3. ARCHITECTURE (LOGICIELLE) DE RESEAU

3.1. Architecture en couches : Services et Protocoles

3.1.1. Définitions

Pour transmettre une information entre deux ETTD (Equipement Terminal de Traitement de Données) il est nécessaire de mettre cette information sous une forme compatible avec :

- La source et le collecteur
- Le support ou le réseau de transmission.

Un ETTD est un ensemble matériel/logiciel permettant de

saisir, traiter, stocker ou restituer de l'information.

Il peut s'agir aussi bien d'une visu que d'un très grand ordinateur ou d'un micro-ordinateur. Le système de communication, placé entre utilisateur et support, doit donc :

- s'adapter aux contraintes variées du support ou du réseau de transmission.
- adapter les informations transmises pour compenser l'Hétérogénéité des ETTD communiquant. Les diverses fonctions nécessaires pour satisfaire ces objectifs sont regroupées en **services** de plus en plus puissants.

Pour pouvoir dialoguer les entités paires doivent suivre des conventions très précises et très strictes qui constituent un **protocole de communication**. Ce protocole doit nécessairement faire l'objet d'une définition non ambiguë. Pour être compatible avec les contraintes venant des réseaux de transmission ou de l'hétérogénéité des matériels et des systèmes d'exploitation il devra être normalisé. Cette normalisation est réalisée par des organismes publics nationaux ou internationaux :

- O.S.I. Organisation de Standardisation internationale.
- C.C.I.T.T. Comité consultatif international télégraphique et téléphonique.
- C.E.I Commission Electrotechnique Internationale
- E.T.S.I. European Telecommunications Standard Institute
- E.C.M.A. Association européenne des constructeurs informatiques
- C.E.P.T. Comité européen des postes et télécommunications.

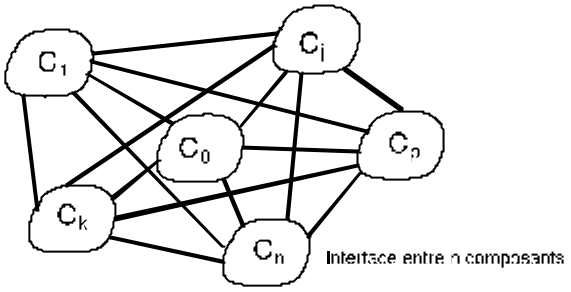
Organismes nationaux.

- AFNOR (France), IEEE, UST1 (USA), DIN(Allemagne), GOSIP(GB), TTC (Japon), etc.
- P.T.T. des différents pays.

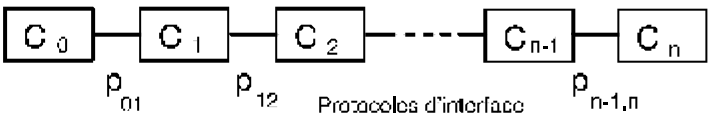
Il existe aussi des standards de fait, protocoles créés par des constructeurs (éventuellement des équipes universitaires), qui se sont imposés par leur diffusion (par exemple des protocoles IBM (SNA,BSC2780) ou les protocoles TCP/IP développés à l'origine pour le DoD (réseau ARPA) et décrits dans des RFC: Request for Comments. l'IAB (Internet Administration Board) commence à mettre en place des procédures strictes pour transformer certaines RFC en standards. Les entités adjacentes d'un même système communiquent par des protocoles d'interfaces spécifiques à chaque implantation.

3.1.2. Organisation des activités

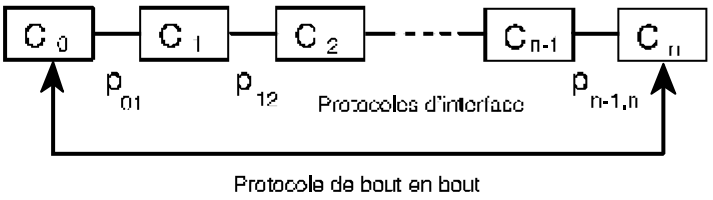
Une interface généralisée de plusieurs composants interconnectés de manière évolutive est actuellement impossible à maîtriser. On doit chercher une organisation plus simple. En pratique on ne rencontre guère que deux types d'assemblage de composants :



assemblage en cascade

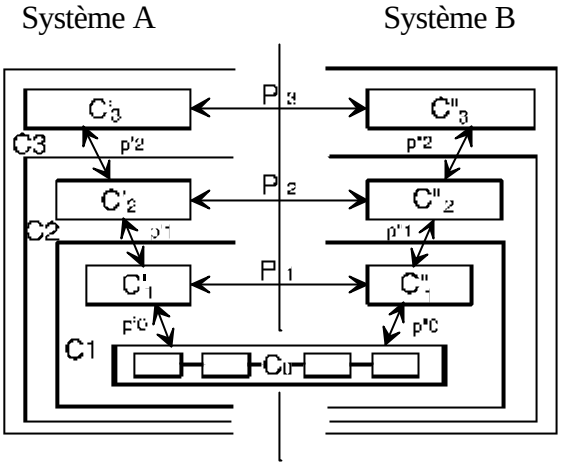


Un tel système a une commande distribuée. Pour avoir un meilleurs contrôle on le muni d'un protocole de bout en bout qui permet un dialogue direct entre les composants d'extrémité par des messages transmis par la chaîne de composants intermédiaires.



On a alors le schéma ci-contre.

assemblage hiérarchisé



Cet assemblage, appelé aussi assemblage en pelure d'oignon, consiste à imbriquer des **cascades de trois composants munies de deux protocoles d'interface et d'un protocole de bout en bout**. Chacune de ces cascades est un nouveau composant qui délivre les fonctions du composant central (niveau inférieur) plus les nouvelles fonctions fournies par les composants latéraux et le protocole de bout en bout.

Tous les logiciels de communication sont construits selon cette architecture.

Chaque composant fournit un service de niveau donné. Chaque service comprend le service de niveau inférieur, donc toutes les fonctions qui y sont traitées. Ces fonctions sont réparties sur l'ensemble des systèmes interconnectés (au moins deux). Un sous-ensemble de fonctions est traité dans les entités paires (appariées) des systèmes communicants. Complété par le service de niveau inférieur, ce sous-ensemble fournit le service du niveau considéré.

3.2. Modèle de Référence pour l'Interconnexion des Systèmes Ouverts de l'OSI

3.2.1. Normalisation - Principe d'architecture

La norme OSI 7498-1 publiée en 1984 (première version vers 1981) décrit un Modèle de Référence pour l'Interconnexion de Systèmes Ouverts. Elle définit un cadre pour les autres normes en donnant les concepts fondamentaux d'une architecture structurée en sept couches ainsi que la description des fonctions à traiter dans ces couches.

Cette norme est reprise par :

les recommandations CCITT 200 et 210
la norme AFNOR NF Z 70-001

Cette norme a été complétée par le standard 7498-2 qui définit l'architecture de sécurité ISO, le standard 7498-3 qui définit les conventions de configuration et de nommage et le standard 7498-4 qui définit l'architecture d'administration ISO.

