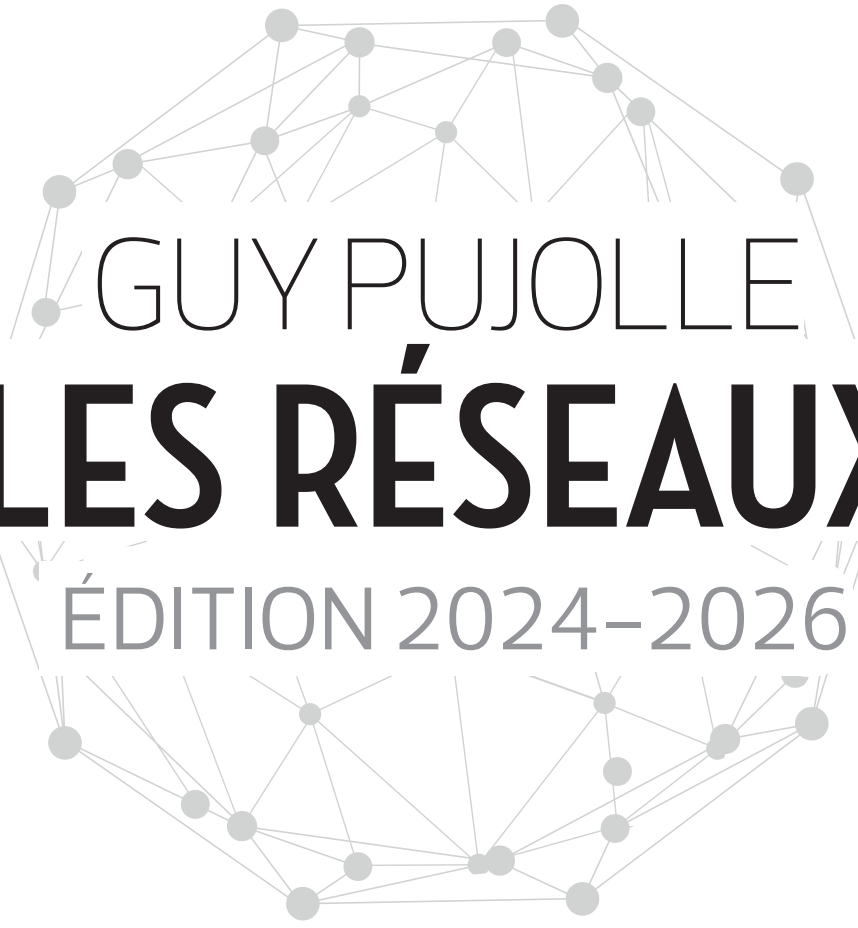


GUY PUJOLLE

LES RÉSEAUX

ÉDITION 2024-2026

ANNEXES

Avec la collaboration de Olivier Salvatori

Éditions EYROLLES

Table des matières

Les Réseaux, 10e édition

Annexes

A

Annexe du chapitre 2 (Les composants des réseaux)

Le RNIS (réseau numérique à intégration de services)

