La gestion de réseau

La gestion de réseau correspond aux actions qui permettent de prendre en charge la configuration, la sécurité, les pannes, l'audit des performances et la comptabilité. La prise en charge de toutes ces fonctions n'est pas un mince problème. De nombreux travaux de normalisation ont été effectués dans ce domaine, mais tous n'ont pas encore abouti. Cependant, une architecture de gestion de réseau et certains protocoles et services ont déjà été adoptés comme standards. Deux grandes tendances se font jour depuis plusieurs années : associer la gestion de service à la gestion de réseau et rapprocher la gestion de réseau et le contrôle de réseau.

La gestion de réseau recouvre de nombreuses opérations, telles que l'initialisation des paramètres de configuration du système, la gestion des erreurs, les statistiques, les diagnostics, la gestion des alarmes et leur rapport, la reconfiguration, la gestion des ressources, la sécurité, etc. Ces activités sont présentées plus précisément par la suite.

Pour interconnecter deux systèmes de gestion, une norme doit être respectée, qu'elle soit de droit ou de fait. Dans les normes de droit, on retrouve la normalisation provenant de l'ISO, que l'on appelle CMIS/CMIP, et celle de l'UIT-T, qui porte le nom de TMN (Telecommunications Management Network), en français RGT (réseau de gestion des télécommunications). Ces deux normes ne sont pas vraiment concurrentes mais plutôt complémentaires.

La norme la plus utilisée est SNMP (Simple Network Management Protocol), qui provient de l'environnement Internet. Les grands constructeurs ont, quant à eux, développé des plates-formes qui permettent d'avoir :

- un service de transport entre les différents processus applicatifs ;
- des adaptateurs de protocoles traduisant les messages échangés ;
- des piles de protocoles de communication ;
- des services supplémentaires internes, comme les annuaires.

Une autre direction, que nous abordons au chapitre suivant, concerne la gestion et le contrôle par politique.

Fonctions de base de la gestion de réseau

Suivant le type de système, les tâches de gestion varient et doivent donc être identifiées et analysées. Des services et des protocoles de gestion sont nécessaires pour gérer les ressources logicielles et matérielles d'un réseau.

L'identification et la mise en œuvre des tâches de gestion sont complexes en raison de la nature distribuée du système. On peut citer les fonctions suivantes :

- **Démarrage et arrêt du réseau.** Fonction de base liée à la configuration du réseau et à l'initialisation des paramètres.
- **Traitement des alarmes.** Permet au réseau de réagir à n'importe quel dysfonctionnement, comme la perte du contrôle d'accès, par exemple.
- **Redémarrage du réseau.** Nécessaire à la reprise d'activité suite à une panne du coupleur, d'une liaison, etc.
- **Reconfiguration du réseau.** Fonction liée à l'ajout ou à la suppression de points d'accès de terminaux. Par exemple, des éléments du réseau doivent pouvoir être mis hors circuit en cas de mauvais fonctionnement.
- **Contrôle de la qualité.** Fonction liée aux techniques de contrôle, aux caractéristiques opérationnelles du réseau et à la gestion des rapports de changement d'états.

Les moniteurs de gestion peuvent être matériels ou logiciels. Les moniteurs matériels s'occupent des phénomènes rapides, tandis que les moniteurs logiciels sont plutôt orientés application.

Les moniteurs de gestion doivent prendre en charge les fonctions suivantes :

- **Tests et diagnostics.** Les erreurs du système doivent être détectées. Un message de diagnostic peut être émis pour signaler qu'une erreur s'est produite et qu'un traitement peut avoir lieu. On doit pouvoir mettre un élément du système en état de diagnostic afin d'exécuter des séquences de tests.
- **Compte rendu d'alarmes.** Fonction destinée à notifier à l'opérateur du système tout mauvais fonctionnement.
- **Contrôle du réseau.** Fonction liée à l'allocation et à la désallocation des ressources et à leur contrôle (prévention des abus et des famines, manque de ressource, etc.).

Le système de gestion peut contrôler tous les changements. Il est aussi responsable des allocations de noms et d'adresses et des associations entre elles.

Le modèle de référence OSI a contribué au développement de réseaux hétérogènes. Cette hétérogénéité se traduit par l'interconnexion de matériels issus de constructeurs différents (Bull, IBM, DEC, HP, etc.) et par l'interconnexion de réseaux de différents types, par exemple un réseau grande distance (X.25 ou autre) relié à un réseau local (Ethernet, etc.).

L'échange d'informations entre systèmes hétérogènes a été rendu possible par l'intermédiaire de la normalisation de l'ISO. De plus, dans son rôle de transporteur de l'information, un réseau doit garantir une certaine qualité de service (débit, temps de réponse, etc.) à ses utilisateurs. Afin d'assurer une qualité de service, il est nécessaire de gérer convenablement de multiples composants (nœud, ligne, abonné, application, etc.). Cette gestion

est à la charge d'entités spécifiques, les entités de gestion. L'ensemble de ces entités et leurs activités constituent la gestion de réseau.

Chaque fournisseur de réseau propose des outils permettant de mettre en place une telle gestion. Toutefois, la répartition de ces fonctions par rapport aux sept couches du modèle OSI est entièrement à l'appréciation du constructeur. De ce fait, si l'on dispose de deux systèmes hétérogènes, il est très difficile de faire coopérer les différents outils de gestion de réseau de chaque système.

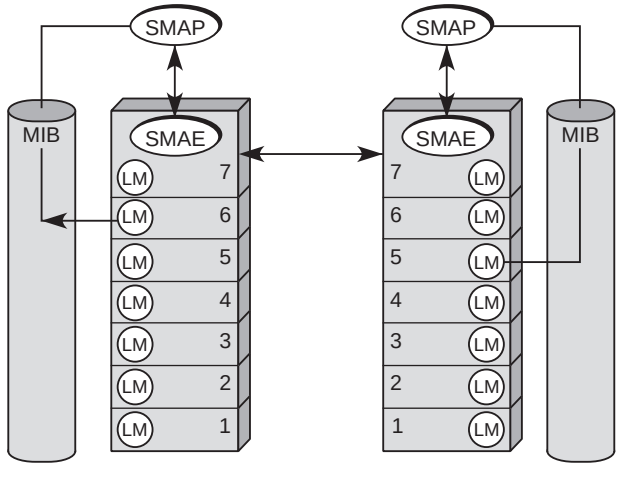
Les deux architectures qui se sont développées en premier, il y a une vingtaine d'années, proviennent du modèle Internet, avec SNMP, et du modèle de référence OSI (Open System Interconnexion) normalisé par l'ISO. Le modèle ISO est aujourd'hui en chute libre, mais il reste un modèle au même titre que le modèle de référence. Au contraire, SNMP a pris totalement le devant de la scène en se présentant sous diverses formes que nous allons étudier dans ce chapitre.

La gestion ISO

La gestion ISO consiste à faire remonter dans un processus appelé SMAP (System Management Application Process) toutes les informations de gestion par l'intermédiaire d'une entité d'application de la couche 7, appelée SMAE (System Management Application Entity), et à les traiter à ce niveau.

Ces informations se présentent sous la forme d'objets dont la syntaxe est normalisée sous le nom d'ASN.1. D'autres choix auraient pu être faits, comme une entité de gestion, à chaque niveau de la hiérarchie ISO, capable de prendre les décisions de gestion de ce niveau, mais tel n'est pas le cas. En outre, toutes les informations de gestion sont mémorisées dans une base de données, appelée MIB (Management Information Base). Cette MIB est, d'une part, remplie par les informations provenant des couches de protocoles à gérer et, d'autre part, consultée par le processus de gestion SMAP. L'entité SMAE récupère les informations demandées par le SMAP par une interface nommée SMI (System Management Interface). Cette architecture est illustrée à la figure 29.1, qui montre également la gestion de couche qui s'effectue, avec des processus de gestion associés à chaque couche.

Figure 29.1
Modèle de gestion ISO

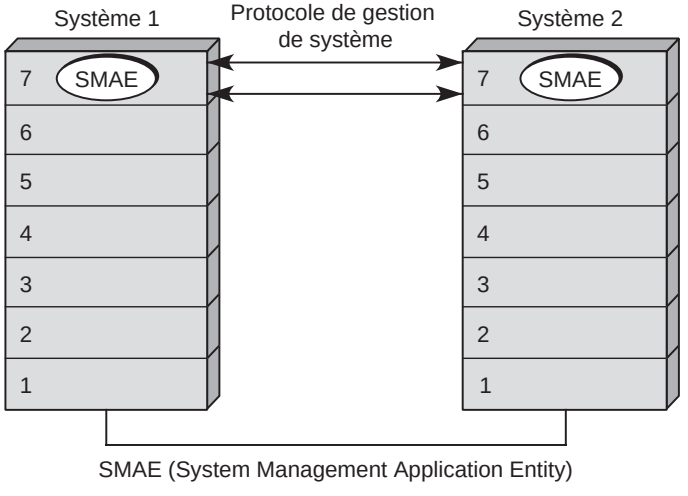


La gestion ISO comprend trois types d'activités :

- la gestion système, ou Systems-Management ;
- la gestion de couche, ou Layer Management (LM sur la figure 29.1) ;
- la gestion d'opération de couche (Layer Operation).

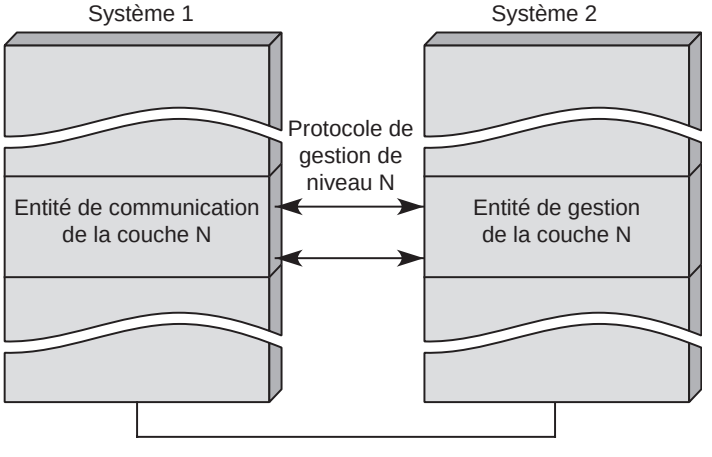
La gestion système définit l'échange de l'ensemble des informations de gestion concernant les ressources (objets gérés) utilisées dans un système ouvert. Ces échanges se font au niveau 7 de l'architecture du modèle de référence entre entités d'application pour la gestion système SMAE (System Management Application Entity), comme illustré à la figure 29.2.

Figure 29.2
Échanges de niveau gestion de système



La gestion de couche, schématisée à la figure 29.3, définit les échanges d'informations concernant la gestion d'une couche *N* particulière. Ces informations ne concernent que les ressources propres à cette couche (mémoires tampons, temporisateurs, connexions, etc.). Cette gestion de couche correspond à des protocoles spécifiques, utilisés uniquement pour la gestion.

Figure 29.3
Échanges de niveau gestion de couche



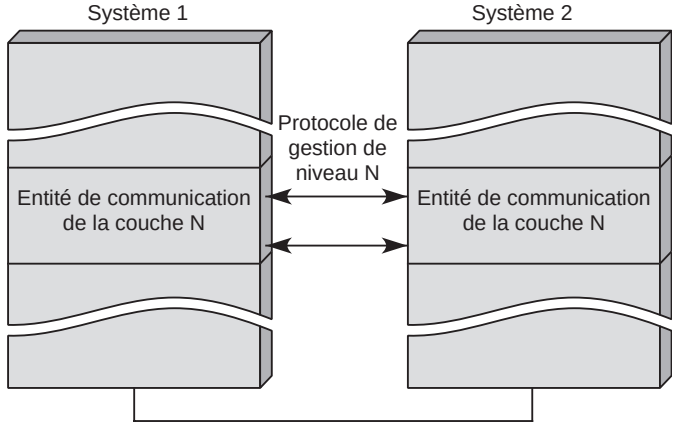
Plusieurs instances de communication sont concernées par ces échanges, qui peuvent se faire soit *via* des protocoles de système (au niveau 7), soit *via* des protocoles de gestion spécifiques de la couche concernée. On peut citer comme exemple de ces derniers le NCMS (Network Connection Management Subprotocol), qui est un additif au protocole de transport OSI et qui spécifie un sous-protocole de gestion de connexions de réseau.

La gestion d'opération de couche couvre les échanges d'informations relatives à une instance de communication (une opération) dans une couche donnée. Cela englobe les données véhiculées par les protocoles de communication OSI. Ces échanges d'opération de couche sont illustrés à la figure 29.4. En voici deux exemples :

- les trames U dans le protocole HDLC ;
- les données de tarification dans les paquets X.25.

Nous revenons plus loin sur la gestion système, puisque les seules normes développées à l'heure actuelle sont relatives à ce type d'activité.

