TELEINFORMATIQUE

TOME 3

ADMINISTRATION ET SECURITE DES RESEAUX ET DES SYSTEMES

IF
Création 1995
Révision 2001

INSTITUT NATIONAL DES SCIENCES APPLIQUÉES DE LYON

FORMATION

Auteur de la ressource pédagogique :
BEUCHOT Gérard

membre de UNIVERSITÉ DE LYON

INSA LYON

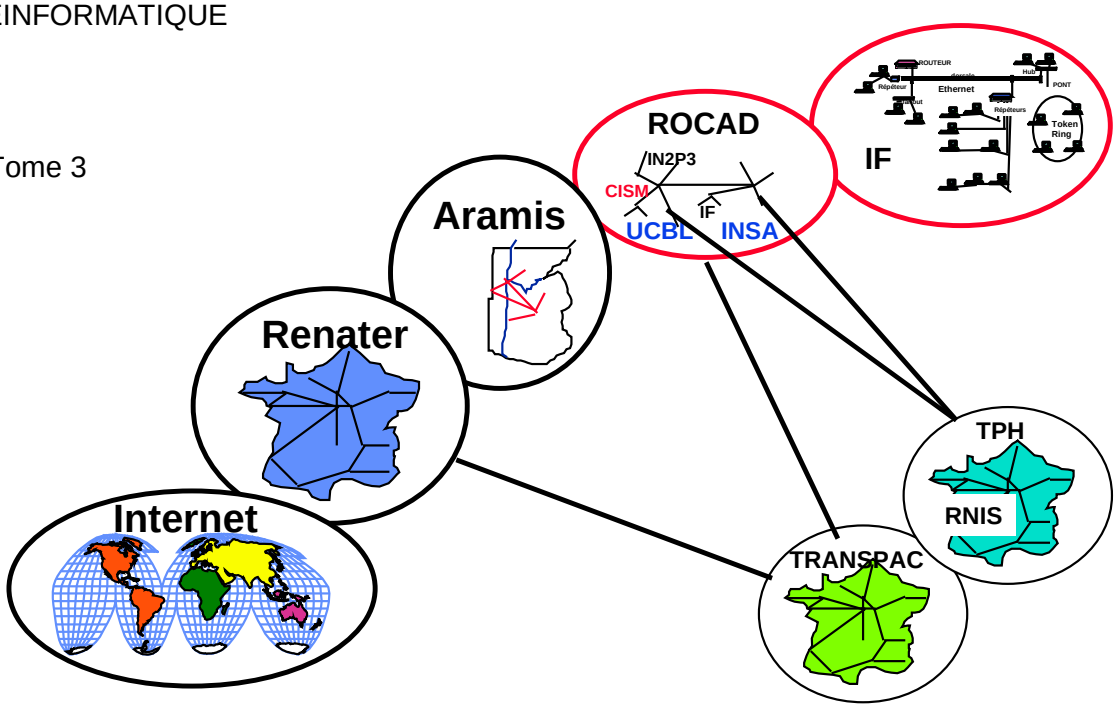
INSTITUT NATIONAL DES SCIENCES APPLIQUEES DE LYON

DEPARTEMENT INFORMATIQUE

ADMINISTRATION ET SECURITE DES RESEAUX ET DES SYSTEMES

TELEINFORMATIQUE

Tome 3



Sommaire

1 ADMINISTRATION DES RESEAUX ET DES SYSTEMES

1.1 Principes et concepts

1.1.1 Définition

L'administration de réseaux englobe les moyens mis en œuvre pour :

- Offrir aux utilisateurs une qualité de service donnée et garantir cette qualité de service.
- Permettre et guider l'évolution du système en fonction
    - du trafic
    - des nouvelles applications
    - des nouvelles technologies
- Représente le partie opérationnelle d'un système, soit
    - la surveillance du réseau informatique :
- Systèmes informatiques et réseaux d'interconnexion
    - le support technique
    - la gestion des coûts, des ressources, etc.
    - la gestion de ressources humaines

L'administration de réseau est appliquée en suivant une politique, c'est à dire des objectifs à atteindre ("**activité administration de réseaux**").

Cette politique spécifie des actions à long, moyen et court terme par :

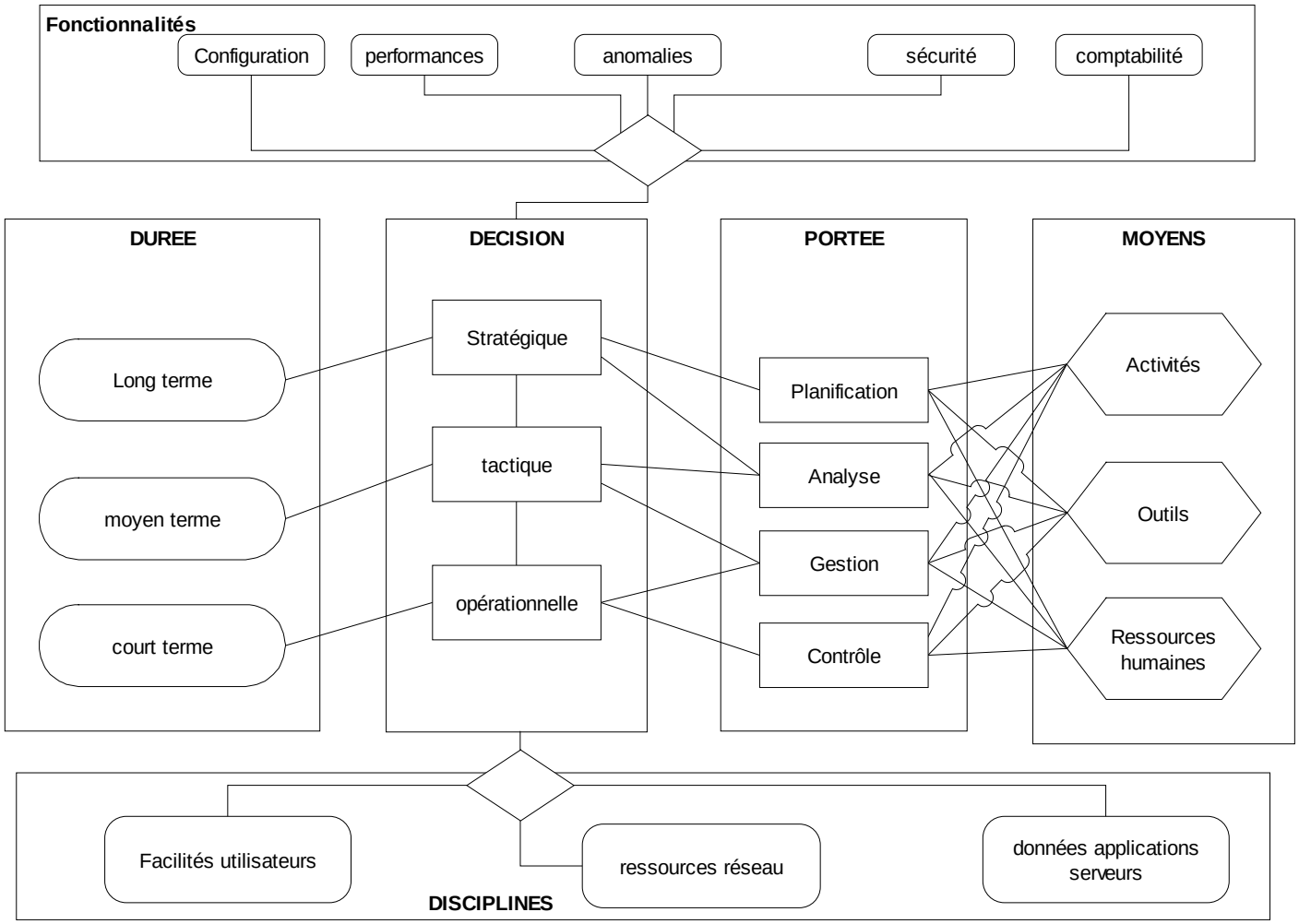
- une stratégie, plan des actions à entreprendre à long terme, de quelques mois à un ou deux ans

- une tactique, plan d'exécution pour atteindre les objectifs à moyen terme, de quelques jours à un ou deux mois

- un fonctionnement opérationnel, pour gérer le réseau en continu, à court terme, de quelques minutes à quelques heures.

Ceci implique la définition de modes opératoires et leur mise en œuvre.

Ces différents aspects sont résumés par le schéma suivant du à J.P. Claudé.



1.1.2 Disciplines

L'administration de réseau ne porte pas seulement sur le réseau de télécommunications au sens strict, mais englobe aussi l'administration

- des utilisateurs
  - qui
  - où
  - comment les atteindre
  - comment les identifier
  - quels sont leurs droits

- des serveurs et des ressources
  - quelles machines
  - quelles ressources
  - quelles fonctions de communication, comment les utiliser
  - quelle sécurité sur les données et les ressources
  - quels sont leurs coûts d'utilisation.

- du (ou des) réseau(x) de télécommunication

C'est une ressource particulière ayant des composants variés:

- informatiques
- de télécommunication pour réseaux informatiques
- modems, concentrateurs, multiplexeurs, commutateurs,etc
- de télécommunications générales :
- PABX, accès aux réseaux publics

1.1.3 Fonctionnalités

Elles sont regroupées en cinq grandes classes

- Gestion des anomalies
- Gestion de la comptabilité
- Gestion de la sécurité
- Gestion des performances
- Gestion de la configuration et des noms

1.1.3.1 Gestion des anomalies

Elle recouvre la détection des anomalies, l'identification et la correction de fonctionnements anormaux. Ces défauts font qu'un système n'atteint pas ses objectifs; ils sont temporaires ou permanents. Ils se manifestent comme des événements.

Elle fournit une assistance pour répondre aux besoins de la qualité de service et à sa permanence.

La gestion d'anomalies comprend les fonctions suivantes :

- réception de et actions sur des notifications de détection d'erreurs
- recherche et identification des anomalies
- exécution des séquences de tests de diagnostic
- correction des anomalies
- tenue et examen des journaux d'erreurs

1.1.3.2 Gestion de la comptabilité

C'est une activité qui peut être complexe car elle doit prendre en compte la totalité du réseau informatique, de ses services et de ses ressources.

Elle comprend les fonctions suivantes :

- information des utilisateurs sur les coûts encourus ou les ressources utilisées
- possibilité de fixer des limites comptables et des prévisions de tarifs, associées à l'utilisation des ressources
- possibilité de combiner les coûts quand plusieurs ressources sont utilisées pour atteindre un objectif de communication donné.

Ceci conduit à la mise en place de classes d'utilisateurs avec des facturations à la consommation ou forfaitaires avec surcoûts pour les dépassements de consommation (temps de communication, temps de traitements, occupation mémoire ou disques, volume des informations transférées, etc.)

1.1.3.3 Gestion de la sécurité (sûreté)

Elle doit répondre à deux types de problèmes :

- garantir les abonnés (utilisateurs)
  - les services et les ressources

- garantir le réseau lui même

contre les intrusions volontaires, agressives ou passives, mais aussi contre des actions involontaires mais dangereuses d'utilisateurs habilités.

Pour cela elle comporte les fonctions suivantes :

- création, suppression et contrôle des mécanismes et services de sécurité (identification, authentification, clés d'accès, groupes fermés d'abonnés, cryptage,...)

- diffusion des informations relatives à la sécurité

- compte rendu d'événements relatifs à la sécurité (audit)

La mise en œuvre des fonctions de sécurité ne fait pas à proprement parlé de la gestion de la sécurité.

1.1.3.4 Gestion des performances

Cette activité sert de base à la fourniture d'une qualité de service garantie. Pour cela elle traite des problèmes à moyen et à long terme. Elle analyse le trafic, le fonctionnement du réseau (débits, temps de réponses) et utilise ces informations pour régler le système en déterminant de nouvelles procédures d'acheminement par exemple et en les mettant en place ou, à long terme, en planifiant l'évolution du réseau (topologie, capacités des canaux).

Elle met en œuvre les fonctions suivantes :

- collecte des statistiques
- définition de la performance du système dans des conditions naturelles ou artificielles (mode dégradé)
- modification des modes de fonctionnement du système pour mener des activités de gestion de performances (acheminement par exemple).

Pour traiter ces fonctions elle doit traiter les données statistiques, modéliser le système et simuler son comportement.

1.1.3.5 Gestion de la configuration et des noms

Elle est à la base des quatre autres activités; elle leur permet de connaître tous les composants des systèmes et de les gérer. Elle permet de les désigner par leur adresse physique ou leur nom (adresse logique) et de maintenir la cohérence de ces noms . Ceux-ci sont consignés dans différents fichiers répartis dans les systèmes interconnectés et leur mises à jour doit en garder la cohérence; on utilise aussi des serveurs de noms, primaires et secondaires dont il faut aussi maintenir la cohérence.

Elle comporte les fonctions suivantes :

- établissement des paramètres contrôlant le fonctionnement normal du système
- association de noms aux objets de gestion ou à des ensembles d'objets de gestion
- initialisation et retrait d'objets de gestion
- récolte d'information sur l'état du système, périodiquement ou à la demande
- acquisition des notifications des modifications importantes de l'état du système
- modification de la configuration du système.

Par ces fonctions, elle permet de préparer, d'initialiser, de démarrer et de terminer les services d'interconnexion et d'en assurer la continuité de fonctionnement.

1.1.4 Portée et responsabilités

La portée des actions à traiter peut être divisée en quatre niveaux :

- planification
- analyse des performances
- gestion des problèmes et des ressources
- contrôle opérationnel

A chacun de ces niveaux sont associées des ressources humaines ayant des responsabilités propres.

1.1.4.1 Contrôle opérationnel

Il est chargé de la surveillance et du support technique du réseau; il est assuré par trois groupes de personnels.

Bureau d'aide

Il réalise l'interface avec les utilisateurs pour les conseiller et traiter les anomalies de type 1, par exemple les mises sous tension de certains composants, les problèmes de modems, les initialisations des coupleurs de communication (débit, parité, etc.). Ces anomalies de types 1 représentent environ 80% des problèmes rencontrés.

Opérateur réseau

Il s'occupe de la surveillance et de la commande du réseau. Il observe la charge du réseau, les anomalies, les incidents, les reprises automatiques etc. et collabore avec le support technique.

Support technique

Il traite les problèmes techniques liés à l'installation de nouveaux équipements ou à leur maintenance . Il fournit cette aide à la maintenance sur la demande du bureau d'aide ou des opérateurs. Partageant cette maintenance avec le fournisseur du matériel ou du logiciel, il analyse les anomalies et assiste le vendeur en cas de télémaintenance en temps réel sur le site. (Il est souvent difficile de savoir où est le cause réelle d'une anomalie observée).

Il traite les anomalies de type 2 qui représentent 10 à 15% des cas (en liaison avec les opérateurs).

1.1.4.2 Gestion des services, des ressources et des problèmes

L'équipe chargée de ces problèmes assure le contact avec les fournisseurs.

Elle réalise :

- l'inventaire des ressources
- l'ordonnancement des changements de topologie (niveau tactique)
- la mise en œuvre des modifications d'acheminement
- la gestion des services : sont-ils possibles, faut-il les ajouter ou en supprimer d'autres ?

La gestion des problèmes complexes (anomalies de type 3). Ceux-ci comportent les bogues logiciels, les différences de comportement entre systèmes, etc. Ces problèmes sont très vite résolus lorsqu'ils sont bien identifiés (par exemple erreur ou omission dans la documentation ...) ou alors très long à corriger.

1.1.4.3 Analyse des performances

Cette responsabilité travaille à moyen et à long terme.

Elle s'occupe

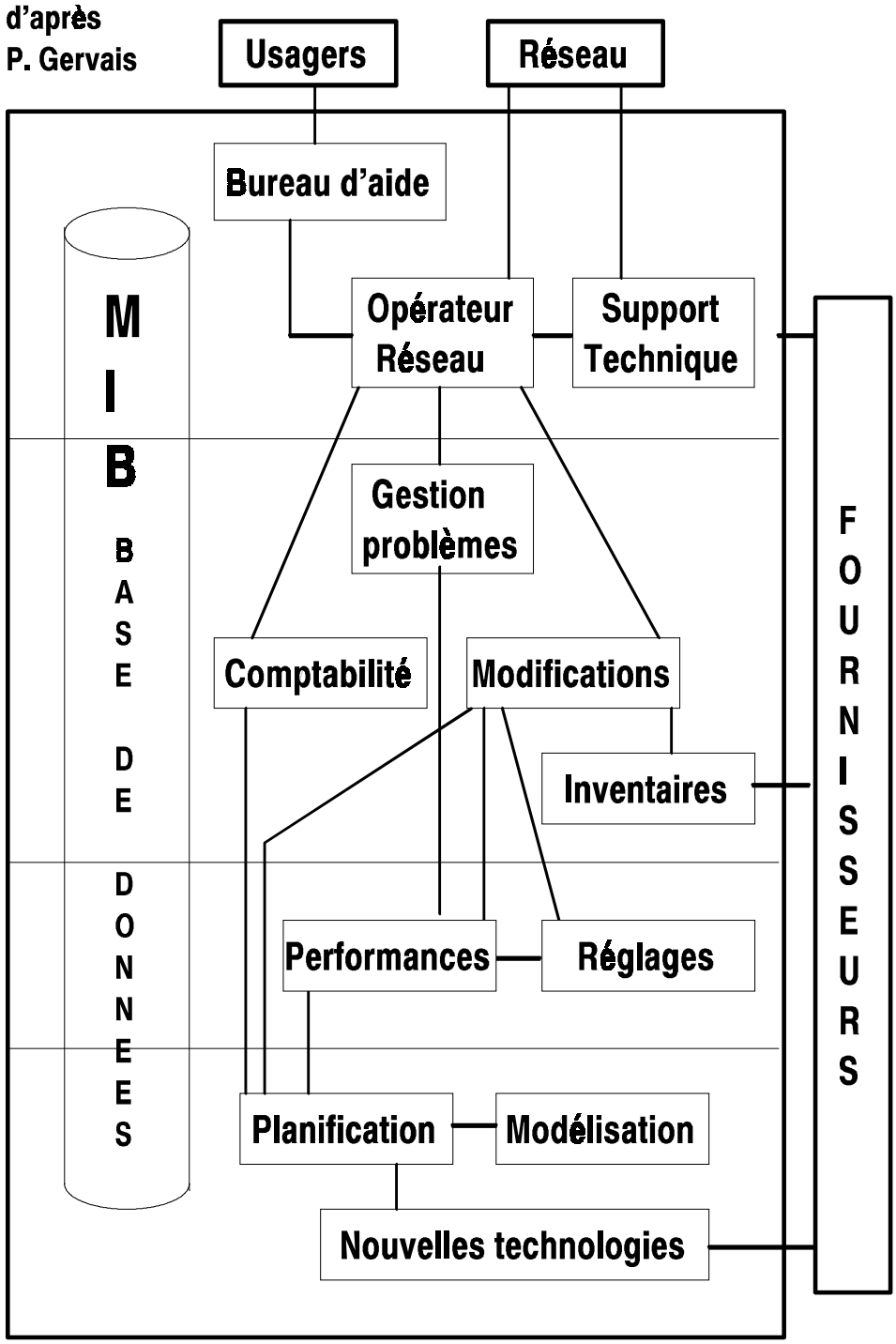
- de la mesure des performances
  - définition des objectifs à atteindre : temps de réponse, nombre de transactions journalières ou horaires, etc.;

- paramètres à prendre en compte, statistiques. Ces paramètres sont pris dans la base de données administrative. Il faut donc qu'elle demande qu'ils y soient consignés.

- des mesures à prendre pour améliorer ces performances
  - en particulier de l'élaboration des tables d'acheminement et des mesures à prendre pour les mettre en œuvre de manière coordonnée.

1.1.4.4 Planification

Elle traite des évolutions à long terme du réseau pour tenir compte des augmentations de trafic, soit pour la mise en œuvre de nouvelles techniques ou de nouveaux services par exemple le RNIS ou la messagerie X400...



Ces nouvelles techniques sont elles applicables à l'entreprise, sont elles disponibles, dans quels délais, à quels coûts, qu'elle est l'évolution prévisible de ces coûts ?

Ceci entraîne en général une modélisation du réseau et des études de comportement par simulation (ou calculs directs approchés)

Les responsables de la planification doivent être à l'écoute des tendances techniques et des besoins exprimés des utilisateurs ou ceux de l'entreprise.

1.1.5 Complexité du problème

L'administration de réseau est une activité très complexe car elle doit répondre globalement aux besoins d'un système distribué et hétérogène.

Cette hétérogénéité est à prendre en compte non seulement au niveau des communications (standards, équipements), mais aussi au niveau des systèmes et des utilisateurs (besoins divergents).

L'ADMINISTRATION DE RESEAU EST GLOBALE

Pour répondre à cette hétérogénéité et à la distribution du système le réseau est partitionné en domaines

- géographiques
- applicatifs
- selon les constructeurs (SNA, DSA, DECNET,etc)
- par normes (OSI, TCP/IP, SNA)

Il n'y a pas de règles générales pour décider de cette partition et celle-ci est souvent double (géographique/norme par exemple).

Cette partition en domaine entraîne un problème de localisation des responsabilités en particulier entre domaine public et domaines privés . Le réseau public apparaît souvent comme une tache blanche dans les domaines administrés qui sépare les domaines privés.

Dans un domaine qui administre ? Quelle est son autorité par rapport à l'administrateur central mais aussi par rapport aux responsables des systèmes informatiques ? Comment peut-il imposer les changements ? En général l'administrateur de réseau doit avoir une responsabilité supérieure au responsable système car il doit tenir compte de toutes les contraintes des systèmes interconnectés.

D'autre part l'administration de réseau doit fonctionner même en cas d'anomalie grave (panne) du réseau.

Pour cela celui-ci peut être maillé ou l'administration doit être supportée par un réseau d'administration distinct.

En cas de réseau d'administration disjoint, qui l'administre, quelles sont ses relations avec le réseau administré ? Quel est son coût (en général réseau public commuté comme réseau de télécommunication support)?

En cas de réseau maillé, quelle doit être sa configuration ? Quels sont les acheminements à prévoir en secours en cas de panne?

1.1.6 Partition en domaines

1.1.6.1 Types de systèmes et composants

Un système appartient à un ou plusieurs domaines. Il peut être système gestionnaire ou système géré (ou administré).

Un domaine doit comporter un système gestionnaire et un ou plusieurs systèmes gérés.

Un système peut être géré dans un domaine et gestionnaire dans un autre. On crée ainsi une relation hiérarchique entre domaines. Le découpage en domaines peut être complexe (par exemple domaines géographique et norme ou constructeur); il peut donc y avoir des "croisements", un système étant gestionnaire dans un domaine et géré dans l'autre et vice versa.

Dans un système gestionnaire on trouve :

- une base de donnée administrative (MIB : management information base) qui contient les objets du système et leurs attributs

- des processus qui permettent l'exécution des fonctions de base (extraction des informations, rangement dans la MIB directement ou après prétraitement) ou qui supportent les outils logiciels de traitement de ces données

- un langage pour les interactions avec les opérateurs

Dans un système géré on ne trouve que :

- une base de données administrative (MIB)
- les fonctions de base

Les traitements sont faits dans le système gestionnaire après transfert depuis le système géré. On doit donc disposer aussi d'un protocole de communication

1.1.6.2 Processus gestionnaire et processus agent

Dans un système géré on dispose d'un processus agent chargé de traiter les objets administrés et leurs attributs.

Dans un système gestionnaire on dispose d'un processus gestionnaire chargé de l'administration de domaine et d'un processus agent chargé des objets locaux. Le processus gestionnaire communique avec les processus agents distants ou l'agent local.

Un domaine existe s'il a au moins un processus gestionnaire et un ou plusieurs processus agents.

Les objets d'un système ne peuvent être manipulés que par l'intermédiaire d'un processus agent. Ils peuvent être raccordés à plusieurs de ces processus.

1.1.6.3 Réseau d'administration et réseau administré

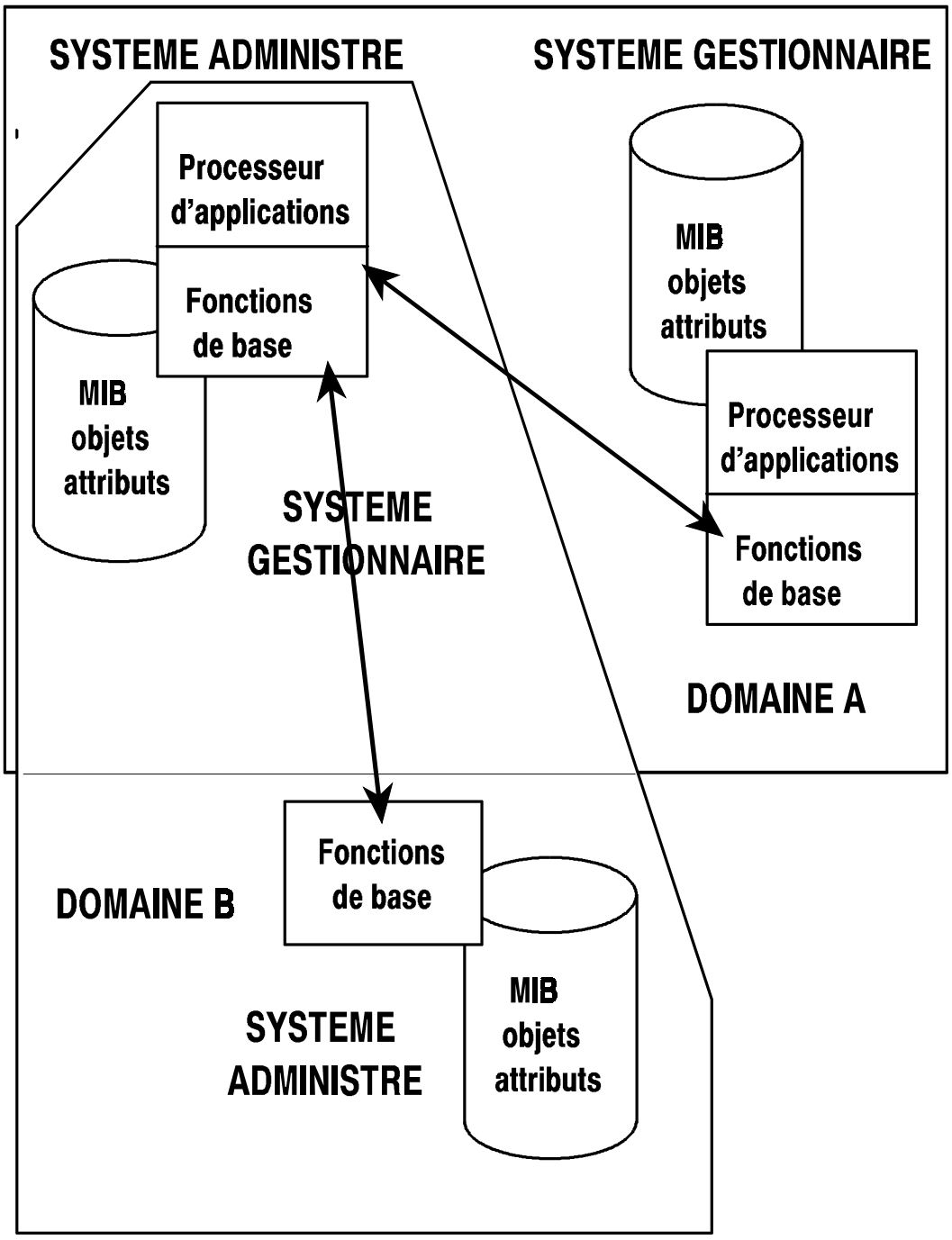
Depuis un système central, système gestionnaire du domaine principal, on peut atteindre

- les nœuds de ce domaine
- les racines des sous-domaines

Ces racines rapatrient et condensent les données administratives de ces sous-domaines

Depuis un nœud (système géré avec son processus agent) on traite des objets. Ces objets sont le passage obligé pour atteindre les informations administratives, codées dans les attributs de ces objets. Les objets représentent le réseau administré et l'ensemble des processus d'administration et des protocoles qui les relient constituent le réseau d'administration.