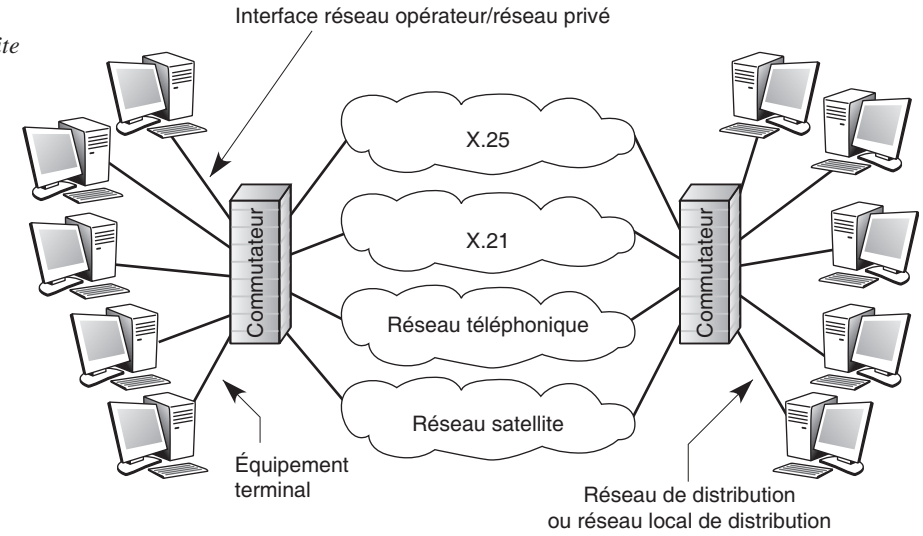
Le RNIS, en anglais ISDN (Integrated Services Digital Network), a été le premier réseau à transporter simultanément la parole téléphonique sous forme circuit et les données sous forme paquet. Bien que ce type de réseau soit en bout de course, il est intéressant de comprendre le chemin parcouru en quelques années par les réseaux multimédias.

Les figures A.1 à A.3 illustrent l'évolution des réseaux à intégration de services. La première étape a consisté à cacher les différents réseaux existants par une interface utilisateur unique, l'interface S, permettant aux équipements terminaux d'accéder à ces réseaux. Pour l'utilisateur, la vue était unique, et les réseaux étaient transparents. Les données devaient être transportées par le meilleur chemin possible, avec une qualité de service déterminée. Ce premier réseau RNIS, dit RNIS bande étroite, est illustré à la figure A.2.

Le RNIS a été étendu par l'introduction d'un réseau de signalisation, encore appelé réseau sémaphore, ayant pour fonction de transporter les commandes. Pour comprendre le rôle de la signalisation, prenons l'exemple simple de l'application téléphonique. Lorsque l'abonné numérote, sa signalisation part par l'interface S et arrive dans le réseau sémaphore, qui véhicule ces quelques octets jusqu'à l'appareil du correspondant en un temps inférieur à 100 ms. Si celui-ci est déjà en train de téléphoner, une signalisation repart vers l'émetteur et produit une tonalité d'occupation. Les circuits du réseau téléphonique ne sont donc pas utilisés. Si le poste du correspondant est libre, la signalisation déclenche la sonnerie. Si l'utilisateur distant est absent, une nouvelle signalisation part de l'émetteur, toujours acheminée par le réseau sémaphore, pour arrêter la sonnerie.

Le réseau téléphonique n'est pas non plus utilisé dans ce cas. Si l'abonné destinataire décroche, une signalisation part pour mettre en place un circuit. Ce circuit a été prévu par la commande initiale, qui, lors de son acheminement, a consulté les nœuds de commutation du réseau téléphonique pour s'assurer de sa mise en place en cas de succès de la communication.

Figure A.1
RNIS bande étroite



Le réseau sémaphore permettait un gain d'utilisation de 10 à 20 % du réseau téléphonique. Ce réseau de signalisation est connu et normalisé depuis de longues années sous le sigle CCITT n° 7, ou, en anglais, SS7. C'est un réseau à transfert de paquets, qui suit l'architecture du modèle de référence. La figure A.2 présente cette extension du RNIS.

L'étape suivante a vu arriver un nouveau réseau, le RNIS large bande, qui permettait de prendre en charge les très hauts débits. La première technique choisie pour ce réseau a été le transfert ATM. Ce réseau supplémentaire s'ajoutait en fait aux réseaux bande étroite, comme l'illustre la figure A.3.