Figure 29.4
Échanges au niveau d'une opération de couche



La gestion système CMIS/CMIP

La gestion système est au cœur du modèle de gestion ISO. C'est là que se prennent les décisions de gestion et que sont élaborées les demandes d'information nécessaires à la réalisation de cette gestion. Comme nous l'avons vu, la gestion système est effectuée par l'entité d'application SMAE, qui regroupe généralement quatre ASE.

Les services rendus par ces quatre ASE sont les suivants :

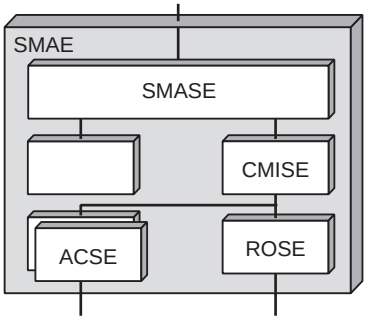
- SMAS (System Management Application Service), ou services d'application de la gestion système ;
- CMIS (Common Management Information Service), ou services communs à toutes les fonctions de gestion ;
- ACSE (Association Control Service Element), ou éléments de services de contrôle d'association ;
- ROSE (Remote Operation Service Element), ou éléments de services d'opération à distance.

Chacun de ces services repose sur un protocole spécifique :

- SMASE s'appuie sur le protocole MAP (Management Application Protocol), qui transporte des MAPDU.
- CMIS s'appuie sur le protocole CMIP (Common Management Information Protocol), qui transporte des CMIPDU.
- Le service rendu par ACSE, utilisant les quatre primitives A-ASSOCIATE, A-RELEASE, A-ABORT et A-P-ABORT, est réalisé par le protocole ACSE, qui transporte des ACSE-PDU.
- Le service rendu par ROSE, utilisant les cinq primitives RO-INVOKE, RO-RESULT, RO-ERROR, RO-REJECT-U et RO-REJECT-P, est réalisé par le protocole ROSE, qui transporte des ROSE PDU.

La figure 29.5 illustre l'architecture de l'entité d'application SMAE avec ses quatre ASE.

Figure 29.5
Architecture de l'entité SMAE



Les normes ISO 9595 et ISO 9596 spécifient respectivement le service commun (CMIS) et le protocole commun (CMIP). L'ensemble des services communs situés dans la couche application fournit les moyens d'échanger des données de gestion entre entités CMISE.

En résumé, une entité d'application SMAE est constituée d'un élément de service de gestion de système SMASE (System Management Application Service Element), d'un élément de service d'information de gestion commune CMISE (Common Management Information Service Element) et d'un élément de service de contrôle d'association ACSE (Association Control Service Element). Le SMASE définit la syntaxe et la sémantique de l'information de gestion transférée par des MAPDU. Les services de l'élément ACSE sont utilisés pour initialiser et terminer les associations.

Par abus de langage, le protocole de gestion d'un réseau OSI est identifié à CMIP/CMIS. En réalité, la gestion du modèle de référence est réalisée par l'entité d'application SMAE. Le service de communication utilisé par le SMASE peut être fourni par un CMISE (CMIS Element) ou tout autre ASE, comme FTAM (File Transfer and Access Management) ou TP (Transaction Processing).

L'utilisation de CMIS requiert la présence d'un ROSE, élément de service pour les opérations distribuées, qui permet de véhiculer de manière asynchrone des échanges de type question-réponse entre sites distants.

Pour compléter cette architecture de gestion du modèle de référence de l'ISO, indiquons que le processus de gestion SMAP travaille sur treize fonctions administratives qui ont été regroupées dans cinq domaines fonctionnels, ou SMFA (Specific Management Func-

tional Area) : la configuration (Configuration Management), la sécurité (Security Management), les pannes (Fault Management), l'audit de performances (Performance Management) et la comptabilité (Accounting Management). Ces fonctions sont détaillées à la section suivante, et les cinq domaines de gestion dans une section spécifique.

Dernier point important, le processus de gestion SMAP peut être soit un processus gérant (Managing Process), soit un processus agent (Agent Process). Les utilisateurs des processus SMAP, que l'on appelle MIS-users (Management Information Service-users), peuvent donc être soit des agents, soit des gérants. Les rôles d'agent et de gérant ne sont pas assignés définitivement. Certains MIS-users peuvent, selon les opérations, être agent ou gérant.

Le service SM

Le service rendu par l'entité SMASE au processus SMAP à travers l'interface SMI (System Management Interface) s'effectue par l'intermédiaire des treize fonctions suivantes :

- Object Management Function
- State Management Function
- Relationship Management Function
- Alarm Reporting Function
- Event Report Management Function
- Log Control Function
- Security Alarm Reporting Function
- Security Audit Trail Function
- Access Control Function
- Accounting Meter Function
- Workload Monitoring Function
- Test Management Function
- Summarization Function

Les services associés à ces fonctions sont parfois appelés SMIS (Specific Management Information Service), mais ce terme trompeur est peu utilisé.

À titre d'exemple, les primitives de service de la fonction Object Management Function sont au nombre de six :

- PT-CREATE
- PT-DELETE
- PT-EVENT-REPORT
- PT-GET
- PT-SET
- PT-ACTION

Comme nous allons le voir, elles correspondent aux primitives du service CMIS.

Le service commun CMIS

CMIS (Common Management Information Service) est le service rendu par l'élément de service d'application CMISE. Six éléments de service ont été retenus dans CMIS pour les services de notification de gestion :

- M-CREATE, qui permet à un gérant de demander à un agent la création d'informations concernant des objets de gestion.
- M-DELETE, qui permet à un gérant de demander à un agent la destruction d'informations concernant des objets de gestion.
- M-EVENT-REPORT, qui permet à un agent de signaler à un gérant les changements d'état d'un objet de gestion sans y être sollicité.
- M-GET, qui permet à un gérant de demander à un agent la valeur des attributs d'un objet de gestion.
- M-SET, qui permet à un gérant de demander à un agent de positionner les valeurs des attributs d'un objet de gestion.
- M-ACTION, qui permet à un gérant de demander à un agent d'entreprendre une action trop complexe pour pouvoir être exprimée à l'aide des services précédents.

Trois autres éléments de service concernent les associations :

- M-INITIALIZE, qui permet l'association entre deux utilisateurs.
- M-TERMINATE, qui permet l'achèvement normal de l'association.
- M-ABORT, qui permet la rupture brutale de l'association par un utilisateur.

Un additif autorise l'ajout d'un service d'annulation :

- M-CANCEL-GET, qui permet à un utilisateur de demander à ne pas recevoir les résultats du GET précédent.

Grâce aux unités fonctionnelles supplémentaires, il est possible de disposer d'autres services. On trouve, par exemple :

- Le service de réponses multiples (Multiple Replies), qui permet à un système d'indiquer à un système distant qu'il peut recevoir plusieurs réponses concernant sa demande de service.
- Le service de filtre (Filter) et de profondeur de sélection (Scope), qui permet à un système d'indiquer à un système distant que l'opération demandée s'applique à plus d'un objet de gestion.

Le protocole commun CMIP

Le protocole CMIP (Common Management Information Protocol) permet à des utilisateurs du service commun CMIS d'effectuer leurs échanges. C'est un protocole de niveau 7, qui spécifie les procédures d'échange d'informations administratives entre ASE. La syntaxe abstraite normalisée ASN.1 (Abstract Syntax Notation 1) est utilisée pour spécifier les éléments de protocole CMIP.

MIB (Management Information Base)

La MIB (Management Information Base) contient l'ensemble des informations de gestion existant dans un système ouvert donné. Ces données administratives se présentent sous la forme de compteurs, de seuils, de répertoires de noms et d'adresses, etc. L'organisation et la mise en œuvre de la MIB ne font pas l'objet d'une normalisation.

Il est possible d'accéder à la MIB localement, par l'intermédiaire de mécanismes non normalisés, ou à distance, *via* des protocoles OSI tels que des protocoles de gestion de système, des protocoles de gestion de couche ou des protocoles de couche.

Fonctions de gestion spécifiques

Comme expliqué précédemment, les fonctions administratives ont été regroupées dans cinq domaines fonctionnels, ou SMFA (Specific Management Functional Area). Ces domaines concernent :

- la configuration (Configuration Management) ;
- la sécurité (Security Management) ;
- les pannes (Fault Management) ;
- l'audit de performances (Performance Management) ;
- la comptabilité (Accounting Management).

Les sections qui suivent décrivent les caractéristiques de chacun de ces domaines.

Gestion de la configuration

L'inventaire des ressources nécessaires à l'initialisation et au lancement du réseau ainsi que la gestion de noms et d'adresses sont à la charge de la gestion de la configuration. Les objets utilisés au niveau de chaque couche du modèle de référence possèdent une adresse N-SAP (Service Access Point de niveau N).

Les propriétés de chaque ressource sont précisées. Par exemple, l'une des propriétés d'un N-SAP concerne le nombre de connexions qu'il peut supporter. Le statut d'un composant peut être spécifié (occupé, disponible, en panne). Les différentes relations entre les ressources sont également représentées. On discerne deux types de relations, les relations statiques, comme les N-entités accessibles à travers un N-SAP, et les relations dynamiques, comme la correspondance entre une N-connexion et une (N – 1)-connexion à un instant donné.

Pour gérer une configuration, quatre procédures sont nécessaires :

- collecte des informations sur l'état du système ;
- contrôle de l'état du système ;
- sauvegarde de cet état en établissant un historique ;
- présentation de l'état du système.

Lors de la collecte des informations, le processus application responsable de la configuration doit consulter certains paramètres dans les différents systèmes du réseau. Ces données sont contenues dans les MIB des systèmes. Chaque système possède sa MIB.

Au cours du contrôle de l'état du réseau, il convient d'entreprendre certaines actions afin de maintenir une cohérence de la configuration, ainsi que de modifier des paramètres et d'ajouter une ressource. Ces opérations peuvent être protégées par des mots de passe dans le but de n'autoriser l'accès qu'à des personnes habilitées à modifier la configuration. Il est possible de déclencher ces opérations à partir d'un système distant. L'administrateur d'une couche est chargé de sauvegarder l'état des ressources de sa couche. Il dispose pour cela d'un accès en écriture sur la MIB.

La présentation de l'état du système indique la liste des nœuds actifs et celle des machines connectées à un nœud. Des primitives d'accès à la MIB en lecture sont disponibles pour le processus application responsable de la configuration.

Gestion de la sécurité

Avant de définir les services de sécurité, il convient de recenser les menaces potentielles. Les causes d'une infraction sont soit accidentelles, soit délibérées. Les premières sont essentiellement dues au mauvais fonctionnement du système, par exemple la livraison incorrecte d'un message à la suite d'une adresse erronée. La seconde catégorie met en jeu un certain savoir afin de passer outre les mécanismes de protection.

Les conséquences de certaines attaques (écoute des messages ou observation du trafic) ne modifient pas le fonctionnement du système. Ces attaques se classent dans la catégorie des infractions passives. Au contraire, les infractions actives ont la possibilité de perturber le déroulement des opérations. Dans cette dernière catégorie, on distingue :

- La mascarade, dans laquelle une entité se fait passer pour une autre afin d'obtenir ses pouvoirs.
- La duplication d'un message.
- La modification d'un message.
- La perturbation d'un service, comme la génération de trafic afin de fausser l'algorithme de routage.
- La modification des services d'une entité. Par exemple, la manipulation de l'entité validant les mots de passe peut autoriser l'accès à un espion.
- L'ajout de service à une entité, comme une entité relais qui, en plus de sa fonction de routage, duplique les messages vers un espion.

Mécanismes de protection

Pour se prémunir des mascarades, il faut se doter d'un service d'authentification des entités. L'authentification peut être obtenue au moyen d'une signature digitale. Deux procédures sont alors mises en œuvre, la production et la vérification. Une signature doit être reconnaissable par l'ensemble des autres entités mais ne peut être produite que par une seule. L'utilisation de mots de passe ou le recours à un « notaire », c'est-à-dire une tierce personne susceptible de certifier l'identité des individus, sont aussi possibles.

La duplication ou la modification des données est rendue caduque par l'utilisation de mécanismes de cryptage. Ce procédé ne permet pas aux indiscrets d'exploiter les renseignements dans un temps raisonnable.

Il existe deux types de cryptosystèmes, ou systèmes de chiffrement *(voir le chapitre 33)*, les systèmes à clé secrète (symétriques) et les systèmes à clé publique (asymétriques). Dans les premiers, la connaissance de la clé de chiffrement permet de déduire celle de

déchiffrement, ce qui donne à cette solution un caractère symétrique. Dans un système à clé publique, l'émetteur dispose d'un annuaire renfermant les clés de cryptage utilisées par le destinataire. La clé de décryptage ne peut pas être obtenue à partir de celle de cryptage dans un temps réaliste et n'est connue que du destinataire.

Si les entités relais sont suspectées de fraude ou ne possèdent pas les mécanismes de sécurité suffisants, ces entités suspectes peuvent être évitées par des mécanismes de contrôle du routage, comme en propose, par exemple, le protocole IP.