Ainsi toutes les informations d'administration peuvent remonter à un point focal d'où est géré l'ensemble des domaines.



Cette architecture est entièrement orientée objet. Le modèle OSI d'administration de réseau fournit les bases et les fonctions pour la réaliser.

1.2 Administration OSI

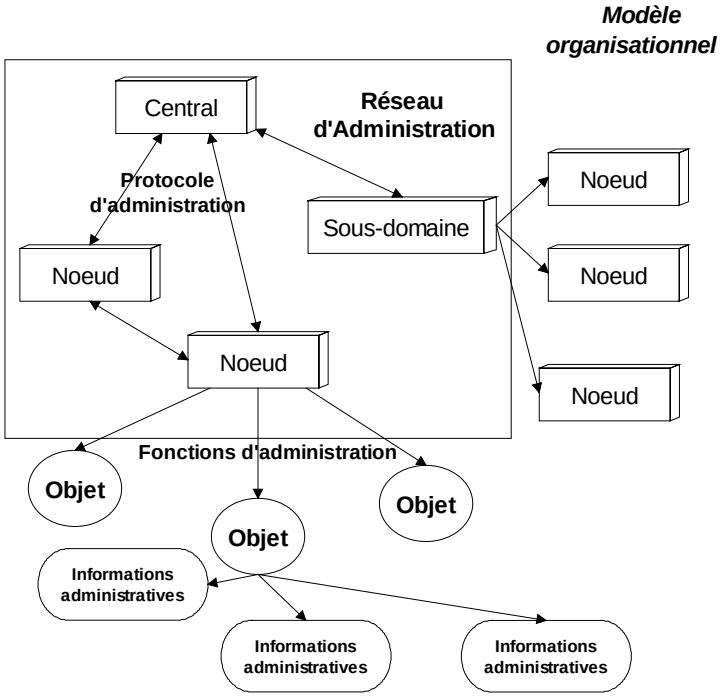
Nota : Les travaux de l'OSI dans le domaine de l'administration de réseaux ont été menés dans deux directions :

- Etudes des principes de base et définition d'une architecture, de services et de protocoles.

- Etude et définitions précises des objets administrés et de leurs attributs. Cette seconde partie a été réalisée par un ensemble de constructeurs regroupés dans l'OSI-NMF : Network Management Forum. Les premiers documents de NMF ne sont disponibles que depuis fin 1990 . Le chapitre ci-dessous ne tient pas encore compte de ces travaux .

L'administration de réseaux OSI repose sur trois modèles :

- un modèle fonctionnel
- un modèle organisationnel
- un modèle opérationnel



Le modèle fonctionnel reprend les grandes fonctionnalités déjà décrites :

- gestion des anomalies
- gestion de la comptabilité
- gestion de la sécurité
- gestion des performances
- gestion de la configuration et des noms

Comme nous le verrons, l'administration de réseaux OSI repose sur la notion d'objets gérés. Des standards décrivent aussi les fonctionnalités applicables à ces objets (voir ci-dessous).

Le modèle opérationnel ou d'information porte sur la description du réseau informatique en terme d'objets avec leurs caractéristiques, les opérations possibles sur ces objets et la manipulation des informations administratives à travers cette structuration en objets (attributs, méthodes (opérations, notifications, comportements), héritage, etc.)

Le modèle organisationnel reprend le découpage en domaines d'administration (par autorité, normes, géographique ou par organismes,...) et la hiérarchisation (partielle) de ces domaines.

Il décrit aussi la mise en œuvre des opérations sur les objets grâce à

- une architecture du logiciel d'administration
- des protocoles d'administration

1.2.1 Modèle d'information

Il est articulé autour de la notion d'objet géré

1.2.1.1 Définition

Un objet est l'abstraction d'un composant physique ou logique . Il est caractérisé par
- un nom
- des attributs
- des opérations
- des notifications sur ces attributs

Appliqué à l'administration de réseaux on parlera d'objet géré, sous-ensemble des objets du système.

Le modèle d'information OSI est décrit dans le projet de standard DP 10165-1

On doit distinguer objet géré et ressource. L'objet géré est visible de l'administration de réseaux. Les ressources ne sont visibles qu'à la surface (boundary) de l'objet géré et traitées de manière interne. Seule cette partie visible est accessible.

Les objets sont regroupés en classes d'objets gérés. Seuls les aspects suivants sont visibles

- attributs visibles à la surface
- opérations applicables
- comportement en réponse à une opération
- notification émise par l'objet géré
- "packages" conditionnels encapsulés dans l'objet
- position de la classe d'objets dans la hiérarchie d'héritage
- spécification des objets allomorphes avec la classe (voir ci-dessous).

1.2.1.1.1 Principes

Encapsulation

L'encapsulation assure l'intégrité d'un objet. Toutes les opérations passent par l'envoi d'un message à un objet. L'opération est interne et non visible sauf par la vue à la surface des attributs, notifications et opérations.

Héritage et classes d'objets

Les instances d'un objet géré qui partagent les mêmes attributs, opérations, notifications, comportement et package font partie de la même classe.

Une classe peut être une extension d'une autre classe par ajout d'attributs, opérations, notifications etc.

On définit ainsi des sous-classes de plus en plus spécialisées.

Une sous-classe hérite de tous les attributs, etc. de sa superclasse. La superclasse ultime est TOP; elle ne comporte aucun attribut ni autre propriété.

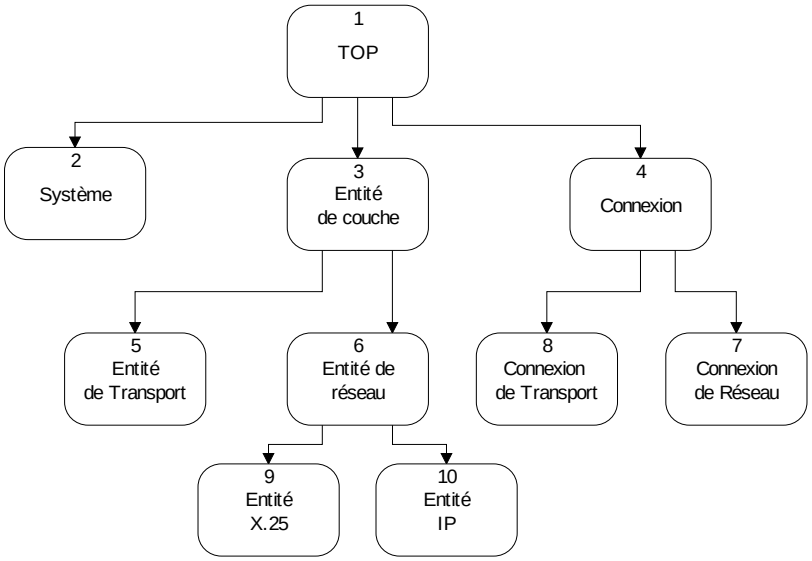
Un objet peut appartenir à plusieurs classes.

Une même sous-classe peut être spécialisée à partie de plusieurs superclasses (optionnel).

Allomorphisme

L'allomorphisme représente la capacité pour une instance d'une sous-classe (sous-classe allomorphe) d'avoir un comportement comparable à celui de sa superclasse tel qu'observé par le protocole d'administration du système.

L'allomorphisme permet d'étendre la définition d'une classe d'objets pour permettre l'interopérabilité avec des administrations ou des objets gérés qui ne supportent pas l'extension de cette sous-classe. Ceci permet la migration des versions.



Cette extension peut se faire par

- addition d'attributs
- extension de portée des attributs
- restriction de portée des attributs
- ajout d'actions ou de notifications
- ajout d'arguments aux actions et notifications
- extension ou restriction sur la portée des arguments

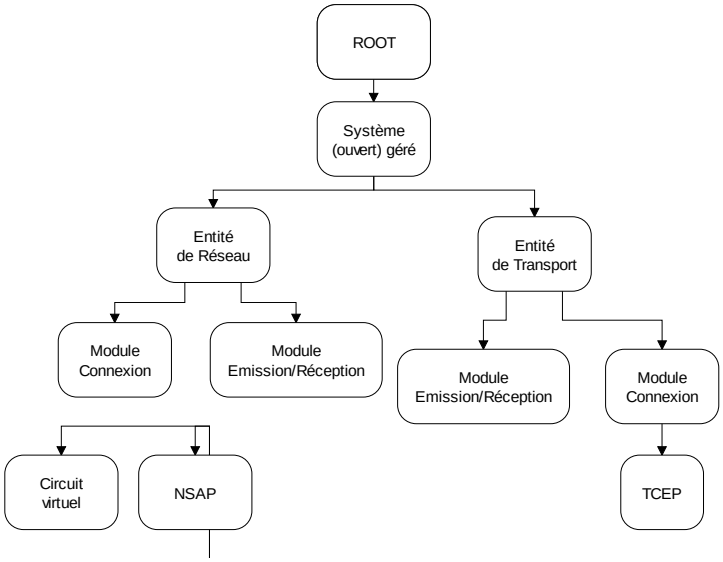
Nous reviendrons plus loin sur les propriétés des objets et de leurs attributs.

1.2.2 Contenance et nommage

Un objet géré d'une classe peut **contenir** des objets gérés de la même ou d'autres classes. Cette relation est appelée contenance. Les objets contenus sont désignés comme étant des objets gérés subordonnés. On définit ainsi une seconde arborescence.

Un objet est subordonné à un objet **supérieur**. Le supérieur ultime est ROOT.

Cette relation de contenance permet de modéliser la hiérarchie du monde réel (assemblage de composants) ou une hiérarchie organisationnelle (répertoires, fichiers, enregistrements par exemple).

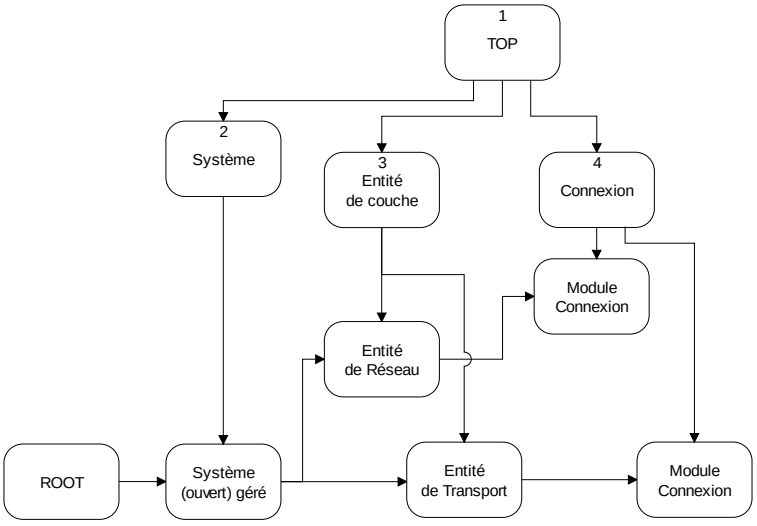


La relation de contenance peut définir un comportement statique ou dynamique de l'objet supérieur et de ses subordonnés.

Cet arbre de contenance est "orthogonal" à l'arbre hiérarchique. Il permet le nommage des objets.

Le nommage est hiérarchique. Un objet subordonné est nommé par :

- le nom de son supérieur
- un identificateur unique de subordonné dans la portée de contenance (du supérieur).



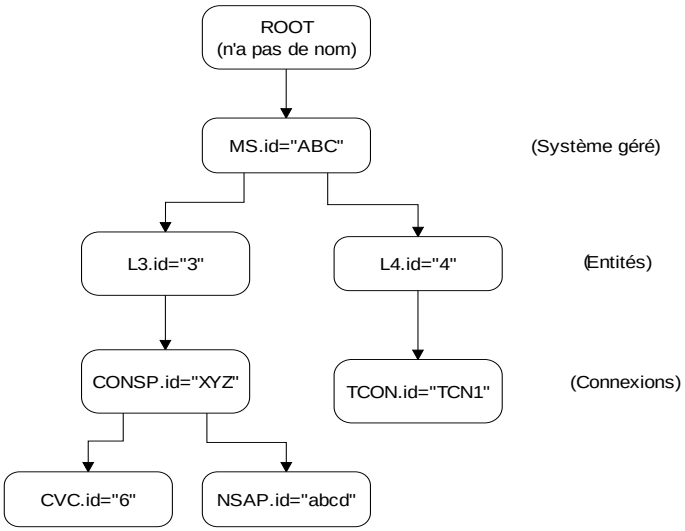
Ce nom peut être non ambigu dans un contexte de nommage local mais il lui peut être difficile de le rester dans des contextes très vastes. Il faut nommer de manière non ambiguë ces contextes (par exemple Domaine) et associer un nom de contexte.

Un objet géré ne peut exister que si son supérieur existe (créé et non détruit). L'objet ultime ROOT est un objet nul qui existe toujours.

Les instances de classes d'objets gérés supérieurs qui peuvent être utilisées pour le nommage d'instances de classes d'objets sont identifiées en utilisant une "**agrégation de noms" (names binding).**
Ces règles de nommage constituent le schéma de nommage. On utilise deux types de noms :

- le nom relatif (relative distinguished name)
  - le nom absolu (global " «)

Une instance d'une classe d'objets gérés doit posséder au moins un attribut utilisable pour le nom relatif.



Noms relatifs	Noms absolus
MS.id = "ABC" L3.id = "3" CONSP.id = "XYZ" CVC.id = "6"	MS.id = "ABC" [MS.id="ABC",L3.id="3"] [MS.id="ABC",L3.id="3",CONSP.id="XYZ"] [MS.id="ABC",L3.id="3",CONSP.id="XYZ",CVC,id="6"]

Ainsi le nom global est bien un "agrégat" de noms relatifs.

Chaque attribut d'un objet géré est identifié par un identificateur, qui le distingue des autres attributs de l'objet. Cet identificateur est associé à l'attribut lui-même et non à son type.

1.2.3 Caractéristiques des objets

1.2.3.1 Attributs

Les attributs expriment les **propriétés** des objets gérés. Un attribut a une structure (ensemble ou séquence d'éléments) et prend une valeur particulière par une assertion de valeur d'attribut (AVA).

En général la valeur d'un attribut est observable (à la surface de l'objet); elle peut déterminer, à la suite d'une opération, ou refléter, par une notification, le comportement de l'objet.

Un attribut ne peut contenir ni un objet ni un autre attribut Il est nommé de manière non ambiguë

Il est lu ou modifié de façon atomique par les opérations GET et SET (ensemble minimal) ou des opérations supplémentaires.

Toutes les opérations qui l'affectent sont faites de manière indirecte via l'objet contenant. Si une opération porte sur plusieurs attributs, un système de synchronisation, géré par l'objet contenant, doit être mis en place.

L'attribut participe à l'héritage **et** à la contenance.

Il peut être obligatoire ou contenu dans un "package" conditionnel. Les attributs obligatoires sont toujours présents dans les instances des objets gérés d'une classe donnée.

Si un attribut est hérité d'une superclasse, il doit avoir un type abstrait qui possède le même ensemble d'opérations que celui de sa superclasse.

Il est possible de définir des groupes d'attributs.

Attributs de base

Cinq attributs sont définis pour tous les objets gérés :

Nom
Cet attribut permet au système gestionnaire de déterminer l'identificateur et la valeur du nom relatif de l'objet géré.

Classe d'objet
identifie la classe actuelle de l'objet géré

Superclasses allomorphes
Identifie l'ensemble des superclasses allomorphes à la classe de l'objet.

Chaînage de nom
Identifie les classes d'objets gérés qui peuvent être nommées à partir de cet objet.

Package
Identifie les packages qui ont été instanciés.

On trouvera ci-dessous une définition de cette caractéristique des objets gérés.

1.2.3.2 Opérations

Il existe 2 types d'opérations :

- celles qui portent sur les attributs
- celles qui portent sur l'objet dans son ensemble.

Opérations sur les attributs :

GET lire la valeur; toujours applicable à un objet lisible.
REPLACE remplacer une valeur d'attribut (si il est inscriptible); ne s'applique pas aux groupes d'attributs.
SET to default remettre la valeur par défaut; s'applique à tous les attributs inscriptibles.
ADD member ajoute des membres fournis par l'opération à un attribut inscriptible et déjà positionné.
REMOVE member retire des membres à l'ensemble des membres d'un attribut positionné.

Opérations globales :

CREATE crée et initialise un objet d'une classe spécifiée en utilisant la hiérarchie de nommage.
DELETE permet de supprimé un objet (s'il n'a plus d'objets subordonnés)
ACTION demande à un objet d'exécuter une action complexe donnée et, éventuellement, de lui en indiquer le résultat.

1.2.3.3 Notifications

Les objets gérés émettent "spontanément" des notifications lorsque des événements internes ou externes surviennent.

Ces notifications sont spécifiques de l'objet. Elles portent des informations définies dans l'objet.

1.2.3.4 Filtres

Les filtres permettent de spécifier des critères auxquels l'objet géré doit satisfaire pour qu'une opération soit exécutée.

Ils permettent la sélection d'objets multiples pour l'exécution d'opérations identiques sur ces objets.

Un filtre s'exprime en termes d'assertions et est satisfait seulement si la réponse à cette assertion est "TRUE". (Il a un comportement similaire à un prédicat)

Les opérateurs suivants sont utilisés par les filtres:
- and, or, not
- tests =, <, >, présent, sous chaîne de, sous-ensemble de, surensemble de, intersection d'ensembles non nulle

1.2.3.5 Comportement

Il définit :

- la sémantique des attributs, notifications, opérations.

- la réponse aux opérations invoquées
- les circonstances dans lesquelles les notifications sont émises
- les dépendances entre valeurs d'attributs particuliers
- les effets des relations sur les autres objets gérés.

1.2.3.6 Packages conditionnels

Un package (conditionnel) est une collection d'attributs optionnels, de notifications, d'opérations et de comportements qui sont tous présents ou absents simultanément. Cette présence (ou absence) est conditionnée par les capacités des ressources de niveau inférieur (par exemple : options dans un protocole de communication).

Pour un tel package une seule instance peut exister. Il n'est donc pas besoin d'un chaînage de nom.

Il ne peut être instancié que si il est encapsulé; cette instanciation est réalisée avec l'objet (les opérations passent toujours par l'objet et ne s'appliquent pas directement au package

1.2.4 Architecture d'administration OSI

L'administration de réseaux OSI supporte la partition en domaine. Elle est donc répartie sur des systèmes gestionnaires et des systèmes gérés.

Dans les systèmes gérés un processus agent traite les objets gérés.

Dans les systèmes gestionnaires on trouve aussi un processus agent pour administrer les objets locaux. Un processus gestionnaire administre l'ensemble du domaine.

Les processus agents réalisent les opérations sur les objets et à travers eux sur leurs attributs. Ils transmettent les notifications.

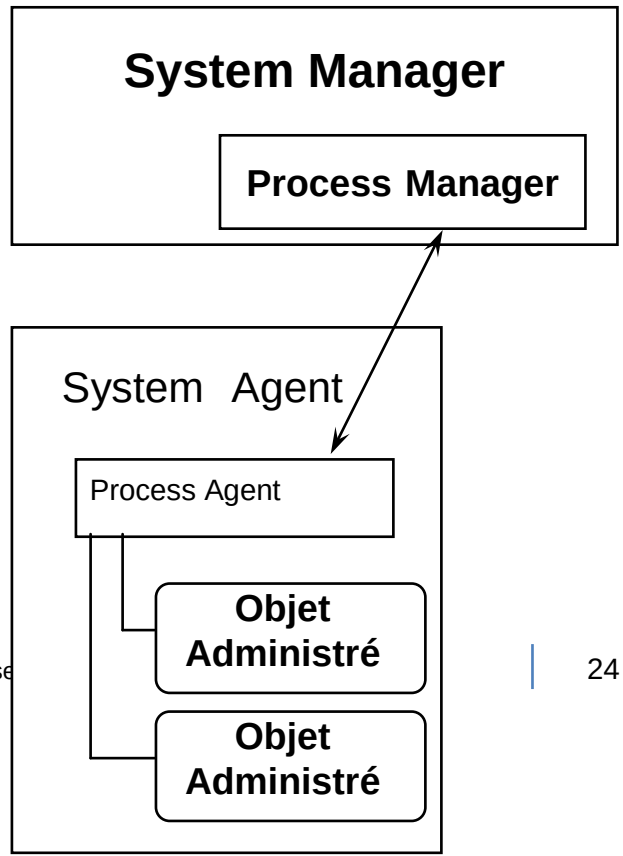
1.2.4.1 Structure de la gestion de réseau OSI

La gestion de réseau OSI est réalisée par

- la gestion-système
- la gestion de couche (N)
- les opérations de couche (N)

Les opérations de couche (N) sont intégrées aux entités de communication de niveau (N).

La gestion de couche (N) est réalisée par une entité d'administration spécifique placée au niveau (N) à coté des entités de communication de ces niveaux.



La gestion-système est réalisée par des entités de la couches Application (niveau 7 OSI).

Les protocoles de gestion de couche ne devraient être utilisés que si des besoins spéciaux rendent inappropriés les protocoles de gestion-système ou si ils ne sont pas disponibles. C'est en particulier le cas pour les commutateurs de paquets ou les ponts de niveau 3 OSI; sur ces systèmes on ne peut installer de gestion-système au niveau 7. Les problèmes d'acheminement qui relèvent de l'administration de réseaux et qui sont mis en œuvre dans ces équipements relèvent dont de la gestion de couche ou d'opérations de couche.

Les opérations de couche peuvent exister dans les 7 couches du modèle de Référence. Les informations transportées doivent être distinguables des données utilisateur. Cette distinction incombe au protocole de niveau N. Par exemple des paramètres de taxation sont transportés au niveau 3 OSI dans des champs de facilités.

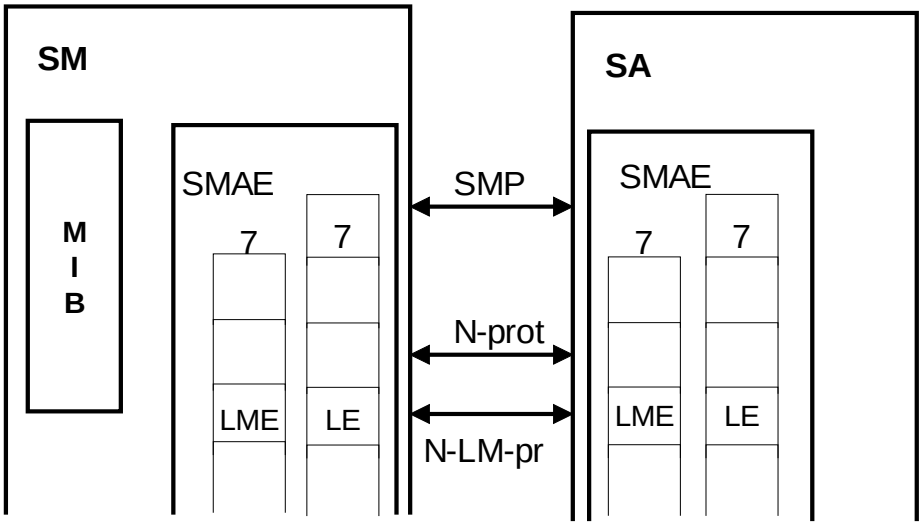
Ces informations ont pour but de commander er de surveiller une **instance de communication unique**. Elles comportent :

- des paramètres dans les PDU de connexion ou d'association
- des paramètres de PDU particulières qui peuvent modifier le comportement de cette instance de communication
- des informations d'anomalies
- des paramètres des PDU de terminaison ou de rupture d'association relatifs à l'instance qui se termine.

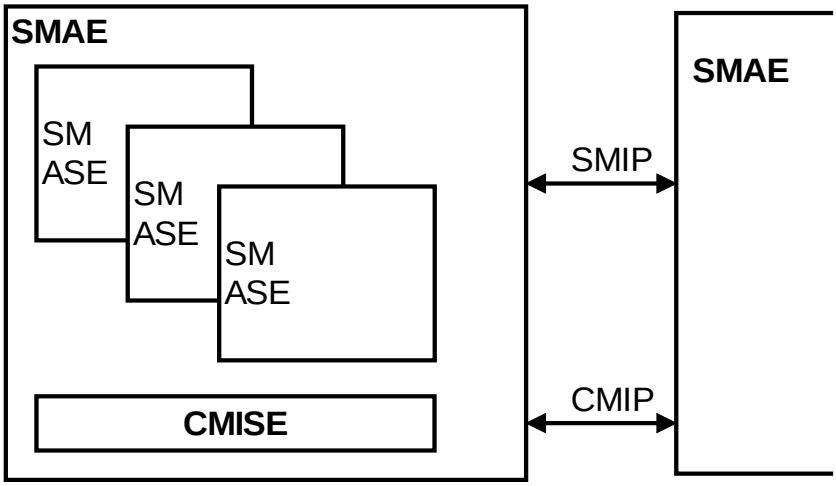
L'essentiel de l'administration de réseaux est traité par la gestion système.

Les schémas ci-dessous illustrent l'architecture de l'administration de réseaux OSI. L'architecture de la gestion-système suit les normes de l'ALS (architecture de la couche Application). Elle comporte un service commun : CMIS et des entités spécifiques d'administration (SMAE).

Modèle Architectural



SMAE : System Management Application Entity



SMIP : System Management Information Protocol
CMIP : Common Management Information Protocol
SM ASE : System Management Service Element

1.2.4.2 Base de données de gestion : MIB

Dans chaque système, une MIB représente les informations qui peuvent être transférées par les protocoles de gestion OSI (gestion système, gestion de couches) ou qui sont concernées par l'utilisation de ces protocoles.

La MIB est constituée par l'ensemble des objets gérés dans un système ouvert. Seuls les objets de l'environnement OSI entrent dans le cadre de la normalisation, qui ne s'applique qu'à leur structure logique. Cependant la MIB peut contenir d'autres objets.

Ceci ne suppose rien non plus quant à la forme de stockage physique ou logique dont la réalisation est locale et propre à chaque système.

Les informations de gestion peuvent être partagées ou structurées suivant les besoins des processus de gestion. Elles peuvent être stockées à l'état brut ou après traitement.

1.2.4.3 Gestion système

Elle fournit les mécanismes nécessaires à la surveillance, au contrôle et à la coordination des objets de gestion par l'utilisation de protocoles dans la couche Application :

- par des entités d'application de gestion-système : SMAE
- par une entité commune d'application : CMISE

Le logiciel de communication doit offrir les fonctionnalités suffisantes pour supporter CMISE et les SMAE (sinon on ne peut utiliser que les systèmes de gestion de couche pour les couches supportées).

La majorité des échanges d'information de gestion entre systèmes ouverts nécessite la négociation d'un contexte de présentation particulier et l'établissement d'une session supportée par un transport fiable. Elle est donc supportée par la couche Application. Ceci n'exclut pas un service en mode sans connexion.

1.2.4.4 Gestion de couche (N)

Elle assure, si nécessaire, la surveillance, le contrôle et la coordination des objets de la couche (N).

Ses protocoles sont pris en charge par le service (N-1). Elle ne fournit aucun service au niveau (N+1).