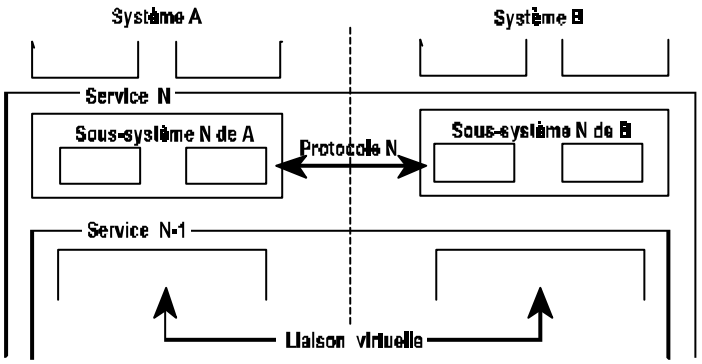
On appelle **système réel** un ensemble comprenant un ou plusieurs ordinateur(s), le logiciel associé, des périphériques, des terminaux, des opérateurs humains, des processus physiques, des moyens de transfert d'information, etc. et constituant un tout autonome capable d'effectuer des traitements et/ou des transferts d'information.

Tout système de communication qui suit le Modèle de Référence d'Interconnexion des Systèmes Ouverts et applique les méthodes et procédures de communication normalisées est appelé "**système ouvert**". De par leur utilisation de ces normes, ces systèmes sont en effet capables de coopérer.

Ce Modèle de Référence est adopté par tous les constructeurs de systèmes informatiques, éventuellement en complément d'un système spécifique (IBM : Architecture SNA, systèmes Unix : Architecture "Arpa" (TCP/IP)). Cependant, chaque constructeur utilise une réalisation particulière de ce modèle (par exemple ISO/DSA pour Bull, Decnet pour DEC, OSI/CS pour IBM).

L'utilisation d'un même modèle et de protocoles normalisés assure la compatibilité entre ces systèmes si le même sous-ensemble de protocoles et les mêmes options ont été choisies. (Les standards MAP ou TOP définissent de tels sous-ensembles ou profils...).

Ce modèle architectural à sept couches est bâti sur un ensemble de services imbriqués: un service de niveau N fournit un ensemble de fonctions soit par l'entremise du service de niveau N-1, soit par les "entités" des sous-systèmes de niveau N. Un processus d'application est un composant effectuant un traitement d'information pour une application particulière qui utilise le service de niveau supérieur (de niveau 7 Application). On appelle entité(N) un composant de niveau N qui traite l'activité dévolue à ce niveau sur un sous-système. L'ensemble des entités(N), paires ou homologues, constitue la couche N.



La couche N et les couches inférieures à celle-ci rendent le service N aux entités(N+1) à la frontière entre la couche N et la couche N+1.

Un système de communication peut comporter un grand nombre de systèmes interconnectés, chaque système pouvant supporter plusieurs processus d'application.

Une couche peut être "vide" si, à un niveau donné, aucune des fonctions prévue n'est nécessaire. Ainsi le standard MAP complet (voir chapitre 3) utilise des fonctions aux sept niveaux du

modèle de référence alors que MiniMAP (Collapsed MAP) n'utilise que les fonctions de niveau 1,2 et 7. Une liaison de données élémentaire ne met souvent en oeuvre que les couches 1 et 2 ; elle ne peut donc fournir que les fonctions attachées à ces niveaux et tous les autres problèmes doivent être pris en compte directement par l'utilisateur.

3.2.2. Services OSI

L'ensemble des activités prises en compte dans le modèle de référence OSI est réparti en 7 services hiérarchisés ou couches, qui peuvent comporter des sous-couches :

*** 7 - Application**
*** 6 - Présentation**
*** 5 - Session**
*** 4 - Transport**
*** 3 - Réseau**
*** 2 - Liaison de données**
*** 1 - Physique**

Les services des niveaux supérieurs: Session, Présentation et Application sont dits "orientés traitements" et traitent les problèmes d'hétérogénéité et de gestion de la communication.

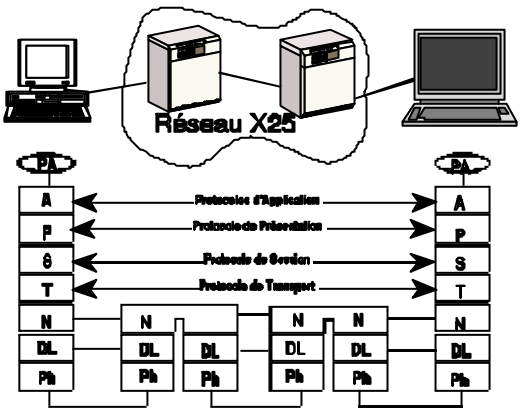
Les autres services, "orientés télécommunications", assurent, par le Service Transport, une liaison de bout en bout de qualité donnée quelque soit le réseau de communication utilisé, entre les applications qui coopèrent.

Le Service Réseau permet d'interconnecter deux systèmes à travers un réseau ou plusieurs réseaux interconnectés; dans ce cas plusieurs sous-couches sont nécessaires.

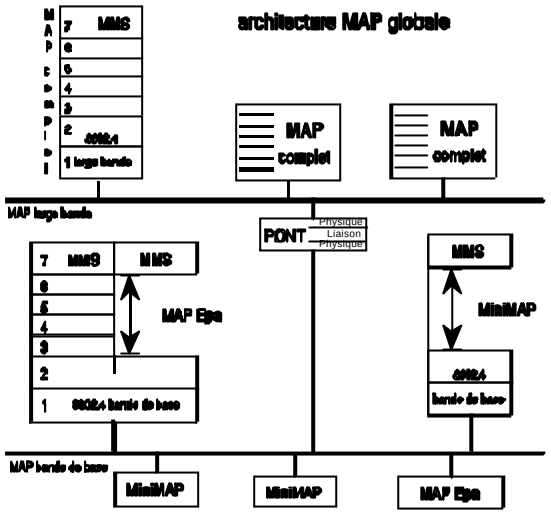
Le service Liaison de données permet à deux systèmes reliés directement par une liaison physique de communiquer

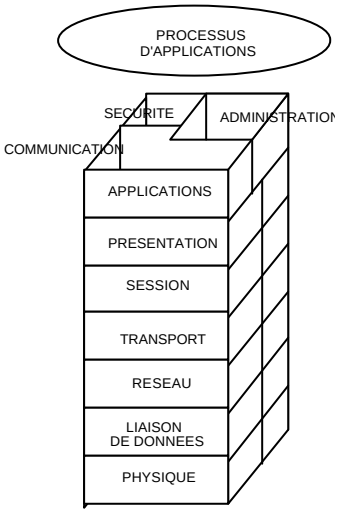
Ces services sont décrits sommairement ci-dessous.

Le schéma ci-contre montre les architectures ISO de deux systèmes reliés par deux relais : commutateurs de paquets d'un réseaux X25 ou routeurs.