Figure A.2
RNIS avec réseau sémaphore

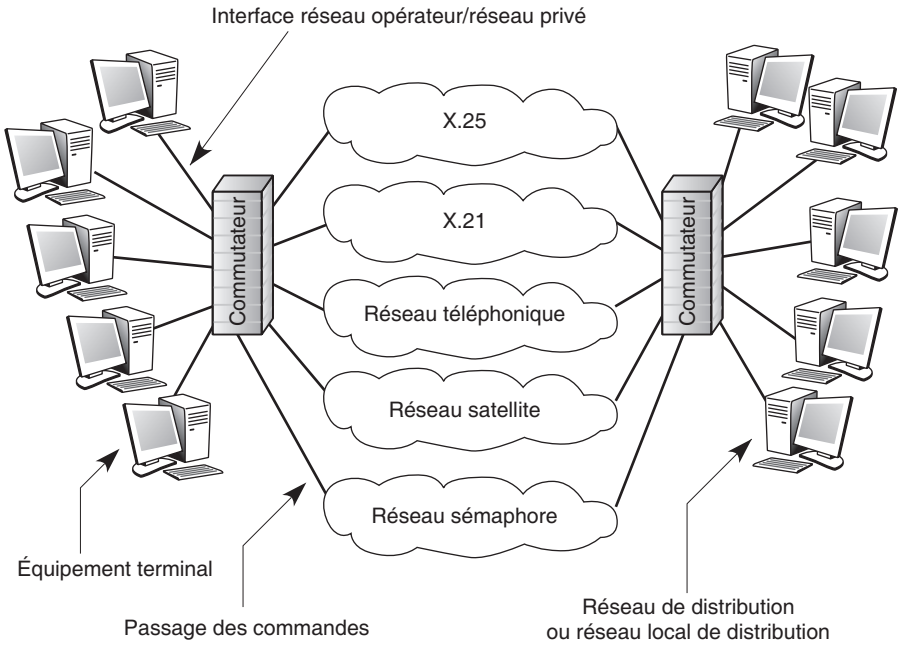
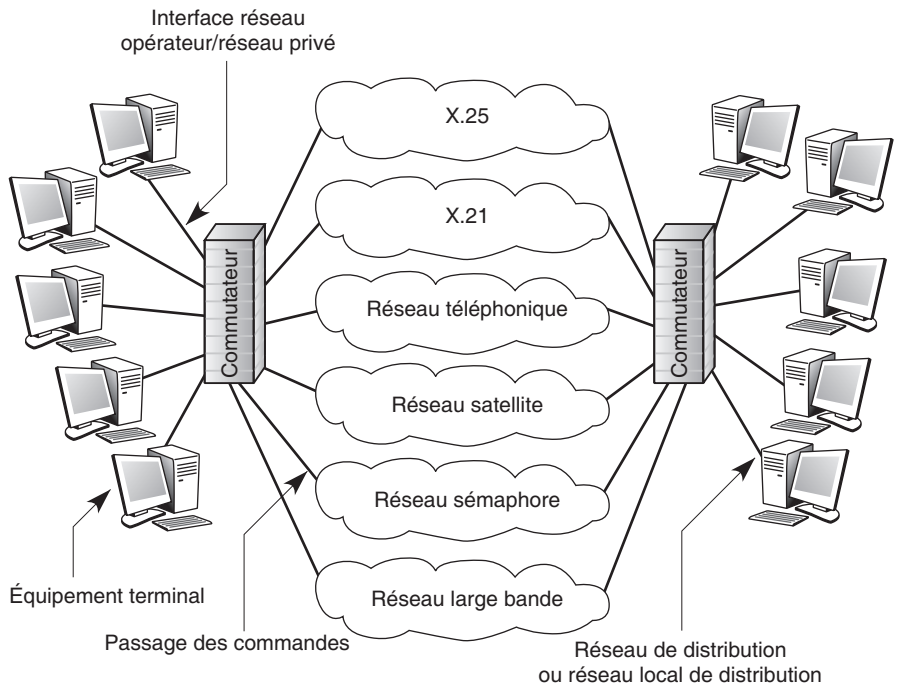