Ces protocoles assurent :

- la communication de valeurs de paramètres liés aux objets de la couche (N)
- le test des fonctions fournies par le service (N-1)
- le transport d'informations d'erreur pour gérer les anomalies et les diagnostics.

1.2.5 Le service commun d'administration OSI: CMISE

Ce service commun, inclus dans la couche Application fournit aux SMAE un certains nombre de fonctions; pour les fonctions d'association et de rupture, ces entités doivent faire appel au service ACSE, par les primitives AASSOCIATE, A-RELEASE, A-ABORT.

CMISE fournit 2 types principaux de transfert d'information :

- un service de notifications de gestion
- un service d'opérations de gestion

Plus 2 services additionnels

- un service de réponses multiples pour confirmer les réponses qui lui seront liées

- un service d'opérations multiples sur des objets gérés multiples qui doivent satisfaire à des critères communs et sont sujets à des conditions de synchronisation.

Ces services sont :

Notifications

M-EVENT-REPORT	confirmé ou non

Opérations

M-GET	confirmé
M-SET	confirmé ou non
M-ACTION	confirmé ou non
M-CREATE	confirmé
M-DELETE	confirmé

Les services **M-CREATE** et **M-DELETE** agissent sur les objets globaux; elles servent à les créer et les supprimer.

Les autres services affectent les attributs des objets via ceux-ci.

M-EVENT-REPORT rapporte un événement affectant un objet
M-GET demande des informations de gestion à une entité paire
M-SET modifie des informations de gestion sur une entité paire
M-ACTION demande l'exécution d'une action complexe à une entité paire.

Les noms des instances des objets gérés sont organisés hiérarchiquement selon un **arbre d'informations de gestion.**

Des opérateurs de filtrage permettent de tester la présence ou la valeur d'attributs.

Un paramètre de synchronisation est fourni pour permettre d'indiquer la manière de synchroniser les opérations dans une instance d'un objet géré, lorsque des opérations multiples sont sélectionnées par filtre.
Deux types de synchronisation sont supportés :
- atomique
- effort maximal (best effort)

CMISE est organisé en unités fonctionnelles :

- une unité fonctionnelle noyau traite tous les services de base listés ci-dessus.

- des unités fonctionnelles additionnelles permettent d'étendre le service :

  - sélection d'objets multiples
  - filtre
  - réponses multiples
  - service étendu (qui permet d'accéder au service P_DATA de la couche Présentation)

Les deux exemples ci-dessous, donnés à titre indicatif, montrent des primitives associées aux services M-EVENT-REPORT et M-CREATE et leurs paramètres.

Notations :

Req/Ind requête ou indication
Resp/Conf réponse ou

confirmation

M	obligatoire
U	utilisateur
C	conditionnel
=	identique à la requête

M-EVENT- REPORT	Req/Ind	Resp/Conf
invoke identifier	M	M=
mode		M
classe d'objet géré	M	U
instance d'objet géré	M	U
type d'événement	M	C=
instant de l'événement	U	
info. sur l'événement	U	
temps courant		U
réponse à l'événement		C
erreurs		C

M-CREATE	Req/Ind	Resp/Conf
invoke identifier	M	M=
classe d'objet géré	M	C
instance d'objet géré	U	C
instance d'objet supérieur	U	
contrôle d'accès	U	
instances d'objets inférieurs	U	
liste d'attributs	U	C
temps courant		U
erreurs		C

1.2.6 Protocol CMIP

Le service CMISE est rendu par des entités d'Application qui mettent en œuvre le protocole CMIP : Common Management Information Protocol.

Ce protocole utilise les services Application

- ACSE
- ROSE
- et le service Présentation P-DATA

Le service ACSE est mis en œuvre pour établir et rompre les associations. L'association utilisée est de classe 3.

Le service ROSE est utilisé pour les opérations et les notifications. Les services

- RO-Invoke
- RO-Result
- RO-error
- RO-Reject

Sont mis en œuvre. Les opérations confirmées sont de classe 2 : asynchrone (retour immédiat) ou 1 : synchrone (retour en fin d'échange). Les opérations non confirmées sont de classe 5 : synchrone avec sortie non rapportée.
CMIP définit donc un ensemble d'opérations qui seront transmises pour exécution par ROSE.

Chaque opération est décrite de ASN1.

Elle est reliée à une primitive CMISE et soumise à ROSE par RO-Invoke (opération).

Exemple : Description du service M-EVENT-REPORT

Procédure.

Sur réception de la primitive M-EVENT-REPORT, la machine CMIP doit :

- en mode confirmé, émettre une APDU demandant l'opération m-EventReport-Confirmed ou
- en mode non confirmé, émettre une APDU demandant l'opération m-EventReport

  - envoyer cette opération en utilisant la procédure RO-INVOKE

  - A la réception de cette APDU, la machine CMIP émet une indication M-EVENT-REPORT à l'utilisateur de CMISE.

En mode confirmé, cet utilisateur fournit une réponse à partie de laquelle la machine CMIP construit une APDU confirmant cette notification

Si les paramètres de la réponse montrent que la notification a été acceptée, émet cette APDU en utilisant le service RO-RESULT (de ROSE); sinon elle émet cette APDU par le service RO-ERROR (de ROSE).

Quand la machine CMIP initiatrice reçoit cette APDU elle transmet, si elle est bien formée, la confirmation correspondante à l'utilisateur de CMISE. Sinon elle construit une APDU contenant notification de l'erreur et l'envoie en utilisant RO-REJECT-U.

Structure des APDU m-EventReport et m-EvenrReport-Confirmed

```
IMPORTS
  OPERATION, ERROR FROM Remote-Operation-Notation

  DistinguishedName, RDNSequence FROM
                                        InformationFramework


m-EventReport        OPERATION
 ARGUMENT EventReportArgument
```

```
  ::= localValue 0

m-EventReport-Confirmed        OPERATION
  ARGUMENT EventReportArgument
  RESULT              EventReportResult      -- optionnel
                        ERRORS
                       {invalidArgumentValue,noSuchArgument,noSuchEventTyp
                       e,noSuchObjectClass,noSuchObjectInstance,processingFa
                       ilure }
                        ::= localValue 1


                       invalidArgumentValue        ERROR
                        PARAMETER InvalidArgumentValue
                        ::= localValue 15

                       noSuchArgument                    ERROR
                        PARAMETER NoSuchArgument
                        ::= localValue 14

noSuchEventType          ERROR
  PARAMETER         NoSuchEventType
  ::= localValue 13

noSuchObjectClass        ERROR
  PARAMETER         ObjectClass
  ::= localValue 0

noSuchObjectInstance     ERROR
  PARAMETER         ObjectInstance
  ::= localValue 1

processinfFailure          ERROR
  PARAMETER         ProcessingFailue  -- optionnel
  ::= localValue 10


EventReply     ::= SEQUENCE {
        eventType           EventTypeId,
        eventReplyInfo      [8]       ANY       DEFINED       BY       eventType
                                                 OPTIONAL }

EventReportArgument      ::= SEQUENCE {
        managedObjectClass            ObjectClass,
        managedObjectInstance ObjectInstance,
        eventTime     [5] IMPLICIT GeneralizedTime
                                                 OPTIONAL,
        eventType     EventTypeId,
        eventInfo     [8] ANY DEFINED BY eventType
                      OPTIONAL }

EventReportResult  ::= SEQUENCE {
```

```
        managedObjectClass                  ObjectClass     OPTIONAL
        managedObjectInstance           ObjectInstance      OPTIONAL
        currentTime     [5]IMPLICIT     GeneralizedTime     OPTIONAL
        eventReply   EventReply OPTIONAL}

EventTypeID  ::= CHOICE {
        globalForm          [6]     IMPLICIT    OBJECT      IDENTIFIER
        localForm       [7] IMPLICIT INTEGER }

InvalidArgumentValue    ::= CHOICE {
        actionValue             [0]             IMPLICIT            ActionInfo
        eventValue  [1] IMPLICIT SEQUENCE {
        eventType  EventTypeId
        eventInfo  [8] ANY DEFINED BY eventType OPTIONAL }}

NoSuchArgument          ::= CHOICE {
        actionId  [0] IMPLICIT SEQUENCE {
        managedObjectClass    ObjectClass OPTIONAL,
        actionType          ActionTypeId }
        eventId       [1] IMPLICIT SEQUENCE {
        managedObjectClass    ObjectClass OPTIONAL,
          eventType             EventTypeId }}

NoSuchEventType ::= SEQUENCE {
        managedObjectClass    ObjectClass                                   ,
          eventType             EventTypeId }

ObjectClass   ::= CHOICE {
        globalForm          [0]     IMPLICIT    OBJECT      IDENTIFIER
        localForm       [1] IMPLICIT INTEGER }

ObjectInstance      ::= CHOICE {
        distinguishedName       [2] IMPLICIT DistinguishedName,
        nonSpecificForm   [3] IMPLICIT OCTET STRING,
        localDistinguishedName [4] IMPLICIT RDN Sequence}

ProcessingFailure   ::= SEQUENCE {
        managedObjectClass    ObjectClass,
        managedObjectInstance ObjectInstance OPTIONAL
        specificErrorInfo    [5] ANY DEFINED BY
                                    managedObjectClass }
```

1.2.7 Gestion-Systeme

Nous n'étudierons pas en détail tous les aspects de la gestion-système.
La description des services correspondants est en cours de normalisation et réalisée dans les divers documents du projet de standard 10164-x.

Les structures de données correspondant aux protocoles sont fournies dans les projets de standard 10165-x.

1.2.7.1 Fonctions (actuellement) supportées

Neuf fonctionnalités sont en cours de spécification. Cinq d'entre elles sont déjà publiées :

- Gestion d'objets
- Gestion d'état
- Gestion des relations
- Compte-rendu d'alarmes
- Compte-rendu d'événements

- Contrôle d'archivage (log)
- Compte-rendu d'alarmes de sécurité
- Synthèse de mesures
- Synthèse de diagnostics

Nous étudierons plus particulièrement les trois premières.

1.2.7.2 Gestion d'objets

Il s'agit d'une fonctionnalité "passe tout droit" (pass-through).

Elle comporte 6 primitives :

- P-create
- P-delete
- P-action
- P-set
  - replace
  - add
  - remove
  - set-to-default
- P-get
- P-event (notifications)

Les objets gérés suivent le modèle d'information décrit plus haut avec leurs caractéristiques

- attributs
- opérations
- comportements
- notifications
- packages conditionnels
- position dans la hiérarchie d'héritage
- allomorphisme

1.2.7.3 Gestion d'états

La gestion d'états traite de la disponibilité des objets du point de vue de leur :

- opérabilité
- usage
- administration

Ces états sont consignés dans deux attributs :

- état opérationnel (opérabilité et usage)

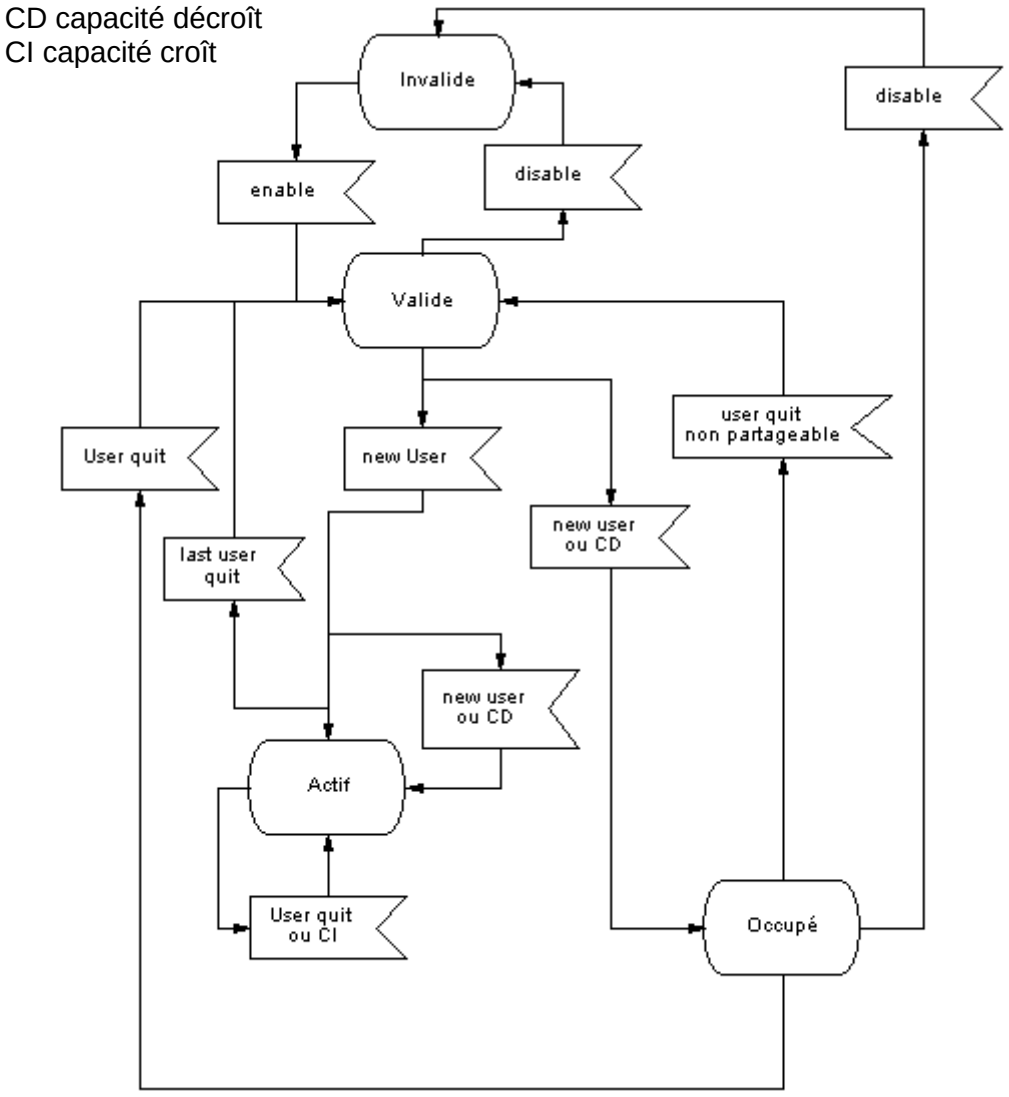
état administratif

L'ensemble de ces deux attributs constitue l'état de gestion.

Etat opérationnel

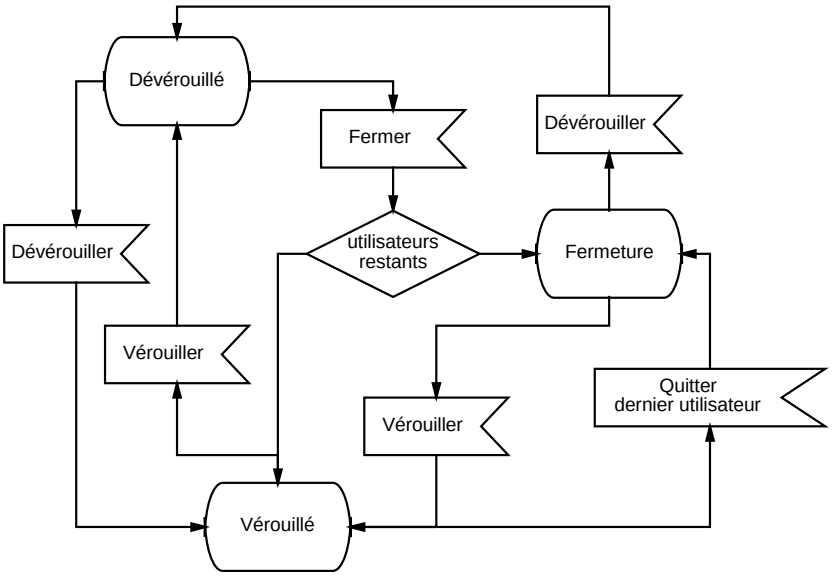
Il peut prendre 4 valeurs :
- invalide (opérabilité)
- valide
- actif (usage)
- occupé

Ces états sont "read-only". Ils ne peuvent pas être modifiés par l'administration de réseaux.



Etat administratif

Il peut prendre 3 valeurs :
- verrouillé
- déverrouillé
- fermeture (en cours)



Etat de gestion

Combinaison des deux états précédents, il peut prendre 10 valeurs. Les états actif-verrouillé et occupé-verrouillé sont interdits. Deux états invalide-fermeture et valide-fermeture sont temporaires et ont une transition spontanée vers les états respectifs invalide-verrouillé et valide-verrouillé.

opérationnel administratif	INVALIDE	VALIDE	ACTIF	OCCUPE
VEROUILLE	Invalide Verrouillé	Valide Verrouillé	impossible	impossible
FERMETURE	basculement automatique vers invalide occupé	basculement automatique vers valide occupé	Actif Fermeture	Occupé Fermeture
DEVEROUILLE	Invalide Déverrouillé	Valide Déverrouillé	Actif Déverrouillé	Occupé Déverrouillé

"Santé" (Health)

Un attribut "santé" contient des informations plus détaillées sur cet état de gestion; il peut prendre les valeurs :

- anomalie rapportée
- en faute
- en réparation
- réservé pour test

- en tests
- non installé
- jamais installé
- jamais utilisé
- hors tension
- hors ligne
- hors usage (après un temps limite)
- initialisation incomplète
- initialisation requise

Un attribut groupe d'états contient l'état de gestion et la santé de l'objet.

1.2.7.4 Gestion des relations

Une relation (relationship) décrit comment une opération portant sur une partie d'un système affecte les opérations d'un autre système.

Cette relation peut être
directe
ou indirecte (via un objet intermédiaire)

Elle peut être aussi
- symétrique (influence identique dans les 2 sens)
- asymétrique (rôle des objets différents)

Catégories de relations

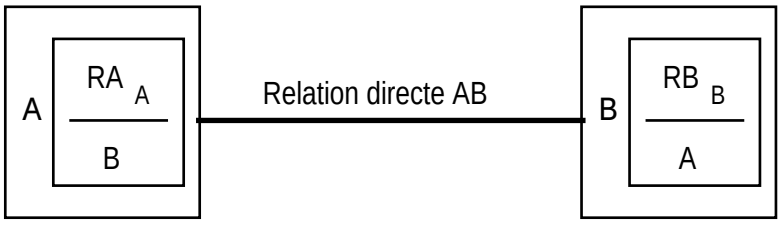
- Contenance

Ce type de relation est créé automatiquement à la création d'un objet.

Elle est utilisée notamment pour la suppression des objets subordonnés : Il n'est possible de supprimer un objet supérieur que si tous les objets subordonnés ont été détruits.
exemple : répertoire / fichiers)

- Relation explicite

Une telle relation crée un lien entre 2 objets. Un attribut contient le nom de l'autre objet (attribut relation RA , ici RA_A contient B)



Les relations explicites sont

crées par Add
supprimées par Remove

modifiées par Replace

La création d'un objet implique la création de ses relations explicites par des attributs que l'on trouve dans create.

Les informations sur les relations explicites peuvent être lues par une opération read.

Une relation explicite peut être unidirectionnelle . Dans ce cas l'attribut relation contenant le nom est dans un seul objet.

- Objets gérés qui représentent des relations

Dans une relation indirecte, l'objet intermédiaire représente la relation indirecte. Cet objet intermédiaire est suffisant pour désigner la relation indirecte (avec ses attributs de relation directe).

Types de relations explicites

- relation de service
  fournisseur / client d'un service

- relation paire (peer)
  entre 2 entités de communication distantes

- relation de repli (fallback)
  primaire / secondaire avec second choix préféré

- relation de remplacement (backup)
  remplaçant / remplacé, si un objet est à l'état invalide

- relation de groupe
  propriétaire / membre

Rôles des relations

Les relations peuvent avoir des rôles identiques ou complémentaires. Dans le premier cas, la relation est symétrique, dans le second elle est asymétrique. Les exemples ci-dessus donnent des exemples de rôles connus.

1.2.7.5 Compte-rendu d'alarme

Ils portent sur différents types d'alarmes
- communications
- qualité de service
- traitements
- équipements

Il est possible de signaler une cause probable pour chaque type, la sévérité perçue, la tendance (alarme plus sévère, moins sévère ou sans changement) et le remplacement d'un objet en alarme.

Causes probables (exemples)

Communications :
perte du signal
erreur trame
erreur de transmission locale
erreur de transmission distante
erreur d'établissement de connexion

Qualité de service
temps de réponse excessif
débordement de queue

Traitements
capacité de stockage dépassée
erreur de version etc.

environnement
incendie - fumées
humidité excessive
température excessive etc.

Sévérité perçue
- clair (cleared) après prise en compte
- indéterminée
- critique
- majeure
- mineure
- attention (warning)

Informations de seuil
- valeur observée
- seuil de déclenchement de l'alarme
- niveaux de seuil en cas d'hystérésis
- temps d'armement (depuis le dernier réarmement)

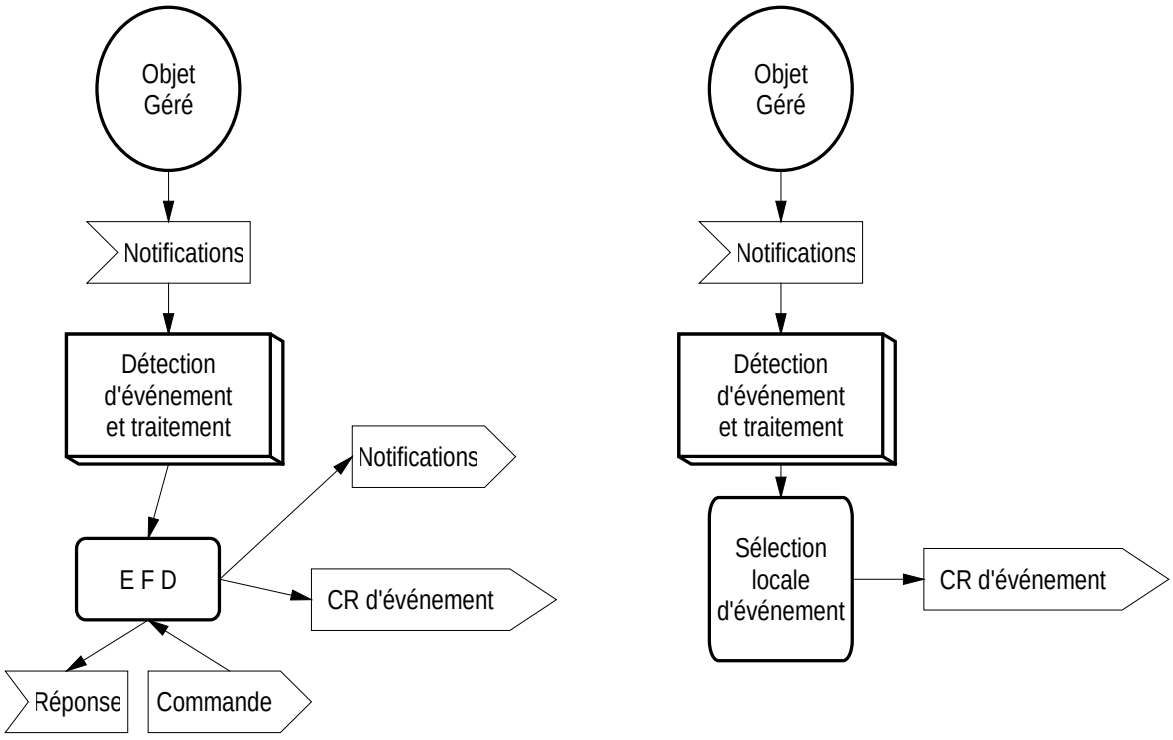
1.2.7.6 Compte-rendu d'événements

Cette fonctionnalité permet de traiter et de rapporter à d'autres systèmes les notifications d'événements.

L'événement notifié est traité localement et/ou rapporté à un autre système (pour traitement local ou rapport à distance) . Ceci est réalisé soit par notification (autre événement) soit par un compte-rendu d'événement.

Modèle

- Ce modèle décrit les composants (conceptuels) qui fournissent le compte-rendu d'événements distants et leur traitement local.



CR : Compte rendu
EFD : Event Forwarding Discriminator

Le "filtre" (discriminator) d'événement est un support d'objets gérés qui permet à un "gestionnaire" de contrôler les opérations de gestion et les comptes-rendus d'événement relatés par d'autres objets gérés.

1.3 Base de données administratives : MIB

Administration de réseaux SNMP

Actuellement l'Administration de Réseaux hétérogènes s'organise essentiellement autour du protocole SNMP (Simple Network Management Protocol) développé dans le cadre de l'architecture Inet (TCP/IP).

1.3.1 MIB pour INTERNET : Objets Gérés

Ils sont décrits par seulement 5 paramètres :

- Descripteur de l'objet
  - Nom et identificateur dans l'arbre de nommage

- Syntaxe
  - Type en ASN.1

- Définition
  - description en texte libre

- Droits d' Accès
  - lecture seule
  - lecture - écriture
  - écriture seule
  - non accessible

- Statut
  - obligatoire
  - optionnel
  - obsolète
  - dépréciée (deprecated)

Ainsi un objet est caractérisé par
un NOM
une SYNTAXE
un CODAGE

La syntaxe utilisée est un SOUS_ENSEMBLE de ASN.1.La structure est une version très simplifiée de la structure des objets OSI avec seulement 2 ATTRIBUTS en plus du nom.