Procédures requises

Le contrôle et la distribution des informations utilisées pour assurer la sécurité constituent l'une des fonctions de la gestion. Un sous-ensemble de la MIB est consacré aux informations de sécurité, ou SMIB (Security MIB). Il renferme, entre autres, les clés de cryptage et la liste des droits d'accès. L'échange des données entre SMIB s'effectue à l'aide de protocoles de gestion, de niveau application.

Les procédures nécessaires à la mise en place des mécanismes de protection concernent la distribution des mots de passe et des clés, le choix de clés de travail utilisées durant un échange et la remontée des événements concernant les tentatives de violation du système de sécurité.

Gestion des pannes

Lors d'un fonctionnement anormal d'un système, deux types de défauts peuvent être mis en cause :

- Les défauts internes, qui résultent d'un composant en panne. À chaque utilisation du composant, le défaut se manifeste. Ce type de problème présente donc un caractère répétitif.
- Les défauts externes, qui dépendent de l'environnement du système. Par exemple, la présence d'un goulet d'étranglement dépend du trafic autour du goulet. Les défauts externes ne se produisent que lorsqu'un contexte particulier est réalisé. Ce contexte dépendant de plusieurs facteurs, ces défauts se produisent de façon intermittente. Leur résolution est plus difficile que celle des défauts du premier type.

Le passage d'un état de fonctionnement correct à celui de panne n'est pas instantané. Un composant commence à fournir un service dégradé avant de tomber en panne. La durée du mode dégradé est plus ou moins longue.

Le traitement d'une panne se décompose en quatre étapes : signalisation du fonctionnement anormal, localisation, réparation et confirmation du retour au fonctionnement normal.

Signalisation du fonctionnement anormal

Trois outils permettent de détecter les défauts : les messages d'erreur, les tests et les seuils. Un composant s'apercevant d'une anomalie génère automatiquement un message d'erreur vers un fichier d'erreur (Error Log). Trois attributs caractérisent une erreur : l'identificateur du composant, le type d'erreur et sa date.

L'identificateur de la ressource permet de déterminer le domaine de gestion responsable de celle-ci. Les principales ressources recensées dans le modèle OSI sont les N-entités, les N-SAP et les N-connexions.

Pour localiser l'erreur dans le temps, il est nécessaire d'avoir une date absolue entre les différents systèmes. Le trafic induit par les messages d'erreur ne doit pas perturber celui des données. Pour limiter le nombre de reports, la mise en place de compteurs permet de signaler des erreurs cumulées. Un compteur reflète les occurrences d'une erreur pendant une certaine durée. Les attributs d'un compteur comprennent un identificateur, le type d'erreur, la date de début, la date de fin et la valeur du compteur.

Un degré de sévérité est attribué à une erreur. Quatre degrés sont retenus :

- Panne interne : la ressource est incapable d'assurer un service.
- Panne externe : la ressource est incapable d'assurer un service à la suite d'une cause externe.
- Panne intermittente : la ressource ne réussit pas toujours à assurer le service.
- Mode dégradé : la ressource assure un service minimal.

À l'aide de ces degrés, des mécanismes de filtrage sont construits, ne rapportant les erreurs qu'au-delà d'un certain degré.

Les tests représentent le deuxième outil permettant de détecter des problèmes dans le réseau. On distingue deux types de tests : les tests de sécurité et les tests de diagnostic. Les premiers ont pour but de tester un maximum d'éléments en un minimum de temps. Plusieurs composants sont éprouvés en parallèle. Au contraire, les composants sont mis à l'épreuve en séquence lors des tests de diagnostic.

Les seuils sont le troisième outil de détection des défauts. En fixant des seuils, il n'est possible d'émettre des alarmes que lors de leur franchissement. On se dote ainsi d'un mécanisme d'anticipation d'erreur. La valeur du seuil est déterminée de façon empirique.

Localisation des défauts et réparation

L'établissement d'un diagnostic comporte deux étapes. La première se présente comme une analyse du passé. Elle se résume à un examen des messages d'erreur et des résultats des tests de sécurité. Si la panne n'est pas localisée au terme de cette étape, il convient de déclencher des tests de diagnostic. Ces tests s'effectuent de façon méthodique, les composants étant éprouvés en séquence. À chaque étape, on essaie de localiser avec plus de précision un élément défectueux. Ces tests pouvant avoir une durée assez longue, il est possible de les suspendre et de les reprendre ultérieurement. Il est envisageable d'utiliser les techniques de l'intelligence artificielle pour automatiser les diagnostics.

Les problèmes logiciels sont résolus en réinitialisant les attributs des ressources et en rechargeant certaines parties du logiciel. Cela revient à faire véhiculer des blocs d'information sur les protocoles de gestion. Une fois la réparation effectuée, il est souhaitable de confirmer explicitement le retour au fonctionnement normal.

Les éléments de service pour la gestion des pannes

L'ISO a recensé un ensemble de services spécifiques de gestion des pannes. La signalisation des incidents met en jeu trois primitives de service :

- FM-ERROR-REPORT, qui permet à un agent SMAP de signaler une erreur à un gérant SMAP.
- FM-GET-ERROR-COUNTER, qui permet à un gérant SMAP de demander à un agent SMAP la valeur d'un compteur.
- FM-ZERO-ERROR-COUNTER, qui permet à un gérant SMAP de demander à un agent SMAP de remettre un compteur à zéro.

La localisation des pannes s'effectue au moyen de tests. Le déroulement des tests est géré à l'aide des primitives de services suivantes :

- FM-INITIATE-TEST, qui permet à un gérant SMAP de demander à un agent SMAP de déclencher un test.
- FM-TEST-REPORT, qui permet à un agent SMAP de restituer le résultat du test à un gérant SMAP.
- FM-TEST-STATUS, qui permet à un gérant SMAP de demander à un agent SMAP les états intermédiaires d'un test.
- FM-TEST-ABORT, qui permet à un gérant SMAP d'abandonner un test.
- FM-TEST-SUSPEND, qui permet à un gérant SMAP de suspendre un test.
- FM-TEST-RESUME, qui permet à un gérant SMAP de reprendre un test suspendu.

L'audit de performances

La gestion des performances permet d'évaluer les performances des ressources du système et leur efficacité. Les performances d'un réseau sont évaluées à l'aide de quatre paramètres : le temps de réponse, le débit, le taux d'erreur bit et la disponibilité. L'évaluation de ces performances s'effectue à partir de statistiques. Le traitement des statistiques se déroule en quatre étapes : la collecte, le contrôle, le stockage et la présentation.

La collecte des informations consiste à mettre à jour un ensemble de compteurs et de temporisateurs (timers). Les compteurs reflètent le nombre de N-PDU, de retransmissions, de déconnexions, etc. Les temporisateurs servent à dater les informations des compteurs. Un gérant est chargé de mettre à jour les compteurs relatifs à la couche sous son autorité. Le contrôle de la collecte consiste à autoriser ou non la lecture des compteurs et à les réinitialiser.

Les statistiques sont stockées dans la MIB. Un gérant dispose d'un accès en écriture sur la MIB afin de sauvegarder la valeur des compteurs et des temporisateurs. Les informations relatives au nombre de TPDU traités par un système sont stockées dans la MIB selon le format illustré au tableau 29.1.

Enregistrement MIB	Identificateur
Système	Nom du système OSI
Couche	Transport
Date début	Heure
Date fin	Heure
Compteur	TPDU
Valeur compteur	Entier

TABLEAU 29.1 • Informations relatives aux TPDU stockées dans la MIB

Un SMAP a la possibilité de déclencher l'analyse de statistiques stockées dans la MIB à l'aide de la requête M-P-ANALYSE, requête qui permet les opérations suivantes : enregistrement MIB, vérification d'un ID de connexion, localisation, type, date de début et date de fin. Les résultats de l'analyse sont stockés dans la MIB. Pour obtenir ces résultats, un

SMAP dispose de la requête M-P-ANALYSE RESULTS pour effectuer un enregistrement dans la MIB, vérifier un ID de connexion et relever la valeur du compteur de PDU.

Un SMAP peut également lire les statistiques et demander leur effacement de la MIB à l'aide de la primitive M-P-READ. Cette requête permet d'effectuer un enregistrement dans la MIB, de vérifier un ID de connexion et d'effectuer un effacement si nécessaire.

Gestion de la comptabilité

Cette gestion a pour fonction de relever les informations permettant d'évaluer les coûts de communication. Cette évaluation est établie en fonction du volume et de la durée de la transmission. Les relevés s'effectuent à deux niveaux du modèle OSI : le niveau réseau et le niveau application.

Au niveau réseau, les informations utilisées pour la comptabilité sont :

- le nombre d'APDU émis/reçus ;
- le nombre de caractères émis/reçus ;
- la date de début/fin de la connexion.

Quatre étapes marquent le déroulement de la comptabilité : la négociation, l'activation, la collecte et le rapport. La négociation permet de désigner les responsables des relevés. L'activation déclenche la collecte des informations, et un rapport des relevés est transmis par un agent à un gérant chargé d'établir la facturation.

Au niveau réseau, on discerne deux types de nœuds, ou systèmes relais : les nœuds avec fonction comptable et les nœuds sans fonction comptable. Un nœud comptable assure la comptabilité d'un ou de plusieurs nœuds non comptables. Les relations entre ces deux types de nœuds sont établies au cours de la phase de négociation. L'activation déclenche la collecte des informations. L'agent SMAP d'un nœud comptable collecte les informations comptables de niveau réseau durant la totalité de la connexion réseau (NETWORK CONNECT REQUEST/NETWORK RELEASE REQUEST). Les noms des entités origine et destinataire sont également repérés.

L'agent SMAP d'un nœud comptable transmet un rapport des relevés vers le gérant SMAP chargé d'établir la facturation en utilisant les primitives de services CMISE M-CONFIRMED-EVENT REPORT et M-NON CONFIRMED-EVENT REPORT.

Le gérant SMAP a la possibilité de demander les relevés d'un agent SMAP en utilisant la primitive de service CMISE M-GET ATTRIBUTES.

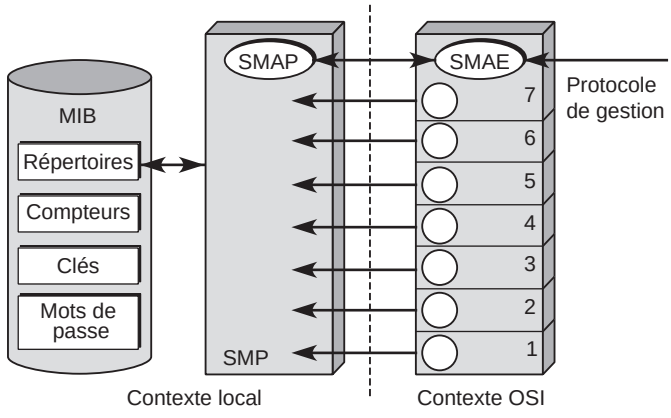
Problématique de la gestion ISO

La gestion des réseaux est devenue primordiale dans les environnements réseau. De ce fait, la plupart des constructeurs de réseaux offrent un système de gestion plus ou moins compatible avec la normalisation ISO.

La figure 29.6 résume le fonctionnement de la gestion ISO. Les protocoles de couches viennent déposer leurs informations dans la MIB, qui peut être interrogée par les processus de gestion.

Cette architecture est conçue pour être générale, ce qui constitue son défaut par rapport à la simplicité de SNMP. En effet, les objets dans la gestion ISO peuvent devenir très complexes mais surtout spécifiques pour une implémentation donnée du modèle.

Figure 29.6
Architecture de la gestion ISO



De ce fait, la plupart des produits compatibles ISO ne sont que faiblement compatibles entre eux puisque que les objets sont spécifiques, tout en étant conformes à la norme.

L'approche TMN

La présente section donne un bref aperçu du TMN (Telecommunications Management Network) en s'appuyant sur la série de recommandations M.3000 de l'UIT-T. Cet organisme de normalisation décrit une architecture physique et fonctionnelle capable de prendre en charge la gestion de tous les types de réseaux de télécommunications.

Le TMN est une norme de l'UIT-T applicable aux réseaux publics et privés, aux réseaux à commutation de circuits et de paquets et aux équipements associés. Même si, dans la recommandation M.3010, l'architecture du TMN est conceptuellement définie comme une base de travail pour tous les types de réseaux, dans les faits, le TMN est plutôt orienté vers l'administration des réseaux à circuits commutés que l'on rencontre dans les environnements de télécommunications. En effet, il n'est pas évident que l'architecture du TMN couvre rigoureusement toutes les possibilités de configuration physique susceptibles d'être rencontrées.

Le TMN détermine une structure de fonctions, de protocoles et de messages que l'administrateur de réseau peut sélectionner. Ces ensembles forment les spécifications d'un système TMN. En revanche, le TMN ne spécifie pas le système d'administration de réseau. Il ne renseigne en rien sur l'implémentation du système et ne spécifie pas la manière dont les fonctions TMN sont mises en œuvre. Seule est disponible une liste de fonctions qui peuvent être utilisées par l'administration de réseau. De plus, le TMN est applicable uniquement pour l'administration des ressources de communication. Cela signifie qu'il ne l'est pas pour l'administration des applications.