Le second schéma illustre une architecture industrielle MAP (Manufacturing Automation Protocol) dans laquelle on utilise un réseau local large bande et un réseau en bande de base (bande porteuse) interconnectés par un *pont* (relais de niveau 2/ISO). Le réseau inférieur supporte principalement des équipements de production qui ont des logiciels de communication MiniMAP qui ne comportent que les services Application, Liaison de données et Physique. La partie supérieure supporte des architectures complètes. La passerelle est réalisée par un (ou plusieurs) systèmes EPA (Enhanced Performance Architecture) qui offrent les deux piles de logiciel.





Si on veut **ajouter** à ce modèle des **activités de sûreté (sécurité) et/ou d'administration de réseaux** cette architecture doit être complétée. En effet si **certains services de communication contiennent quelques fonctions dans ces domaines** (supportées par des *opérations de couche*), une surveillance ou une administration efficiente ne peut qu'être externe. Ces activités peuvent traitées de deux manières :

- par des éléments du service Application (voir ci-dessous) qui utilisent le service ACSE/Présentation pour coopérer entre systèmes distants.
- par des services et des protocoles spécifiques situés à chaque niveau du Modéle de Référence et qui utilisent le service de communication inférieur (service N-1).

3.3. Services Application

Les services Applications sont rendus par des "Entités d'Application" constituées d'au moins deux "Eléments de Service Application" (ASE). L'organisation de ces entités est normalisée par la "Structure de la couche Application" (ALS : Application Layer Structure).

Sept services standards actuellement normalisés ou en cours de normalisation sont mis directement à la disposition des utilisateurs. D'autres sont à l'étude. Un service d'annuaire augmente la convivialité. Un service d'Administration de Réseaux complexes, dont certains éléments sont disponibles facilite la gestion des réseaux. Ces services spécifiques s'appuient, selon leurs besoins, sur des éléments de service communs.

3.3.1 Courrier électronique : X400 (SMTP)

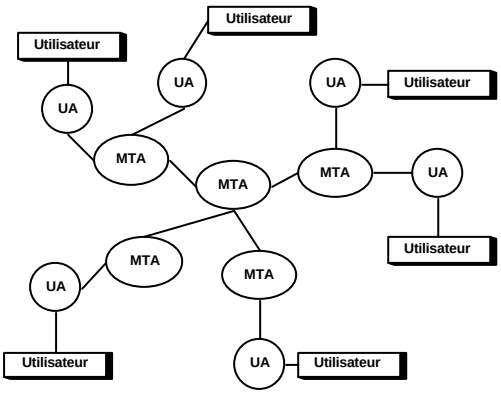
Le service de courrier électronique X400, spécifié dès 1984, est disponible auprès de certains constructeurs depuis 1988 environ. C'est le service Application OSI le plus répandu. Il est notamment disponible auprès des grands opérateurs de télécommunications (en France, service Atlas 400).

Ce service permet un échange de messages entre des personnes par l'intermédiaire de systèmes informatiques hétérogènes. Il reproduit le fonctionnement d'un service de courrier classique avec des temps d'acheminement beaucoup plus courts.

Il réalise l'interconnexion des systèmes de messagerie disponibles sur les équipements des utilisateurs. Après leur rédaction les messages sont :

- déposés dans la messagerie locale
- acheminés vers la (ou les) messagerie(s) distante(s) où sont connectés le (ou les) destinataire(s).
- délivrés au(x) destinataire(s)

Le transfert des messages est réalisé par un *système de transfert de messages* (MTS) constitué d'*agents de transfert de messages* (MTA) interconnectés entre eux par un réseau de communication.



Un usager est représenté auprès d'un MTA par un "*Agent utilisateur*" (UA). Celui-ci modélise :

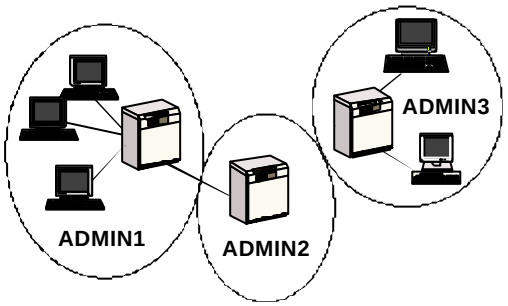
- une boite à lettres
- le logiciel de dialogue qui assiste l'usager pour préparer, émettre et recevoir les messages.

L'ensemble des MTA et des UA constitue de système de messagerie MHS (Messsage Handling System)

La syntaxe de transfert utilisée (ASN.1) n'impose pas de restriction pour les messages à transporter.

L'UA dépose ses messages dans une MTA pour qu'il les envoie. Ce dépôt est acquitté. Le MTA le plus proche de l'UA destinataire lui remet les messages lorsqu'il est disponible; sinon il les stocke.

En service optionnel, le service de transfert de messages (MTS) peut générer et transmette des "*avis de remise*" ou des "*avis de non-remise*" selon que le message a pu ou non être distribué. (Ce système ne garantit pas que le message a été lu par l'utilisateur; certains produits commercialisés offrent en plus cette information.)



Le service de messagerie X400 dispose d'un système d'adressage assez puissant. Chaque utilisateur est relié à un seul UA, il est désigné par son *nom d'O/R* (origine/remise). Ce nom est constitué par une séquence composée d'une liste d'attributs standards et d'une liste spécifique du domaine auquel appartient son MTA de rattachement.

Cette liste standard est une séquence de 9 éléments tous optionnels mais dont on doit fournir un sous-ensemble suffisant. Ce sont :

- nom de pays
- nom de domaine administratif
- adresse X121 (par exemple adresse Transpac)
- identificateur de terminal (par exemple telex, télétex)
- nom de domaine privé
- nom d'organisation
- identificateur unique d'UA
- nom de personne
- séquence de noms d'unités organisationnelles

La séquence suivante est un exemple de nom d'O/R (adresse Atlas 400)

X400: /C=FR /A=ATLAS /P=PAPYetFils /O=LYON /OU=Syst1 /S=PDupont

/C : Pays	/A : Domaine d'administration public
/P: domaine d'administration privé	/O : Organisation
/OU : Unité d'organisation	/S : Nom (prénom, initiales, généalogie)

Messagerie SMTP (Simple Message Transfert Protocol)

Sur le réseau Internet on dispose d'une messagerie plus simple. Elle est réalisée par un service Application supporté par TCP/IP. Elle ne dispose pas d'avis de remise ou de non-remise mais les messages qui n'ont pu être distribués sont en général retournés à l'expéditeur (non-remise). Le codage des données se fait uniquement dans un alphabet texte à 7 bits ne permettant pas les lettres accentuées (sauf mise en oeuvre de fonctionnalités supplémentaires encore peu répandues). Les données différentes (binaires par exemple) doivent être converties dans cet alphabet. Son système d'adressage est plus contraignant. Un utilisateur est désigné par son nom, l'identificateur du système qui supporte sa boite à lettre (nom réel ou alias) et le nom du domaine de rattachement de ce système, soit par exemple :

beuchot@if.insa-lyon.fr

domaine :	insa-lyon.fr
alias du système :	if
nom d'utilisateur :	beuchot

3.3.2 Gestion de fichiers répartis : FTAM (FTP)

Le service Application FTAM : *File Transfert Acces and Manipulation* fournit les fonctions nécessaires à l'interconnexion des systèmes de gestion de fichiers de deux systèmes hétérogènes permettant le transfert de fichiers, mais aussi leur manipulation à distance.