1.3.2 Syntaxe ASN.1 pour MIB INTERNET

Le sous-ensemble utilisé comporte les types suivants :

INTEGER	SEQUENCE { }
OCTET STRING	SEQUENCE OF
OBJECT IDENTIFIER	NULL

et les types Applications :

NetworkAdress		(choix { internet IpAdress})
IpAdress		(chaine de 4 octets)
Counter		(entier 0..4294967295)
Gauge	Seuils	(entier 0..4294967295)
Timeticks	Temporisation	(entier 0..4294967295)
Opaque	Masque tout type spécifique	(chaine d'octets)

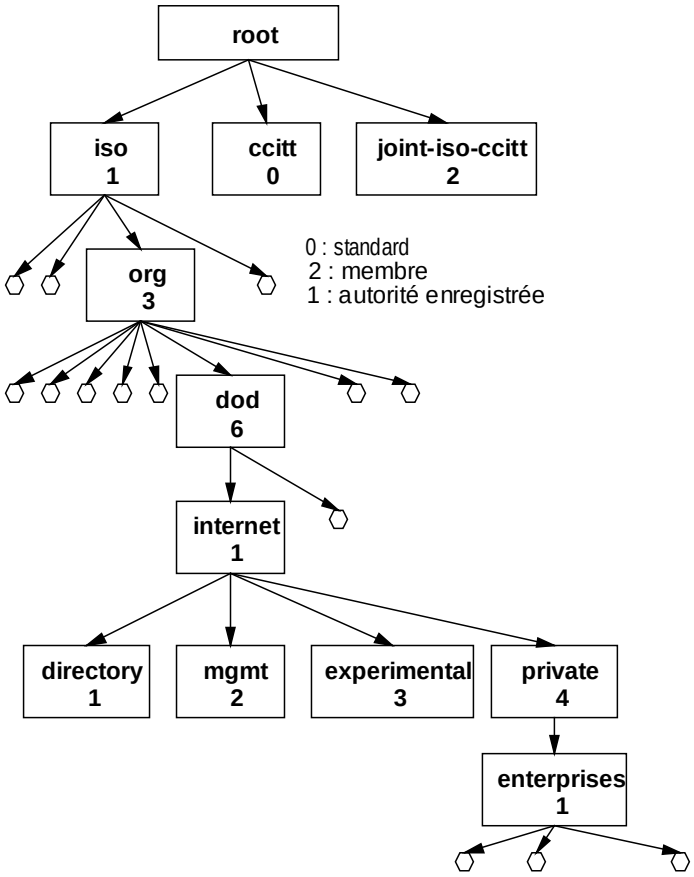
Exemple issu de la MIB II :

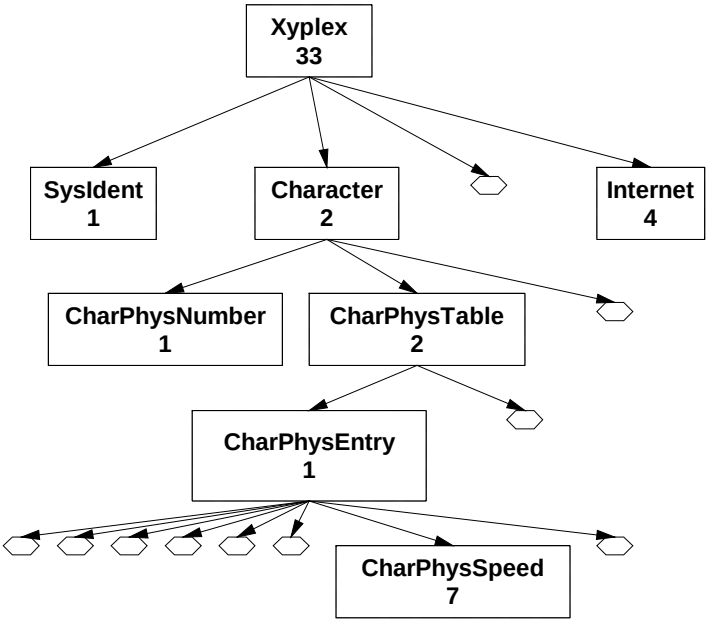
OBJECT :
IpAddrTable {ip 20}
Syntax :
SEQUENCE OF IpAddrEntry
Definition:
The table of adressing information relevant to this entity's IP adresses

Acces : read-only
Status : mandatory

1.3.3 Arbre de nommage

Il est défini par l'OSI et utilisé par toutes les autres organisations en particulier INTERNET pour sa MIB





1.3.4 Exemple de description d'un objet

Débit d'un port d'un concentrateur de terminaux Xyplex pour SNMP
entreprise XYPLEX 1.3.1.6.1.4.1.33

```
OBJECT
        SysIdent        {system 1}
        Syntax :        DisplayString (SIZE (0..40))
        Definition :    (chaîne d'identification ......)
        Acces :         read-only
        Status :        Mandatory
OBJECT
        charPhysNumber      {character 1}
        Syntax :        INTEGER
        Definition :    (Nombre de ports physiques ......)
        Acces :         read-only
        Status :        Mandatory
OBJECT
        charPhysTable       {character 2}
        Syntax :        INTEGER
        Definition :    (Liste des ports d'entrée arythmiques......)
        Acces :         read-only
        Status :        Mandatory

OBJECT
        charPhysEntry       {charPhysTable 1}
        Syntax :        charPhysEntry ::= SEQUENCE {
                                charPhysIndex,
                                INTEGER,
                                charPhysSpeed,
                                INTEGER,
                                        }
        Definition :    (Caractéristique d'un port d'entrée ......)
        Acces :         read-only
        Status :        Mandatory

OBJECT
        charPhysSpeed       {charPhysEntry 7}
        Syntax :        INTEGER
        Definition :    (vitesse du port.)
        Acces :         read-write
    Status :        Mandatory
```

Ainsi la vitesse d'un port de ce concentrateur est un objet administrable qui peut être lu ou positionné. Il est identifié de manière unique par

```
charPhysSpeed       OBJECT IDENTIFIER ::=
{org dod internet private enterprises XYPLEX
                    character charPhysTable charPhysEntry 7}
```

soit 1.3.6.1.4.1.33.2.2.1.7

1.3.5 MIB-II

Elle suit la RFC 1158

1.3.5.1 Contenu

L'objet MIB-II correspond au nœud 1.3.6.1.2.1 dans l'arbre de nommage

Nœud	Type	Nombre	Commentaires
1	system	7	Nœud administré
2	interface	23	Attachement réseau (Ethernet, TokenRing, X25, etc)
3	at (ARP)	3	Translation de l'adresse IP en adresse niveau 2/OSI
4	IP	38	Protocole IP (niveau 3)
5	ICMP	26	Protocole ICMP (niveau 3 - supervision)
6	TCP	19	Protocole de Transport avec connexion TCP
7	UDP	7	Protocole de Transport sans connexion UDP
8	EGP	18	Routeurs (Gateway)
9	transmission	0	Objets réseau spécifique
10	SNMP	30	Niveau 7 - Administration de réseaux SNMP

Ainsi le groupe IP correspond au nœud 1.3.6.1.2.1.4

1.3.5.2 Exemple

systemGroup
system OBJECT IDENTIFIER :: { mib 1 }
sysDescript : description de l'appareil
sysObjectId : identificateur de l'appareil
(N° d'objet dans MIB privée 1.3.2.45....)
sysUpTime : durée (en seconde) depuis laquelle l'appareil est actif
sysContact : nom de la personne à contacter pour cet appareil
(ex: adm@ifhpserv.insa-lyon.fr)
sysName : nom de l'appareil (ifpc56)
sysLocation : localisation de l'appareil (bâtiment 501 T202)
sysServices : services offerts ; code les niveaux OSI par $\Sigma\ 2^{L-1}$
(ex : transport + administration = 8+64 = 48 hexa)

1.3.6 Opérations SNMP

1.3.6.1 Types

Chaque équipement géré est vu comme un ensemble de variables que l'on peut:

consulter Get-Request

Get-Next-Request

Table "Traversal" : Traversée pour parcourir des tables (en particulier les tables de routage)

modifier Set-Request

à distance. Cet ensemble correspond à un objet dans le modèle d'information OSI, les variables étant des attributs.

On peut aussi en recevoir spontanément des informations (notifications) :

trap

1.3.6.2 Le "puissant" GET-NEXT

La primitive Get-Next permet les opérations de type "Traversal" pour explorer les tables. Il est en particulier utilisé pour les tables d'adresses ou les tables de routage; il permet aussi de trouver des objets dans une liste.

Le problème à résoudre est le suivant: comment trouver une valeur dans une table de la MIB avec SNMP qui ne traite que des objets simples (contrairement à l'Administration OSI qui traite les listes d'attributs).

Si par exemple on présente la requête "get-next (sysDescript)
on obtient la valeur de l'objet suivant soit : sysObjectId

Cette primitive est donc utile pour traiter des tables dont on ne connait pas le contenu réel ou la taille.

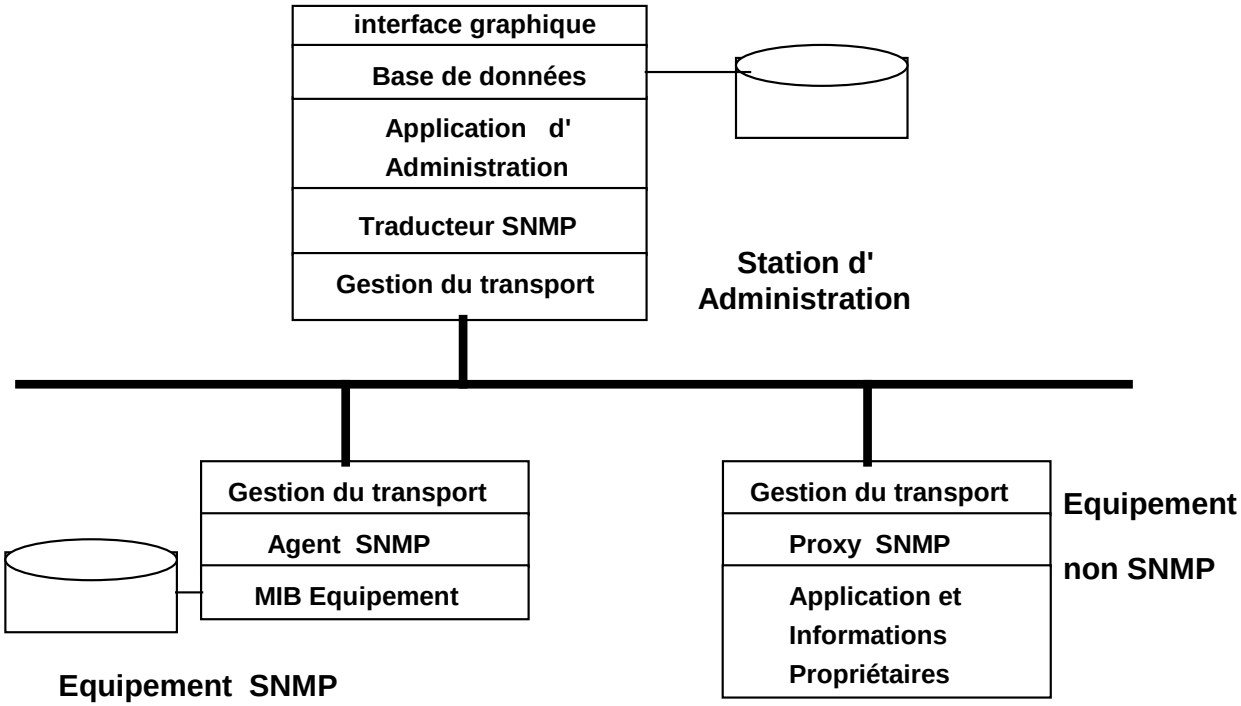
Get-next peut avoir plusieurs paramètres (comme set ou get) pour explorer les tables à plusieurs colonnes.

Exemple : get-next (ipRouteDest, ipRouteIfIndex, ipRouteNextHop)
donne la première ligne de la table de routage
si on rappelle get-next avec la valeur reçue on obtient la ligne suivante dans la table de routage.

Rq: ipNextHop identifie le routeur suivant dans le réseau; il peut ainsi être testé à son tour.

1.3.7 Architecture SNMP

1.3.7.1 Architecture : stations SNMP et Proxy



1.3.7.2 .Equipements administrés

systèmes hôtes : stations de travail, serveurs
concentrateurs de terminaux
imprimantes
etc.
routeurs, passerelles

Equipements de transmission :Ponts, multiplexeurs
Les messages sont transportés par des datagrammes UDP (port 161)

1.3.8 Messages SNMP

Ces messages sont codés dans un sous-ensemble de la syntaxe ASN.1.
Un message est codé par une séquence ASN.1 :
message ::SEQUENCE { version, community, data}

La version 1 correspond au standard RFC 1157
La communauté constitue le mécanisme d'authentification de SNMP; ce paramètre agit comme un mot de passe transmis du l'administrateur client à un agent administré.

Le champ data contient une PDU correspondant à une des requêtes ou trap.

Requêtes :

GetRequest-PDU
GetResponse-PDU
GetNextRequest-PDU
SetRequest-PDU

Paramètres :

identificateur
type d'erreur
noError (0)
tooBig (1)
noSuchName (2)
BadValue (3)
readOnly (4)
genErr (5)
index d'erreur (numéro de la variable en erreur)
liste (agrégat) de variables (nom et valeur)

Trap :

Trap-PDU

Paramètres :

identification de l'agent source
adresse de l'agent
type de trap
coldStart (0)
warmStart (1)
linkDown (2)
linkUp (3)
authentificationFailure (4)
egpNeighborLoss (5)
enterpriseSpecific (6)
champ spécifique pour traps particuliers
date de l'événement
liste des variables associées à ce trap

2 ROUTAGE ET ACHEMINEMENT

Pour transférer les données entre des systèmes hôtes d'un réseau, les messages suivent un chemin, souvent appelé circuit virtuel, dans le réseau. Ils sont relayés, après un stockage temporaire de plus ou moins longue durée, dans les nœuds intermédiaires du réseau : routeurs ou commutateurs de paquets. Ceci met en œuvre des fonctions complémentaires : routage et acheminement qui s'appuient sur des mécanismes d'adressage.

2.1 Définitions

ES (End system) Système terminal (synonyme ETTD) système qui émet et reçoit des "messages"

IS (Intermediate System) Système intermédiaire. Nœud de réseau possédant des fonctions de routage et de transmission des messages en provenance des systèmes terminaux.

Appellation : identificateur permanent d'une entité

Adresse réseau : Adresse logique d'un équipement connecté à un réseau. Ce terme peut servir à désigner différents éléments selon le contexte de l'étude. Il convient donc de le préciser.

Adresse de (sous-)réseau ou adresse de point d'attache de sous-réseau : terme qui désigne le point ou un système terminal réel, un réseau réel où une unité d'interfonctionnement sont attachés à un (sous-)réseau réel.

Adresse NSAP : point d'accès au service réseau (NSAP) où le service réseau est offert à un utilisateur (interface niveau 3/4 de l'OSI). Cette valeur est un paramètre des primitives de connexion, de déconnexion ou de données unitaires (datagramme)

Information d'adresse de protocole de réseau (NPAI) Partie "adresse" de l'Information de commande de protocole (PCI) dans une NPDU.

Il existe une relation entre adresse NSAP et NPAI en ce sens que la sémantique de l'adresse NSAP est préservée par la NPAI

SNPA (Sub Network Point of Attachment) Point d'attachement au sous-réseau : Interface physique entre une machine et le sous-réseau (en quelque sorte la prise).

Routage : fonction traduisant l'appellation d'une entité ou l'adresse SAP(-N) à laquelle l'entité est reliée en un itinéraire permettant d'atteindre l'entité.

Relais(N) : Fonction (N) au moyen de laquelle une entité (N) retransmet des PDU(N) d'une entité correspondante (N) à une autre entité correspondante (N)

Acheminement : Action de conduire un message à une destination prévue à l'avance.

2.2 Introduction

Les réseaux d'entreprise sont souvent réalisés par une interconnexion de réseaux locaux ou étendus privés ou publics. Dans ces réseaux la couche 3/OSI est décomposée en plusieurs sous-couches :

SNAP, Sub Network Access Protocol, qui traite de l'accès au réseau. Le protocole X25, supportant les réseaux de paquets en circuit virtuel commuté peut entrer dans cette catégorie.

SNDCP Sub Network Dependent Convergence Protocole qui traite les sous-réseaux de base. Ce peut être un réseau utilisant le protocole IP et géré, du point de vue routage, de manière homogène et connue de son administrateur (un seul protocole routé, dans un domaine de routage). Ce peut être aussi un réseau en commutation de paquets X25.

SNICP Sub Network Independent Convergence Protocol qui traite l'interconnexion de ces sous-réseaux de base, par exemple couche IP/ISO ou IP. Ce type de réseau est souvent multi protocole (IP, IPX, etc.) et possède un grand nombre de domaine de routage.

Dans ce cas les mécanismes de routage et d'acheminement doivent être considérés au deux niveaux SNDCP et SNICP.

Ces mécanismes constituent un des facteurs fondamentaux pour obtenir les meilleures performances d'un réseau. Ils doivent être pris en compte dès la phase de conception, lorsque la topologie du réseau a été déterminée. On choisit alors un routage optimal pour lequel le réseau sera calculé. L'optimisation de ce routage consiste essentiellement à minimiser le nombre d'étapes moyen.

En phase d'exploitation, le réseau étant complètement déterminé, l'optimisation en fonction de la topologie, du trafic et des facteurs de coûts, permet d'obtenir les performances les meilleures.

Un grand nombre d'étude théoriques ont été menées sur ce problème et diverses techniques ont été proposées. Seules les plus simples d'entre elles semblent jusqu'ici utilisées. Cependant depuis quelques années, l'optimisation des performances (ou des coûts d'exploitation) est devenue un objectif de l'administration de réseaux (on ne se contente plus d'un fonctionnement correct...). Des techniques adaptatives seront de plus en plus utilisées. Depuis quelques années une normalisation se met en place.

ISO9542 (1988) pour l'échange d'information de routage entre ES et IS sur un réseau sans connexion (ISO8473 = IP)

ISO10030(12-1190) pour l'échange d'information de routage entre ES et IS sur un réseau en mode connecté (ISO8878 = X25)

ISO10589 (10-1990) pour l'échange d'information de routage entre IS sur un réseau en mode non connecté

Nous allons examiner successivement les problèmes à résoudre, les différentes méthodes de routage, la normalisation OSI et la mise en œuvre du routage sur différents types de réseaux.

Par ailleurs sur Internet, un certain nombre de protocoles se sont imposés comme des standards de fait. Par exemple RIP (Routing Information Protocol) est installé sur tous les systèmes utilisant IP, en mode actif sur les routeurs et en mode passif sur les stations de travail (démon routed). Des protocoles "propriétaires" sont aussi très souvent utilisés.

2.3 Expression des besoins

Pour transférer un "message" à travers un réseau, il est nécessaire de déterminer quel itinéraire il va suivre (fonction routage), puis à chaque nœud du réseau d'aiguiller et de retransmettre ce message sur une liaison de données convenable (fonction acheminement).

Le calcul du routage nécessite de connaître la topologie du réseau et selon le niveau d'optimisation recherché, une estimation du trafic à acheminer et une expression des coûts respectifs des chemins possibles.

Si la topologie et les coûts ne subissent que de rares modifications, à des intervalles de temps de plusieurs mois, leur prise en compte peut être faite en temps quasi réel. Cette prise en compte va conduire à des solutions très différentes.

Les modifications topologiques par suite de panne doivent aussi être prises en compte dans un délai très bref mais elles ont pu être prévues à l'avance et ne nécessitent, après que cette modification topologique a été signalée, qu'une modification de l'acheminement (routage alternatif).

Le résultat du calcul des routes est traduit dans des tables de routage qui sont transmises aux nœuds du réseau à partie d'une table globale (routage centralisé) ou élaborées localement à chaque nœud (routage distribué). Dans chaque nœud relais, l'acheminement est traité à partir
des adresses de réseau (NPAI)
de la table de routage locale

En effet les normes OSI précisent qu'il n'est pas possible de déduire l'acheminement de la seule analyse des adresses, même si la structure de celles-ci peut faciliter le calcul des tables de routage.

Dans les systèmes transportant des NPDU unitaires (datagrammes), ceux-ci sont indépendants et chaque PDU de données porte l'adresse de destination et la route peut être différente pour chacune.

Dans les systèmes en mode connecté les NPDU d'une connexion suivent le même itinéraire, le circuit virtuel, qui est établit durant la phase d'appel. Les PDU de données portent une adresse temporaire plus courte (NVL : Numéro de voie logique) que l'adresse absolue de destination. Cette route reste fixe pendant toute la durée de connexion. Elle peut être différente d'une connexion à la suivante pour un même couple appelant-appelé.

L'examen de ces besoins montre que le problème essentiel réside dans l'élaboration des tables de routage de chaque nœud.

2.4 Algorithmes de routage

2.4.1 Types de routage

Fixe -déterministe
- avec alternative
-aléatoire
- par inondation

Adaptatif - centraliséy
- distribué
- à contrôle local
- par domaine

Les routages fixes utilisent des algorithmes qui ne tiennent pas compte des fluctuations du trafic (sauf certains routages fixes avec alternative).

Un routage fixe peut être déterminé "manuellement" et chargé sur un routeur. On parle alors de "routes statiques". S'il peut être modifié automatiquement en fonction des modifications de l'état du réseau (liens ou nœuds en défaut par exemple) on parle de "routes dynamiques".

Un routage fixe déterministe est utilisé en phase de conception pour spécifier les caractéristiques des différentes liaisons. Il tient compte essentiellement de la topologie et minimise le nombre d'étapes moyen. En cas de chemin équivalent selon ce critère, un critère d'optimisation secondaire: concentration du trafic sur les nœuds les plus importants (critère de performance) ou équilibrage du trafic entre les nœuds (critère de sécurité) sera pris en compte. Ces critères étant fixés on peut calculer le réseau optimal correspondant. Toute modification du routage pour la même répartition de trafic ne peut qu'entraîner une dégradation des performances.

En cas de défaillance d'un nœud ou d'une liaison, il y a modification de la topologie du réseau et une autre table de routage optimale peut être déterminée. On obtient ainsi des alternatives à la table de base.

Les routages aléatoires ou par inondation peuvent sembler une solution très mauvaise au vu des performances très médiocres qu'ils entraînent. Ils ont toutefois leur utilité

- soit pour les réseaux peu fiables
  - réseaux militaires
  - réseaux radio
- soit pour mettre à jour les tables de routage des réseaux classiques.

Le routage aléatoire consiste à acheminer un message reçu à un nœud K vers un des nœuds voisins (connecté) désigné au hasard. de proche en proche, le message atteint sa destination quelque soit la topologie actuelle du réseau (sauf si le nœud chargé de l'acheminement tombe en panne à cet instant ...)

Le routage par inondation consiste à acheminer un message reçu à un nœud K vers tous les nœuds voisins connectés (sauf éventuellement le nœud précédent). Dans chaque relais traversé,

le passage d'un message est noté pour éviter de renvoyer une seconde fois ce message. On peut aussi dater les messages et les extraire après un certain délai.

2.4.1.1 Routage adaptatif centralisé

Dans ce type de routage, les itinéraires s'adaptent aux modifications topologiques du réseau et surtout aux fluctuations du trafic. Il nécessite donc de connaître à tout instant l'état du réseau. Ceci entraîne la transmission à travers le réseau, depuis chaque nœud, de messages indiquant la charge de ces nœuds, donc un accroissement du trafic (en particulier dans des périodes où il est déjà trop élevé). Ces messages sont collectés par un nœud central d'administration qui calcule les nouvelles routes et transmet à chaque nœud sa table de routage avec une heure de prise d'effet

2.4.1.2 Routage adaptatif distribué

Chaque nœud reçoit les messages indiquant l'état des autres nœuds et calcule sa table d'acheminement optimal. Le nombre de messages d'état peut être supérieur au cas précédent mais cette technique évite la transmission des tables de routage.

2.4.1.3 Routage adaptatif local

Chaque nœud établit sa table d'acheminement en fonction de sa propre observation du trafic. Il n'y a plus de messages de routage à travers le réseau mais il n'y a aucune assurance que les décisions locales convergent vers une optimisation globale. On peut aussi observer des fluctuations (pompage) de fonctionnement.

Avec un routage non centralisé, les modifications d'acheminement ne sont pas synchronisées, et il est difficile d'assurer une optimisation globale du réseau. seules des simulations permettent de juger de la qualité des algorithmes utilisés.

2.4.1.4 Routage distribué par région (domaine)

Les grands réseaux peuvent être découpés hiérarchiquement en domaine (et sous domaines)

Les nœuds de niveau 1 ne sont habilités à router les messages qu'au sein de leur domaine. Ils n'ont aucune connaissance topologique sur les autres régions (si ce n'est l'appartenance d'un nœud à une région et le ou les nœuds de sortie de son domaine vers les autres domaines).

Les nœuds de niveau 2 ont une vision plus globale du réseau. Ils ne connaissent pas la topologie exacte des autres domaines mais la topologie du réseau (partiel) constitué ,par les nœuds frontières.

A chaque niveau (intra ou inter domaine) les nœuds s'envoient les informations de routage par un mécanisme d'inondation mais à un rythme bien plus faible pour le niveau 2 (interrégion).

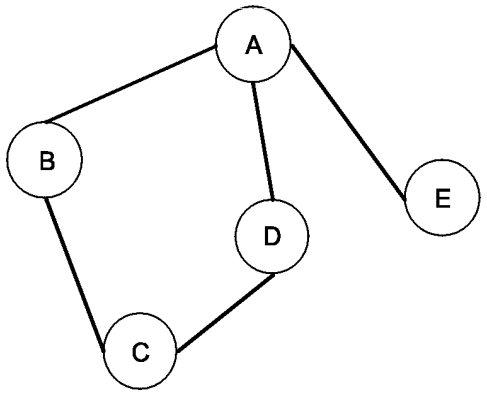
2.5 Tables de routage

Le résultat du calcul des routes est consigné dans les tables de routage. Pour un routage centralisé une table complète, décrivant l'ensemble des itinéraires, est créé au Centre de Gestion du réseau. Des parties de cette table sont transmises aux différents nœuds. Pour un routage distribué, les tables partielles sont élaborées dans chaque nœud.

Dans ces tables on indique pour chaque destination le **prochain nœud** à atteindre (nœud voisin).

2.5.1 Exemple :

On étudie le réseau suivant



2.5.1.1 Table complète pour un routage fixe

Destination / Source	A	B	C	D	E
A	A	B	B	D	E
B	A	B	C	C	A
C	B	B	C	D	D
D	A	C	C	D	A
E	A	A	A	A	E

2.5.1.2 Table complète pour routage avec alternatives

Destination / Source	A	B	C	D	E
A	A	B	B,D	D	E
B	A	B	C,A	C	A
C	B,D	B	C	D,B	D
D	A	C,A	C	D	A
E	A	A	A	A	E

2.5.1.3 Tables pour le nœud C

Routage fixe

Destination	A	B	C	D	E
	B	B	C	D	D

Routage avec alternatives

Destination	A	B	C	D	E
	B,D	B	C	D,B	D

2.6 Comparaison des méthodes

La comparaison des méthodes de routage est difficile car les performances observées dépendent d'un grand nombre de facteurs souvent mal maîtrisés.

Kleinrock et son équipe, en particulier, ont montré , par simulation, quelques propriétés générales.

En phase de conception,

- il est souhaitable de minimiser le nombre moyen d'étapes.
- si pour aller d'un nœud j à un nœud k, il y a deux chemins possibles de même longueur, le temps de transit moyen sera toujours réduit si **on ne garde qu'un seul** de ces chemins.
- si le réseau a été optimisé pour un routage donné, ce routage fixe est préférable à tout système de routage avec alternative. Plus la table de routage présente d'alternatives, moins le routage est performant. (accroissement du nombre d'étapes moyen).
- si le réseau n'a pas été conçu de manière optimale, par exemple avec des liaisons toutes identiques ou proportionnelles au trafic circulant, des chemins avec des alternatives limitées améliorent les performances. Trop d'alternatives peuvent les dégrader.

si à un nœud j on dispose de M canaux Ci possibles pour atteindre un nœud k et si les capacités de ces canaux sont telles que $C_1 > C_2 > C_3 > C_M$, on peut déterminer à quelle condition un message en position qi dans la file d'attente doit emprunter le canal Ci ou attendre qu'un canal plus performant soit libéré. La règle suivante améliore le routage :

$$q_i < \frac{\sum_{j=1}^{i-1} C_j}{C_j} \leq q_1 \qquad \text{avec } q_{1=1}$$

Pour un réseau existant,

- L'introduction de chemins alternatifs peut compenser l'écart entre le réseau réel existant et sa version optimisée lors de sa conception, écart du à une variation du trafic par rapport au trafic prévu.

- L'introduction de chemins alternatifs utilisés uniquement en cas de panne sur les chemins de base assure la sécurité du réseau.

Routage aléatoire ou par inondation,

Ce type de routage peut multiplier par 10 ou plus le temps de transit moyen sur un réseau comme le montre le tableau ci-dessous (r est le facteur d'utilisation moyen du réseau). Les valeurs sont obtenues par simulation sur un réseau à 13 nœuds où chaque nœud est connecté à 4 autres nœuds (réseau 4-connecté)

r	1/128	1/64	1/32	1/16	1/8	0.25	0.5
Fixe	87,5	88,4	93,7	102	120	170	580
Aléatoire	728	731	774	1803	∞	∞	∞

Nous observons que lorsque r reste inférieur à quelques % le temps de transit moyen reste stable quoique très élevé. La saturation commence pour un facteur d'utilisation de 5 % environ contre 50 % pour une procédure fixe. Le nombre d'étapes moyen est passé de 1,67 à 14 !