Le TMN identifie cinq catégories de fonctions de gestion, définies dans la recommandation X.700 : la gestion des fautes, la gestion comptable, la gestion de configuration, la gestion des performances et la gestion de la sécurité.

Cette architecture propose un découpage en couches des fonctions de gestion. Quatre grandes catégories ont été déterminées par l'UIT-T :

- Business Management
- Service Management

- Network Management
- Element Management

Le premier niveau concerne les besoins de l'entreprise et de la gestion de l'entreprise au niveau global. Le niveau de gestion de service se préoccupe des points d'accès aux utilisateurs et de l'administration des services offerts aux utilisateurs. Ces services peuvent aussi s'adresser aux fournisseurs de services. Le niveau de gestion gère les éléments du réseau, le mot élément étant pris ici au sens d'un ensemble d'éléments de base. Le dernier niveau gère cet ensemble d'éléments de base pris individuellement, comme les lignes, les multiplexeurs, les commutateurs, etc.

Architecture du TMN

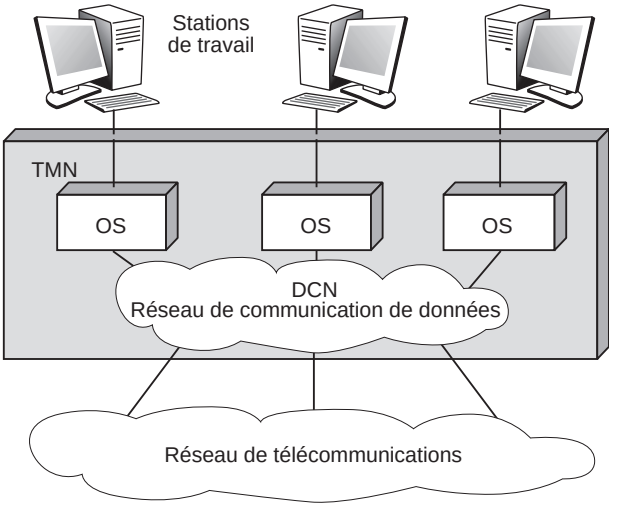
Le TMN offre une structure de réseau définie, qui permet l'interconnexion de différents types de systèmes d'exploitation et des équipements de télécommunications regroupés en architectures hétérogènes. Cela rend possible l'administration de différents réseaux et fournit un ensemble de normes à respecter par les constructeurs des équipements de télécommunications. De façon conceptuelle, c'est un réseau indépendant, qui interface les réseaux de télécommunications en différents points pour en recevoir les informations et en contrôler les opérations.

Le TMN utilise les architectures normalisées existantes, comme le modèle OSI ou celui de l'UIT-T pour l'ATM. Dans le cas du modèle OSI, on retrouve naturellement l'architecture de gestion normalisée par l'ISO avec l'environnement CMIP/CMIS. Pour le modèle UIT-T, qui est beaucoup plus large que le modèle OSI, la partie spécifique concernant la gestion des équipements s'effectue avec CMIS/CMIP.

Architecture physique

Le TMN se fonde conceptuellement sur un réseau de communication de données, appelé DCN (Data Communication Network), séparé du réseau de télécommunications à gérer, comme illustré à la figure 29.7.

Figure 29.7
Architecture physique du TMN



Le TMN est divisé en cinq catégories de blocs fonctionnels principaux :

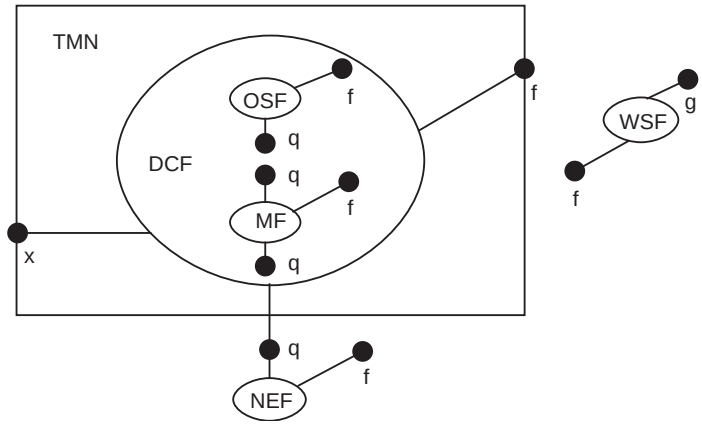
- OSF (Operations System Function), ou bloc fonctionnel des systèmes d'exploitation, traite les informations d'administration prises en charge et contrôle la réalisation des différentes fonctions d'administration de télécommunications. En d'autres termes, un bloc OSF offre des applications d'administration. Il existe trois types d'OSF : les OSF de base, qui gèrent les éléments de réseau, les OSF du réseau, qui réalisent les fonctions de TMN relatives au réseau en coopérant avec les OSF de base, et les OSF de service, qui fournissent les moyens de gérer les services de télécommunications.
- NEF (Network Element Function), ou bloc fonctionnel d'élément de réseau, qui communique avec un TMN dans le but d'être géré. Il peut être considéré comme un objet administré.
- MF (Mediation Function), ou bloc fonctionnel de médiation, qui opère sur l'information transitant entre les blocs NEF et OSF dans le but d'établir une communication entre les fonctions primitives et le stockage des données. Il doit également adapter, filtrer et condenser l'information du NEF d'une manière conforme à la demande de l'OSF. Parmi les exemples de MF, citons les convertisseurs de protocole, les contrôleurs de communication, les gestionnaires de prise de décision, les éléments de stockage des données, etc.
- DCF (Data Communication Function), ou bloc fonctionnel de communication de données, qui offre les moyens de transporter les informations relatives à l'administration des télécommunications entre les blocs fonctionnels. Son existence est souvent supposée implicite.
- WSF (Work Station Function), ou bloc fonctionnel du poste de travail, qui offre les moyens de communication entre les blocs fonctionnels et l'utilisateur.

Un sixième bloc fonctionnel, le bloc d'adaptation, a été ajouté pour permettre une meilleure intégration dans un environnement hétérogène. Ce bloc propose une interface permettant la connexion des éléments de réseau ne supportant pas les interfaces normalisées. Il propose de raccorder des réseaux s'appuyant sur un système de gestion propriétaire. Ce bloc peut être considéré comme similaire à NEF.

Les blocs fonctionnels ci-dessus sont connectés de façon hiérarchique, comme illustré à la figure 29.8. Les points de référence de cette figure, indiqués par les valeurs f, g, q, x, sont expliqués dans la suite.

Figure 29.8

Architecture fonctionnelle du TMN

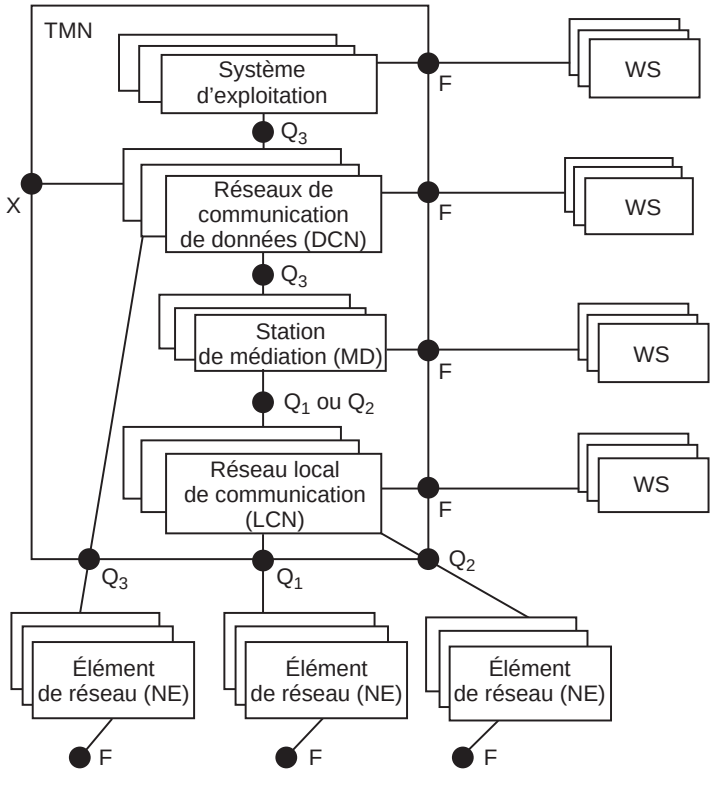


Les points de références définissent un point conceptuel d'échange d'information entre des blocs ayant des fonctions distinctes. Un point de référence devient une interface quand les blocs de fonctions connectés sont réalisés dans des équipements séparés. Il existe cinq types de points de référence : q, f, g, x et m.

- Les points de référence q connectent les blocs de fonctions entre NEF et MF, MF et MF, MF et OSF, OSF et OSF, soit directement, soit *via* le DCF. Plus précisément, l'interface q1 se place entre NEF et MF, q2 entre deux MF et q3 entre les équipements se connectant à un OSF.
- Les points f connectent les stations WSF.
- Les points g sont des points entre les WSF et les utilisateurs.
- Les points x connectent un TMN à un autre réseau d'administration incluant d'autres TMN.
- Les points m permettent le raccordement d'éléments non-TMN vers un bloc d'adaptation QAF. Cette interface est en dehors du champ du TMN.

Comme illustré à la figure 29.9, l'architecture physique du TMN, schématisée ici avec les interfaces, est calquée sur l'architecture fonctionnelle.

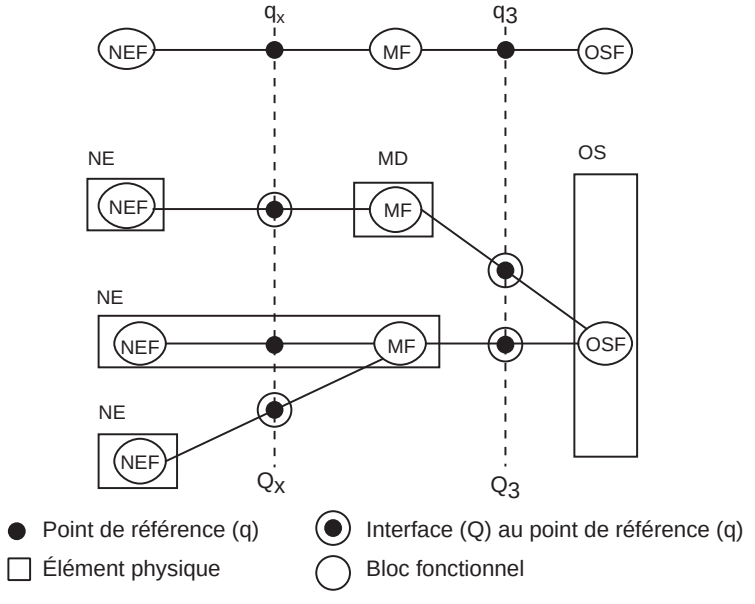
Figure 29.9
Architecture physique du TMN



Les interfaces normalisées sont définies en correspondance avec les points de référence. Elles sont signalées par des lettres majuscules pour les différencier des points de référence. L'interface Q est appliquée au point de référence q, F au point f, X au point x, etc.

La figure 29.10 montre un exemple de relations entre une configuration physique et une configuration de référence dans laquelle le DCF est implicite.

Figure 29.10
Exemples de relations entre une configuration physique et une configuration de référence



Q3 est l'interface qui normalise les équipements les plus complexes, comme les nœuds de commutation. Les spécifications de cette interface suivent diverses recommandations de l'UIT-T. La recommandation G.503 recommande l'utilisation de l'interface D au niveau physique ainsi qu'au niveau 2, et X.25 au niveau 3. Pour les niveaux supérieurs, on se réfère aux protocoles de la gestion OSI.

Le système d'exploitation est le système qui exécute les OSF. Les NE sont constitués des équipements de télécommunications (groupe ou partie d'équipement) et des équipements qui exécutent les NEF. Ils comportent une ou plusieurs interfaces standards de type Q. Le LCN est un réseau de communication dans un environnement TMN. Il supporte le DCF en un point de référence de type q_1 ou q_2. Le DCN est un réseau de communication dans un environnement TMN, qui supporte le DCF en un point de référence de type q_3. Le MD est le matériel actif qui exécute les OSF, et le WS le matériel actif qui exécute le WSF.

Dans le TMN, les éléments physiques doivent contenir plus d'un bloc fonctionnel. Il est aussi possible que les objets administrés (NE) contiennent plus d'un bloc fonctionnel.

Architecture fonctionnelle

L'architecture fonctionnelle du TMN offre les moyens de transporter et de traiter les informations relatives à l'administration des réseaux de communication. Elle définit les points de référence, les interfaces et les protocoles. Elle offre aussi une description des fonctions nécessaires à l'administration d'un réseau de télécommunications. Ainsi, il existe une liste des fonctions de base utilisées par les fonctions d'application du TMN.