Figure A.3
Extension du RNIS avec un réseau large bande

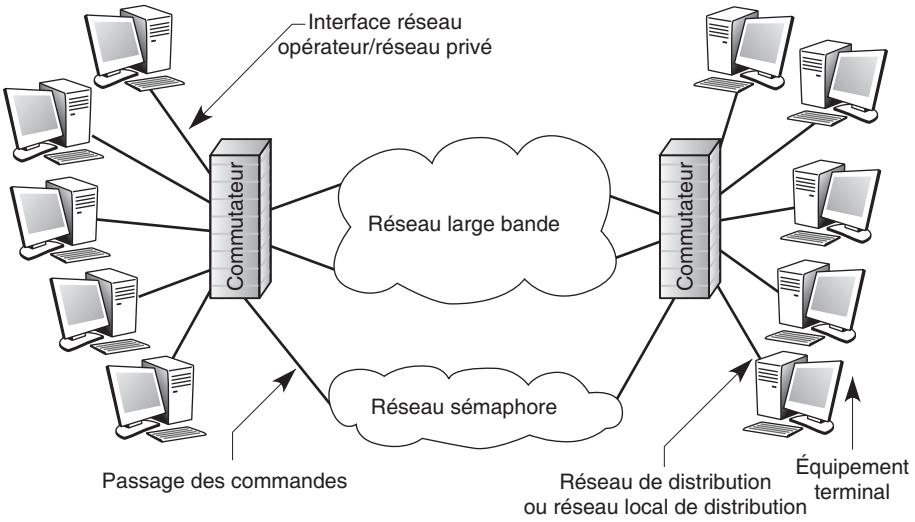


L'étape ultime a visé l'intégration de tous les réseaux en un seul et même réseau, le réseau large bande. Le réseau sémaphore était lui-même intégré au réseau large bande. Les équipements terminaux comportaient des organes permettant de produire et de recevoir directement des paquets IP.

Ce réseau est illustré à la figure A.4. Il s'agit du réseau large bande intégré, ou IBCN (Integrated Broadband Communication Network). Ce réseau forme les prémices du réseau qui porte le nom de NGN (Next Generation Network), parce que l'IBCN a été introduit en pensant que le cœur du réseau serait ATM, alors que les choix se sont portés vers d'autres solutions.

Le réseau de signalisation, qui était spécifique, s'est transformé en un réseau IP. Les réseaux de ce type sont aujourd'hui des réseaux MPLS (MultiProtocol Label Switching) ou GMPLS (Generalized MPLS).

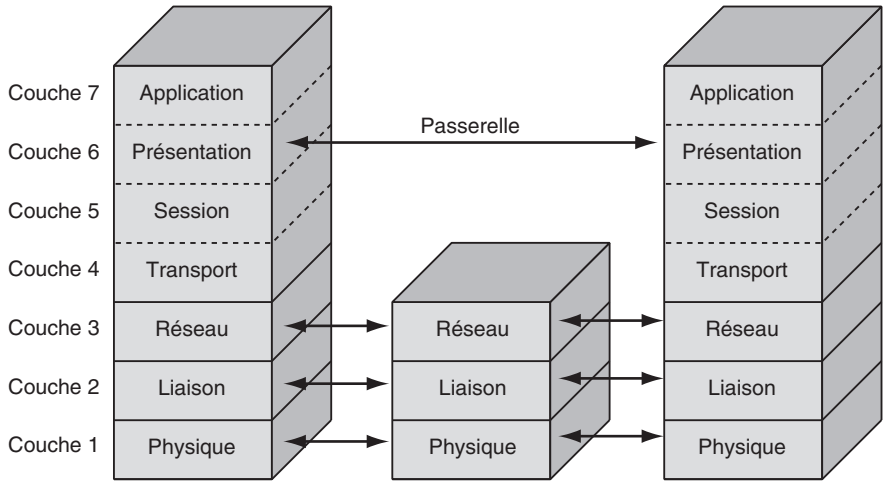
Figure A.4
Réseau large bande intégré



Le modèle de référence

La figure A.5 illustre l'architecture en sept couches du modèle de référence.