Ce type de procédure n'est donc utile que dans des applications particulières :
- réseaux peu fiables : réseaux radio, réseaux militaires
- **diffusion des informations de routage.** Dans ce cas les informations clientes du réseau sont transmises par un routage adaptatif.

2.7 Calcul du chemin le plus court

Les informations nécessaires au calcul du routage étant connues soit à un nœud central soit localement, il convient de calculer le chemin optimal.

- A chaque lien est affectée une métrique (un coût). La distance d'un nœud à la destination finale est la somme des "longueurs" des liens constituant le chemin.

- Plusieurs types d'algorithmes permettent d'effectuer ce calcul (Dijkstra, Pape, Déviation de flux (Gerla), etc.)

Nous devons donc choisir une métrique puis un algorithme d'optimisation

2.7.1 Métriques

Une métrique de coût prend en compte le coût de fonctionnement d'une liaison pour le calcul du chemin optimal.

Une métrique de performance minimise seulement de délai de transmission moyen d'un paquet sur un intervalle de temps donné grâce à la mesure directe de la disponibilité des ressources indispensables à la transmission: nombre de circuits disponibles, débits, nombre de buffers, temps de calcul...

Les deux métriques peuvent être utilisées conjointement : chemin de coût minimal parmi les plus performants ou chemin le plus performant parmi les moins coûteux.

Ce système fournit un **"vecteur distance"** donnant, pour chaque routeur, la "distance" à tous les autres. Ces distances peuvent indiquer simplement le nombre d'étapes
(distance 1 entre nœuds voisin) ou tenir compte des caractéristiques les liens

2.7.2 Algorithme

L'algorithme décrit ci-dessous est l'un des plus simples utilisables. Il est donné à titre indicatif pour illustrer le problème à traiter.

2.7.2.1 Algorithme du plus court chemin

Nota : Cet algorithme n'est pas adapté à déterminer rapidement le plus court chemin si le critère de distance est le nombre de nœuds traversés. Un algorithme utilisant les élévations à la puissance k (k allant de 1 à kmax) de la matrice de connexion pour trouver les chemins de k étapes est plus efficace.

Initialisation :

Ni = nœud courant N_a = nœud de départ
L'algorithme s'applique en prenant successivement les nœuds du réseau comme nœuds de départ. A chaque nœud on assigne un couple de valeurs (nœud, distance)
Le nœud indiqué est le prochain nœud sur le chemin le plus court. S'il n'est pas encore connu il est noté :● La distance notée d_i est la distance au nœud origine par le plus court chemin connu. Si elle n'est pas déterminée est vaut l'infini : ∞ pour tous les nœuds sauf le nœud de départ pour lequel elle vaut 0.

l(i,j) désigne la distance entre les nœuds Ni et Nj.
à l'état initial $d_a = 0$, di = ∞ si a ¹ i couple = (●, di)

Plus courte distance :
Méthode par balayage

On recherche pour tout couple i,j une branche i,j telle que di + l(i,j) < dj On associe au nœud Nj le couple (Ni, di + l(i,j))

On dispose alors pour chaque nœud de la plus courte distance au nœud source Na et le nœud voisin le plus proche.

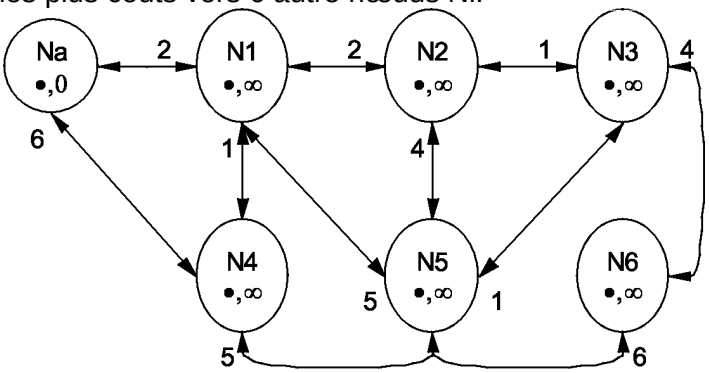
Chemin le plus court pour le nœud Nb :

1) faire i = b
2) identifier Nk par le couple (Nk , db) associé à Nb
Si Nk n'existe pas, il n'y a pas de chemin liant Na à Nb.
3) faire = = k si i = a Fin
sinon retourner à 2)

Cet algorithme donne tous les nœuds intermédiaires entre Na et Nb par le chemin le plus court.

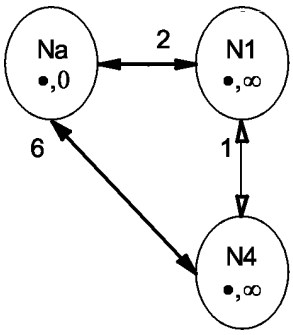
2.7.2.2 Exemple :

On considère le réseau ci-dessous vu du nœud initial Na à partir duquel on calcule les chemins les plus coûts vers 6 autre nœuds Ni.



Les "distances" entre nœuds sont indiquées sur le graphe initial ci-contre. Par exemple la distance l(3,6) entre les nœuds N3 et N6 vaut 4.

On détermine successivement le chemin le plus court depuis les différents nœuds.



Pour le Nœud N4 :

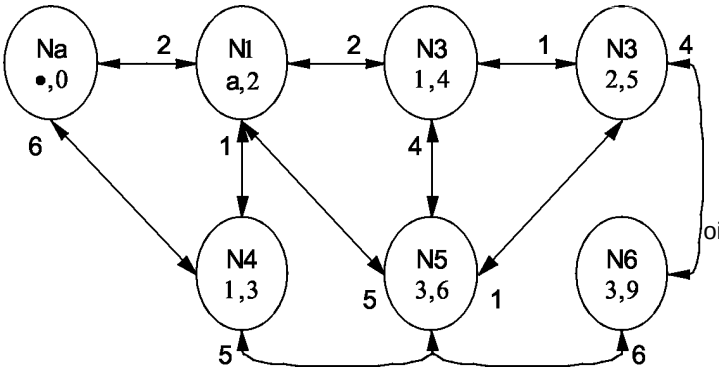
d(4) = ∞ > d(a) + l(a,4) = 0 + 6 = 6
N4 (● , ∞) → N4(a,6)

Pour le nœud N1 :

d(1) = ∞ > d(a) + l(a,1) = 0 + 2 = 2 N1 (● ,∞) → N1(a,2)

On revient au nœud N4

d(4) = 6 > d(1) + l(1,4) = 2 +1 = 3
N4 (a,6) → N4(1,3)



On poursuit l'algorithme pour tous les nœuds et on obtient le graphe ci- dessous :

Le chemin de N5 à Na passe par N3 . Il a une distance 6. {N5 (3,6) }

Il est établi par
N5(3,6) → N3(2,5) → N2(1,4) → N1(a,2) → Na(●,0)

Soit b = 5 → 3 → 2 → 1 → a. Sa distance est 6.

2.8 Normalisation

2.8.1 ISO9542

Echange d'information de routage entre ES et IS ou IS et ES sur un réseau sans connexion.

- pour permettre aux ES de trouver les IS permettant de relayer les NPDU vers d'autres sous-réseaux
- pour permettre aux ES de trouver d'autres ES sur le même sous-réseau si l'adresse du NSAP destinataire est insuffisante.
- pour permettre aux IS de connaître l'existence des ES situés sur chaque sous-réseau auquel ils sont connectés
- pour permettre aux ES quel IS utiliser quand plusieurs IS sont possibles.

Le protocole garantit que le routage à un Point d'attachement de sous-réseau (SNPA) du sous-réseau est supporté par le sous-réseau lui-même mais celui-ci n'est pas capable de le faire sur la seule base des adresses NSAP. Il fournit aussi des fonctions de diffusion totale (Broadcast) ou partielle (Multicast).

Ce protocole doit aussi minimiser

- l'échange d'informations à entrer dans chaque ES avant qu'il puisse commencer à communiquer
- la taille mémoire nécessaire au routage
- la complexité de calcul de l'algorithme de routage

Il spécifie

- les procédures de transmission d'information de configuration et de routage entre ES et IS
- le codage des PDU
- les procédures nécessaires à l'interprétation correcte des PCI

Le protocole 9542 fournit deux types d'information

- **informations de configuration**

  Elles permettent

  - aux ES et IS de découvrir dynamiquement leurs existences réciproques et leur disponibilité (signalisation de présence et de disponibilité)
- aux ES d'obtenir des informations sur d'autres ES en l'absence d'IS disponible

- **informations de redirection (reroutage)**
  qui permettent aux IS d'indiquer aux ES des routes potentiellement meilleures pour expédier une NPDU à une destination particulière.
  Les adresses utilisées sont les adresses de NSAP données dans le protocole OSI 8348/add2 : service sans connexion IP/ISO

2.8.2 ISO10030

Protocole d'échange d'information pour le routage pour les systèmes d'extrémité utilisant un service réseau connecté en commutation de paquet ISO8878 (X25)

Ce protocole apporte des solutions aux problèmes suivants :

- Comment les ES découvrent les IS pouvant router des NPDU à des destinations situées sur d'autres sous-réseaux
- Comment les ES découvrent d'autres ES sur le même sous-réseau (quand la connaissance de l'adresse de NSAP ne donne pas d'information sur l'adresse de sous-réseau du système destinataire
- Comment une entité de résolution des adresse de sous-réseau : SNARE (Subnetwork adress resolution entity) découvre les ES de son sous-réseau.

Ce protocole garantit que le routage à un SNPA du sous-réseau est supporté par le sous-réseau lui-même ; Mais le sous-réseau n'est pas capable de router sur la seule base des adresses de NSAP. Les ES utilisant ce protocole doivent connaître l'adresse d'au moins un SNPA permettant d'atteindre un SNARE.

Ce protocole doit minimiser

- l'information à entrer à priori dans chaque ES avant qu'il puisse commencer à communiquer
- dans les ES la mémoire nécessaire au routage et la complexité de calcul des algorithmes de routage

Ce protocole est un complément du protocole ISO9542 pour les environnements sans diffusion (pour la partie configuration) et pour les environnements avec diffusion totale pour lesquels le sous-ensemble redirection n'est pas valable (pour la partie redirection)

2.8.2.1 Vue générale

Ce protocole comporte deux sous-ensembles

- Information de Configuration
- Information de Redirection

Il s'articule autour de la fonction **SNARE**
Un SNARE est un fournisseur d'information de routage pour un seul sous-réseau. Il doit aussi communiquer avec des IS mais ceci n'est pas pris en compte par le protocole ISO 10030. La fonction SNARE est supportée par un ou plusieurs ES ou IS du sous-réseau. Dans un sous-réseau X25, il est possible que les opérations de SNARE soient supportées par le sous-réseau lui-même.

Information de configuration

Ce sont des informations sur les ES et les IS attachés à un sous-réseau en termes de types de système, Adresses Réseau présentes, Nom d'Entités Réseau (NET) présents, correspondances entre systèmes, adresse SNPA et routes potentielles. Les ES communiquent leur adresse réseau (NA) à un SNARE

Les ES découvrent (pour certaines NA éloignées) les adresses SNPA du système du sous-réseau (IS) par lesquelles la communication pourrait être acheminée.

Pour réaliser ceci une ES établit une connexion X25 vers un SNARE par une demande d'appel. Dans ce paquet d'appel, le premier octet des données utilisateur contient un identificateur de protocole spécifique. Si le SNARE accepte l'appel, l'ES peut alors lui transmettre des détails sur ses Adresses Réseau puis lui envoyer une PDU "information complète". L'ES peut aussi demander une information sur les NA éloignées. La SNARE envoie alors l'information correspondante, les SNPA par lesquelles celles-ci peuvent être atteintes et la qualité de service (QoS) associée. L'ES libère alors la connexion

Ainsi les ES présents se signalent dynamiquement les uns aux autres (et aux SNARE) : on obtient ainsi la configuration du sous-réseau sans intervention manuelle d'un opérateur dans chaque entité du réseau

Informations de redirection

Cette fonction comporte deux parties. La première est utilisée lorsqu'un ES veut établir une connexion de réseau (X25) mais ne dispose pas des informations nécessaires pour déterminer l'adresse appropriée de sous-réseau. Dans ce cas, l'ES s'adresse au SNARE par une demande d'appel (X25) à celui-ci.;

Si le SNARE est un ES ou un IS attaché au sous-réseau il peut

- utiliser la facilité de réacheminement d'appel pour rerouter l'appel vers un ES ou IS approprié
- libérer l'appel en indiquant le SNPA approprié qui doit être utilisé dans l'avenir
- s'il contient une fonction relais, accepter l'appel et acheminer celui-ci.

Si la fonction SNARE est intégrée au sous-réseau elle peut utiliser des moyens spécifiques pour appeler le SNPA approprié.
L'établissement de connexion de l'ES d'origine peut alors se poursuivre normalement si une libération n'a pas été émise.

La Réception d'une indication de libération provoque la mise en œuvre de la seconde partie. Les champs cause et diagnostic du paquet de libération montre quel celle-ci n'a pas été initiée par l'Utilisateur du service Réseau. L'ES appelant recherche dans les données utilisateurs un PDU d'information du protocole 10030 indiquant une adresse de sous-réseau appropriée par laquelle une connexion équivalente à celle qui vient d'être rejetée peut établie (mêmes NSAP avec même qualité de service). l'ES peut alors utiliser ces informations pour ses futurs appels.

En résumé cette fonction permet d'établir un appel vers un équipement d'un sous-réseau dont on ne connaît pas l'adresse complète directement par l'intermédiaire d'un SNARE ou grâce aux informations fournies par celui-ci.

Un ES peut supporter soit la fonction "information de configuration", soit la fonction "information de redirection" soit les deux fonctions.

2.8.2.2 Adresse sous-réseau d'un SNARE

Chaque ES doit connaître au moins une adresse de réseau à laquelle un SNARE peut être joint. Certaines méthodes spécifiques pour cela peuvent être utilisées si les ES sont connectés à un réseau local utilisant un protocole ISO 8802.2 de type LLC1 à l'aide de mécanismes de diffusion totale (Broadcast).

2.8.2.3 PDU utilisés

2.8.2.3.1 Structure

Ils sont composés d'une en-tête sur 3 octets et éventuellement d'un champ de données portant des paramètres. L'en-tête a la composition suivante :

- identificateur de protocole
- numéro de version
- type du PDU

Les paramètres d'adresse comportent un champ longueur un champ valeur (l'adresse SNPA a aussi un champ type sur 2 bits)

Les autres paramètres ont une structure TLV : type-longueur-valeur

2.8.2.3.2 Types de PDU

Emis pas les ES

ECQ :End System Configuration Query	Code : 1
ENC : End System Notification Complete	2
ESC : End System Connect	3
ESH : End System Hello	4
SRH : SNARE Request Hello	11 hexa

Emis par les SNARE

RD : Redirect	Code : 8
SCC : SNARE Configuration Complete	9
SCR : SNARE Configuration Response	A hexa

SNC : SNARE Notification Complete	B hexa
SRN : SNARE Received Notification	C hexa
SHL : SNARE Hello	10 hexa

2.8.2.3.3 Paramètres :

Adresse réseau

Sa longueur est codée sur un octet. Elle suit les règles définies dans OSI8348/add2

Adresse SNPA

Elle spécifie une adresse qui peut être utilisée pour atteindre l'adresse réseau requise.
Dans le premier octet 2 bits de type indiquent le type de codage (normalisé ou local). Les 6 autres bis donnent la longueur de l'adresse qui peut être codée sous d'une suite d'octets (adresse MAC de réseau local ou adresse codée en AI5) ou sous forme de demi-octets pour une adresse codée en décimal. dans ce cas le dernier octet est éventuellement complété par 1111.

Masque d'adresse (champ optionnel)

Ce champ indique que les informations d'expédition fournies par la PDU s'appliquent à une plus large population d'adresses réseau que celle associée à la SCR PDU ou la RD PDU. Ce paramètre crée une classe d'équivalence d'adresses réseau pour laquelle d'applique les mêmes règles d'expédition.

Masque SNPA (Paramètre optionnel)

Si ce paramètre est présent, la classe d'équivalence définie par le masque d'adresse a aussi une structure commune dans la partie du masque d'adresse à 0. Le masque SNPA fournit des indications sur ce champ, en particulier la position de l'adresse SNPA dans l'adresse réseau.

Qualité de service

- Débit (maximal et minimal)
- Délai de transit (maximal et minimal)
- Priorités (maximale et minimale) pour obtenir une connexion
    - Garder une connexion
    - Transmettre des données
- Protection (niveaux maximal et minimal)
- Temps de maintien (durée de validité des données émises)
- Temps de rétention (durée de validité des données dans une SRH PDU)
- Limite de recherche (permission pour un ES de demander de nouvelles informations de configuration)
- Temps d'appel (intervalle de temps permis entre 2 requêtes à un SNARE)
- Notification demandée (intervalle de temps suggéré pour envoyer la notification).

2.8.2.4 Eléments de procédure

Etablissement de connexion

Un ES établit une connexion vers un SNARE par une demande d'appel X25 contenant une ESC PDU dans les données utilisateurs. Le champ de facilité "Sélection rapide sans restriction" (Unrestricted Fast Select) doit être utilisé et pas de bit Q. Si le SNARE peut accepter l'appel, il envoie un Appel accepté contenant une SNC PDU dans les données utilisateur (avec paramètre "temps d'appel").
La communication est alors établie. Les informations nécessaires sont alors échangées dans une séquence complète de paquets de données X25.

Notification de configuration

L'ES transmet au SNARE une ESH PDU pour chaque adresse réseau accessible à travers son SNPA (paramètres adresse réseau et qualité de service). Il termine cette séquence par une ENC PDU. Le SNARE acquitte ces informations par une SRN PDU (paramètre "Notification demandée")
La connexion peut alors être libérée.

Collecte de configuration

L'ES demande des informations à un SNARE par l'envoi d'une ESC PDU (paramètre "Adresse réseau"). Le SNARE répond par des SCR PDU (pour chaque SNPA pouvant être utilisée) contenant les paramètres suivants : temps de maintien, adresse réseau, adresse SNPA (qui permet d'atteindre l'adresse demandée), masque d'adresse, masque SNPA, qualité de service. Le SNARE termine la collecte par le transfert d'une SCC PDU (paramètres adresse réseau, limite demandée).
La communication peut alors être libérée.

Invocation de redirection

Un ES qui ne connaît pas l'adresse réseau d'un système appelé peut utiliser le mécanisme de redirection. Pour cela il établit une connexion X25 vers un SNARE avec le champ de facilité "Extension d'adresse" contenant l'adresse NSAP du système à atteindre. Si le SNARE peut relayer l'appel (par son relais local) il achemine celui-ci et la connexion est établie par son intermédiaire.
Il peut aussi rerouter l'appel vers un autre SNARE susceptible d'établir la communication.
Il peut enfin libérer l'appel (code 0 diagnostic 230) en plaçant une RD PDU dans le champ de données utilisateur du paquet de libération.
Cette RD PDU contient en paramètre un temps de maintien, une adresse SNPA permettant d'atteindre la destination souhaitée, un masque d'adresse et un masque SNPA.

Utilisation d'un réseau local avec service de liaison de données de type LLC1

Sur un réseau local fournissant des fonctions de diffusion partielle et totale, les ES peuvent découvrir un SNARE permettant de découvrir des adresses SNPA de SNARE. Pour cela un SNARE peut envoyer dans une trame en diffusion une SHL PDU contenant une "notification demandée" et un "temps de rétention" lui permettant de connaître d'adresse SNPA du SNARE.

Un ES qui n'a pas reçu de SHL PDU peut en solliciter un en envoyant une trame contenant une SRH PDU en diffusion partielle avec comme adresse "tous les SNARE x25".

2.8.3 ISO10589

Protocole intra-domaine de routage d'un système intermédiaire à un système intermédiaire utilisable avec un protocole de réseau en mode non connecté (IP/ISO 8473)
Ce protocole est utilisé dans les réseaux très étendus ayant une organisation hiérarchique. Les domaines sont divisés en régions gérées par un centre de gestion de routage. A l'intérieur d'une région le routage est de niveau 1. Entre deux régions il est de niveau 2. Les IS de niveau 1 relayent les messages des ES de leur région soit dans la région soit vers un IS de niveau 2 pour les ES d'une autre région.

2.9 Routage sur le réseau Transpac

Le routage de Transpac est adaptatif. Il s'adapte dynamiquement aux modifications éventuelles de l'état du réseau : panne ou surcharge très importante sur une artère ou sur un commutateur. Pour cela les commutateurs surveillent leur environnement local et le compare à des seuils préenregistrés. Lors d'un dépassement de seuil un nouvel itinéraire est choisi. Le retour au dessous d'un seuil inférieur (hystérésis) ramène au chemin initial.

Dans une première version l'algorithme de routage était centralisé : des messages étaient créés à la suite des dépassements de seuils et transmis à un Centre de Gestion du Réseau qui analysait l'état global du réseau et calculait éventuellement de nouvelles routes. Les nouvelles tables de routage étaient transmises à tous les nœuds concernés et pris en compte pour les nouveaux appels. En cas de panne du Centre de Gestion et du Centre de Secours, les décisions étaient purement locales.

Ce système présente des limitations, en particulier avec l'extension du réseau et la mise en place de nouveaux commutateurs. En 1984, il a été remplacé par un algorithme distribué sur l'ensemble des commutateurs.

Chaque commutateur est autonome et détermine son routage en fonction de l'état de son environnement local et de l'état de l'ensemble du réseau dont il est informé par ses voisins et un mécanisme de propagation de proche en proche de l'état de chaque commutateur.

Lorsque les itinéraires doivent emprunter des "liaisons périphériques" (réseaux extérieures, par exemple partie du réseau téléphonique) particulières, un algorithme particulier est mis en œuvre pour tenir compte du coût de ces liaisons (par exemple en fonction de la distance). En cas de panne ou de surcharge de ces liaisons leur "coût" est augmenté pour les pénaliser et éviter qu'elles continuent à être (trop) utilisées.

Ce routage est hiérarchisable : lorsque le nombre de commutateurs croît seuls les commutateurs qui ont vocation de transit entre régions connaissent finement l'état des autres commutateurs. Les commutateurs qui ont un rôle de concentrateur n'ont qu'une connaissance partielle (locale) de l'état du réseau. Pour un transfert assez proche, un commutateur peut avoir

une connaissance fine des routes possibles. Pour un transfert éloigné, il peut se contenter de calculer globalement le "coût" d'accès à un "point visé" proche de la destination finale.

2.10 Routage sur le Réseau Internet

Sur les (sous-) réseaux de l'Internet le routage utilise le plus souvent un protocole RIP : Routing Internet Protocol qui suit la RFC 1088 (C.Hedrick 1988). Toutefois le protocole OSI 10589 (IS-IS) peut être utilisé en suivant la RFC 1195 (R. Callon 1990) : Use of OSI IS-IS for Routing in TCP/IP and Dual environments. Une nouvelle proposition : OSPF Open Shortest Path First (RFC 1247 J.Moy 1991) peut aussi être utilisé pour transporter les messages RIP.
Dans IS-IS et OSPF, les routeurs sont responsables de l'identification de leurs voisins et de la création de "paquets d'état des liens" (LSP Link State Packet). Les deux protocoles supportent un routage hiérarchique.

Ces informations, plus riches qu'un "vecteur distance" permettent d'établir les tables de routages en tenant compte d'autres facteurs sur le fonctionnement du réseau et **d'éviter des problèmes de bouclage de routes ou de convergence lente dans les réseaux maillés** (problèmes qui autrement doivent être réglés par des mécanismes annexes, par exemple des temporisations pour certaines demandes de mises à jour).

Une différence essentielle réside dans l'architecture logicielle. OSPF est situé au dessus de la couche IP et utilise des paquets IP pour transférer ses informations. IS-IS (OSI) est de niveau IP et utilise directement la couche Liaison de données.

2.10.1 RIP : Routing Information Protocol

Ce protocole est un standard de fait pour échanger des informations de routage entre des routeurs et des hôtes dans l'architecture Inet (TCP/IP). Il utilise un algorithme de type "vecteur distance" (Bellman-Ford). La mise à jour des routes est limitée à un minimum de 30 secondes. Le chemin le plus long est limité à 15 étapes (ce qui permet d'éviter les boucles infinies mais limite la taille "gérable" du (sous-)réseau. Il utilise des métriques fixes pour comparer les routes et n'est pas approprié pour un routage adaptatif tenant compte de paramètres temps réels comme les temps de transit, la fiabilité de l'information ou la charge du réseau.

La métrique la plus simple consiste à utiliser le nombre de routeurs traversé **(nombre d'étapes ou sauts).** On peut aussi ajouter un "coût" à chaque étape.
Le coût D(i,j) d'une liaison entre i et j passant par le voisin k de j est D(i,j) = mink d(i,k) + D(k,j)
La meilleure route est celle qui passe par le nœud k qui rend d(i,k) + D(k,j) minimal.
Sur cet algorithme on établit pour chaque nœud une table de routage donnant la distance vers chaque destination et le prochain nœud à emprunter. Périodiquement cette table est envoyée pour mise à jour à chaque voisin. A partir de cette mise à jour il est possible de calculer une nouvelle version de la table de routage locale tenant compte des modifications données par les voisins ou observées localement.
Ceci suppose que la topologie reste fixe. Si elle change la liste des voisins est modifiée et la modification sera répercutée graduellement dans tout le réseau.
Les messages RIP sont transportés par le protocole de transport sans connexion UDP.

2.10.2 .EGP: Exterior Gateway Protocol

Le protocole RIP est adapté aux réseaux "convergents" de taille limitée, appelés "systèmes autonomes". Les grands réseaux sont constitués de plusieurs systèmes autonomes. EGP est utilisé par un routeur d'un système autonome pour faire connaître ses routes à un routeur d'un autre système autonome.
EGP comporte un mécanisme d'acquisition de voisinage pour demander à un voisin (externe) d'échanger des informations de routage: il acquiert ainsi un "voisin EGP" ou "pair EGP". (il n'y a aucune notion de distance géographique dans ce concept…). Un routeur EGP vérifie en permanence que ses "pairs EGP" sont toujours accessibles (donc que les réseaux autonomes externes auxquels il est relié sont joignables). Enfin il échange régulièrement des informations de mise à jour du routage.
Pour cela, il supporte 9 types de messages: Demande d'acquisition, Confirmation d'acquisition, Refus d'acquisition, Demande de cessation, Confirmation de cessation, Hello (Signe de vie), Je t'ai entendu (réponse Hello), Demande de mise à jour, Mise à jour de routage, Erreur.

EGP n'interprète aucune des indications de distance qu'il transmet. En fait il ne propage que des indications sur l'accessibilité et limite la topologie des réseaux Internet qui l'utilisent à une structure d'arbre entre les systèmes autonomes reliés.

Il est donc généralement abandonné au profit de OSPF ou de protocoles propriétaires comme EIGRP de Cisco.

2.10.3 OSPF

OSPF comporte le routage par type de service: les administrateurs peuvent définir plusieurs routes vers une destination donnée en fonction de qualité de service requise (haut débit, faible délai, sécurité par exemple). Il assure l'équilibrage de charge en plusieurs routes de même coût (voir avantages et inconvénients dans "Conception Optimale des Réseaux…).
Pour les grands réseaux :

- Il travaille à deux niveaux dans des "zones" (systèmes autonomes) interconnectées.
- Il assure une certaine sécurité des messages de routage en les authentifiant.
- Il permet aux routeurs d'échanger des informations de routage acquises de sites extérieurs.

2.10.4 EIGRP

Le protocole permet d'utiliser un routage hybride, s'appuyant sur des vecteurs distances et l'état des liens (bande passante, mémoire, surcharge des processeurs) comme le fait le protocole ISO 10589 (IS-IS). Ce type de routage assure une convergence plus rapide.

