargement de logiciel de test)
- «Testing» (exécution du test)
- «Idle»
- «Reporting» (annonce des résultats)
- «Termination».

64 Fonction de journal

La fonction de journal *(log)* est encore mal décantée [15]: Un processus agent peut agir sur un objet représentant la fonction de mise en journal d'informations de gestion (logging, *fig. 17)*. Le journal est un fichier d'enregistrements d'informations de gestion *(log records)*, tels que les enregistrements d'opérations de gestion ou de notifications («event records» ou plus précisément «error event records», etc.).

Les opérations identifiées pour la fonction de journal sont:

- «Initiating the log»
- «Terminating the log»
- «Suspending logging»
- «Resuming logging»
- «Modifying logging attributs»
- «Retrieving logging attributs».

La notification spécifique identifiée se rapportant au journal est celle indiquant que la capacité maximale de mise en journal a été atteinte.

Les «log records» sont également des objets gérés, auxquels on peut accéder pour la gestion (M-GET, Retrieve event information).

7 Gestion de la sécurité

Les objets liés à la sécurité (Security Object) représentent, du point de vue de la gestion, les mécanismes et les services de sécurité implantés dans un système ouvert (liste de contrôle d'accès par les usagers, NUI: Network User Identification, clefs d'autorisation, etc.). Ces mécanismes permettent, entre autres choses, d'identifier de manière sûre les usagers qui utilisent des ressources du système ouvert.

Selon [16], quatre fonctions ont été identifiées *(fig. 18)*:

- *Security Audit Trail*
  Cette fonction envoie les notifications de sécurité (security events) à un journal (log) en vue d'une analyse ultérieure, afin que l'on puisse détecter une éventuelle faille dans la sécurité. Pour ce faire, on utilise essentiellement la fonction M-EVENT-REPORT.
- *Security Alarm Function*
  Dès qu'une atteinte à la sécurité ou une anomalie concernant la sécurité sont détectées, cette fonction émet une notification par le biais de la fonction M-EVENT-REPORT.
- *Security Object and Attribute Management Function*
  Cette fonction permet de gérer les objets liés à la sécurité.
- *Security Alarm and Audit Trail Management Function*
  Cette fonction permet de configurer le discriminateur examinant les événements de sécurité.

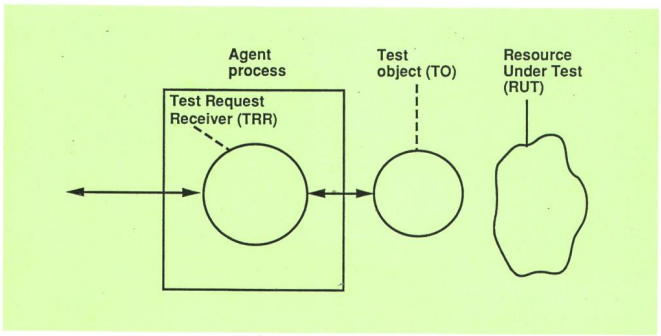


Fig. 16
Exécuteur de test (FM et PM)

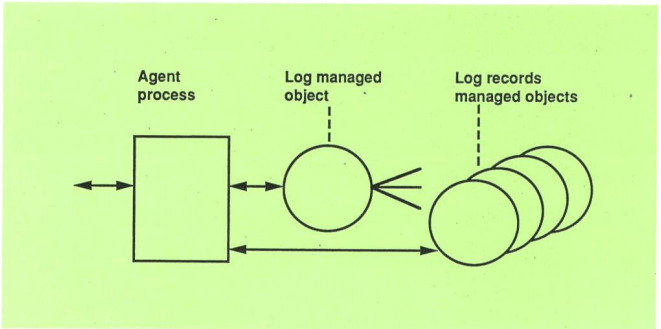


Fig. 17
Journal (Log FM, PM, AM)

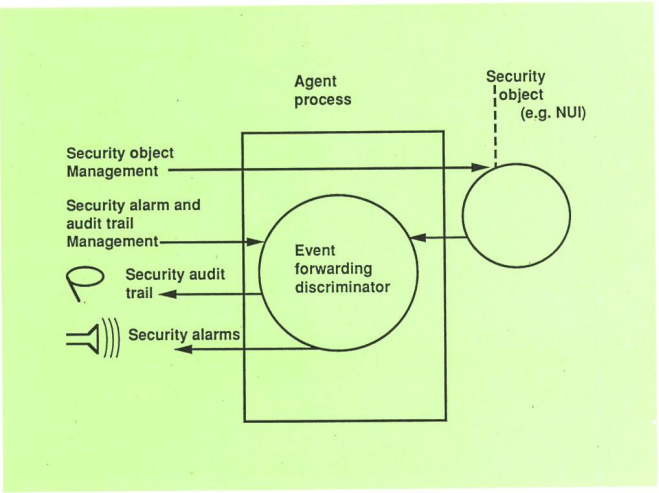


Fig. 18
Gestion de la sécurité (SM)