Les fonctions générales du TMN constituent le support pour les applications du TMN. Elles peuvent être considérées comme équivalentes aux services d'information d'administration commune de l'administration OSI. Les cinq aires fonctionnelles correspondantes sont souvent appelées FCAPS par référence à leurs cinq initiales :

- Fault Management, ou gestion des fautes, qui regroupe les alarmes, la localisation des fautes et les tests.
- Configuration Management, ou gestion des configurations, qui comporte la définition de la configuration, le statut de la configuration, l'installation, l'initialisation, les inventaires, les reprises, la restauration, etc.
- Accounting Management, ou gestion de la comptabilité, qui comprend la récupération, l'émission et la modification des factures.
- Performance Management, ou gestion des performances, qui inclut l'obtention et la récupération d'informations de performance, le filtrage de ces informations, la gestion du trafic, etc.
- Security Management, ou gestion de la sécurité, qui nécessite un contrôle d'accès au réseau et aux applications ainsi qu'à des composants du TMN.

Les applications TMN sont des applications d'administration utilisant l'infrastructure du TMN et s'exécutant sur le réseau d'administration. Elles ne doivent pas être confondues avec les applications de communication, qui s'exécutent sur le réseau de communication.

Le rôle de l'UIT-T est de spécifier toutes les interfaces du TMN. Ces spécifications permettent d'assurer la compatibilité des dispositifs interconnectés pour accomplir une fonction d'application du TMN donnée, indépendamment du type du dispositif ou du fournisseur. À cet effet, des protocoles de communication compatibles et une méthode de représentation des données (acceptable pour les messages) sont nécessaires. Cela inclut en outre la définition des messages génériques compatibles avec les fonctions d'application TMN.

Le modèle informationnel de la gestion TMN

Le TMN doit permettre à des informations de gestion traversant les points de référence d'avoir un modèle commun défini par le modèle informationnel. Une approche orientée objet a été choisie en commun avec l'ISO. En suivant cette approche, les ressources sont représentées comme des classes d'objets gérés. Les règles définies par l'ISO pour la gestion système et la représentation des objets sont reprises par l'UIT-T. Les classes d'objets gérés sont spécifiées dans la notification internationale de gestion ISO GDMO (Guidelines for the Definition of Managed Objects).

Le modèle informationnel d'un réseau générique GNMI (Generic Network Information Model) a pour rôle d'identifier et de standardiser les classes d'objets gérés qui se retrouvent dans tous les réseaux de télécommunications. Cette approche devrait permettre de définir des services de gestion indépendants de la technologie utilisée et de la manière de réaliser le réseau physique. Le modèle GNMI détermine les classes de base qui sont utilisées dans les architectures de réseau d'opérateur.

Pour conclure cette section sur l'architecture TMN, indiquons qu'elle est fortement utilisée, en particulier chez les opérateurs, même si souvent la gestion d'équipements spécifiques est effectuée par SNMP. En fait, les solutions de gestion utilisées dans les grands réseaux mettent en jeu, la plupart du temps, à la fois le TMN et SNMP.

La gestion dans les réseaux Internet avec SNMP

SNMP (Simple Network Management Protocol) est un protocole simple de gestion de réseau développé par un groupe de travail de l'IETF dans le cadre de la définition d'un système de gestion pour les réseaux utilisant les protocoles TCP/IP. Trois versions se sont succédé dans le temps : SNMPv1, SNMPv2 et SNMPv3.

Le protocole de gestion SNMPv1 est très répandu dans le domaine des réseaux locaux, principalement pour le contrôle de réseaux locaux interconnectés. C'est aujourd'hui un standard de fait quasi incontournable pour les réseaux qui n'appartiennent pas au monde des télécoms.

SNMP a été approuvé par l'IAB (Internet Activities Board), responsable des spécifications de TCP/IP. Plusieurs documents définissent ce standard, parmi lesquels :

- RFC 1155 SMI (Structure of Management Information)
- RFC 1156 MIB (Management Information Base)
- RFC 1157 SNMP Protocol
- RFC 1158 MIB II (Management Information Base II)

Dans ce cadre, trois composants essentiels ont été définis :

- Le protocole SNMP, situé au niveau application de l'architecture en couches de TCP/IP, définit la structure formelle des communications.
- La base d'informations de gestion, ou MIB (Management Information Base), regroupe l'ensemble des variables relatives aux matériels et aux logiciels supportés par le réseau et définit les objets de gestion dans l'environnement TCP/IP.
- Les spécifications de la structure de l'information de gestion SMI (Structure of Management Information) définissent comment sont représentées dans la MIB les informations relatives aux objets de gestion (ressources) et comment sont obtenues ces informations.

Le protocole SNMP

Toutes les stations du réseau possèdent une base de ressources. Une station de gestion, la NMS (Network Management Station), contient une base maître qui représente toutes les ressources du réseau et les informations de gestion associées.

La structure des paquets SNMP est définie par la syntaxe ASN.1 (Abstract Syntax Notation 1). L'environnement SNMP est destiné à surveiller la performance d'un réseau, à détecter et à analyser ses fautes ainsi qu'à configurer ses éléments.

Les premiers produits implémentant SNMP sont apparus à la fin des années 80 dans de petites entreprises du marché TCP/IP, parmi lesquelles Cisco Systems, qui était alors minuscule, Advanced Computer Communications et Proteon Inc. Depuis, la quasi-totalité des constructeurs informatiques, dont IBM et Hewlett Packard, ont intégré le support de SNMP dans leur architecture globale de gestion de réseau.

Les systèmes SNMP possèdent deux éléments-clés :

- L'agent logiciel, qui fonctionne dans les stations gérées. Ces stations sont généralement des nœuds de réseau IP, qui peuvent être des systèmes hôtes (stations de travail,

serveurs, etc.), des équipements de transmission (multiplexeurs, etc.), des sondes ou des routeurs. Chaque agent comprend une MIB, base d'objets gérés, et des variables.

- La station de gestion de réseau (manager), système hôte qui contient le protocole de gestion de réseau et les applications de gestion. Elle est généralement composée d'un calculateur contenant une console et une base de données représentant tous les périphériques gérés du réseau et toutes les variables MIB de ces agents. Elle permet de récolter et d'analyser les données relatives aux équipements physiques connectés au réseau (ponts, routeurs, hubs) et de les gérer. Un agent peut être géré par plusieurs stations centrales. Certains agents, appelés agents proxy, permettent à un système de gestion SNMP de gérer des nœuds ne supportant pas la suite des protocoles Internet, c'est-à-dire des nœuds dialoguant avec un protocole propriétaire ou ISO.

La figure 29.11 illustre l'architecture SNMP.

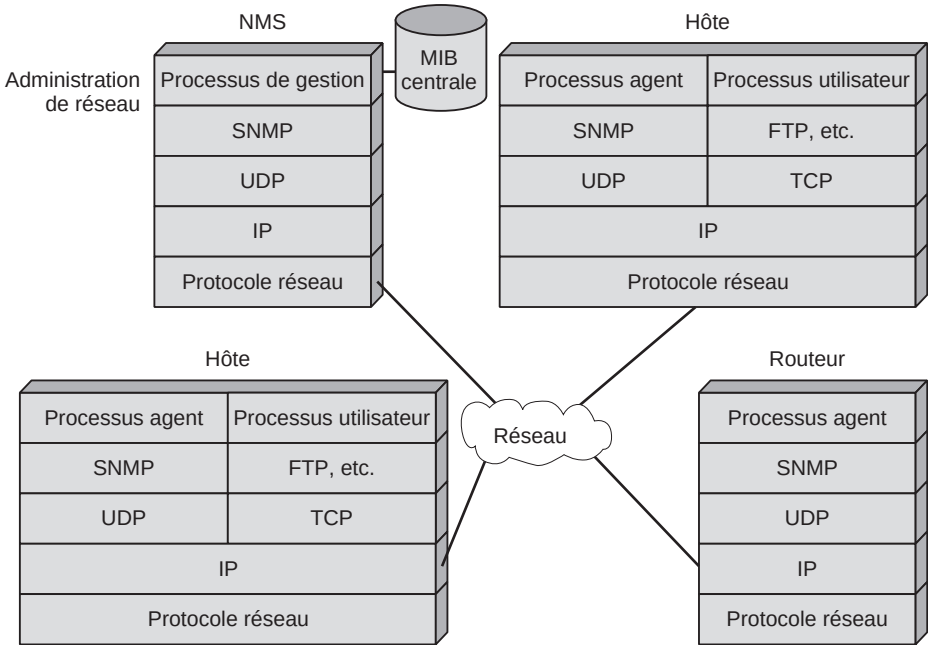


Figure 29.11
Architecture SNMP

La syntaxe des informations de gestion, intitulée SMI (Structure and Identification of Management Information for TCP/IP Based Internet), définit comment chaque élément d'information, concernant les périphériques gérés et les agents, est représenté dans la base d'information de gestion.

La syntaxe utilisée est un sous-ensemble de celle définie par la norme ASN.1.

Seuls quatre types de données sont utilisés :

- Integer : type de données qui n'accepte que des valeurs entières.
- Octet String : suite de 0 ou de plusieurs octets pouvant accepter des valeurs comprises entre 0 et 255.

- Object Identifier : suite de numéros référençant un objet enregistré par une autorité compétente.
- Null.

Deux types de données structurées sont autorisés : les listes et les tables à deux dimensions.

La MIB (Management Information Base) contient l'ensemble des variables gérées suivantes :

- Jeu de variables ayant trait à la fois au matériel et au logiciel.
- Jeu de points de test et de contrôle qu'un système supportant la gestion SNMP est censé vérifier.

La MIB attribue des noms aux éléments selon une hiérarchie d'enregistrements définie par l'ISO pour le nommage des objets réseau. Il en résulte une structure dans laquelle les variables ayant une relation logique sont regroupées en table. Par exemple, les variables concernant la vitesse, le taux d'erreur et les adresses d'interfaces de communication sont placées dans une table interface. Les objets de la MIB sont classés en une structure hiérarchisée de classes d'objets.

Le premier niveau de cette hiérarchie de classes d'objets de la MIB, ou MIB 1, comprend les huit groupes d'objets suivants :

- system : pour la gestion du nœud lui-même ;
- interfaces : pour les ports et interfaces réseau ;
- address translation : pour la traduction d'adresses IP ;
- IP (Internet Protocol) ;
- ICMP (Internet Control Message Protocol) ;
- TCP (Transmission Control Protocol) ;
- UDP (User Datagram Protocol) ;
- EGP (Exterior Gateway Protocol).

Suivant le type d'équipement à gérer, seuls certains groupes d'objets peuvent être implémentés.

Cette structure propose un grand nombre d'entrées permettant de décrire la majorité des objets réseau, mais certains fabricants ont défini leur propre MIB. Des entrées propres aux constructeurs ont donc été prévues dans cette organisation. De nombreuses extensions ont été effectuées au cours du temps, et des objets spécifiques de chaque nouveau protocole forment aujourd'hui le corps de plusieurs RFC.

La MIB 2 comprend, outre ce qui a été défini pour la MIB 1, des attributs ou objets, et deux groupes supplémentaires d'objets ont été définis : transmissions et SNMP. La MIB 2 gère environ 200 variables.

Une autre version, RMON MIB (Remote MOnitor Network Management Information Base), permet d'étendre les possibilités de SNMP. Elle autorise les moniteurs distants à contrôler les flux de trafic circulant à travers le réseau et est notamment utilisée pour les sondes.

RMON a été ratifié par l'IETF en novembre 1991 (RFC 1271). Le standard RMON couvre neuf groupes de données :

- Les statistiques, telles que le taux de collision pour un réseau Ethernet.
- Les historiques, qui décrivent le comportement du réseau pendant certaines périodes.
- Les alarmes.
- Les données relatives à la gestion des hôtes (enregistrement des hôtes sur le réseau, etc.).
- Les données se rapportant à la gestion de N hôtes, qui regroupent les statistiques d'hôtes faisant partie d'un groupe vérifiant un critère commun relatif à une donnée statistique.
- Les matrices de trafic, qui contiennent des données relatives aux communications entre groupes d'adresses.
- Les filtres.
- Les paquets capturés, qui contrôlent les données envoyées aux stations de gestion.
- Les événements générés par les agents.

RMON définit des variables relatives au contrôle du trafic sur les réseaux de niveau trame tels qu'Ethernet. Le protocole SNMP est le langage que les agents et les stations de gestion (managers) utilisent pour communiquer. C'est un protocole asynchrone de type question-réponse.

Les stations de gestion interrogent les agents pour observer leur fonctionnement et leur envoient des commandes pour leur faire exécuter certaines tâches. Les agents adressent les informations requises aux stations de gestion. Certains événements du réseau, tels que des erreurs de transmission, peuvent déclencher des alarmes envoyées aux stations de gestion. Cependant, l'envoi de messages de façon spontanée de l'agent vers le manager est limité. Les managers effectuent une interrogation périodique des agents de manière à vérifier leur état.

Si SNMP a l'avantage d'être simple, ses capacités à l'égard de la sécurité sont toutefois limitées, principalement en ce qui concerne l'authentification.