Il est utilisable sur des réseaux maillés en définissant des routes avec des distances différentes pour atteindre le même réseau externe. La route la plus courte est choisie tant qu'elle reste opérationnelle.

Il supporte différentes protocoles: IP, IPX, AppleTalk.

3 SECURITE DES RESEAUX ET DES SYSTEMES

Lu dans *Informatique Magazine* [1] de janvier 1997 : « Une caisse d'allocations familiales se voit soutirer 7 MF par un groupe de 6 ou 7 personnes ... », « Les attaques logiques ont entraîné une perte estimée à 1,2 milliards de francs en 1995 en France dont 65% touchent des réseaux étendus », « On estime que d'ici l'an 2000 le commerce électronique sur Internet représentera un chiffre d'affaire compris entre 150 et 600 milliards de US$ (moins de 1 milliard aujourd'hui) ».

La disponibilité de plus en plus grande des réseaux et l'accès de plus en plus fréquent à Internet provoque une demande urgente de sécurisation des échanges sur ces réseaux. Celle-ci induit la mise en place ou l'amélioration de moyens techniques et l'évolution des législations.

3.1 Quelques considérations historico-juridiques en guise d'introduction

Depuis toujours les hommes d'état, les militaires mais aussi les banquiers ou les commerçants se sont posé le problème de la sûreté de leurs communications. Celle-ci était généralement assurée par l'envoi d'un « messager » de confiance, sûr. S'il était connu des personnes qui communiquaient il permettait de garantir, d'authentifier, la source des messages et, à son retour auprès de cette source, que le message avait été bien remis. Sinon, ce messager était porteur d'une lettre de créances. Ce messager pouvait être agressé, ou n'être pas réellement sûr ; l'information dont il était porteur pouvait être volée ou modifiée sous la contrainte ou le chantage : cette information n'était plus sûre. On pouvait la sceller par le sceau de l'émetteur (sceau réputé non copiable ou falsifiable ....). Pour plus de sûreté on pouvait chiffrer le message par un code secret (voir Jules César) : si le message pouvait être intercepté, il ne pouvait plus être lu ou falsifié.

Les besoins et ces techniques millénaires restent d'actualité ; seul le messager a changé avec l'arrivée des moyens de télécommunications modernes.

Un autre élément doit être pris en compte : garantir la sûreté ou la confidentialité des communications est-il compatible avec la sécurité des états ou de la société en général. Ce problème politique et juridique pèse très largement sur les solutions à mettre en œuvre. De manière générale un état ne peut consentir à ce que les moyens de communications qu'il met directement ou indirectement à la disposition du public sur son territoire se retournent contre lui en permettant à un « ennemi », état ou entreprise criminelle ou terroriste, d'utiliser sans contrôle ses moyens de télécommunications. Jusque très récemment, toutes les sociétés ont interdit l'usage sans contrôle de moyens de communications confidentiels ou non. Par exemple la loi française de 1837 stipulait dans un article unique : « *Quiconque transmettra sans autorisation des signaux d'un lieu à un autre, soit à l'aide de machines télégraphiques, soit par tout autre moyen, sera puni d'un emprisonnement de un mois à un an et d'une amende de 1000 à 10000F. Le tribunal fera en outre démolir la machine et les moyens de transmission.* »[2] Cet article était repris pratiquement tel quel dans le code des télécommunications ..... Par ailleurs les moyens de chiffrement sont considérés comme des armes de guerre et, comme tels, soumis à des restrictions d'usage draconiennes.

Un débat de plusieurs années vient de se terminer devant la Cour Suprême aux Etats Unis opposant la raison d'état au droit à l'intimité des citoyens. Il a provoqué l'édition d'une nouvelle loi aux Etats-Unis qui a pris effet le 1 janvier dernier et qui permet l'usage, mais aussi l'exportation, des moyens de chiffrement. En France, une nouvelle loi ou des décrets d'applications à la loi actuelle devrait sortir dans les mois à venir pour fixer la réglementation dans ce domaine et assouplir le régime de quasi interdiction actuel.

Les travaux publiés sur la sécurité des réseaux de données datent de la fin des années 60 (IBM) et des années 70 comme le montre la bibliographie donnée par A. T. Karila dans « Open Systems Security. An Architectural Framework » [3] : initiation des travaux sur le système DES en 1973 par le National Bureau of Standards d'après les projets IBM, travaux de Diffie et Hellman en 1975/1978 pour casser le DES puis utiliser la cryptographie pour la confidentialité et l'authentification, de Merckle et Hellman, de Needham, de Rivest, Shamir et Adleman en 1978, etc.

Des solutions d'architecture ont été proposées pour le DoD (Ministère de la Défense des Etats-Unis) fin 1985 dans le cadre du projet « Kerberos ».

Les concepts de base ont été précisés et un cadre (« framework ») proposé en 1988 à l'OSI dans la norme ISO 7894-2 « Information Processing Systems, Open Systems Interconnection Référence Model, Part 2 : Security Architecture ».

3.2 Les menaces : sécurité et sûreté

Lors du transfert de l'information sur un réseau de télécommunications, différents types d'agression peuvent perturber le message.

La première cause est naturelle et provient des caractéristiques physiques du circuit de communication : bande passante réduite et de mauvaise qualité, bruits et parasites ou utilisation d'une technologie (par exemple le multiplexage harmonique) qui introduit des perturbations. Des solutions techniques classiques et éprouvées (filtres adaptés, égaliseurs de voie, modems, détecteur de qualité de signal, redondance et codes correcteurs d'erreurs) sont couramment utilisées. Elles sont regroupées dans les fonctions de sécurité qui garantissent la fiabilité de l'information : pas de pertes, pas de duplications et taux d'erreurs résiduelles négligeable.

Les autres menaces ont des origines humaines et peuvent être des agressions passives ou actives. Elles relèvent non plus des lois de la nature mais des lois des états et peuvent faire l'objet de poursuites judiciaires. La protection correspondante est assurée par les fonctions de « sûreté ». (Les deux types sont souvent regroupés dans la sécurité, « security » ayant les deux sens en anglais).

Les agressions passives consistent à « voler » des données ou des programmes lors de leur passage sur le réseau. Elles ne causent apparemment aucun préjudice direct puisque contrairement au bien matériel, le propriétaire d'une information volée la possède toujours ; seul un clone en a été réalisé et volé. Les préjudices secondaires peuvent être considérables.

Les agressions actives consistent :

- soit à modifier ou détruire les informations en cours de transfert
- soit à s'introduire (« intrusion ») dans un système informatique via le réseau pour voler des donnés ou des programmes, les détruire, les modifier (virus ..), etc.
-

Elles peuvent être le fait d'intrus ou de pirates (ou internes) à l'entreprise ou de personnes habilitées, maladroites, qui détruisent ou modifient involontairement des informations. Se protéger contre ce dernier type d'agression involontaire est un problème très difficile à résoudre. Il passe en général par un éclatement des droits d'accès pour limiter les risques.

L'OSI a spécifié une architecture de sécurité décrite dans le standard IS 7498-2 ou la norme AFNOR Z 70-102.

Ce standard définit avec précision les types de menaces visées, les concepts de sécurité à utiliser et prévoit une architecture fonctionnelle permettant de mettre en œuvre une *politique de sécurité* dans le cadre d'une architecture de communication qui suit le Modèle de Référence ISO.

3.3 Architecture de Sécurité OSI

3.3.1 Services fournis

3.3.1.1 Services de sécurité

Quatorze services de sécurité sont définis que nous regroupons en cinq parties :

3.3.1.1.1 .Authentification

L'*Authentification de l'entité homologue* fournie au niveau N confirme à une entité de niveau (N+1) que l'entité paire distante est bien l'entité déclarée.
L'*Authentification de l'origine des données* (par le niveau N) confirme que la source des données est bien l'entité (N+1) homologue déclarée.

3.3.1.1.2 Contrôle d'accès

Le service *Contrôle d'accès* assure une protection contre toute utilisation non autorisée des ressources accessibles via l'environnement OSI (ressource OSI ou non-OSI). Ce contrôle se fera conformément aux politiques de sécurité.

3.3.1.1.3 Confidentialité des données

Les services ci-dessous assurent la protection des données contre toute divulgation non autorisée.
La *Confidentialité des données en mode connexion* protège toutes les données d'un utilisateur au cours d'une connexion.

La *Confidentialité des données en mode sans connexion* assure la confidentialité de toutes les données d'un utilisateur dans une Unité de données de service (SDU) en mode non-connecté.
La *Confidentialité sélective par champ* n'assure la confidentialité que des champs de données sélectionnés (en mode connecté ou non).
La *Confidentialité du flux de données* assure la protection des informations qui pourraient être dérivées de l'observation du flux de données.

3.3.1.1.4 .Intégrité des données

Ces services contrecarrent les menaces actives. Ils peuvent prendre cinq formes:

L'*Intégrité en mode connexion avec reprise* assure l'intégrité des données d'un utilisateur au cours d'une connexion et détecte toute donnée modifiée, insérée, supprimée ou rejouée dans une séquence entière d'unité de données de service (SDU) , avec tentative de reprise.
L'*Intégrité en mode connexion sans reprise* rend le même service sans tentative de reprise.
L'*Intégrité en mode connexion sélective par champ* porte seulement sur un ensemble de champs sélectionnés d'une SDU.
L'*Intégrité en mode sans connexion* porte sur l'intégrité d'une SDU; elle peut prendre la forme d'une indication indiquant qu'une SDU a été modifiée. Une forme limitée de protection contre les données rejouées peut aussi être fournie.
L'*Intégrité en mode sans connexion sélective par champ* permet d'indiquer si des champs sélectionnés dans une SDU ont été modifiés.

3.3.1.1.5 Non-répudiation

Ce service peut prendre l'une des deux formes suivantes ou les deux :
La *Non-répudiation avec preuve de l'origine* protège contre toute tentative de l'expéditeur de nier le fait qu'il a envoyé des données ou leur contenu.
La *Non-répudiation avec preuve de la remise* protège contre toute tentative ultérieure du destinataire de nier le fait d'avoir reçu les données ou leur contenu.

3.3.1.2 .Mécanismes spécifiques

Ces mécanismes peuvent être incorporés dans une couche (N) pour fournir certains services décrits ci-dessus.

3.3.1.2.1 Chiffrement (A)

Ce mécanisme peut assurer la confidentialité soit des données soit du flux de données et peut jouer un rôle dans un certain nombre d'autres mécanismes. Il implique l'utilisation d'un mécanisme de gestion des clés (sauf pour des algorithmes irréversibles).

3.3.1.2.2 Signature numérique (B)

Ces mécanismes définissent deux procédures:
- signature d'une entité de données

- vérification d'une unité de données signée

Le processus de signature implique soit un chiffrement soit la production d'une valeur de contrôle cryptographique. Le processus de vérification implique l'utilisation de procédures publiques. La caractéristique essentielle du mécanisme de signature est qu'elle ne peut être produite qu'en utilisant l'information privée du signataire.

3.3.1.2.3 Contrôle d'accès (C)

Les mécanismes correspondants peuvent utiliser l'identité authentifiée d'une entité ou des informations relatives à l'entité. Si une entité essaie d'utiliser une ressource non autorisée (ou avec un type d'accès incorrect) la fonction rejette cette tentative et peut consigner l'événement pour générer une alarme et/ou l'enregistrer dans le *journal d'audit de sécurité*.

3.3.1.2.4 Intégrité des données (D)

Deux aspects sont pris en compte: intégrité d'une seule unité de données (ou d'un seul champ) et l'intégrité d'un flot d'unités de données (ou de champs). Deux processus, l'un au niveau de l'entité émettrice et l'autre au niveau de l'entité destinataire, sont mis en jeux. L'entité émettrice ajoute à une entité de données une quantité qui est une fonction de la donnée. Ce mécanisme ne protège pas contre le fait de rejouer. Pour cela on peut utiliser un horodatage.

3.3.1.2.5 .Echange d'authentification (E)

Ces mécanismes peuvent utiliser des mots de passe, des techniques cryptographiques et/ou des caractéristiques propres aux entités. Ils provoquent le rejet de la connexion ou sa terminaison et une entrée dans le journal d'audit de sécurité et/ou un rapport au centre de gestion de sécurité.

Très souvent il faut utiliser un horodatage et des horloges synchronisées, deux et trois échanges (authentification unilatérale et mutuelle) et des services de non-répudiation réalisés par signature numérique et/ou notarisation.

3.3.1.2.6 Bourrage (F)

Ces mécanismes peuvent être utilisés pour assurer différents niveaux de protection contre l'analyse du trafic. Ils ne sont efficaces que si le bourrage est protégé par un service de confidentialité.

3.3.1.2.7 Contrôle de routage (G)

Les routes peuvent être choisies de façon dynamique. La politique de sécurité peut interdire le passage de données portant certaines étiquettes de sécurité à travers certains sous-réseaux, relais ou liaisons.

3.3.1.2.8 Notarisation (H)

Des propriétés relatives à des données échangées (intégrité, date, origine, destination par exemple) peuvent être garanties par la fourniture d'un mécanisme de notarisation. La garantie est fournie par un *notaire* (tierce personne) en qui les entités communicantes ont confiance et qui détient les informations nécessaires pour *fournir la garantie de manière vérifiable*. Les données doivent être communiquées via des instances de communication protégées et le notaire.

3.3.1.3 Mécanismes communs de sécurité

Ils ne sont pas spécifiques d'un service particulier et ne sont pas incorporés dans une couche spécifique.

3.3.1.3.1 Fonctionnalités de confiance

Toute fonctionnalité qui fournit des mécanismes de sécurité devra être digne de confiance. Ces procédures sont en général coûteuses et difficiles à mettre en œuvre.

3.3.1.3.2 Etiquettes de sécurité

Les ressources comprenant des éléments de données peuvent avoir des étiquettes de sécurité associées pour, par exemple, indiquer leur niveau de sensibilité. Il faut souvent acheminer l'étiquette de sécurité avec les données en transit.

3.3.1.3.3 .Détection d'événements

Cette détection porte sur des violations apparentes de la sécurité et peut également inclure des événements normaux, tels qu'un accès réussi (logon). Les événements détectés peuvent être notifiés aux entités, enregistrés ou entraîner une action de reprise.

3.3.1.3.4 Journal d'audit de sécurité

Les journaux d'audit de sécurité fournissent un mécanisme de sécurité appréciable étant donné qu'ils permettent potentiellement de détecter et d'enquêter sur la violation de la sécurité en permettant un audit ultérieur. (L'analyse et la production de rapports sont considérés une fonction de gestion de sécurité faisant partie de l'administration de réseaux).

3.3.1.3.5 Reprise de sécurité

Elle traite des demandes provenant des fonctions de traitement et de la gestion d'événements. Les actions de reprise peuvent être immédiates (par exemple création d'une coupure immédiate de la connexion), temporaires (par exemple invalidation temporaire d'une entité) ou à long terme (par exemple changement de clé ou introduction d'une entité sur "une liste noire").

Le tableau ci-dessous indique les mécanismes spécifiques utilisés par chaque service de sécurité OSI. (Ces mécanismes sont repérés par l'index A à H correspondant du texte)

Services	**Mécanismes**							
	A	B	C	D	E	F	G	H
Authentification de l'entité homologue	Q	Q			Q			
Authentification de l'origine des données	Q	Q						
Service de contrôle d'accès			Q					
Confidentialité en mode connexion	Q						Q	
Confidentialité en mode sans connexion	Q						Q	
Confidentialité sélective par champ	Q							
Confidentialité du flux de données	Q					Q	Q	
Intégrité en mode connexion avec reprise	Q			Q				
Intégrité en mode connexion sans reprise	Q			Q				
Intégrité en mode connexion sélective par champ	Q			Q				
Intégrité en mode sans connexion	Q	Q		Q				
Intégrité en mode sans connexion sélective par champ	Q	Q		Q				
Non-répudiation, origine		Q		Q				Q
Non-répudiation, remise		Q		Q				Q

3.3.2 Utilisation et placement dans les couches du Modèle ISO

Les services décrits ci-dessus doivent être coordonnés. Leur ordre d'enchaînement est souvent crucial.

3.3.2.1 Etablissement et fonctionnement d'une connexion protégée

La couche N peut imposer des *contrôles d'accès sortant* en déterminant localement si l'établissement de la connexion protégée peut être tenté ou si cela est interdit.

Si l'entité destinataire nécessite une *authentification de l'entité homologue*, un échange d'authentification en deux ou trois échanges doit avoir lieu. Cet échange peut être intégré dans les procédures habituelles d'établissement de connexion.
L'entité destinataire ou les entités intermédiaires peuvent imposer des restrictions de contrôle d'accès.

Si un *service de confidentialité* totale ou sélective a été choisi, une connexion protégée doit être établie (au niveau N). Ceci comprend l'établissement de la (des) clé(s) de travail et la négociation des paramètres cryptographiques.

Un *service d'intégrité des données* requiert aussi une connexion protégée; elle peut être la même que celle établie pour fournir le service de confidentialité et permettre l'authentification.

Si un des *services de non-répudiation* ou les deux ont été choisis, les paramètres cryptographiques appropriés ou une connexion protégée avec une entité de notarisation doivent être établis.

En cours de fonctionnement , durant le transfert de données, l'**authentification** de l'entité homologue doit être fournie **à intervalles réguliers** avec une protection sélective par champ et une notification des attaques actives. **L'enregistrement dans le journal d'audit de sécurité** et la détection/traitement d'événements peuvent être nécessaires.

3.3.2.2 Transmission protégée en mode sans connexion

Les services de sécurité ne sont pas tous disponibles dans ce mode. Les services appropriés sont l'authentification de l'entité homologue, l'authentification de l'origine des données, un service de contrôle d'accès, la confidentialité en mode sans connexion ou la confidentialité sélective par champ, l'intégrité en mode sans connexion sélective par champ ou non et la non-répudiation d'origine..

3.3.2.3 Placement dans le Modèle de Référence

La sécurité des communications dans l'environnement OSI peut être assurée soit par des services de sécurité introduits à certains niveaux du Modèle de Référence, soit par l'introduction de mécanismes de sécurité dans les services de communication.

3.3.2.3.1 Couche Physique

Les seuls services fournis sont la confidentialité en mode connexion et la confidentialité totale ou limitée du flux de données.

Le mécanisme de chiffrement total du flux de données est le principal mécanisme de sécurité au niveau Physique.

3.3.2.3.2 Couche Liaison de données

Les seuls services fournis sont la confidentialité en mode connecté ou en mode sans connexion.

Le mécanisme de chiffrement est disponible; il est sensible au protocole de la couche Liaison utilisé.

3.3.2.3.3 Couche Réseau

La couche Réseau peut fournir 8 services de sécurité: authentification de l'entité homologue et de l'origine des données, service de contrôle d'accès, confidentialité en mode connexion, en mode sans connexion et du flux de données, intégrité en mode sans connexion sans reprise et intégrité en mode sans connexion.

Il est aussi possible d'utiliser les mécanismes de sécurité suivants: échange d'authentification, chiffrement, signature numérique, contrôle d'accès, contrôle de routage, confidentialité du flux de données et intégrité des données.

3.3.2.3.4 Couche Transport

La couche Transport peut fournir 8 services de sécurité: authentification de l'entité homologue et de l'origine des données, service de contrôle d'accès, confidentialité en mode connexion et en mode sans connexion, intégrité en mode sans connexion avec et sans reprise et intégrité en mode sans connexion.

Il est aussi possible d'utiliser les mécanismes de sécurité suivants: échange d'authentification, chiffrement, signature numérique, contrôle d'accès, et intégrité des données.

La **couche Session** ne comporte aucun service ou mécanisme de sécurité.

3.3.2.3.5 Couche Présentation

La couche Présentation ne fournit **aucun service de sécurité** mais offre des mécanismes de sécurité qui peuvent être utilisés conjointement avec les mécanismes de la couche Application pour fournir les services de sécurité au niveau Application.

Il s'agit essentiellement des mécanismes de transformation syntaxique (chiffrement), d 'intégrité des données, de signature et de notarisation.

Seuls les services de confidentialité peuvent être entièrement fournis par des mécanismes de sécurité contenus dans la couche Présentation en utilisant une syntaxe de transfert appropriée.

3.3.2.3.6 Couche Application

La couche Application peut fournir tous les services de sécurité décrits ci-dessus (§ 1.1).

La couche Application peut aussi offrir des mécanismes de chiffrement, de signature numérique, de contrôle d'accès, de bourrage et de notarisation. Elle utilise des mécanismes offerts par les couches inférieures, notamment la couche Présentation.

Notons enfin que le **Processus d'Application** lui-même peut fournir des services de sécurité.

Le tableau ci-dessous indique de manière synthétique l'emplacement des services de sécurité OSI dans l'architecture de communication.

Services	Couche						
	1	2	3	4	5	6	7
Authentification de l'entité homologue			Q	Q			Q
Authentification de l'origine des données			Q	Q			Q
Service de contrôle d'accès			Q	Q			Q
Confidentialité en mode connexion	Q	Q	Q	Q			Q
Confidentialité en mode sans connexion		Q	Q	Q			Q
Confidentialité sélective par champ							Q
Confidentialité du flux de données	Q		Q				Q
Intégrité en mode connexion avec reprise				Q			Q
Intégrité en mode connexion sans reprise			Q	Q			Q
Intégrité en mode connexion sélective par champ							Q
Intégrité en mode sans connexion			Q	Q			Q
Intégrité en mode sans connexion sélective par champ							Q
Non-répudiation, origine							Q
Non-répudiation, remise							Q

3.4 Architectures de sécurité

Dès 1978 les réseaux en commutation de paquets en mode connecté (protocole X25, utilisé sur Transpac par exemple) fournissaient un certain niveau de sécurité par la mise en œuvre des Groupes Fermés d'Usagers (GFU). Un GFU est représenté par des listes de ses membres situées dans les commutateurs d'accès au réseau. Ceux-ci refusent l'accès à tout hôte ne faisant pas partie du GFU s'il veut communiquer avec l'un de ses membres. Ce contrôle d'accès peut être bidirectionnel ou limité aux appels entrants ou sortants. Il est possible, sur les réseaux privés, de compléter ce mécanisme de contrôle d'accès par une authentification des systèmes appelants.

Les travaux sur la sécurisation des réseaux de paquets ont été initiés à la demande du DoD (Ministère de la Défense des Etats Unis) et ont été développés dans le cadre du projet Kerberos au début des années 1980 (document de base : 1985) [4]. Ces travaux ont servi de base aux propositions de l'OSF (Open System Facilities) pour son environnement DCE (Distributed Communication Environnement).

D'autres travaux ont été menés dans le cadre des banques pour sécuriser leurs échanges. Ils ont donné lieu à des protocoles comme PSIT ou ETEBAC 3 ou 5. [5] [6] [7]

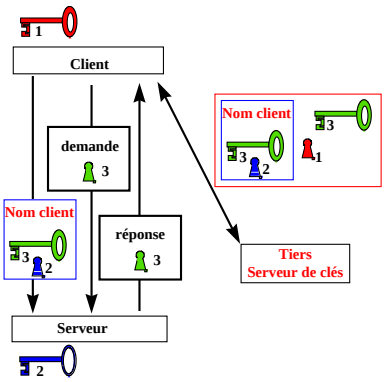
Enfin certains constructeurs, notamment IBM, ont développé leurs propres outils de base (par exemple le code à clé privée DES et les moyens pour sécuriser les échanges par son utilisation).

3.4.1 Architecture Kerberos

Elle est fondée sur l'utilisation d'un système de chiffrement des mots de passe à clés privées qui utilise le DES. Un Tiers de confiance hiérarchique connaît les clés utilisateur et serveur.

Kerberos établit une relation de bout en bout asymétrique entre utilisateur et serveur. Aucun mot de passe n'est transmis sur le réseau mais les mots de passe utilisateur sont utilisés comme clés de chiffrement de clés. Cette architecture prototype présente quelques problèmes légaux en mettant en œuvre le DES dont l'usage est encore limité ou au moins interdit d'exportation dans certains pays. Ainsi il peut être légalement très difficile d'authentifier une signature ou une clé d'intégrité dans des échanges internationaux. Prototype, il fait l'objet de différentes "incarnations". Il ne possède pas d'interface standardisée et présente certaines faiblesses.

Le schéma ci-dessous illustre les mécanismes d'échange de clés qui permettent l'authentification réciproque par un échange de mot de passe sécurisé. Il nécessite un tiers de confiance serveur de clés.



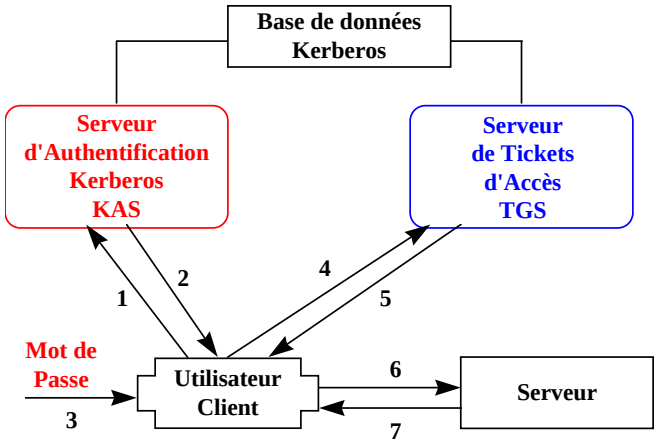
Les échanges entre un client et un serveur sont sécurisés par une clé 3.

Cette clé est transmise au client dans un « coffret » fermé par sa clé privée 1. Dans ce coffret le serveur de clés lui envoie aussi un coffret destiné au serveur, fermé par la clé privée 2 de celui-ci, et contenant la clé 3 de sécurisation des échanges.
Le client retransmet ce coffret au serveur pour lui communiquer la clé 3.

Le protocole d'authentification utilise une base de données sûre Clients - Services

Le schéma ci-dessous montre l'enchaînement des échanges entre client, serveur, serveur d'authentification et serveur de tickets d'accès.

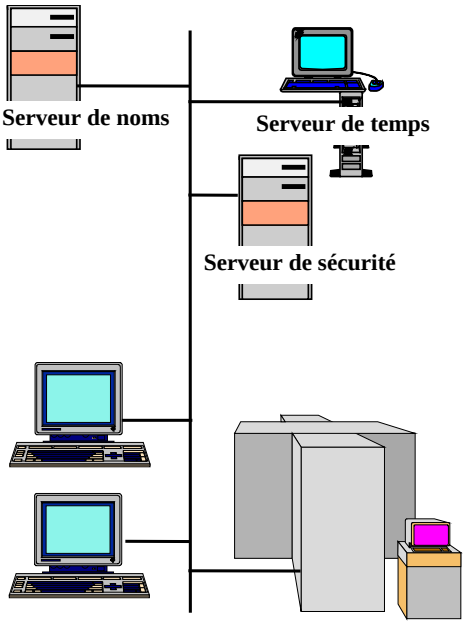
1: demande initiale d'authentification
2: paramètre d'authentification chiffré
enregistrement chiffré par le mot de passe de l'utilisateur
3: mot de passe pour déchiffrer le ticket
4: requête au service de Ticket
5: réception d'un Ticket de service chiffré
6: envoi du Ticket de service et de paramètres au serveur
7: contrôle du Ticket de service;
renvoi de l'heure chiffrée pour authentification



3.4.2 Environnement DCE

(Distributed Communication Environment) [8]

Les stations clientes ont des accès sécurisés aux serveurs grâce à un protocole d'authentification et de contrôle d'accès mettant en jeu plusieurs serveurs collaborant à la sécurité.