Pour obtenir ce service en milieu hétérogène il comporte deux sous-ensembles :

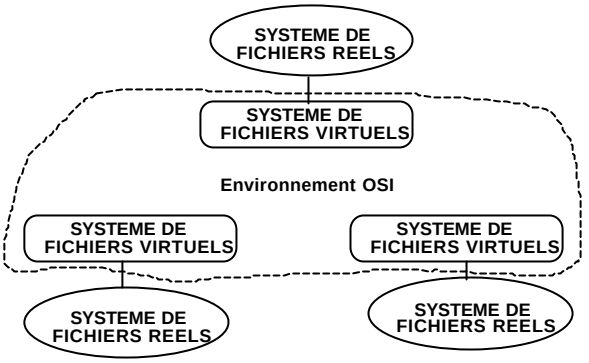
- un système de fichiers virtuels
- des fonctions permettant l'accès, la manipulation ou le transfert de ces fichiers dans un environnement de communication OSI.

Un fichier virtuel est une entité qui possède :

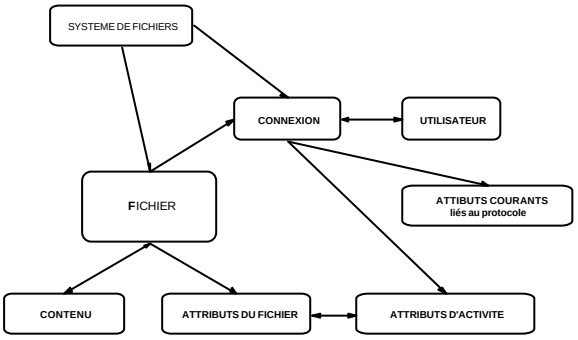
- un nom simple, non ambigu
- des attributs qui expriment ses propriétés : compte, droits d'accès, historique ....
- des attributs décrivant sa structure logique et la taille des données stockées

- des unités de données formant le contenu du fichier

Le système de fichiers virtuels est projeté (mise en correspondance, mapping) sur le système de fichiers local dans chaque système interconnecté. Il possède une structure arborescente. Ce système de fichiers virtuels possède des propriétés suffisantes pour correspondre aux systèmes de fichiers réels existants. Il peut donc supporter différentes organisations hiérarchiques ou non.



Actuellement 7 structures de présentation sont supportées: non structuré, séquentiel plat, ordonné plat, ordonné plat à noms uniques, ordonné hiérarchique, hiérarchique général et hiérarchique général à noms uniques.



Pour augmenter la convivialité, des modèles de documents permettent de regrouper, dans un type donné, les caractéristiques des documents rencontrés les plus fréquemment.

Au système de fichiers virtuel est aussi associé un préodre (selon l'arborescence) permettant un transfert ou une manipulation ordonné.

Les fonctions fournies permettent :
- l'établissement et la rupture de l'association entre les systèmes de fichiers distants
- La création, l'effacement ou la suppression de fichier(s)
- la sélection, la désélection d'un fichier, la lecture ou la modification d'attributs
- l'ouverture, la localisation ou la fermeture d'un fichier
- la commande de lecture ou d'écriture
- le transfert de ces données avec indication de sa terminaison

Lors de l'établissement de l'association les entités initiateur et répondeur peuvent établir leurs identités mutuelles.

3.3.3 Systèmes Transactionnels : TP

TP : *Transaction Processing* a été spécifié pour permettre une **mise à jour sûre** d'un système de bases de données réparties. Une telle base de données doit rester cohérente quelles que soient les incidents qui interviennent durant la phase de mise à jour. Pour cela TP permet une **validation à deux phases (Commit)** des mises à jour locales ainsi qu'un **contrôle de concurrence**

et le rétablissement sur l'ensemble de la base répartie de l'ancienne version en cas d'échec de la mise à jour. Ces fonctions sont réalisées sur une base organisée de manière arborescente à partir du noeud racine qui sollicite la mise à jour.

Après transfert des données (par exemple par FTAM) le noeud racine demande à chaque système de réaliser la mise à jour (remplacement de l'ancienne version). Les réponses donnant le résultat des noeuds ou feuilles de l'arbre sont transmises au noeud racine qui valide la mise à jour (vers tous les noeuds) ou demande le **recouvrement** (retour à l'ancienne version) si un noeud n'a pas pu réaliser sa mise à jour.

Un tel service peut être appliqué à tout système réparti dont on doit assurer la cohérence.

3.3.4 Accès aux données distantes : RDA

Le service d'*accès aux données distantes* : RDA (Remote Data Acces) est complémentaire du service de traitement transactionnel. Il permet de rechercher des données dans une base de données répartie.

Il permet de rechercher les données dans la partie locale de la base puis, en cas d'échec, de rechercher ces données dans ses autres parties.

Il est couplé avec un langage d'interrogation SQL : *Structured Query Languag*e. Des langages d'interrogation spécifiques existent depuis plus de 20 ans pour faciliter la consultation des systèmes de gestion de base de données relationnels; ils ont été enrichis de nouvelles fonctions et sont devenus plus ou moins incompatibles. Une normalisation OSI est donc devenue indispensable. Un tel langage doit permettre de selectionner des enregistrements d'une base de données en fonction de critères de recherche et de les trier, les regrouper, etc.

Ce service est en cours de spécification pour normalisation à l'OSI

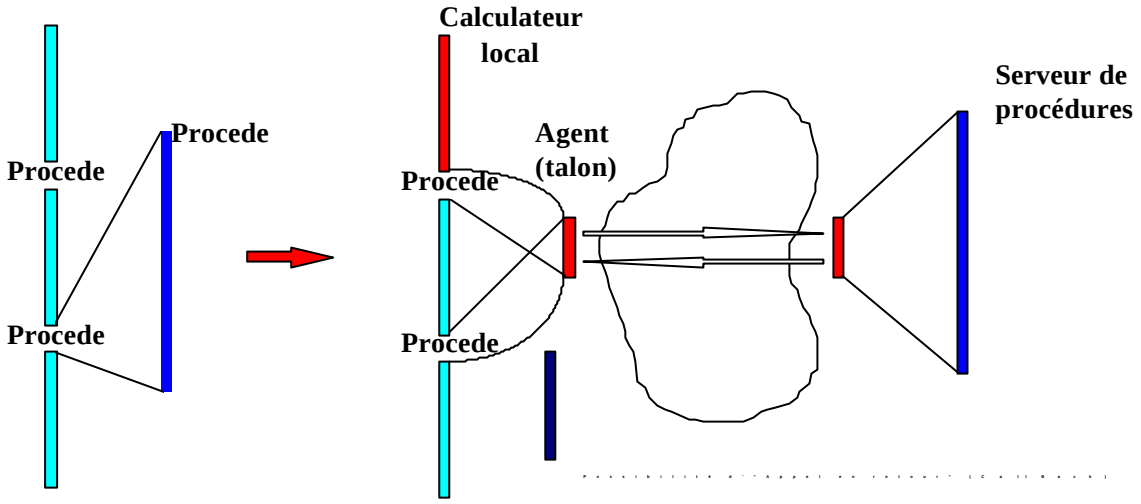
3.3.5 Traitement à distance : RPC

L'*appel de procédures distantes* RPC : Remote Procedure Call est en cours d'étude à l'OSI. Un standard européen ECMA a été défini depuis plusieurs années. Un tel système est un modèle d'**architecture Client-Serveur**.