Les requêtes SNMP

Le protocole SNMP est un protocole sans connexion, qui utilise principalement le protocole UDP (User Datagram Protocol). Un système SNMP supporte trois types de requêtes : GET, SET et TRAP :

- **GET.** La commande GET REQUEST permet aux stations de gestion (managers) d'interroger les objets gérés et les variables de la MIB des agents. La commande GET NEXT REQUEST permet aux stations de gestion de recevoir le contenu de l'instance qui suit l'objet nommé. Grâce à cette commande, les stations de gestion peuvent balayer les tables des MIB. La commande GET RESPONSE est le message retourné par les entités interrogées (agents) en réponse aux commandes de type GET REQUEST, GET NEXT REQUEST et SET REQUEST.

- **SET.** La commande SET REQUEST permet aux stations de gestion de modifier la valeur d'un objet de la MIB ou d'une variable et de lancer des périphériques. SET REQUEST autorise, par exemple, un manager à mettre à jour une table de routage.
- **TRAP.** La commande TRAP permet à un agent de notifier un événement. Cette alarme, envoyée lors de la détection d'une anomalie par l'agent (initialisation de l'agent, arrêt de l'agent, dépassement d'un seuil, etc.), n'est pas confirmée par le manager. À l'exception des messages d'alarme (TRAPS), chaque message SNMP contient, entre autres :
  - un identificateur de requête ;
  - une liste de variables (noms et valeurs) ;
  - un champ pour les types d'erreurs ;
  - un index d'erreur signalant le numéro de la variable en erreur.

Tous les agents ne supportent pas obligatoirement toutes les commandes. Ainsi, SET REQUEST n'est pas toujours implémentée, car le protocole SNMP n'étant pas pourvu de dispositifs de protection, un mauvais usage de cette commande peut endommager des objets du réseau.

SNMP ne stocke et ne restitue que des types de données simples et ne travaille pas, à la différence de CMIP, sur des structures de données complexes. La plupart des fournisseurs d'outils d'interconnexion ont intégré SNMP dans leur offre. Le protocole SNMP est largement utilisé pour la gestion des matériels d'interconnexion de réseaux locaux, tels que ponts, routeurs, passerelles, hubs, etc.

SNMPv2 et SNMPv3

Une version plus avancée de SNMP, SNMPv2, a été proposée à l'IETF, mais elle n'a pas engendré de produits en grand nombre, et l'on peut même parler dans son cas d'échec cuisant. En revanche, la version SNMPv3 est bien acceptée par les entreprises, et de nombreuses implémentations sont disponibles sur le marché.

Le tableau 29.2 recense les principales RFC et normes du monde IP pour la gestion de réseau des domaines SNMPv2 et v3.

RFC	Titre de la RFC
RFC 1901	Introduction to community-based SNMPv2
RFC 1902	Structure of management information for SNMPv2
RFC 1903	Textual conventions for SNMPv2
RFC 1904	Conformance statements for SNMPv2
RFC 1905	Protocol operations for SNMPv2
RFC 1906	Transport mappings for SNMPv2
RFC 1907	Management Information Base for SNMPv2
RFC 1908	Coexistence between version 1 and version 2 of the internet-standard Network Management Framework
RFC 2573	SNMPv3 applications
RFC 2263	SNMPv3 applications
RFC 2273	SNMPv3 applications
RFC 2574	User-based Security Model (USM-SNMPV3)

TABLEAU 29.2 • RFC du domaine SNMPv2 et SNMPv3

SNMPv2 essaie principalement de limiter les flots d'information de contrôle par une nouvelle commande GETBULK et une commande GET améliorée. Pour prendre en charge la coopération entre managers, SNMPv2 introduit deux nouvelles caractéristiques : une commande INFORM et une MIB manager à manager. Un manager utilise une commande INFORM pour envoyer une information non sollicitée à un autre manager. Il peut, par exemple, signaler un débit excessif sur une ligne de communication. Cette information est consignée dans la nouvelle MIB manager à manager.

En septembre 1996, l'IETF a formé un nouveau comité dans le but d'examiner les problèmes de sécurité dans SNMP. Début 1997, ce comité a proposé une nouvelle génération, appelée SNMPng, qui rassemble les possibilités de SNMPv2 en incluant de nouveaux éléments de sécurité. Après un certain nombre d'améliorations supplémentaires, ce protocole SNMPng s'est transformé en SNMPv3, standard du domaine depuis la parution des RFC correspondantes, en 1998.

SNMPv3 est composé de trois modules :

- Message Processing and Control, qui définit la création et les fonctions d'analyse des messages.
- Local Processing, qui s'occupe des contrôles d'accès et de l'exécution des données.
- Security, qui permet l'authentification et le chiffrement ainsi que la prise en compte de contraintes de temps de certains messages SNMP.

L'amélioration la plus importante apportée par SNMPv3 concerne la sécurité, notamment l'authentification, le secret et le contrôle d'accès *(voir les chapitres 33 et 34)*.

Comparaison de CMIP et de SNMP

CMIP et SNMP doivent, à terme, coexister. L'objectif de SNMP, qui était d'obtenir une gestion correcte à un coût raisonnable, a été atteint. Sa facilité d'utilisation et sa simplicité d'implémentation ont favorisé son rapide développement dans le monde TCP/IP. Cette simplicité pose néanmoins quelques problèmes lorsqu'il s'agit de gérer de nouveaux équipements et logiciels non conformes aux standards SNMP, les fournisseurs étant contraints d'écrire des extensions propriétaires.

Contrairement à CMIP, SNMP est un protocole de type datagramme, c'est-à-dire un protocole travaillant dans un mode sans connexion. De plus, les systèmes SNMP reposent sur IP, et donc sur un autre protocole de type datagramme. Cependant, SNMP peut être utilisé dans des environnements autres qu'IP, par exemple, pour la gestion de ponts 802.1. CMIP, quant à lui, se doit de fournir un cadre d'architecture pour systèmes distribués et une application de gestion. Sa portée, qui est plus ambitieuse que celle de SNMP, a provoqué de nombreuses critiques, car elle engendre une forte complexité ainsi qu'une implémentation délicate.

Une autre différence importante entre SNMP et CMIP réside dans la façon de représenter l'information. CMIP distingue les notions d'objets et d'attributs, alors que SNMP ne possède pas la notion d'attribut : un objet peut être un système à gérer comme une caractéristique qui décrit ce système. Un attribut peut correspondre à

l'état du système ou à un paramètre décrivant comment le système devrait fonctionner dans des conditions optimales. À chaque objet est associée une description unique, et un objet ne peut pas être défini à partir d'un autre.

CMIP utilise six primitives et effectue une distinction très nette entre un objet et ses attributs. CMIP et SNMP fournissent tous deux des directives sur la définition des objets de gestion et permettent aux fournisseurs d'ajouter tout ce qu'un système a besoin de savoir pour contrôler un objet. Le fait que SNMP ne fasse pas la distinction entre objet et attribut a de fâcheuses conséquences : la réutilisation d'un attribut ou d'une définition pour présenter une information générique est impossible, d'où la difficulté de gérer de nouveaux objets. Sous CMIP, un certain nombre d'objets totalement différents peuvent avoir un attribut commun, par exemple l'état opérationnel. SNMP n'est pas apte à supporter la notion d'héritage, contrairement à CMIP, et ne fournit pas le concept d'évolution d'un objet. En revanche, SNMP autorise les fournisseurs à définir de nouveaux objets et à les stocker de façon que les systèmes de ces fournisseurs puissent être gérés. Cette aide a sans doute contribué au développement de SNMP.

SNMP et CMIP sont tous deux spécifiés en ASN.1, mais SNMP est restrictif en ce qui concerne le codage des éléments complexes, comme les listes. De même, les deux protocoles comportent un certain nombre d'options qui permettent aux fournisseurs d'étendre les informations transportées par ces protocoles.

Les deux protocoles ont trois primitives en commun :

- GET, qu'un système gérant envoie à un agent en vue d'obtenir la valeur d'un objet.
- SET, utilisé pour initialiser la valeur d'un attribut.
- EVENT-REPORT, ou TRAP dans la terminologie SNMP, qui permet de signaler une occurrence d'un événement important concernant un objet.

Les performances de SNMP et de CMIP sont à peu près équivalentes. Leur fiabilité dépend essentiellement de la qualité de développement du logiciel et du mécanisme de transport des données. L'architecture CMIP est plus ouverte aux extensions, dans la mesure où elle peut davantage accepter de nouvelles définitions d'objets. La distinction entre objet et attributs rend cependant les extensions plus difficiles que dans SNMP. Enfin, la place mémoire nécessaire pour stocker les informations de gestion donne sans aucun doute un avantage à SNMP, qui est beaucoup plus concis que CMIP.

Le protocole CMOT (Common Management Information Services and Protocol Over TCP/IP), promu par un groupement de constructeurs réunis sous le nom de Netman, devrait offrir le moyen de gérer les éléments d'un réseau TCP/IP à partir de logiciels de gestion ISO. Le protocole CMOT implémente les prémices de la gestion définis par l'ISO, tels ROSE et ACSE.

Une couche présentation a été développée et intégrée à CMOT de façon que ROSE et ACSE puissent s'y référer. Cette couche de présentation, LPP (Lightweight Presentation Protocol), travaille au-dessus d'UDP ou de TCP et assure la présentation des messages dans l'environnement TCP/IP.

Cette version de SNMP pallie un certain nombre d'inconvénients de la précédente. Elle permet notamment de diminuer le nombre de paquets générés sur le réseau et offre la possibilité à une station d'être à la fois manager et agent.

La gestion par le Web

SNMP est devenu le protocole standard pour la gestion de réseau en se développant au début en parallèle à la version ISO, représentée par CMIP/CMIS, puis en prenant pratiquement l'ensemble du marché. Cependant, le processus de décision n'est pas inclus dans le protocole de gestion. L'ajout d'un environnement Web permet d'intégrer la gestion dans le système d'information des entreprises. C'est l'un des rôles de l'architecture de gestion WBEM (Web-Based Enterprise Management).

WBEM provient d'une initiative de plus de soixante-quinze sociétés visant à définir une architecture de gestion complète pour l'entreprise. Les composants principaux de cette architecture sont les suivants :

- Modèle de données simple et extensible pour définir et manipuler les états du système.
- Architecture côté client utilisée pour implémenter le modèle comme un ensemble d'objets.
- Modèle de distribution globale et de propagation des informations entre les clients et les sites où les actions de gestion sont décidées.

Le processus de normalisation a été réalisé sous l'égide du DMTF (Distributed Management Task Force) et de l'IETF. Le premier modèle adopté, en avril 1997, est le CIM (Common Information Model). Son principe de fonctionnement consiste à réutiliser l'environnement Web pour gérer le réseau.

Deux nouveaux modules de gestion sont ajoutés :

- CIMOM (CIM Object Manager), pour interpréter les requêtes en utilisant le modèle d'information.
- HMMP (HyperMedia Management Protocol), un protocole d'encodage qui permet le transport d'informations de gestion dans d'autres protocoles, tels que TCP/IP.

L'architecture WBEM

Comme expliqué précédemment, WBEM permet de gérer les réseaux et les applications à partir d'un navigateur Web. WBEM décrit une architecture, un protocole, un schéma de gestion et un gestionnaire d'objets. Il doit permettre de prendre en charge les cinq aires de gestion et de donner naissance à un modèle de données adapté à la gestion de systèmes, de réseaux et d'applications. La proposition utilise le HTML pour la description des informations et HTTP.

Illustrés à la figure 29.12, les principaux composants de WBEM sont les suivants :

- HMMS (HyperMedia Management Schema), qui définit un schéma, ou une description, des données indépendant de leur implémentation et acceptant les données de différentes sources.

- HMMP (HyperMedia Management Protocol), qui définit un protocole permettant d'accéder aux données de gestion et fournit des solutions de gestion indépendantes de la plate-forme et de la distribution.
- HMOM (HyperMedia Object Manager), qui propose une définition générique pour les applications de gestion. Ce composant permet d'agréger les données de gestion et utilise un ou plusieurs protocoles pour fournir une représentation uniforme au navigateur utilisant HTML.

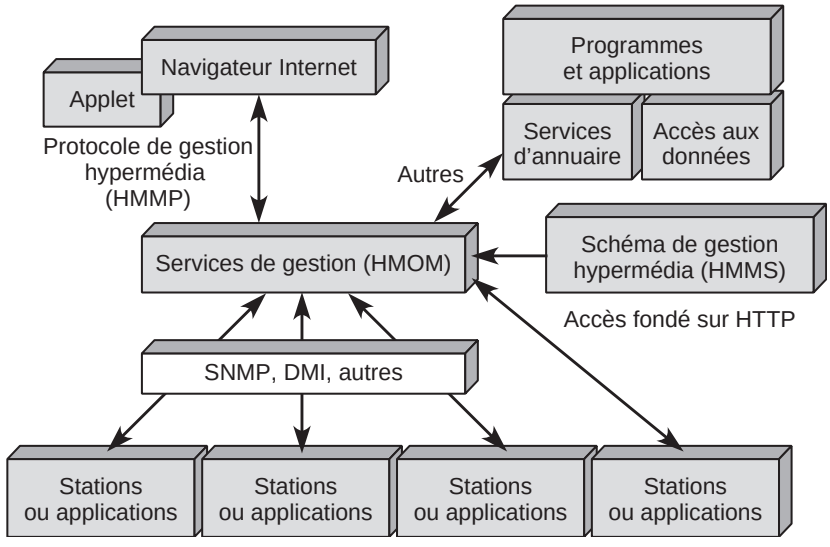


Figure 29.12

Composants de l'architecture WBEM

JMAPI (Java Management API)

Dans la perspective de l'unification de la gestion de réseau à travers le Web, JMAPI (Java Management API) a été définie par le consortium Java afin de simplifier la gestion. L'initiative JMAPI a principalement consisté en une extension du noyau de Java pour y intégrer des mécanismes permettant de développer des logiciels de gestion de réseau fondés sur le Web.