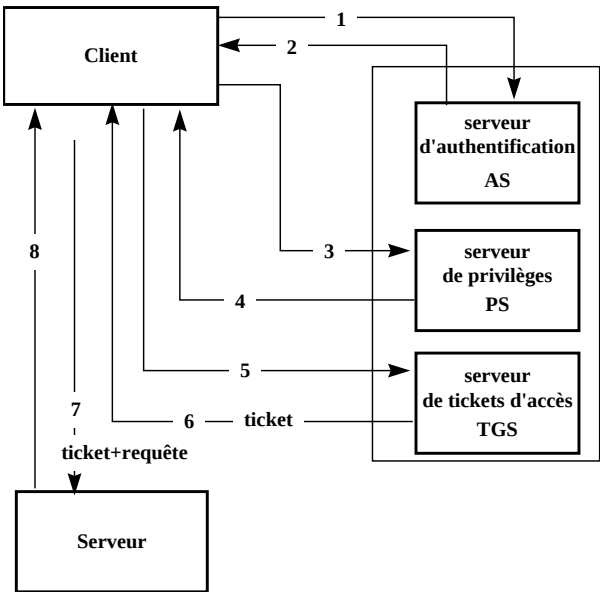


Un Serveur de sécurité permet de centraliser les mots de passe en un seul endroit. Lors du « login » il délivre un ticket.
Un Serveur de temps permet d'utiliser des estampilles temporelles ou une durée de vie limitée aux tickets pour éviter qu'ils puissent être rejoués.

Le réseau peut être scindé en plusieurs cellules : un Serveur de noms de cellule concentre les droits d'accès en un lieu unique . Des protocoles de sécurité inter-cellules permettent d'avoir un «login» unique; ils utilisent un protocole d'appel de procédures distantes (RPC) sécurisé

L'authentification est basée sur la délivrance de tickets de validité limitée dans le temps :
TGT : Ticket-Granting Ticket
PAC : certificat d'attribution de privilège
Cki : temps i (time stamp)

Elle suit le schéma de fonctionnement simplifié suivant :



login DCE
1: demande de TGT
login sans mot de passe
2: TGT et CK1 (chiffré par pwd)
déchiffrement TGT et CK1 par pwd
1 : demande ticket pour SP
2: ticket pour SP et CK2
3: demande de PTGT
4: PTGT avec PAC et CK3

Demande de service
5: demande de ticket pour un service
6: ticket du service et CK4
7: présentation du ticket
8: échange d'aléas

3.5 Internet, Intranet et réseaux virtuels privés : « coupe-feu » et « tunnels » [9] [10]

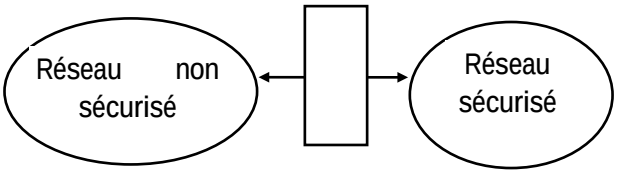
Les entreprises souhaitent généralement disposer de réseaux privés (Intranet) interconnectés entre eux par un réseau étendu privé mais aussi connectés à Internet ou interconnectés via Internet et constituer un réseau virtuel privé (VPN).

La technologie Inet n'a pas été conçue pour être sûre et des équipements matériels ou logiciels doivent être introduits pour améliorer la sécurité.

3.5.1 Fonctions

Les coupe-feu (firewall) sont des systèmes ou ensembles de systèmes qui renforcent les contrôles d'accès aux frontières entre des réseaux, généralement un réseau privé sécurisé et un réseau public comme Internet, entre lesquels ils constituent un goulot d'étranglement. Ils ne correspondent pas à un équipement très précis mais plutôt à une grande variété d'équipements qui reposent sur deux mécanismes de base :

- bloquer une partie du trafic qui les traverse
- permettre la traversée des messages pour certaines applications.



Ils constituent en pratique la mise en œuvre d'une politique de contrôle d'accès qui doit être très bien définie. Les utilisateurs doivent disposer des accès et des services dont ils ont besoin et on ne doit pas leur laisser plus de droits que nécessaire. Tout se trouve dans cet équilibre besoins / restrictions et les coupe-feu ne sont qu'une implémentation de cette politique. Elle consiste à restreindre les accès depuis l'extérieur (du réseau sécurisé) à :

- l'ensemble du réseau ou seulement une partie de ses composants
- à certains services : courrier électronique (Email), Web, transfert de fichiers FTP, accès distants (Telnet, Rlogin, Finger, ...) par exemple

mais aussi à restreindre les services vers l'extérieur, pour éviter la sortie d'informations non seulement de la part des usagers mais à la suite d'intrusions depuis l'extérieur.

Certains services sont très peu sûrs. Par exemple le serveur POP pour le courrier électronique demande la transmission en clair et à intervalles réguliers de l'identificateur et du mot de passe de chaque client. Le service d'administration de réseaux SNMP (v1) permet de découvrir facilement la composition et les caractéristiques d'un réseau et même d'agir à distance sur ces composants ; dans chaque message le champ « Communauté » (Community), sorte de mot de passe qui peut surpasser les droits de «root », est transmis en clair.

3.5.2 Contre quoi se protège-t-on ?

Les coupe-feu peuvent protéger contre les accès non-autorisés du monde extérieur. Ils constituent un goulot d'étranglement où la *sécurité* et l'*audit* peuvent être imposés. Par contre ils ne protègent pas contre les attaques internes ou les attaques qui ne passent pas par eux. Ils ne protègent pas non plus contre les attaques transmises par l'intermédiaire des données introduites dans le réseau sécurisé : virus ou attaques indirectes par des « Applets » Java ou AptiveX.
L'arrivée de ces nouveaux objets crée ainsi un trou de sécurité via les serveurs Web qui jusqu'ici étaient souvent considérés comme un moyen assez sûr de se protéger (les serveurs WEB présentent d'autres trous de sécurité, par exemple à travers des défauts ou insuffisances de l'interface CGI (Common Gateway Interface) qui peut permettre de passer des appels système dans les champs de données RHF (Request Header Field) et de retourner directement des informations au client, sans passer par le serveur, par les programmes « nph-» (non parsed header program)[19].

L'implantation des coupe-feu nécessite de réduire les points d'accès au réseau sécurisé en interdisant tout accès, par exemple par des liaisons téléphoniques directes ou par Transpac, qui ne passent pas par les coupe-feu (backdoors : portes de derrière) : il ne sert à rien de mettre des portes blindées à une maison de papier ou aux fenêtres béantes.

3.5.3 Comment se protège-t-on ?

Deux types de fonctions, offrant plus ou moins de transparence ou de contraintes à l'usager peuvent être implantées :

- un filtrage des paquets IP au niveau Réseau dans les routeurs d'entrées (routeurs filtrants ou sous-ensemble d'un coupe-feu).

- un filtrage des messages au niveau Application par une passerelle logicielle spécialisée (*proxy*). Ce système est plus opaque et contraignant. Un proxy doit être mis en place pour chaque type d'application à protéger. L'accès n'est autorisé qu'après identification ou identification avancée. Après ce contrôle, le proxy permet à l'utilisateur de se connecter au service réel.

3.5.3.1 Serveurs de noms

Ils posent problèmes, le principe du cloisonnement étant de rendre opaque le réseau pour des usagers externes et en particulier de ne pas leur fournir les véritables adresses des systèmes hôtes.

Ils seront donc en général dédoublés :

Un serveur de noms externe (DNS) public est placé hors du périmètre cloisonné ; un autre, qui contient les vrais adresses est placé à l'intérieur et n'est pas visible des usagers externes. Il résout directement les noms pour les accès internes. Il sert de relais aux usagers internes vers le serveur externe pour résoudre les noms des usagers externes.

Pour un usager externe, le serveur de noms externe fournit une résolution normale et une résolution filtrée pour le mode interne ; en général on opérera une translation des adresses.

Un problème va se poser pour les serveurs ftp anonymes qui veulent connaître leurs correspondants (s'ils font partie du monde interne).

3.5.3.2 Autres services : E-Mail, Web, FTP, Gopher, Archie, ...

utilisation d'un proxy
restriction sur les "ports" accessibles
modifier les clients FTP internes ...
inhiber FTP et ne permettre que accès FTP par le Web

Problème pour exporter des fichiers ....

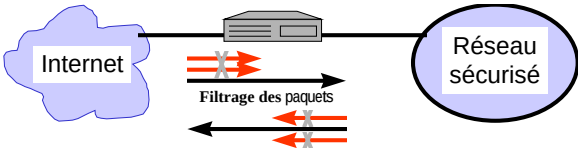
On peut implanter une « méthode PUT » et sécuriser les accès par un formulaire et l'échange de tickets. Cette méthode n'est normalement pas disponible sur les serveurs Web actuels mais peut être implantée assez aisément.

option "PASV"
serveur FTP distant doit permettre au client d'initier la connexion

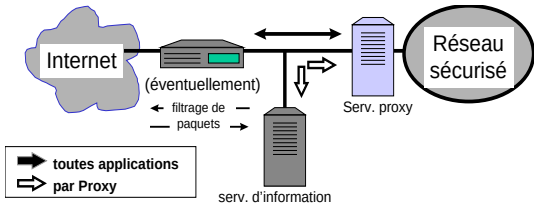
Gopher, Archie
accès par le Web seulement (proxy Web)

3.5.3.3 Configurations:

Plusieurs configurations plus ou moins complexes ou contraignantes peuvent être mise en place :

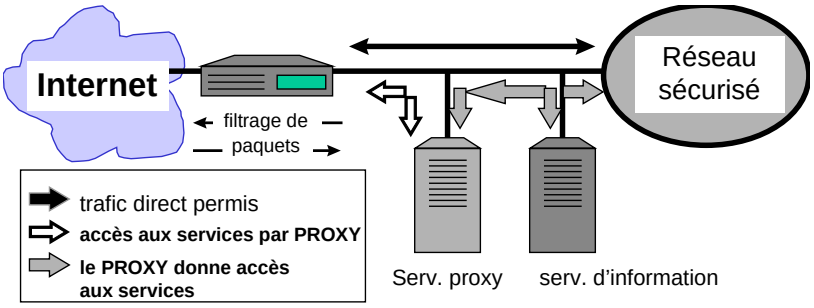


- filtrage des paquets. Le coupe-feu effectue le contrôle d'accès et ne laisse passer que les paquets IP autorisés.

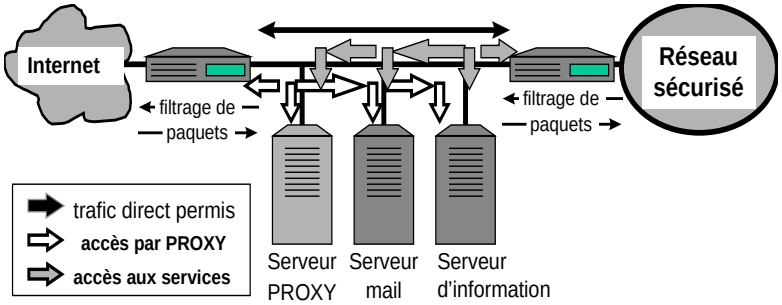


- Passerelle à double attachement

- Masquage du réseau sécurisé par une traduction d'adresses et identification avancée des utilisateurs. Un historique et des statistiques de sécurité sont disponibles.



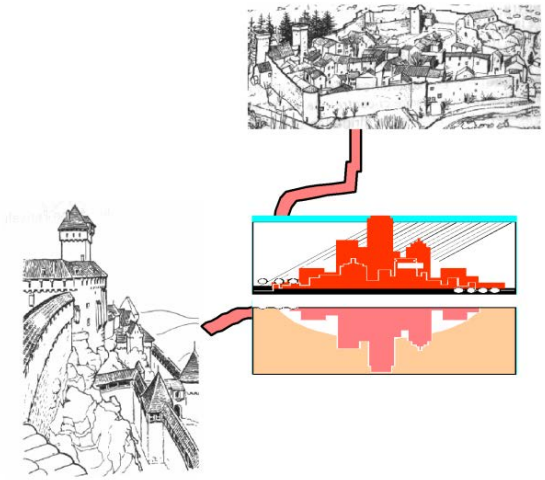
- Hôte écran. Plus souple et moins sûr que le système précédent, il permet le trafic direct entre réseau sécurisé et Internet ; le passage par le proxy n'est obligatoire que pour certains services sensibles.



- Sous-réseau écran : placé entre Internet et réseau sécurisé, un sous-réseau est le seul point commun accessible depuis les deux réseaux interconnectés. Il masque le réseau sécurisé et permet des débits plus importants que le système précédent. On peut également permettre un certain trafic direct. Il héberge différents serveurs : Serveur Web, Serveur FTP anonyme, Serveur de courrier public, etc

Les analyseurs de sécurité constituent une technique voisine de celle des coupe-feu. Ils analysent le trafic destinés à certains serveurs et forcent la déconnexion des usagers non autorisés.[11]

3.5.4 Réseaux virtuels privés



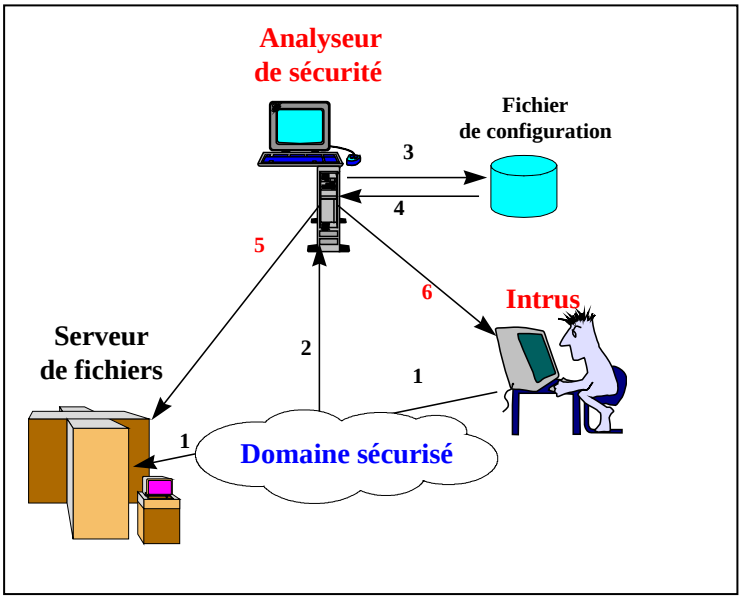
Un réseau virtuel privé est constitué par la réunion de plusieurs réseaux privé (réels) par l'intermédiaire d'un réseau public. Chacun des réseaux composants est accessible via un coupe-feu. Ces coupe-feu sont interconnectés deux à deux par des « tunnels » sécurisés qui transportent des informations chiffrées et protégées par des clés d'intégrité ou des signatures digitales. Ces « tunnels » doivent constituer des *moyens de communications sûrs* entre les réseaux interconnectés. Le protocole PPTP (Point-to-point Tunneling Protocol, projet de l'IETF [18], permet de construire ce type de tunnels.

Digital Equipment offre un tel service à travers Altavista.

3.5.5 Utilisation d'un serveur de sécurité

Cette technique est une alternative simple au système de "coupe-feu"

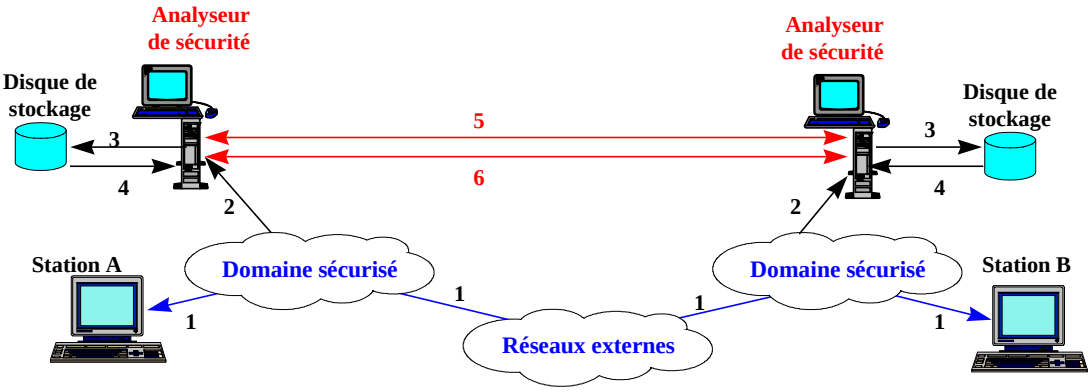
3.5.5.1 Contrôle d'accès Intra-domaine



1: Invisible; fonctionnement réseau non modifié
Coupure de connexion
2: Observation du message de l'intrus par l'analyseur
5: Fermeture en se faisant passer pour l'intrus
6: Fermeture en se faisant passer pour le serveur

3.5.5.2 Intégrité des données « inter-domaines »

3: Analyseurs créent et stockent les sceaux pour les messages
4: Analyseurs retrouvent les sceaux pour les messages
5: Authentification mutuelle
6: Comparaison des sceaux pour un message: les messages sont signés
analyseurs peuvent aussi servir à la non-répudiation (s'ils sont "notaires")



3.6 La sûreté sur Internet : nouveaux développements (12) [13]

La sûreté sur Internet ne peut s'appuyer sur des coupe-feu : par définition ce réseau est public et accessible à tous. Cependant son développement doit permettre de l'utiliser pour des services qui doivent être sécurisés, par exemple pour le commerce électronique ou le transfert d'informations sensibles.

3.6.1 Présentation

Ces nouveaux développements s'articulent autour de trois axes :

- l'authentification des utilisateurs et des serveurs
- l'authentification des données, la garantie de leur intégrité et leur non-répudiation d'origine par signature digitale
- Le chiffrement des données.

Les deux premiers points ne posent plus de problèmes légaux. Le troisième est encore en discussion. Tout le monde admet que la protection de certains champs de données sensibles doit être assurée (par exemple les mots de passe, les signatures digitales, les clés d'intégrité, les codes des cartes bancaires...) mais un chiffrement vraiment sûr de toutes les données est encore interdit et risque de rester soumis à des restrictions. L'une des deux solutions suivantes, par exemple, pourrait être retenue :

- Chiffrement à deux niveaux avec l'un des deux codes déposé auprès des organismes de sécurité
- Utilisation sans contrainte d'un chiffrement d'un niveau (assez) faible (embrouillage) et obligation de dépôt des clés d'un niveau fort auprès d'un tiers de confiance.

Les travaux en cours sont nombreux et publiés sur le Web depuis quelques mois ; les propositions fleurissent et des choix vers des standards doivent se dessiner dans les mois prochains. Les grands fournisseurs de moyens informatiques et de produits réseaux : Microsoft, Netscape, HP, IBM, Bull, Schlumberger, Siemens, RSA, Spyrus, BBN, Cylink, etc. collaborent entre eux et avec des organismes utilisateurs comme Visa, Mastercard ou American Express ou des prestataires de services, comme Verisign, GTE, Verifone, etc. candidats aux postes de tiers de confiance.

A l'heure actuelle une solution est librement disponible gratuitement sur Internet : le protocole PGP (Pretty Good Pricacy) de P. Zimmermann [14] ; ce logiciel est exportable depuis que P. Zimmermann a gagné son procès devant la Cour Suprême des Etats Unis durant l'été 1996. Il reste cependant interdit de le distribuer en France (6 mois d'emprisonnement, 200 000F d'amende selon la loi 96-959 du 26 juillet 1996 [1]. Il présente différentes fonctions de sécurité dont certaines sont autorisées (ou plutôt tolérées ...) :

- envoi de documents signés et intègres (clé d'intégrité et signature électronique chiffrés par un code RSA)
- envoi de données embrouillées (chiffrement faible).

Il permet aussi le transfert (interdit en France) de données chiffrées.
Il offre donc de facto un ensemble de fonctions que les projets indiqués ci-dessus prévoient de mettre en place de manière standard.

En effet le client demande le secret de ses échanges, l'intégrité des données transmises, l'authentification des utilisateurs, des serveurs et des données et la possibilité de réaliser des transactions sûres. Ces fonctions doivent être intégrées dans les services existants, être interopérables entre différents types de services et de serveurs, administrables et utilisables même à grande échelle.

L'industrie demande la définition des standards, la fiabilité des systèmes mais aussi la mise en place de tiers de confiance susceptibles de délivrer des certificats de confiance pour authentification, de les révoquer, de les doter d'estampilles temporelles ou de stocker des informations permettant de garantir la non répudiation d'origine et de remise des messages échangés même à long terme.

Les services de sécurisation peuvent être regroupés dans quelques sous-ensembles :

- Protocoles de Transfert sécurisés :
  - SSL (Secure Socket Layer) de Netscape, PCT (Private Communication Technology) ou plutôt TLS (Transport Secure Layer) qui résulte de la fusion de SSL et PCT (plus précisément de l'ajout de fonctions de PCT dans SSL ; projet commun Microsoft - Netscape).
  - Secure TCP/IP prévoit l'intégration de fonctions de sécurité dans le protocole IP (v6). Il introduit un champ d'en-tête pour l'authentification et un champ de données utilisateurs (payload) encapsulé confidentiel et intègre.

  D'autres propositions, non traitées ici, sont aussi soumises à l'IETF.

- Protocoles d'application :
  - PFX : Personnal Information eXchange de Microsoft
  - Portefeuille sécurisé de Microsoft,
  - S-HTTP : proposition de Veriphone, IBM, Compuserve, America-on-line, etc. pour sécuriser les accès Web. Ce protocole constitue une sur-couche à HTTP. Clients et Serveurs reçoivent des services équivalents permettant le chiffrement des données et l'authentification par échange de certificats. Il permet de négocier le type de chiffrement et d'échanger des clés et des résumés d'information.
  - SET : Secure Electronic Transaction, proposition de Visa, Mastercard, American Express, IBM, Netscape, SAIC, Microsoft, etc. est basé sur l'utilisation de certificats d'authentification.
  - JEPI : Joint Electronic Payement Initiative proposé par WWW Consortium et Commerce Net, propose les moyens de construire une plate-forme de paiement universelle en permettant une négociation entre différents protocoles ou logiciels de paiement. Il comporte deux parties : PEP, insérée dans HTTP pour assurer le transport des informations vers/ou depuis des serveurs Web, et UPP, syntaxe de transfert standard entre les systèmes de paiement.

- Authentification des clients et des serveurs : par exemple authentification des serveurs de logiciels pour garantir l'origine des produits acquis par téléchargement à travers Internet.
- Signature digitale : pour garantir l'intégrité et l'intégrité de la source des données. Elle permet aussi la non répudiation d'origine.

- Chiffrement : il constitue le service de base qui assure la mise en place des autres services et le chiffrement des données utilisateur proprement dites.

3.6.2 Signature digitale et authentification [15]

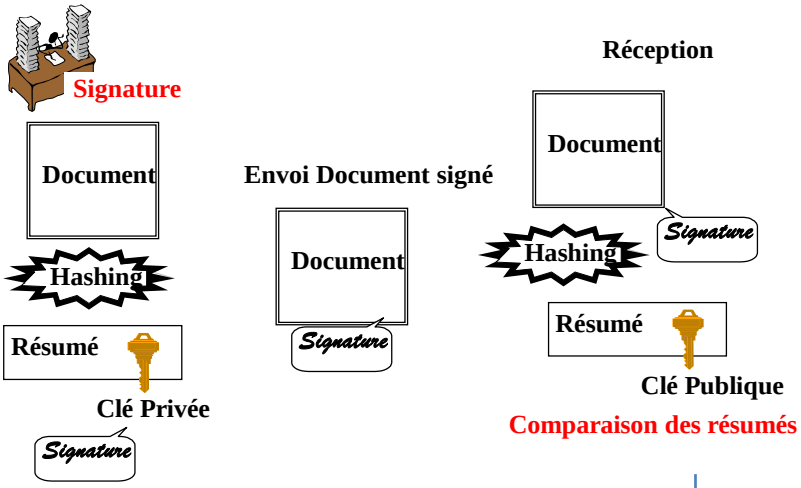
Si le chiffrement des données garantit leur confidentialité, il est insuffisant car il ne permet pas de garantir leur intégrité (modification, destruction partielle, virus), ni leur origine. Un utilisateur qui reçoit ces données doit aussi être sûr de son origine (serveurs pirates ...).

Les fonctions d'intégrité et d'authentification sont fournies par un mécanisme de signature digitale qui offre un degré de sécurité supérieur à une signature manuscrite puisqu'elle fournit les fonctions de signature et de scellement. Cette signature est nécessaire pour le courrier électronique, le commerce, les transferts de fond ou la garantie des produits numérisés. Elle est délivrée ou garantie par une autorité de certification (CA). Elle utilise un système de chiffrement à clé publique (par exemple RSA) et comporte 6 champs (clé publique du propriétaire - nom du propriétaire - date d'expiration de la clé publique - nom du distributeur - numéro de série de la signature digitale - signature digitale du distributeur).

Une signature digitale a une durée de vie limitée et doit pouvoir être révoquée. Par contre un document signé peut avoir une durée de vie longue. Une estampille temporelle, qui ne doit pas pouvoir être contrefaite même à très long terme, permet de prouver la validité de la signature même après sa durée de vie. Pour cela une empreinte (résumé) du document, signée et horodatée, est chiffrée et estampillée par un tiers de confiance. Le mécanisme utilisé (DTS : Digital Time Service) est le suivant :

- une empreinte, résumée du document (par une fonction de hachage), est envoyée au service DTS.
- le DTS retourne l'empreinte *horodatée et signée par lui*. Il peut en prendre une copie (*notarisation*). Le DTS ne peut connaître le document dont il ne reçoit que l'empreinte et reste ainsi confidentiel.
- le document et son estampille prouve la date de dépôt de ce document (par exemple pour prouver l'antériorité d'un brevet secret) En cas de contestation, il suffit de comparer une empreinte du document et l'empreinte estampillée.

La signature digitale permet aussi *l'authentification de l'origine et le contrôle d'intégrité des données*. Pour cela le document, signé par signature digitale, est résumé par une fonction de hachage. Cette empreinte est chiffrée par la clé privée du signataire. Elle constitue la signature du document ; elle est transmise avec lui. A la réception, on réalise une empreinte du document avec la même fonction de hachage et on déchiffre la signature par la clé publique de l'émetteur pour retrouver l'empreinte émise. Il suffit de comparer les empreintes pour garantir que le document reçu est

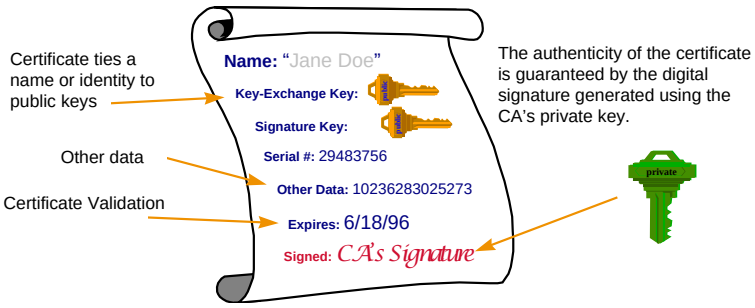


intègre et qu'il a été scellé par la clé privée de l'émetteur. L'authentification est réalisée par analyse de la signature en contrôlant le numéro de série, la clé publique et la date de validité garantis par la clé privée du serveur d'authentification.