En milieu homogène de tels systèmes sont réalisés depuis plus de dix ans. Un système RPC est en cours de standardisation dans le monde Unix (OSF et X-Open Group). Il est destiné à permettre des traitements répartis transparents entre des stations de travail Unix interconnectées sur un réseau local et communiquant par un logiciel de communication TCP/IP.

Dans un tel système les procédures appelées depuis un programme exécuté sur un système *client* s'exécutent à distance sur un *serveur* de procédures.

Sur le système client le programme appelant est lié à un "agent local" (talon, stub) de la procédure distante. Lors de l'appel de procédure cet agent établit l'association d'application entre le client et le serveur, puis envoie les opérations à réaliser au système serveur. Celui-ci peut demander en retour l'exécution de procédures de second niveau sur le système client (*call back*).



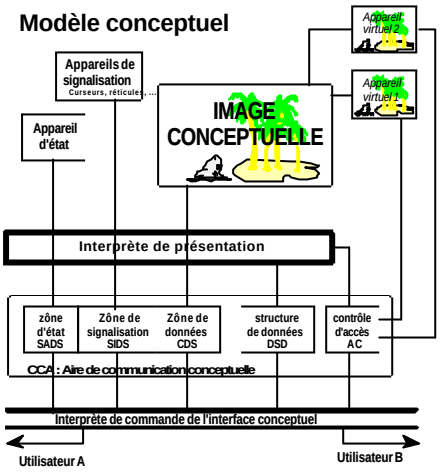
3.3.6 Travail à distance : VTP (Telnet)

Ce service Application est le plus ancien des services de communication étudié. Le service "Telnet" dans l'architecture TCP/IP existe depuis longtemps. Cependant le *service de terminal virtuel* : VTP (Virtual Terminal Protocol) n'a été normalisé à l'OSI que vers 1990.

L'évolution de la technologie vers des terminaux couleur, offrant des images "bitmap", supportés par des micro-ordinateurs ou des stations de travail a modifié profondément la problématique de ce genre de service au cours des années 80. Le terminal virtuel doit **masquer aux usagers la diversité des terminaux réels** et la manière par laquelle ils réalisent une fonction donnée. Les **données échangées entre terminal et système de traitement** peuvent être quelconques: **textuelles et/ou graphiques**.

Un terminal comporte un (ou plusieurs) équipement(s) d'affichage, des éléments de signalisation (curseur, réticule, pointeur, ..), des équipements d'entrée (clavier, souris, etc.), des éléments permettant d'en connaître l'état et d'en contrôler l'accès.

Le standard OSI de Protocole de Terminal Virtuel propose un modèle conceptuel permettant de définir toutes les caractéristiques d'un terminal. Dans chaque système terminal réel, ce modèle peut être implanté et projeté sur (mis en correspondance avec) l'équipement réel. Ce modèle est illustré par le schéma ci-contre. Il est organisé autour de l'*aire de communication conceptuelle*.



Cette entité permet de coder dans sa zone de données l'image à afficher. Elle possède aussi une zone d'état et une zone de signalisation. Elle comporte en outre des fonctions permettant de contrôler l'accès du terminal au système de traitement. Les données sont décrites de manière générique selon des structures de données types.

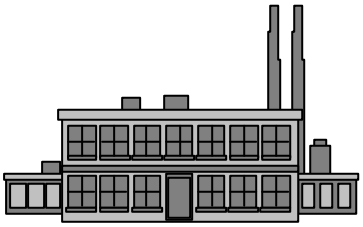
Ce modèle permet de représenter des images en trois dimensions. La "profondeur" est représentée par plusieurs plans (et non par un dessin plan vu en perspective).

L'image et la signalisation sont projetés sur l'équipement réel en fonction des possibilités de celui-ci. L'important est que les usagers aient **la même conception** des objets réels visualisés.

Par ailleurs une image bitmap occupe en mémoire un très grand volume. Elle ne peut être stockée sous cette forme (ni transmise) et le système de terminal virtuel doit aussi prévoir un mode de description de l'image aisément mémorisable.

Dans l'architecture TCP/IP, le service **Telnet** spécifie un terminal virtuel fonctionnant uniquement en mode caractère et possèdant très peu d'éléments annexes.

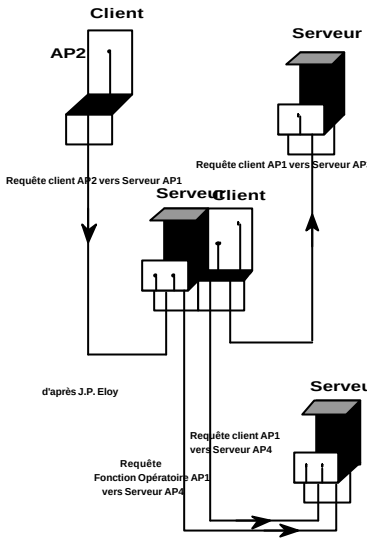
3.3.7 Applications industrielles : MMS



Le service ce messagerie industrielle MMS (Manufacturing Message Specification) constitue la base du standard MAP (Manufacturing Automation Protocol), profil fonctionnel créé pour supporter les applications de production industrielle. Il est basé sur un mécanisme client-serveurs. Les serveurs: automates industriels, robots, manipulateurs, machines outils, etc. sont utilisés par des processus clients situés dans les calculateurs de pilotage ou les automates superviseurs.

MMS offrent une très grande variété de fonctions: 84 services élémentaires et 2 modalités, regroupés en 9 sous-ensembles. La plupart de ces services sont optionnels et beaucoup ne sont pas encore commercialement disponibles.

La Gestion de *contexte* permet d'initialiser et de rompre les échanges entre deux entités paires et de négocier les options. Elle utilise ACSE.



La gestion de l'*Equipement Virtuel de Production* EVP (VMD: Virtual Manufacturing Device) n'est installée que sur les serveurs. Elle permet de résoudre les problèmes d'hétérogénéité en plaçant un EVP en "frontal" de la partie visible de l'équipement réel de production. Les interactions entre EVP et équipement réel sont de la responsabilité de celui-ci. MMS assure un transfert des messages qui transportent les fonctions à réaliser entre client et EVP. Sur le système client on dispose d'une bibliothèque de fonctions (MMS-I).

Une variable correspond à un ou plusieurs éléments de données référencés, pour le partenaire, par un nom ou une description. La *gestion de variables* permet d'envoyer des commandes à un équipement réel ou de lire des informations sur un appareil. Une partie des fonctions qu'elle comprend est nécessaire pour communiquer avec des automates programmables industriels ou des équipements équivalents.

La *gestion de programme* permet lancer, arrêter ou relancer un programme. Le téléchargement (ou déchargement) de programme, leur sauvegarde, fait partie de la *gestion de domaine*.