JMAPI est un ensemble de classes dérivées permettant d'accéder aux services de gestion SNMP sous-jacents. Grâce à cette approche, il est possible de s'affranchir des problèmes de portabilité des applications et d'obtenir des capacités étendues d'affichage.

Au niveau le plus haut, JMAPI propose une interface de navigateur, un module de gestion et des équipements à gérer. L'interface utilisateur du navigateur est le mécanisme par lequel un administrateur peut accéder aux opérations de gestion. Le module de gestion définit les mécanismes qui prennent en charge les objets gérés. Il inclut des interfaces objet pour les agents, des interfaces de notification et des interfaces avec les objets gérés.

L'architecture JMAPI est illustrée à la figure 29.13.

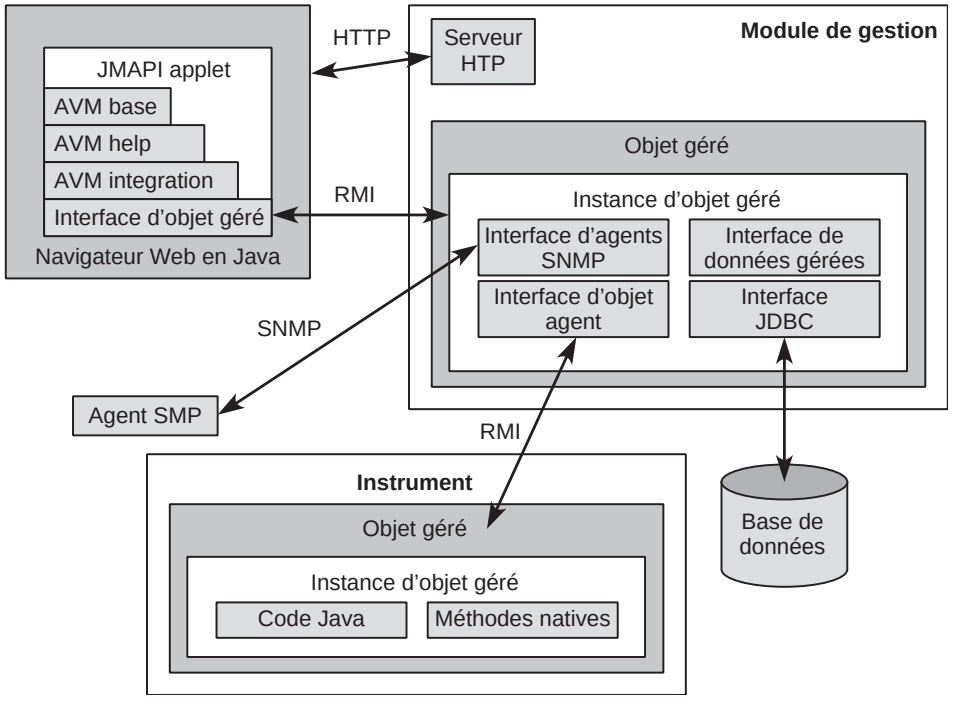


Figure 29.13
Architecture JMAPI

Tout l'intérêt de JMAPI est de distribuer géographiquement différents composants du système et de rendre possible les interactions entre composants grâce à RMI (Remote Method Invocation). Dans ce cas, le gestionnaire de réseau devient complètement indépendant du protocole de gestion spécifique, et l'on peut dès lors télécharger différentes applets au niveau du site agent pour réaliser des tâches de gestion sans surcharger le réseau.

Ce type d'intégration est illustré à la figure 29.14.

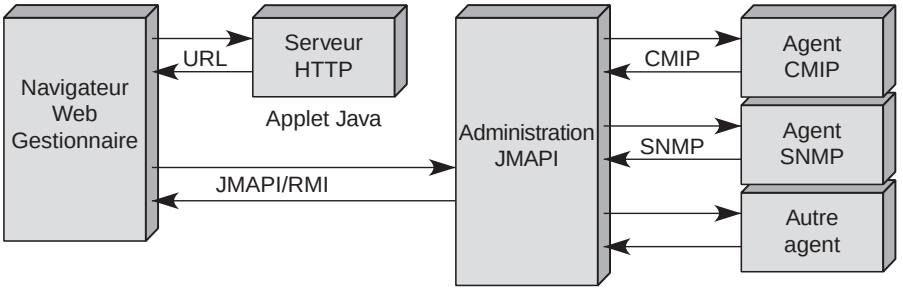


Figure 29.14
Exemple d'intégration de Java dans le modèle agent-manager

Dans son utilisation actuelle, l'approche JMAPI ne définit pas un nouveau modèle de gestion mais offre un niveau intermédiaire permettant de s'affranchir de l'hétérogénéité des systèmes et des protocoles de gestion sous-jacents. L'approche fondée sur Java offre un environnement de développement d'applications de gestion homogène, cachant entièrement l'hétérogénéité sous-jacente, tout en permettant une extensibilité et une portabilité simples.

La gestion par le middleware

Nous allons maintenant examiner comment le middleware, c'est-à-dire un logiciel intermédiaire entre les équipements et les processus de décisions, peut aider à la réalisation d'un système de gestion de réseau intégré en prenant l'exemple du middleware CORBA.

Dans le cadre de la gestion de réseau, l'architecture CORBA (Common Object Request Broker Architecture) a pour principal intérêt d'offrir aux applications de gestion une abstraction suffisante vis-à-vis des technologies système sous-jacentes. Elle permet ainsi de concentrer l'intelligence sur les services de gestion plutôt que sur la manière d'interagir avec le système ou la communication entre applications. Néanmoins, il est nécessaire de spécialiser ces environnements de manière à introduire un ensemble de fonctionnalités communes spécifiques de la gestion de réseau et permettant de mieux maîtriser le cycle de vie des services de gestion.

Cette gestion est illustrée à la figure 29.15.

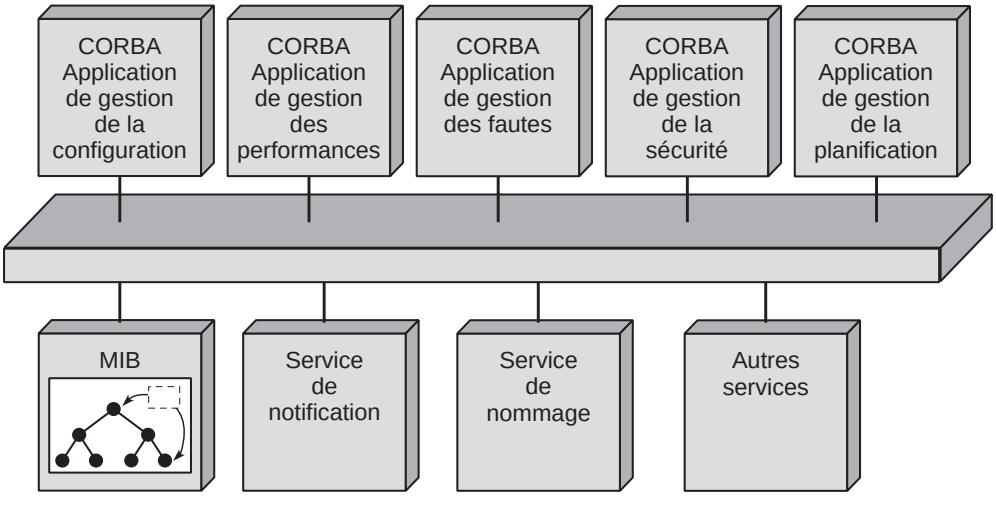


Figure 29.15

CORBA et la gestion de réseau

L'intégration de l'existant est un aspect crucial de la gestion de réseau, du fait notamment du parc logiciel et matériel déjà présent et du délai d'adoption par les constructeurs d'une nouvelle approche. Dans cette optique, de nombreuses initiatives ont été lancées afin de définir des mécanismes de migration du modèle agent-manager de CMIP/CMIS vers un modèle client-serveur CORBA.

Ces différentes initiatives ont abouti à la spécification de mécanismes permettant d'intégrer soit des objets issus de la normalisation ISO dans des environnements CORBA, soit des objets CORBA dans un environnement ISO. Ces deux approches correspondent à des processus d'intégration distincts : l'encapsulation ou la passerelle, comme illustré à la figure 29.16.

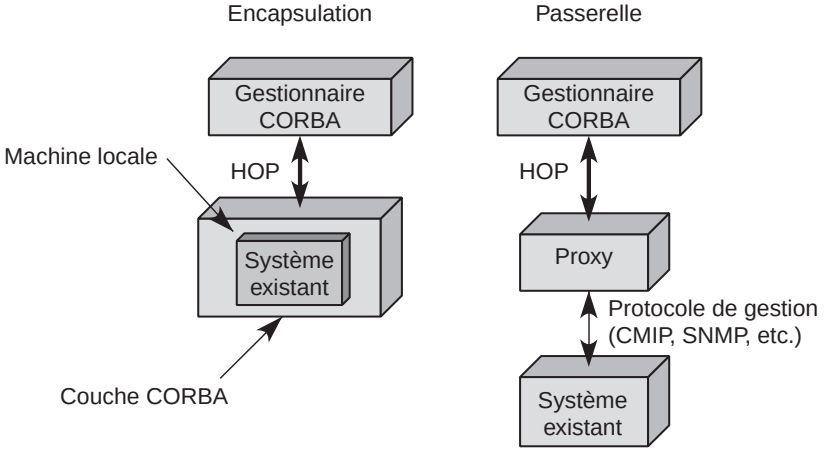


Figure 29.16

Intégration des objets de gestion par encapsulation ou passerelle

Ces travaux ont été repris par le groupe de travail XoJIDM (Joint Inter-Domain Management) de l'X-Open et du NM Forum et le groupe de télécommunications de l'OMG (Object Management Group) afin d'uniformiser les différentes approches d'intégration.

Les passerelles ont pour rôle de mettre en place des mécanismes de conversion dynamique. Ces mécanismes permettent la mise en correspondance de modèles d'information de gestion définis dans des environnements différents. Les modèles d'information les plus importants mis en correspondance sont CORBA et SNMP/SMI (System Management Interface), ainsi que CORBA et GDMO (Guidelines for the Definition of Managed Objects). Dans ce cadre, plusieurs architectures de passerelles ont été proposées, qui permettent au concepteur de systèmes de gestion de s'affranchir des protocoles et des services sous-jacents afin de collecter des informations sur les éléments physiques ou logiques du réseau. Cette architecture est illustrée à la figure 29.17.

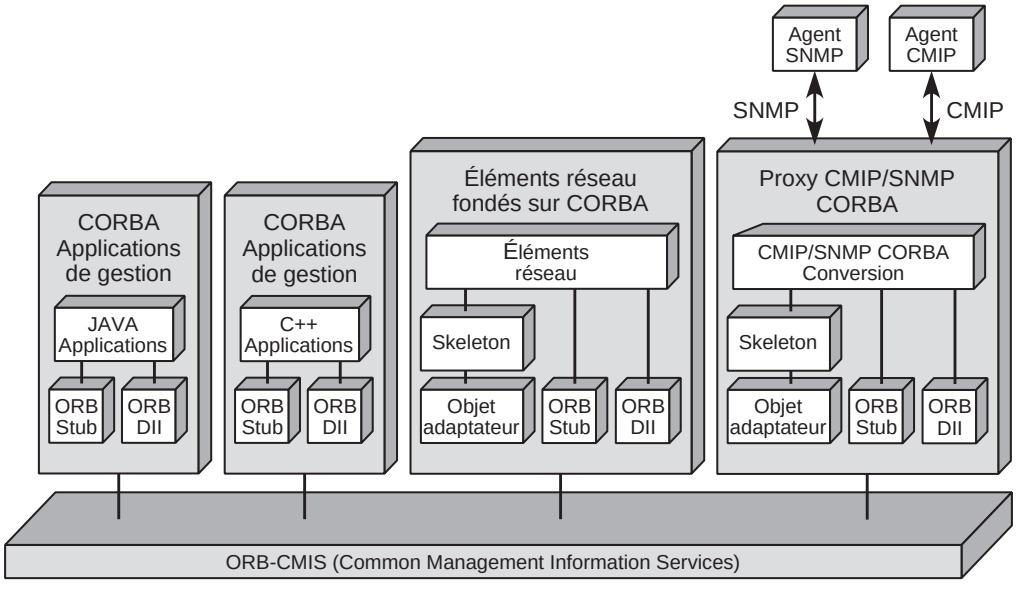


Figure 29.17

Intégration de CORBA dans le modèle agent-manager

Architecture Java/CORBA des systèmes de gestion

L'intégration de CORBA et de Java dans le même middleware offre à la gestion de réseau des perspectives séduisantes. Cette intégration, déjà réalisée dans certains middlewares, permet de résoudre les problèmes d'interopérabilité entre des applications Java et des applications développées dans d'autres langages. Il est notamment possible de rapprocher le processus de traitement des informations de gestion du système cible, par exemple le nœud du réseau lui-même, de façon à diminuer le trafic et à distribuer le contrôle. L'introduction des technologies agent dans la gestion de réseau en est facilitée. Les agents ne sont autres que des programmes autonomes possédant une certaine intelligence (agents intelligents) et pouvant se déplacer (agents mobiles) et communiquer entre eux à travers le réseau. Cette approche peut être utilisée dans le cadre de la gestion de réseau afin de disposer d'une plus grande efficacité dans le contrôle.