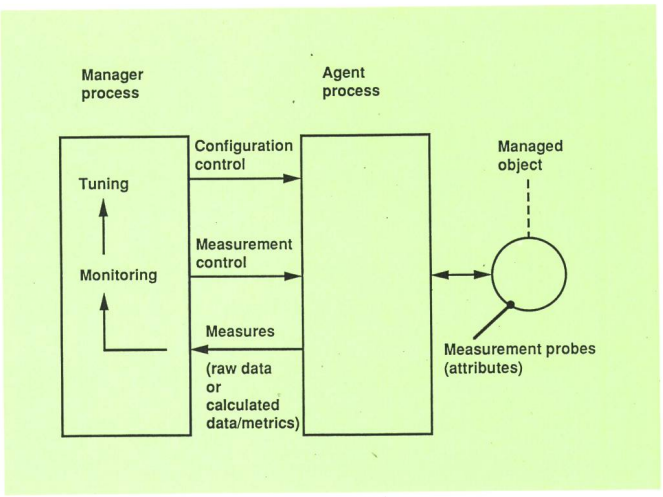


Fig. 20
Gestion des performances (PM)

8 Gestion de la taxation

La fonction de taxation (Accounting Management, AM) est encore très mal étudiée dans les organismes de normalisation de la gestion OSI de systèmes [17].

Pour le moment on distingue approximativement les éléments suivants *(fig. 19):*

- *End user:* usager utilisant une ressource
- *Subscriber:* autorité d'un domaine administratif dont l'usager (end user) est un membre et qui a un rapport contractuel avec l'autorité du domaine administratif dont l'usager utilise les services
- *Accounting meter:* objet géré (managed object) qui a comme attribut la faculté d'enregistrer les informations de taxation pour une ressource donnée
- *Quotas:* Quantité d'une ressource qu'un usager donné a le droit de «consommer».

9 Gestion des performances

La gestion des performances (PM) d'un système ouvert a été déjà largement étudiée, mais les différents éléments n'ont pas encore été intégrés de manière cohérente [18] et [19].

On distingue entre autres les éléments suivants *(fig. 20):*

Measurement probes: Sondes de mesures, définies en tant qu'attributs d'objets gérés. Elles émettent des notifications (M-EVENT-REPORT) au cas où des seuils de performance (threshold) sont dépassés. Elles peuvent également être lues à l'initiative du système gestionnaire (M-GET).

Measures: Valeurs brutes ou calculées mesurées. En cas de calcul (metrics), les opérations typiques sont l'établissement de la moyenne, du maximum, du minimum, de la déviation de la moyenne, etc.

Measurement control: Gestion des sondes mesurées.

Configuration control: Modification des paramètres configurables pour optimiser la performance du système géré en fonction des résultats mesurés.

Deux aspects particuliers ont été largement étudiés: Le «Response Time Monitoring function» et le «Workload Monitoring function». Pour le temps de réponse, la *figure 21* présente la conception de la mesure du délai de transit, ainsi que la difficulté de synchroniser les horloges aux deux extrémités de la mesure. En ce qui concerne la performance, la *figure 22* présente l'un des modèles étudiés pour l'utilisation d'une ressource, avec deux sortes de seuil, l'un d'alarme avancée (early warning threshold) et l'autre d'alarme sévère (severe threshold).