La *gestion d'événements* et la *gestion de sémaphores* fournissent les fonctionnalités nécessaires aux systèmes temps-réel industriels (fonctions de base pour un système d'exploitation temps-réel réparti).

La *communication opérateur* permet de lire ou d'écrire sur les appareils d'entrée-sortie distants (communication homme-machine).

Enfin la *gestion de journal* permet de créer un journal des événements avec le contenu des variables associées, permettant un audit en cas d'incident.

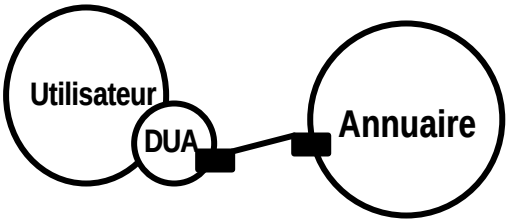
3.3.8 Service d'annuaires : X500

Un *service d'annuaire* (Directory) permet d'associer une adresse à un nom de ressource ou d'utilisateur ainsi qu'un certain nombre d'autres attributs qui les caractérisent. Dans les systèmes répartis il est vite apparu qu'il était plus fiable et moins redondant de permettre à des systèmes hétérogènes d'interroger leurs annuaires particuliers, voire de les faire coopérer. Il s'agit en pratique d'une application de base de données avec des contraintes de mise à jour assez faibles (volumes restreints).

L'ISO et le CCITT ont normalisé conjointement un système d'annuaire spécifié par le CCITT dans la série X500.

Composants de l'annuaire X500

L'annuaire (Directory) est une collection de systèmes ouverts qui coopèrent pour maintenir une **base de donnée**s logique d'informations portant sur un **ensemble d'objets du monde réel**. Les *utilisateurs*, hommes **et** programmes d'ordinateurs, peuvent lire ou modifier l'information, ou une de ses parties, s'ils en ont la permission. Chaque utilisateur est représenté par un Agent Utilisateur de l'Annuaire: DUA (Directory User Agent). Celui-ci permet d'utiliser l'annuaire par l'intermédiaire d'un *point d'accès*. L'information dans la base est collectivement connue comme la Base d'Information de l'Annuaire: DIB (Directory Information Base).



L'annuaire X500 fournit à ses utilisateurs un service abstrait, ensemble de facilités d'accès bien définies.

La base de données (DIB) est constituée d'informations sur des objets. Elle est composée d'*entrées* (d'annuaire) dont chacune consiste en un ensemble de données sur *un objet*. Ces entrées sont organisées sous forme d'un arbre (DIT: Directory Information Tree). Chaque entrée a un identificateur (distinguished name) constitué à partir de l'identificateur de son supérieur dans l'arbre.

Service d'annuaire

On peut le décomposer en quatre parties:

- Service de qualification

  Il comporte des commandes (**requêtes**) pour imposer des limites à l'usage des ressources. Chaque requête peut être accompagnée de **paramètres de sécurité** pour la protection des informations (*signature numérique*). Un service d'*authentification forte* peut aussi être fourni. Ces requêtes peuvent être appliquées à plusieurs entrées grâce à des *filtres*.

- Service d'interrogation de l'annuaire

  Il comporte des fonctions de lecture d'une entrée, de comparaison d'un attribut particulier, de listage des subordonnés d'une entrée, de recherche d'information pour toutes les entrées qui répondent à un filtre, par exemple pour fournir un service de type "**pages jaunes**". Il permet aussi d'abandonner une requête en cours.

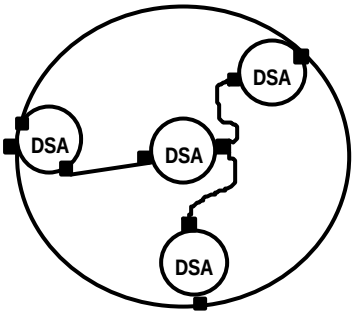
- Service de modification de l'annuaires

  Il permet d'ajouter ou de retrancher une entrée ou d'en modifier les attributs (ajout, retrait, modification), modification en particulier de l'identificateur.

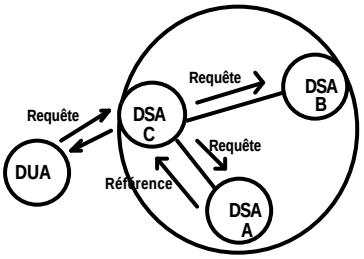
- Autres fonctions

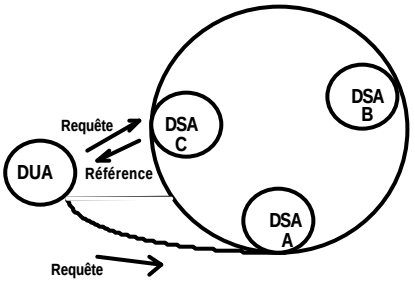
Si un service tombe en défaut, une indication d'erreur est transmise. Un service peut ne pas aboutir parce que l'agent ne peut transmettre sa requête au point d'accès approprié. Dans ce cas l'annuaire peut **renvoyer une référence** (*referral*) qui suggère un point d'accès alternatif. Il peut aussi **chaîner la requête**.

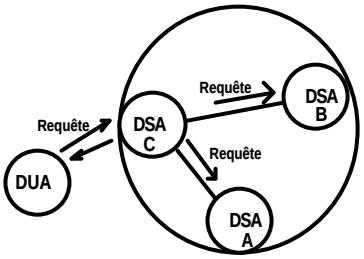
Annuaire distribué



La base de données (DIB) peut être répartie sur des systèmes interconnectés. Les bases locales sont entièrement dépendantes de l'implantation. Chacune est accessible par l'intermédiaire d'un *agent du système d'annuaire* (DSA: Directory System Agent). Un DSA peut utiliser des informations de sa base locale ou interagir avec d'autres DSA pour transmettre les requêtes. Il peut utiliser les renvois de références (referral) ou le chaînage. Il peut aussi diffuser les requêtes.







3.3.9 Services d'Administration de Réseaux : CMIP (SNMP)

L'administration de réseaux englobe les moyens mis en oeuvre 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 oeuvre.

3.3.9.1. 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 télécommunications

C'est une ressource particulière ayant des composants variés:

informatiques

de télécommunication pour réseaux informatiques

modems, concentrateurs, multiplexeurs, commutateurs,etc

de télécommunication généraux :

PABX, accès aux réseaux publics

3.3.9.2. 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

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

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.)

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, chiffrement,...)
- diffusion des informations relatives à la sécurité
- compte rendu d'événements relatifs à la sécurité (audit)

La mise en oeuvre des fonctions de sécurité ne fait pas partie de la gestion de la sécurité.

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, par exemple en déterminant de nouvelles procédures d'acheminement et en les mettant en place ou, à long terme, en planifiant l'évolution du réseau (topologie, capacités des canaux).

Elle met en oeuvre 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.

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 adresses 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 mise 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.

Les informations administratives sont rangées dans une *base de données administrative*: MIB (Management Administration Base).