Dans ce contexte, le gestionnaire a la possibilité de déléguer complètement certaines tâches et de les distribuer sur le réseau sans avoir à contrôler d'une manière centralisée le déroulement des processus. Une fois les tâches achevées, les agents reviennent vers le centre de gestion pour rendre compte de l'exécution de la tâche ou des tâches qui leur ont été assignées. Les agents sont supportés dans leur déplacement par des interfaces CORBA, tandis que Java fournit la base de l'environnement d'exécution sur les nœuds du réseau. Dans ce cadre, l'OMG a spécifié les interfaces permettant de mettre en place les fonctionnalités des agents mobiles fondées sur CORBA.

Le modèle DME

DME (Distributed Management Environment) est un modèle d'architecture pour la gestion des réseaux locaux. Mis au point par l'OSF (Open Software Foundation), qui regroupe la plupart des grands constructeurs informatiques (IBM, DEC, Bull, Hewlett Packard, etc.), DME a pour but de résoudre le problème de la gestion de réseaux hétérogènes en proposant un environnement de traitement réparti.

Plusieurs points ont permis les avancées suivantes :

- DCE (Distributed Computing Environment), qui est un environnement développé pour le traitement distribué en milieu hétérogène.
- DME, qui s'appuie sur DCE et permet de gérer les ressources d'un environnement réseau contenant des systèmes, des éléments de réseau et des applications. Il s'agit d'un environnement assez complexe, qui inclut de nombreux composants :
  - Une interface utilisateur de gestion, qui permet d'obtenir une vue unique des objets de l'environnement.
  - Un ensemble de services destinés à la gestion des objets de l'environnement (logiciels, matériels, impression, configuration, etc.).
  - Des services de gestion permettant la mise en œuvre d'un modèle de gestion.
  - Des services d'objets qui gèrent les objets de l'environnement, tels un gestionnaire de requêtes inclus dans DME pour localiser et enregistrer les objets stockés dans les serveurs d'objets.
  - Des serveurs d'objets.
  - Des services de gestion d'événements provenant de requêtes du modèle OSI ou d'architectures non compatibles par l'intermédiaire d'un langage de description. Les communications sont fournies à distance par des RPC (Remote Procedure Call) ou en local par des IPC (Inter Process Communication).
  - Des protocoles de gestion, notamment une interface CMIP, une interface SNMP et un protocole de gestion spécifique de l'OSF, qui utilise les RPC pour communiquer.
  - Des outils de développement, qui comprennent des langages et des compilateurs ainsi que des appels système. Ces appels système, ou API (Application Programming Interface), reposent le plus souvent sur une architecture orientée objet. Pour les applications de gestion, l'API définie par l'OSF se fonde sur le protocole CMIS.

En conclusion, DME est une plate-forme de développement complète, qui doit pouvoir s'interfacer avec tous les grands standards d'aujourd'hui et de demain.

Conclusion

Commençons cette conclusion par une comparaison des différents systèmes de gestion de réseau. Le tableau 29.3 compare les caractéristiques des principaux protocoles conduisant à une gestion de réseau.

	CMIP	SNMP	DMI	HTTP
Modèle informationnel	Orienté objet	Orienté objet	Orienté objet	Hypermédia
Langage	GDMO	SMI	MIF	HTML
Architecture	Manager-agent, manager-manager	Manager-agent, manager-manager	Manager-agent	Client-serveur
Primitive	M-Get, M-Set, M-Action, M-Create, M-Delete, M-Event-Report	Get, Set, action implicite (effets secondaires), Trap	Get, Set, action implicite, Add, Delete, Event	Get, Post, Link Ne supporte pas la primitive Trap.
Mode de communication	Orienté transactions Requête/réponse	Requête/réponse	Requête/réponse	Requête/réponse asynchrone
Adressage	Par filtrage	Par arbre	Par attribut	URL
Application de gestion	Cinq aires fonctionnelles	Non spécifiée	Non spécifiée	Plug-in Java
Organisme de standardisation	ITU-T, ISO/OSI	IETF	DMTF	IETF

TABLEAU 29.3 • Comparaison des solutions proposées pour la gestion de réseau

Le système de gestion nécessite une définition de sa structure, de son fonctionnement et des protocoles d'échange. La gestion de ressources distribuées est une tâche complexe, qui requiert une bonne fiabilité, certaines opérations devant pouvoir être réalisées en dépit d'une quelconque panne. De plus, des contraintes de temps réel sont souvent à prendre en compte.

Ce chapitre a présenté l'environnement de gestion OSI, ainsi que les autres solutions constructeur disponibles sur le marché. SNMP est le protocole aujourd'hui de loin le plus utilisé. Ayant été développé pour gérer les architectures TCP/IP, la vogue de l'environnement TCP/IP lui a fortement profité. L'avantage de SNMP par rapport à la normalisation ISO est sa simplicité, puisque c'est un environnement inspiré de la normalisation ISO mais simplifié. On ne trouve que trois primitives dans SNMP, au lieu de six dans CMIP : GET, SET et EVENT. De plus, le logiciel SNMP a été fortement simplifié par rapport à celui de l'ISO car il n'est pas possible d'adresser un attribut d'un objet de gestion, ce qui est possible dans l'architecture OSI. Enfin, des architectures plus globales s'appuyant sur le succès du Web se mettent en place et devraient prendre le devant de la scène dans ce domaine.

Enfin, la gestion de réseaux continue à progresser surtout dans le sens de la généralisation : il faut gérer les éléments de réseau mais également de plus en plus les applications qui tournent autour ainsi que l'ingénierie, la planification et la sécurité du réseau sous surveillance. Le nom de OSS (Operation Support System) a été adopté pour cette généralisation de la gestion de réseaux.

Références

Un excellent livre, réalisé par un ensemble de spécialistes de la gestion de réseau, qui fait le tour du problème :

S. AIDAROUS, *et al.* – *Managing IP Networks: Challenges and Opportunities*, Wiley-IEEE Press, 2003

Un livre général et complet sur la gestion de réseau :

R. J. BATES – *Network Management*, McGraw-Hill, 2002

Un des très nombreux livres de U. Black. Celui-ci porte sur les protocoles de gestion de réseau :

U. BLACK – *Network Management Standards: SNMP, CMIP, TMN, MIBs and Object Libraries*, McGraw-Hill, 1994

Un livre complet sur SNMPv3 :

U. BLUMENTHAL, N. HIEN, B. WIJNEN – *SNMPv3 Handbook*, Addison Wesley, 1999

Un excellent livre sur la gestion de réseaux aussi bien sur la partie conceptuelle que pratique :

J. R. BURKE – *Network Management: Concepts and Practice, A Hands-On Approach*, Prentice Hall, 2003

Les protocoles de gestion sont très bien décrits dans ce livre dévolu à l'ensemble des systèmes de communication :

P. BYRNES – *Protocol Management in Computer Networking*, Artech House, 2002

Un livre très complet sur le TMN :

FAULKNER INFORMATION SERVICES – *Telecommunications Management Network (TMN) Standard*, 2001

Livre plus orienté vers la gestion de l'ATM que du monde IP, avec de nombreuses bonnes idées :

A. GILLESPIE – *Broadband Access Technology, Interfaces and Management*, Artech House, 2001

Livre complet sur le protocole SNMP :

S. J. HARNEDY – *Total SNMP: Exploring the Simple Network Management Protocol*, Prentice Hall, 1997

Livre complet sur tous les aspects de la gestion de réseau et de système :

H.-G. HEGERING, S. ABECK – *Integrated Network and System Management*, Addison Wesley, 1994

La gestion des réseaux locaux et plus généralement des réseaux passe de plus en plus par l'établissement de réseaux virtuels, qui doivent être correctement mis en place et gérés. Le livre suivant aborde ce problème de façon très pragmatique :

G. HELD – *Virtual LANs: Construction, Implementation, and Management*, Wiley, 1997

Un autre livre de Gilbert Held très pédagogique et facile à lire :

G. HELD – *LAN Management with SNMP and RMON*, Wiley, 1996

Un des livres de base pour la gestion de l'environnement IP :

C. HUNT – *TCP/IP, administration de réseau*, O'Reilly, 1998

Une très bonne présentation de la problématique de gestion des réseaux IP :

F. JACQUENET – *Administration des réseaux*, CampusPress, 2002

Un livre pratique très complet :

> T. L. LIMONCELLI, C. HIGAN – *The Practice of System and Network Administration*, Addison Wesley, 2001

Ce livre est beaucoup plus général que la seule gestion de réseau et s'intéresse à tout l'environnement réseau :

> T. MANN-RUBINSON, K. TERPLAN – *Network Design: Management and Technical Perspectives*, CRC Press, 1998

Livre à lire pour ceux qui veulent se diriger vers la gestion de réseau. Très complet et orienté vers la gestion par le Web :

> J. P. MARTIN-FLATIN – *Web-Based Management of IP Networks and Systems*, Wiley, 2002

Très bonne introduction de la gestion par le Web :

> D. R. MAURO, K. J. SCHMIDT – *Essential SNMP*, O'Reilly, 2001

Un livre spécialisé sur la gestion des réseaux locaux. Très complet puisque de nombreux aspects, comme la sécurité, y sont également introduits.

> A. MIKELSEN, P. BORGESEN – *Local Area Network Management, Design & Security*, Wiley, 2002

La généralisation de la gestion de réseaux prend le nom d'OSS (Operation Support System). Ce livre en propose une introduction.

> K. MISRA – *OSS for Telecom Networks: An Introduction to Network Management*, Springer Verlag Telos, 2004

Un livre de gestion dévolu aux réseaux locaux de toute nature :

> S. B. MORRIS – *Network Management, MIBs and MPLS: Principles, Design and Implementation*, Prentice Hall, 2003

La gestion de réseaux ATM effectuée par le protocole SNMP :

> H. OAN – *SNMP-Based ATM Network Management*, Artech House, 2002

La gestion de réseau ATM par un environnement SNMP est abordée avec beaucoup de précision dans le livre suivant :

> H. PAN – *SNMP-Based ATM Network Management*, Artech House, 1998

Les MIB sont particulièrement importantes dans le processus de normalisation du protocole SNMP. Ce livre en fait l'analyse :

> D. PERKINS, E. MCGINNIS – *Understanding SNMP MIBs*, Prentice Hall, 1996

Un livre consacré au protocole RMON :

> D. T. PERKINS – *RMON: Remote Monitoring of SNMP-Managed*, Prentice Hall, 1998

Un excellent livre sur les techniques de gestion SNMP et RMON :

> W. STALLINGS – *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, Third Edition*, Addison Wesley, 1990

Un excellent livre pour réaliser des MIB et s'occuper de la gestion SNMP :

> L. A. STEINBERG – *Troubleshooting SNMP; Analyzing MIBs*, McGraw-Hill, 2000

Un des premiers livres sur la gestion de réseau, dont de nombreux développements sont toujours valables :

K. TERPLAN – *Communication Networks Management*, Prentice Hall, 1987

Un livre général très pédagogique de K. Terplan, qui est un des meilleurs spécialistes en gestion de réseau :

K. TERPLAN – *OSS Essentials: Support System Solutions for Service Providers*, Wiley, 2001

Autre livre de Terplan, mais consacré à la gestion d'un réseau intranet :

K. TERPLAN, S. ZAMIR – *Intranet Performance Management*, CRC Press, 1999

Encore un livre de Terplan, cette fois consacré à la gestion par des techniques Web :

K. TERPLAN, S. ZAMIR – *Web-Based Systems and Network Management*, CRC Press, 1999

Un livre orienté vers un domaine spécifique de la gestion, la sécurité :

M. WEBSTOM – *Managing Cisco Network Security*, Cisco Press, 2001

Livre très général sur la gestion de réseau :

S. WISNIEWSKI – *Network Administration*, Prentice Hall, 2000

Livre entièrement consacré à SNMPv3, pour ceux qui souhaitent aller plus loin dans le domaine de la gestion :

D. ZELTSERMAN – *Practical Guide to SNMPv3 and Network Management*, Prentice Hall, 1999