10 Etat des documents et continuation des travaux

ISO, contrairement au CCITT, a deux états intermédiaires pour ces documents, entre la première ébauche

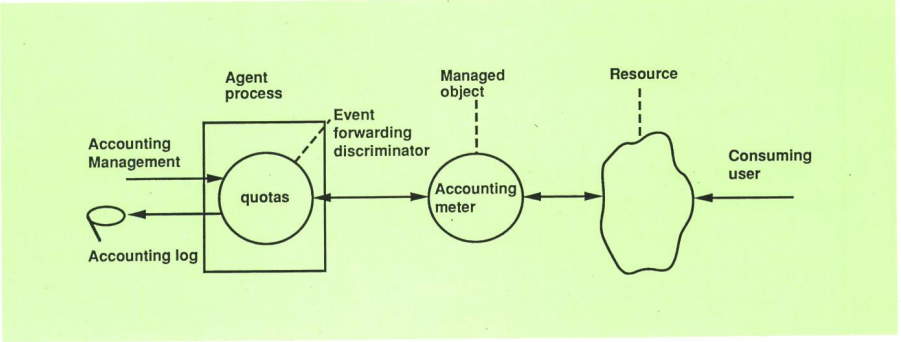


Fig. 19
Gestion de la taxation (AM)

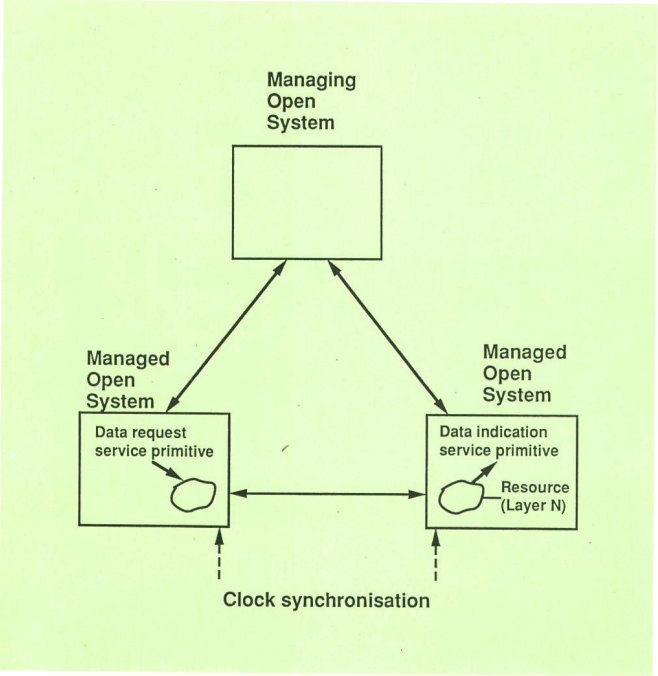


Fig. 21
Surveillance du temps de réponse (délai de transit, PM)

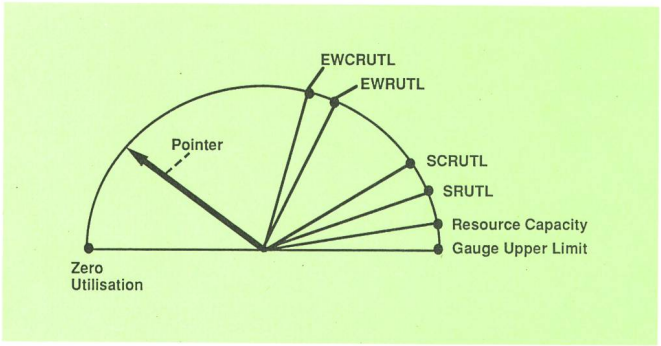


Fig. 22
Jauge d'utilisation d'une ressource (PM)

(Working Draft) et le standard *(International Standard)*. Ce sont les propositions préliminaires (Draft Proposal) et les normes internationales provisoires (Draft International Standard), tous deux soumis à une période de gestation (6 mois et 3 mois) durant lesquels les organismes de normalisation nationaux peuvent exprimer leur point de vue (Ballot).

Vu l'initiative prise par l'ISO, son rythme et sa procédure influenceront largement les travaux du CCITT sur la gestion OSI de systèmes.

En ce qui concerne les travaux en cours, un certain nombre de documents clefs sont à l'état de propositions préliminaires, c'est-à-dire que d'ici 6 mois ils passeront à l'état normes internationales provisoires. C'est donc le dernier moment pour influencer les conceptions, raison pour laquelle le programme des réunions de travail ISO/CCITT de 1990 est assez chargé. L'une de ces réunions aura lieu en septembre 1990 à Montreux, sous les auspices des PTT suisses.