3.6.3 Authentification par certificat [12]

Un serveur de confiance délivre des certificats d'authentification qui peuvent permettre un accès contrôlé et sécurisé à des serveurs. Munis d'une signature digitale, ces certificats évitent de se faire identifier par mot de passe auprès de chaque site Web sécurisé auquel on veut avoir accès. Ces mots de passe ne circulent plus sur le réseau et ne peuvent plus être interceptés et rejoués ; seul un mot de passe local, sur la machine du client, est utilisé. Le butineur (browser) client présente un certificat au serveur Web qui vérifie l'identité de l'usager, contrôle ses droits d'accès et, grâce à des informations spécifiques, peut personnaliser ses accès. Microsoft propose la structure ci-dessous pour les certificats d'authentification :

- Nom du client
- Clé publique pour l'échange de clés
- Clé publique pour signature
- Numéro de série
- Informations spécifiques
- Date d'expiration
- Signature du tiers de confiance délivrant le certificat et générée en utilisant sa clé privée.



Ainsi les serveurs n'ont à connaître que la clé publique des Tiers de confiance.

Les serveurs de certificats et les clients doivent chacun générer un couple clé publique/clé privée. Le client demande son inscription au serveur (enrolment) en lui envoyant un identificateur de client et un identificateur du fournisseur de service, signé par sa signature digitale. Le serveur d'authentification vérifie ses droits et lui délivre un certificat signé contenant des extensions liées à sa demande et ses droits.

3.6.4 TLS : Transport Layer Structure [16]

Strictement basé sur SSL (Socket Secure Layer) [17], surtout conçu pour sécuriser les accès Web par HTTP, dont il reprend les mécanismes de chiffrement et d'acquittement (Handshake) ; il contient des extensions issues de PCT (Private Communication Technology) pour assurer l'interopérabilité, l'extensibilité, par exemple pour FTP ou Telnet, et de meilleures performances. Le « draft » TLS clarifie aussi la proposition SSL.

Comme SSL et PCT, il constitue une couche de sécurité au dessus de la couche Transport TCP. Sa sous-couche inférieure permet d'encapsuler des protocoles de sécurité variés fournis

par la sous-couche supérieure, par exemple un protocole avec acquittement (HandShake) utilisé pour sécuriser la connexion ou un protocole d'intégrité en phase de transfert.
Dans la phase de connexion, on peut négocier des algorithmes, échanger des valeurs aléatoires, des paramètres cryptographiques ou des certificats d'authentification. Il permet, en particulier, de générer un message « secret maître » partagé de 48 octets (384 bits) à partir du secret « pré-maître » et des valeurs aléatoires. La demande d'authentification est normalement basée sur un échange de clés publiques, mais des clés privées, partagées à l'avance, peuvent aussi être utilisées.
Durant la phase de transfert un service d'intégrité est assuré ; il est éventuellement complété par un service de chiffrement des données par clés privées (basé sur le DES ou IDEA) qui utilise une clé secrète calculée à partir de la clé maître et des valeurs aléatoires échangées durant la connexion.

3.6.5 Services Application

3.6.5.1 Portefeuille électronique [12]

Ce « portefeuille » (wallet), proposé par Microsoft, peut contenir de manière sûre toutes les références sensibles d'un utilisateur : Certificats - Numéro de cartes à puce - Informations privées, etc. Ces informations ne pas accessibles directement mais à travers des services pour des opérations spécifiques.
Le portefeuille ne peut être dupliqué ; il est situé sur un seul système à la fois, celui sur lequel travaille l'utilisateur et il doit pouvoir se déplacer avec lui de manière sûre. Pour cela Microsoft propose d'utiliser PFX (Personal inFormation eXchange)

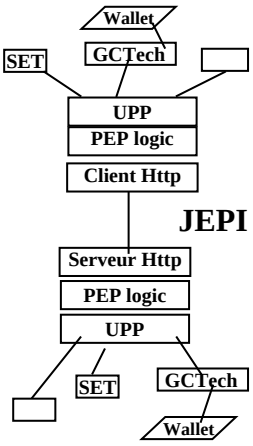
3.6.5.2 Echange d'informations personnelles (PFX) [12]

Accéder à des serveurs sécurisés multiples pose, à l'utilisateur, le problème de l'authentification de ces serveurs et de son authentification auprès d'eux qui requiert d'utiliser une grande variété d'identificateurs et de mots de passe. Un utilisateur doit pouvoir transmettre de manière sûre des informations relatives à son « identité » : Clés privées, Certificats, Certificats des partenaires récents, secrets assortis ...
Pour cela il est souhaitable de disposer d'une syntaxe de transfert unique indépendante de la plate-forme sur laquelle doit être déposées ces informations.

Ces plates-formes peuvent être rangées dans deux ou trois mondes :

- en ligne. Les systèmes (Network Computer, «Internet Toaster») ne comportent pas de disque dur, de disquette, de carte à puce. Les secrets doivent alors être transportés sur le réseau.
- hors ligne. Les systèmes sont munis de lecteurs de disquettes. Le transport des secrets est effectué par celles-ci. La protection physique des secrets n'est plus du ressort du réseau ; ceci réduit la difficulté de chiffrement.
- moyens annexes. On utilise des cartes à puce pour porter les clés et des cartes à mémoire (fat card.) pour données privées

3.6.5.3 JEPI: Joint Electronic Payement Initiative



Proposé récemment (fin 1996- début 1997) par l'organisme W3C ce service est destiné à fournir les services de communications sur lesquels doivent reposer les moyens de payement sécurisé comme SET (voir ci-dessous), mais aussi des systèmes plus spécifiques (propriétaires) comme Gctech, CyberCash, etc. **Il introduit des mécanismes permettant de négocier les moyens de payement.**

Ceux-ci sont inclus dans des compléments au protocole HTTP:

- UPP: Préambule
- PEP: Extensions à HTTP

3.6.5.4 SET : Secure Electronic Transaction

SET propose une solution qui n'implique pas la transmission des coordonnées bancaires du client sur le réseau et permet à un commerçant de s'assurer de la validité d'une commande.

Le client demande, via Internet et le Web, un certificat d'authentification basé sur des clés publiques RSA auprès de l'organisme gérant sa carte bancaire. Ce certificat est utilisé par le client Web du client ... commercial, au moment de l'achat, le client Web envoie ce certificat au commerçant dont le serveur Web peut vérifier la validité directement auprès du serveur bancaire. SET peut être utilisé conjointement avec SSL ou TLS ou S-HTTP. Un complément, C-SET (Chip-SET) est à l'étude pour permettre la sécurisation des transactions au moyen d'une carte bancaire lue par un lecteur de carte à puce sur le poste client.

3.7 Politiques de sécurité : Niveau de sécurité des systèmes

3.7.1 « Orange book »

3.7.1.1 Présentation

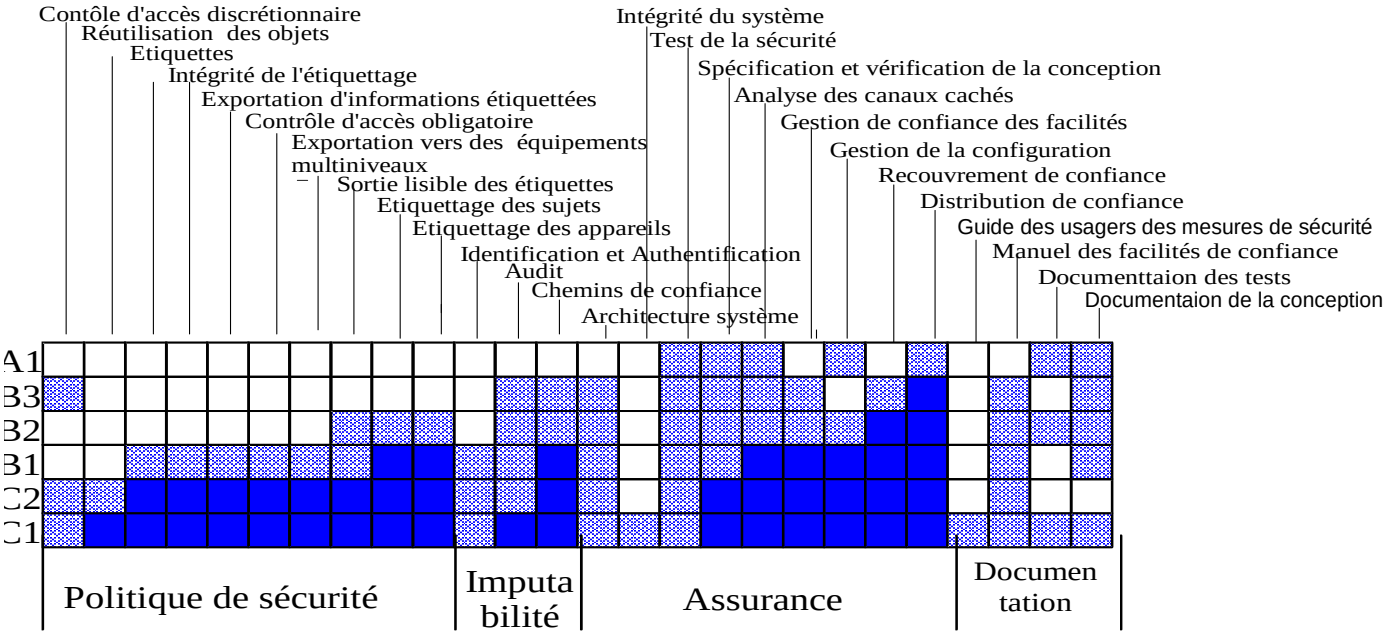
Basé essentiellement sur la confidentialité
Besoins fondamentaux

- Politique de sécurité
- Marquage:
- étiquettes de contrôle d'accès associées aux objets
- Identification des usagers individuellement
- Imputabilité:
  - garder les traces sélectives des audits pour retrouver les responsables
- Assurance:
  - mécanismes hard/soft évalués indépendamment
- Protection continue

3.7.1.2 Classes de critères

D : Protection minimale
C1: Protection de sécurité discrétionnaire
Séparation des usagers et des données
limitation d'accès sur une base individuelle
C2: Protection par contrôle d'accès
Login
Audit des événements de sécurité
Isolation des ressources
B1: Protection de sécurité étiquetée
Etiquetage des données
Contrôle d'accès obligatoires sur des sujets et des objets nommés
B2 : Protection structurée
Relativement résistant à la pénétration
B3 : Domaines de sécurité
Haute résistance à la pénétration
Administrateur de sécurité requis
A1 : Conception vérifiée
Comme B3 mais vérifications

La table ci-dessous permet d'évaluer ces critères.



pas de demande additionnelle

demande nouvelle ou renforcée

pas de demande

3.7.2 Standard européen : ITSEC

Information Technology Security Evaluation Criteria

Cible d'évaluation : TOE (Target Of Evaluation)
- Produit ou système
- Cible de sécurité associée à TOE
- Niveau visé
- Fonctionnalité de la TOE

* Objectifs de sécurité
* Fonctions de sécurité : 8 titres
  - Identification et authentification
  - Réutilisation d'objets
  - Contrôle d'accès
  - Fidélité
  - Imputabilité
  - Continuité de service
  - Audit
  - Echange de données
* Mécanismes de sécurité

Assurance

* Critères de correction : E0 à E6
  vérifier spécification et réalisation de la fonctionnalité visée
* critères d'efficacité

10 classes: codées C1, C2, B1, B2, B3, E2, E3, E4, E5, E6

Leur combinaison correspond sensiblement aux classes définies dans l'Orange Book

F/C1+E2 = C1
F/C2+E2= C2
F/B1+E3= B1
F/B2+E4= B2
F/B3+E5= B3
F/B3+E6= A1

3.7.3 Common criteria (CC)

Les différentes instances mondiales chargées de l'évaluation de la sécurité se sont regroupées pour définir les concepts et les critères permettant d'évaluer la sécurité des systèmes. Leur approche est différente de celle de l'Orange Book ou des ITSEC : elle n'essaie plus de définir des niveaux de sécurité universels mais d'associer le niveau de sécurité au **profil** des applications utilisatrices.

Document en cours de rédaction (voir aussi http://csrc.nist.gov/cc/)

Regroupement de 6 organismes autour d'un projet commun : Common Criteria
Différents aspects
- Exigences fonctionnelles
- Exigences d'assurance
- Profils de protection (PP)
  définis à partir d'un ensemble d 'objectifs et d'exigences de sécurité
  pour un groupe d'utilisateurs ayant des besoins de même type
  indépendant de l 'implémentation

7 niveaux d'assurance de l'évaluation : EAL
- niveaux 1 à 4 : possible à atteindre avec des produits déjà développés
- niveaux 5 à 7 : exigences spéciales

Cibles :
- d'évaluation (TOE) : partie du système soumise à évaluation
- de sécurité (ST) : objectifs, mesures de sécurité et d'assurance, spécifications,

3.7.3.1 Concepts clés

Cible de sécurité (ST)
- objectifs et exigences de sécurité pour un produit ou système spécifique

mesures fonctionnelles et d'assurance offertes par ce produit
Conforme à un ou plusieurs profils de protection
base de l'évaluation

Cible d'évaluation (TOE)

Produit ou système TI, Objet de l 'évaluation

avec documentation utilisateur et administrateur

Fonctions de sécurité de la TOE (TSF)

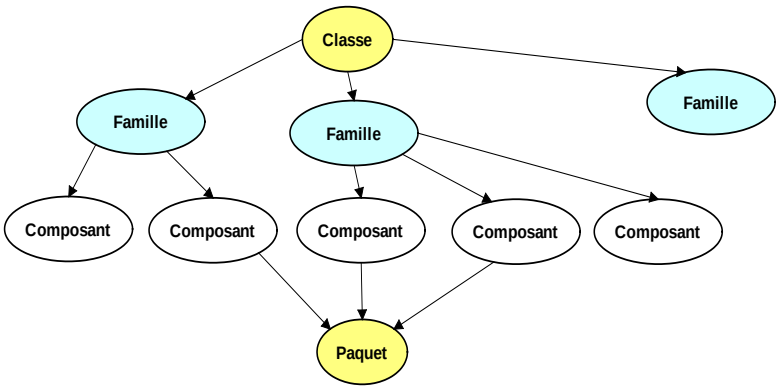
parties de la TOE auxquelles il faut se fier pour que la politique de sécurité soit correctement appliquée

Politique de sécurité de la TOE (TSP)

Règles de gestion, de protection et de répartition des biens au sein d'une TOE

3.7.3.2 Composants

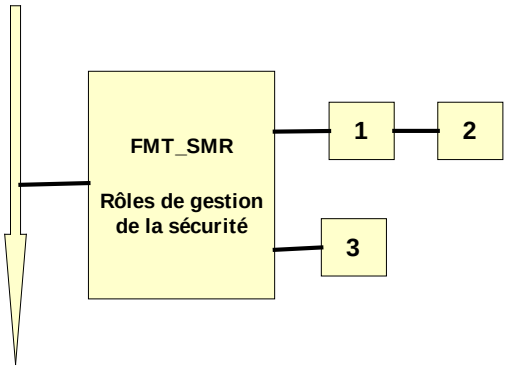
Prise en compte de menaces
Organisation hiérarchique
familles
classes



Désignation : concaténation
nom de classe
nom de famille
numéro d'ordre

Dépendances
entre composantes fonctionnelles
entre composants d 'assurance
mixtes (plus rarement)

Opérations
pour contrer une menace particulière
spécification, sélection, itération, raffinement



3.7.3.2.1 Exigences fonctionnelles

Ensembles ordonnés d'éléments fonctionnels
11 classes
FAU : Audit de la sécurité
FCO : Communication

garantir l'identité
non répudiation d'origine
non répudiation de la réception
FCS : Support cryptographique
FDP : Protection des données de l'utilisateur
FIA : Identification et Authentification
FMT : Gestion des attributs de sécurité
Intégrité
Définir et attribuer aux utilisateurs les rôles de gestion de la sécurité
FPR : Protection de la vie privée
Protection des utilisateurs contre connaissance ou utilisation indue de son identité
FPT : Protection des fonctions de sécurité de la TOE
Gestion des mécanismes et des données de la TSF
FRU : Utilisation des ressources
Disponibilité (CPU, stockage)
Tolérances aux pannes, priorités de service, allocation de ressources
FTA : Accès à la TOE
Etablissement d'une session
FTP : Chemins et Canaux de confiance
Chemins entre utilisateurs et TSF ou entre TSF
Echanges garantis'

Extensible : agréés par organisme de certification

3.7.3.2.2 Exigences d'assurance

2 classes pour évaluation des PP et des ST
APE : Évaluation d'un Profil de Protection
ASE : Évaluation d'une cible de sécurité
7 classes pour évaluation d 'une TOE
ACM : Gestion de configuration
ADO : Livraison et exploitation (et installation …)
ADV : Développement
AGD : Guides
ALC : Support au cycle de vie
outils et techniques de développement, sécurité des développeurs, correction des erreurs trouvées par les utilisateurs
ATE : Tests
AVA : Estimation des vulnérabilités
1 classe pour la maintenance de l'assurance
AMA : Maintenance de l 'assurance

3.7.3.3 Niveaux d'assurance

Ensembles de niveaux d'assurances
Composants issus de familles d 'assurance
Offrir des paquets d'assurance génériques dotés de cohérence interne
Niveaux (+) spécifiques

répondre à des besoins spécifiques
ajouts de composants aux niveaux standards

Echelle croissante
7 niveaux
Compromis entre niveau d'assurance visé et coût et faisabilité de l'évaluation

3.7.3.3.1 Niveaux d'assurance EAL1 à EAL4

Pas de techniques de développement spécialisées. Introduction de
rigueur croissante
détails supplémentaires

EAL1 : testé fonctionnellement
fonctionnement correct
menaces considérées comme non sérieuses
analyse des fonctions de sécurité et tests indépendants de ces fonctions

EAL2 : testé structurellement
analyse de vulnérabilité
tests du développeur

EAL3 : testé et vérifié méthodiquement
pratiques de sécurité dès la conception
TOE non piégée durant le développement

EAL4 : conçu, testé et vérifié méthodiquement
plus haut niveau d 'adaptation d'une gamme de produits existante
accroissement significatif par rapport à EAL3

3.7.3.3.2 Niveaux d'assurance EAL5 à EAL7

Techniques spécialisées de développement sécurisé
produits et systèmes conçus et développés spécifiquement

EAL5 :Conçu de façon semi-formelle et testé
conception modulaire
analyse des canaux cachés (« trous de sécurité »)
garantie que TOE non piégée au cours du développement

EAL6 :conception vérifiée, de façon semi-formelle et testée
techniques d'ingénierie de sécurité
environnement de développement rigoureux
TOE de qualité élevée pour protéger des biens de grande valeur
analyse approfondie de la vulnérabilité, étude systématique des canaux cachés , ...

EAL7 : conception vérifiée, de façon formelle et testée
TOE dédiés à la sécurité
Risques extrêmement élevés ou très grande valeur des biens
fonctionnalités de sécurité extrêmement concentrées : analyse formelle extensive
tests étendus

3.7.3.4 Profils de protection

3.7.3.4.1 Objet

Ensemble d ’objectifs et d ’exigences de sécurité
indépendant de l ’implémentation
formulation des problèmes de sécurité à résoudre
Ensemble de composants fonctionnels et d’assurance (niveau en général)
    choix expliqué dans un argumentaire
Contenu :
    description de la TOE
    environnement de sécurité de la TOE
        hypothèses sur sécurité physique, personnels, etc.
        menaces présumées
        politique organisationnelle
    Objectifs de sécurité
    Exigences de sécurité
    Argumentaire
        sur objectifs
        sur exigences

3.7.3.4.2 Exemples de profils de protection

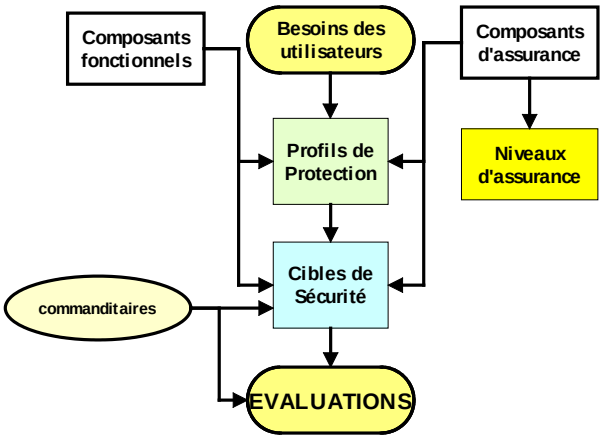
Circuits imprimés pour cartes à puce
    microcontrôleur pour carte à puce
    EAL4+
Coupe-feu à protection élevée
    passerelle filtrante configurable
    EAL5+
Infrastructure de Gestion de Clés (IGC)
    mise en œuvre d’une IGC (certification, enregistrement ,…)
    EAL4+
    outils de sécurisation de messages
    inclus une IGC et serveurs de messagerie
    ressources cryptographiques
        identification , authentification, signatures,
        génération de clé, de condensats, …
        vérification des certificats, signatures - protection des clés
    EAL5+
Échanges de données informatisées (EDI)
    EAL3+
Sécurité commerciale CS1
    Protection d ’accès contrôlée de base
Sécurité commerciale CS3
    Protection d ’accès basée sur des rôles (RBAC)
Standard ECMA E-COFC
    Extended Commercially Oriented Functionnality
    2 classes

Enterprise Business class (besoins internes)
Contract Business class (B to B)

3.7.3.5 Cible de sécurité (ST)

Base de l'évaluation de la TOE
définit les mesures de sécurité offertes par la TOE
spécifique à une TOE (PP est générique)
fait en général référence à un ou plusieurs PP
éventuellement auteur complète les exigences
Contenu :
Description de la TOE
Environnement de sécurité de la TOE
Objectifs de sécurité
Exigences de sécurité
Spécifications globales de la TOE
définition des fonctions de sécurité et des mesures d'assurance
Annonce de la conformité à un PP
Argumentaire

3.7.3.6 Evaluation



Faite par rapports aux critères définis dans les CC
Plusieurs types
Évaluation d'un PP
conformité d'un PP aux CC
intelligible
techniquement correct
Évaluation d'une ST
mêmes objectifs que PP
facilitée si s'appuie sur de PP
Évaluation d'une TOE
TOE satisfait aux exigences de la ST
recherche des vulnérabilités
tests de pénétration
Maintenance de l'assurance selon AMA

3.7.3.7 Bibliographie

INTERNET SECURITY - Professional Reference D. Atkins & al. New Riders ISBN 1-56205-557-7
" http://ictt.insa-lyon.fr/TeleRegionsSUN2/
Pour compléter ces informations, les sites suivant peuvent être pris comme point de départ :
Bases de liens : http://www.ins.com/knowledge/whitepapers/#security,
http://www.dharris.com/French.html
Aspects légaux : http://www.scssi.gouv.fr/document/chiffre.html et
http://www.legifrance.gouv.fr/citoyen/officiels.ow

Aspects organisationnels :
http://ictt.insa-lyon.fr/TeleRegionsSUN2/aesopian_security_management.pdf
IGC (PKI) : http://www.pkilaw.com/
et http://www.scssi.gouv.fr/document/igc.html
Evaluation - Critères communs : http://csrc.nist.gov/cc/
et http://www.scssi.gouv.fr/document/certif.html
Aspects techniques : http://www.cs.auckland.ac.nz/~pgut001/tutorial ,
http://www.netsec.psu.edu/netsec/kerberos.html
http://www.ins.com/knowledge/whitepapers/#security
Standards :Les RFC portant sur le sujet …
http://www.semper.org/sirene/outsideworld/standard.html
Vulnérabilités, tests : http://www.cert.org

3.8 Gestion des utilisateurs et Stratégie de sécurité dans Windows NT

3.8.1 Gestion des utilisateurs

Groupes dont un utilisateur est membre
Gestion des droits d'accès aux ressources (voir ci-dessous)
Profil de l'utilisateur, scripts d'accès, répertoire de base
Horaires durant lesquels le compte d'utilisateur peut se connecter aux serveurs
Accès depuis les stations de travail à partir desquelles un utilisateur peut ouvrir une session
Compte global ou local; date d'expiration ; validité (max, min), unicité, longueur minimale du mot de passe
Audit

Groupes

Contrôleurs de domaines
Administrateur Un administrateur doit avoir un compte utilisateur
Utilisateurs
Invités

Opérateurs

de serveur
d'impression
de sauvegarde
de comptes
Duplicateur
Stations de travail et serveurs
Administrateur
Utilisateurs
Utilisateurs avec pouvoir
Invités local ou réseau
Opérateurs de sauvegarde

Duplicateur

3.8.2 Groupes globaux et groupes locaux

Groupe global
- ensemble de comptes utilisateurs d'un domaine
- moyen d'**exporter** des utilisateurs vers d'autres domaines
- **droits dans son domaine et dans les domaines qui approuvent le sien**
- ne contient pas d'autres groupes
- seulement sur des serveurs

Groupe local
- ensemble d'utilisateurs et de groupes globaux d'un ou plusieurs domaines
- permet d'**importer** des utilisateurs et des groupes d'autres domaines
- droits d'accès seulement sur les serveurs **du seul domaine** du groupe local
- groupe local d'une station n'est pas utilisable sur un autre ordinateur

3.8.3 Domaines et relations d'approbation

Domaine
- unité administrative de base pour administration et sécurité
  - base de données des utilisateurs
    - Contrôleur principal
    - Dupliquée sur contrôleurs secondaires
  - stratégie de sécurité
- groupe de serveurs
  - notion de "workgroup"
- ne pas confondre avec les domaines "protocolaires" : TCP/IP

Relations d'approbation
- liaisons entre domaines qui permettent **l'authentification par traversée**

pas transitif: l'approbation n'est pas exportée ...
- **compte utilisateur unique**
- si un domaine A approuve un domaine B, les utilisateurs du domaine B peuvent obtenir des permissions et des droits dans le domaine A (même s'ils n'ont pas de comptes dans ce domaine)

3.8.4 Protections

3.8.4.1 Protection contre les virus

Sensibilisation des utilisateurs

Droits d'accès aux fichiers
- lister répertoires
- lire (lecture et exécution)
- Ajouter de nouveaux fichiers (pas de lecture ni de modification)
- Ajouter et lire
- Modifier les fichiers et les répertoires

Contrôle total: modifier + changer les permissions et les droits d'accès

Test du fichier par anti-virus

sur machine isolée

sur poste réseau mais avec seul droit d'invité

Sauvegardes régulières

3.8.4.2 Protection contre les chevaux de Troie

Cheval de Troie

Programme déguiser en programme ordinaire pour obtenir des informations

Ex: Se faire passer pour un écran d'accès au système pour tenter d'obtenir des informations sur les utilisateurs et les mots de passe

Ouverture de session protégée par mot de passe

Ctrl+Alt+Supp active directement l'écran d'ouverture de session

si station verrouillée

déverrouillage par ctrl+alt+supp et mot de passe

Verrouiller en "Lire" les applications sensibles pour éviter leur remplacement par des applications déguisées

3.9 Conclusion

La sécurisation d'Internet est en plein développement sous la contrainte des besoins croissants et urgents des utilisateurs, mais aussi grâce à la libéralisation (au plan légal) des moyens de sécurité à mettre en œuvre. Ces moyens existent depuis plusieurs décennies pour les applications « autorisées » (militaires, services de sécurité, banques,...). Leur mise à disposition légale pour le grand public, droit d'importation ou d'exportation et droit d'usage, devrait se produire courant 1997 (des travaux en ce sens sont aussi en cours au plan européen).

Un grand effort de standardisation reste à faire. Une solution alternative ou complémentaire à cette standardisation consiste à fournir les moyens de négocier des protocoles variés entre les plates-formes hétérogènes.

3.10 Annexe : Concepts « Sécurité »

Ils sont résumés sur le graphe conceptuel ci-dessous/