Le réseau est parfois très étendu ou très complexe; il peut aussi utiliser un réseau de télécommunications plublic (par exemple Transpac) qui échappe à l'autorité de ses administrateurs. Il est alors partitionné en *domaines d'administration*. Chaque domaine comporte un système gestionnaire qui supporte la MIB et des systèmes agents (au moins un .....) qui sont administrés. Le système gestionnaire d'un domaine peut être système agent d'un autre domaine, permettant ainsi une vision globale du réseau depuis le système gestionnaire de plus haut niveau.

3.3.10. Services communs : ACSE, ROSE, RTSE, CCR

Association des Applications : ACSE

Une Entité d'Application regroupe une ensemble d' "Eléments de Service Application" (ASE). Pour interagir, ces Entités d'Application doivent être associées.

Cette "Association" d'Entités d'Application est réalisée explicitement et permet d'identifier l'ensemble des ASE qui constituent l'entité, les options retenues et toutes les autres informations nécessaires pour obtenir l'**interopérabilité des processus d'application**. Ces informations (ASEs, options,etc.) constituent un "*Contexte d'Application*".

ACSE (Association Control Service Element) est un élément de service (ASE) constituant de **toute Entité d'Application** (sauf dans X400 qui est un service sans connexion). Il permet d'établir et de rompre l'association entre deux Entités d'Application paires. Il permet de réaliser une *Association simple* entre deux invocations d'Entités d'Application.

Deux services confirmés permettent d'**associer** et de **dissocier** des applications en fonctionnement normal. Le premier initie une Association et permet de définir le Ccntexte d'Application utilisé (nom de contexte et paramètres).

Deux autres services traitent les ruptures anormales d'association (sur défaut). L'un est un service simple (non confirmé); il signale au système distant une rupture sur un incident au niveau d'un processus d'Application. L'autre est un service fourni directement par ACSE aux deux entités utilisatrices pour indiquer une anomalie du système de communication lui-même.

Opération distantes : ROSE (Remote Operation Service Element)

Le concept d' "opérations distantes" est utilisé comme véhicule supportant des applications interactives.

D'une manière générale, le concept d' "opération" est introduit dans le cadre d'une architecture **orientée objet**: une opération, distante ou locale, est une interaction élémentaire demande/réponse [request/reply], quelquefois demande seulement. Si la structure d'une

telle opération entre deux entités est simple et régulière, son contenu syntaxique et sémantique peut être très complexe.

La demande prend la forme d'une structure de données :

< invoque > ::= < type d'opération > < arguments >

Le type d'opération distingue les différentes opérations applicables au type d'objet; les arguments portent les types de données des paramètres fournis par le demandeur (Invoker). L'élément "réponse" prend la forme d'une structure de données **retour**, soit retour immédiat, soit retour erreur.

Une telle structure de commande, qui prévoit un retour normal et une ou plusieurs exception contribue beaucoup à la fiabilité du système. Une opération est dite *totale* si elle inclut tous les cas possibles, y compris les cas de défaut. Si chaque opération d'un type est une opération totale, ce type est *robuste.*

Dans le cas d'une opération distante, la fiabilité d'exécution peut être rangée dans une des trois classes suivantes :

- Exécution **une fois exactement** c'est la garantie la plus forte.
- Exécution **au moins une fois**. Ce cas est valable pour les opérations "idempotent" (par exemple une lecture de données).
- Exécution **au plus une fois.**

Les opérations sont classées selon la réponse fournie en deux modes :

- synchrone : réponse en fin d'échange
- asynchrone : d'autres opérations peuvent être demandées sans attendre l'arrivée de la réponse.

On définit ainsi 5 classes :

1 - synchrone avec réponse en cas de succès ou de défaut
2 - asynchrone avec réponse en cas de succès ou de défaut
3 - asynchrone avec réponse en cas de défaut seulement (résultat négatif)
4 - asynchrone avec réponse en cas de succès seulement (résultat positif)
5 - asynchrone sans réponse (résultat non signalé)

Une demande d'opération peut provoquer, pour réaliser son exécution, des demandes d'autres opérations. On dit que ces opérations sont **reliées** (linked) et on distingue les opérateurs parents et enfants.

Service de transfert fiable :RTSE (Reliable Transfert Service Element)

Dans l'environnement OSI, les Entités d'Application (AE) communiquent en échangeant des APDU: Unités de Données de Protocole d'Application (Application Protocol Data Unit). **Le**

transfert fiable garantit que chaque APDU est entièrement transférée entre les Entités d'Application **une fois exactement** ou que l'entité **expéditeur est avisé d'une anomalie**. Le **transfert fiable assure la reprise sur défaillance de la communication et du système terminal** et minimalise l'importance des retransmissions nécessaires pour la reprise (performances). Les APDU transférées sont transparentes pour le transfert fiable.

RTSE fournit plusieurs services élémentaires:

- Etablissement et Rupture d'association (grâce à ACSE)
- Rupture d'association par le fournisseur et l'utilisateur (via ACSE)
- Transfert fiable
- Demande de Changement de tour et Changement de tour

Le service *Transfert* permet à l'utilisateur qui bénéficie du **Tour** de demander le transfert fiable d'une APDU sur une Association d'application. Ce service est un service confirmé positivement ou négativement. L'utilisateur expéditeur est donc **averti du bon transfert des donnés dans l'entité distante homologue dans le délais demandé et de leur mise en sécurité (par elle)** .

Le service *Demande de Changement de Tour* permet à un utilisateur de RTSE de demander le Tour (s'il n'en bénéficie pas déjà). Ce Tour permet de **transférer des APDU** ou de **terminer l'association**.

Le service *Changement de tour* permet à un utilisateur de céder le Tour à son homologue, s'il en bénéficie.

Traitement transactionnel point-à-point : CCR

CCR (Commitment, Concurrency, Recovery) fournit les fonctions de base nécessaires au systèmes de traitement transactionnel réparti. Dans ces systèmes (voir TP ci-dessus) les applications transactionnelles sont organisées selon une structure arborescente. Les fonctions de **validation** : *commit* (à une ou deux phases), de contrôle de la concurrence ou de recouvrement sur une branche de l'arbre sont du ressort de CCR. Ce service peut être appliqué pour fournir ces fonctions de sécurité dans n'importe quelle Entité d'Application.

3.4. Service Présentation

La couche Présentation permet à des applications de communiquer en échangeant des données structurées dans le cadre d'un dialogue ordonné. Elle fournit une représentation commune de ces données; cette représentation porte aussi sur les actions effectuées sur les structures de données. Son rôle est semblable à celui d'un langage dans la communication entre deux personnes: elle doivent utiliser une même langue c'est à dire une grammaire et un vocabulaire communs. Ce vocabulaire est constitué des objets à manipuler par la couche et la grammaire aux fonctions qui s'y rapportent.

La couche Présentation fournit les éléments syntaxiques communs utilisés par les entités d'application qui peuvent ainsi utiliser n'importe qu'elle syntaxe locale spécifique qui est transformée

en une syntaxe de transfert commune (ASN.1/X208). La couche Application peut ainsi choisir et négocier une ou plusieurs syntaxes de transfert pour assurer sa communication ("Contexte(s) de présentation") et éventuellement renégocier cette syntaxe.