11 Conclusions

111 Puissance des outils développés

La gestion OSI de systèmes met au point des outils puissants qui permettront de construire des applications de gestion sophistiquées. Les outils principaux sont:

- Le *modèle de données (data model)* développé, c'est-à-dire
  - les objets gérés
  - leurs attributs
  - les classes d'objets
  - la base de gestion d'information («Management Information Base»)
  - le «patron» (template) de définition ASN.1 des objets gérés.
- Le *protocole commun d'interaction* (CMIP) entre système ouvert gestionnaire et système ouvert géré.
- Les fonctions de contrôle de gestion pouvant impliquer un système géré (managed system), deux systèmes de gestion (managing system) ou trois systèmes ouverts (third system).

Cet ensemble d'outils, identique pour les différents constructeurs, permettra d'échanger des informations de gestion entre systèmes hétérogènes. Les standards OSI de gestion de systèmes ne vont pas remplacer des architectures de gestion des constructeurs, telles que «SNA/Net View» de IBM ou «Enterprise Management Architecture» de DEC, mais leur permettre d'échanger des informations de gestion, tout en gardant leur spécificité.

112 Vision bilatérale des choses

L'approche de la normalisation a été essentiellement une vue des constructeurs de systèmes à gérer (IBM, DEC, etc.), donc une vue légèrement «Bottom-up» à partir des ressources à gérer. Il semble donc que les administrations et le CCITT devraient apporter leur vue complémentaire «Top-down», fondées sur les exigences de gestion des opérateurs de réseaux. Les notions de responsabilité de gestion, de domaine administratif de gestion et de gestion de la taxation pourront, en particulier, être affinées par le point de vue des opérateurs.

On peut donc espérer une stabilisation conceptuelle des normes d'ici deux ans, et leur application concrète dans les systèmes réels de gestion d'ici 10 ans. Les standards ne forment que les briques à partir desquelles les implémenteurs pourront soit réaliser des produits de gestion conviviaux, soit bricoler des systèmes inadaptés à la gestion, tout en proclamant dans les deux cas une compatibilité «OSI Systems Management».

Puisse cet article aider le lecteur à comprendre les travaux de normalisation en cours, à se rendre compte de la puissance des outils développés, mais aussi des limites des normes de gestion. Qu'ainsi, la lecture des textes originaux «OSI Systems Management» lui devienne plus aisée, tel est le souhait de l'auteur!

Bibliographie

Architecture

[1] IS ISO/IEC 7498-4: 1989 (E), Proof/épreuve
Information processing Systems. Open Systems Interconnection – Basic Reference Model – Part 4: Management framework

[2] ISO/DP 10040 (12 September 1989)
Information Processing Systems. Open Systems Interconnection – Systems Management Overview

Structure of Management Information
[3] ISO/DP 10165-1 (27 June 1989)
Information Processing Systems. Open Systems Interconnection – Management Information services – Structure of Management Information – Part 1: Management Information Model
[4] ISO/DP 10165-2 (September 1989)
Part 2: Definitions of Support objects
[5] ISO/DP 10165-3 (September 1989)
Part 3: Definitions of Management Attributes
[6] ISO/Working draft 10165-4 (April 1989)
Guidelines for the Definition of Managed Objects

Common Management Information
[7] ISO/DIS 9595 (3/11/89) + Addendum 1
Information processing systems – Open System Interconnection – Common Management Information Service Definition
[8] ISO/OIS 9596 (7 April 1989) + Addendum 1
Common Management Information Protocol Definition

Configuration Management
[9] ISO/DP 10164-1 (11 September 1989)
Information Processing Systems – Open Systems Interconnection – Systems Management – Part 1: Object Management Function
[10] ISO/DP 10164 2 (11 September 1989)
Part 2: State Management Function
[11] ISO/DP 10164-3 (11 September 1989)
Part 3: Relationship Management Function

Fault Management
[12] ISO/DP 10164-4 (September 1989)
Part 4: Error Reporting and Information Retrieval Function
[13] ISO/DP 10164-5 (September 1989)
Part 5: Management Service Control Function
[14] ISO/Working Draft 10164-6 (June 1989)
Fault management working document/Section 2: Confidence and diagnostic testing function
[15] ISO/Working Draft 10164-7 (May 1989)
Log Control function

Security Management
[16] ISO/Working Draft (15 January 1989)
OSI Security Management

Accounting Management
[17] ISO Working Draft (June 1989)
OSI Accounting Management

Performance Management
[18] ISO Working Draft (27 June 1989)
OSI Performance Management
[19] ISO Working Draft (26 June 1989)
Workload Monitoring Function

Die nächste Nummer bringt unter anderem:

Vous pourrez lire dans le prochain numéro:

3/90