Cette syntaxe peut être transformée par exemple pour assurer la compression ou le chiffrement des données.

Ainsi le Service Présentation peut offrir des **connexions sécurisées** (confidentialité) que peuvent utiliser les applications en empruntant un "contexte de présentation" convenable.

3.5. Service Session

Le service Session doit fournir aux entités de Présentation les moyens pour **organiser et synchroniser** leur dialogue et gérer leurs échanges de données. Au cours d'une connexion de session, le service Session maintient l'état du dialogue entre utilisateurs même en cas de perte de données par le service Transport

Entre deux entités de Présentation on peut établir simultanément et/ou consécutivement plusieurs connexions de Session. Pour réaliser ce dialogue ordonné, le service Session peut fournir les fonctions suivantes : Etablissement (négocié) et libération de connexions, échanges de données normales, express ou typées, transfert simultané ou à l'alternat et éventuellement mise en quarantaine de ces données, synchronisation du dialogue (découpage temporel) et resynchronisation en cas de défaut (reprises).

De plus une "activité" d'un utilisateur peut se poursuivre durant plusieurs connexions de session successives (ou ne durer qu'une partie de la durée d'une connexion). Le service Session permet d'assurer la gestion de cette activité : la lancer, l'interrompre, la reprendre ou la terminer à la demande. La couche Session fournit aussi les moyens de gérer toutes ces fonctions en définissant à tout instant quel utilisateur a le droit de les mettre en oeuvre. Pour simplifier sa mise en oeuvre, plusieurs sous-ensembles du service Session ont été (BCS, BSS, BAS...) ou pourront être définis.

Les mécanismes de synchronisation/resynchronisation et de gestion d'activité améliorent la sécurité (fiabilité) des échanges.

3.6. Service Transport

La couche Transport joue un rôle charnière dans le modèle de référence OSI en fournissant un moyen de télécommunications de bout en bout (entres utilisateurs finaux) de qualité donnée. Elle offre **un transfert de données transparent et fiable** aux entités de Session, en les déchargeant des détails d'exécution de ce transfert et à un bon rapport qualité/prix. En utilisant les services des couches inférieures, elle offre un **service de transmission "idéal" et optimisé**.

Pour offrir la qualité de service souhaitée (dans la mesure du possible) indépendamment des moyens (réseau de télécommunications) utilisés, la couche Transport doit

pouvoir fournir certaines fonctions traitées parfois par les couches inférieures (par exemple la **détection et la correction** des erreurs de transmission dans le cas (habituel) des réseaux locaux).

Pour offrir un service économiquement optimisé, la couche Transport permet, d'une part, un choix du meilleur service réseau disponible (si il y en a plusieurs) et, d'autre part, une utilisation optimale de chaque connexion de réseau en mettant en oeuvre le multiplexage. L'optimisation des performances est obtenue par un choix convenable de la taille des blocs de données transférées et, si nécessaire, l'éclatement du transfert sur plusieurs connexions de réseau.

3.7. Service Réseau

Une liaison de données implique une connexion physique directe entre les entités à relier. Pour interconnecter à la demande deux systèmes ouverts quelconques, on doit utiliser un réseau de télécommunications réel public ou privé (Sous-réseau au sens du modèle de référence) qui permet d'établir, à la demande, les interconnexions nécessaires.

La couche Réseau fournit donc aux entités de Transport des connexions transparentes en leur masquant les problèmes de routage et de relais liés à l'établissement de ces connexions. Elle met en oeuvre une cascade de liaisons de données. Sur ces liaisons de données elle peut multiplexer plusieurs connexions de Réseau.

Le service Réseau assure en particulier :

- l'indépendance par rapport aux supports de transmissions
- le transfert de bout en bout entre systèmes à travers un (Sous-)réseau (et non entre utilisateurs...)
- la transparence des informations transférées (suite d'octets)
- le choix d'une **qualité de service**
- l'adressage d'un utilisateur du service de Réseau (système) en l'identifiant de manière non ambiguë.

La couche Réseau exploite ces adresses et, éventuellement, détermine le chemin à suivre pour les données (routage) et réalise l'aiguillage des données sur ce chemin dans les systèmes intermédiaires. Les fonctions d'administration de réseau (administration de couche) permettent de surveiller et de gérer le (sous-réseau) de télécommunications.

Durant la phase de connexion, on peut restreindre les accès aux services distants en utilisant des **groupes fermés d'usagers** et/ou des **interdictions d'appels entrants ou sortants**; ces fonctionnalités sont gérées par le réseau (et non par les utilisateurs).

3.8. Service Liaison de Données

La couche Liaison de données permet de transférer des unités de données (trames) entre entités de réseau par l'intermédiaire d'une ou plusieurs connexions physiques. Elle permet aussi d'établir, de maintenir ou de libérer une connexion entre ces entités.

Dans la mesure du possible, elle doit assurer un transfert fiable de données. Pour cela, elle **détecte et corrige les erreurs** pouvant se produire dans la couche physique, assure un maintient en séquence des données et un contrôle de flux sur la liaison. En pratique une liaison de données permet un transfert d'information entre deux systèmes, ou plus, partageant le même circuit physique, ou entre un système et un point d'entrée d'un réseau de télécommunications.

Lorsque le Service Physique est un service multipoint, il offre une ressource partagée sur laquelle un seul système peut émettre à un instant donné. Dans le cas d'une architecture dissymétrique (maître-esclave) l'accès peut être géré par le protocole de *Commande de la liaison logique* (LLC: Logical Link Control).

Sur un réseau local, où le contrôle est réparti entre les systèmes, un service de *Commande d'accès au médium* (MAC: Method Acces Control) gère le partage de ressource. Dans ce cas la détection d'erreur (par code cyclique) est descendue à ce sous-niveau.

3.9. Service Physique

La couche Physique fournit les moyens mécaniques, électriques, fonctionnels et procéduraux nécessaires à l'activation, au maintient et à la désactivation des connexions physiques destinées à la transmission transparente des bits entre les entités de liaison de données.

Une connexion physique peut mettre en jeu plusieurs systèmes ouverts intermédiaires. Les entités de la couche Physique sont interconnectées au moyen d'un support physique de communication : câble, fibre optique, onde hertzienne. Le composant de base au niveau physique est le **"circuit de données"**, chemin de communication dans le support physique d'interconnexion de systèmes ouverts, muni des moyens nécessaires à la transmission des bits sur ce chemin.

Une connexion physique est assurée par un ou plusieurs circuits de données (interconnectés par des systèmes relais). Les moyens à mettre en oeuvre comportent notamment les modems, les coupleurs de communication et les interfaces entres ces composants. Sur une connexion physique, il n'est pas possible de garantir une transmission sans erreurs du flux d'information.

L'apparition des réseaux à très haut débit (FDDI: Fiber Distributed Data Interface, ATM: Asynchronous Transfert Mode) a induit une structuration de ce service en 2 ou 3 sous-couches, en particulier pour traiter l'adressage dans les réseaux en commutation de cellules (ATM).