Figure A.5
L'architecture OSI



Le concept d'architecture en couches consiste à attribuer trois objets à chaque couche. Pour une couche de niveau N, ces objets sont les suivants :

- **Service N.** Désigne le service qui doit être rendu par la couche N de l'architecture à la couche supérieure (N + 1). Ce service correspond à un ensemble d'actions devant être effectuées par cette couche, incluant événements et primitives, pour rendre ce service au niveau supérieur.
- **Protocole N.** Désigne l'ensemble des règles nécessaires à la réalisation du service N. Ces règles définissent les mécanismes permettant de transporter les informations d'un même service N d'une couche N à une autre couche N. En particulier, le protocole N propose les règles de contrôle de l'envoi des données.
- **Points d'accès au service N, ou N-SAP (Service Access Point).** Les points d'accès à un service N sont situés à la frontière entre les couches N + 1 et N. Les services N sont fournis par une entité N à une entité N + 1 par le biais de ces points d'accès. Les différents paramètres nécessaires à la réalisation du service N s'échangent sur cette frontière. Un N-SAP (Service Access Point) permet donc d'identifier une entité de la couche N + 1, et chaque N-SAP peut être mis en correspondance avec une adresse.

Chaque service, protocole ou N-SAP d'une couche N comporte les attributs suivants :

- sémantique d'association ;
- sémantique de fonctionnalité ;
- syntaxe de codage.

La sémantique d'association désigne la façon de dialoguer de deux entités communicantes. Elle peut être de deux types : avec ou sans connexion. Dans un dialogue avec connexion, trois phases se succèdent dans le temps :

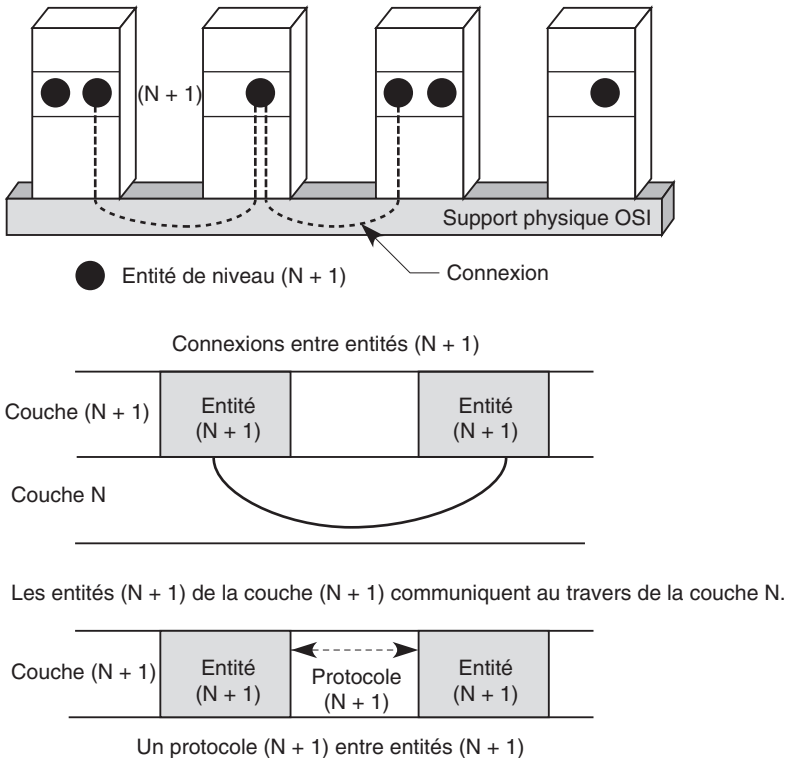
1. Établissement de la connexion entre les deux entités communicantes.

2. Transfert des données.
3. Fermeture de la connexion.

Ces phases sont longuement décrites dans cette annexe.

La figure A.6 illustre les concepts de base du modèle de référence.

Figure A.6
Concepts de base du modèle de référence



Les différentes phases de la communication sont caractérisées par l'échange de primitives de service et d'unités de donnée de protocole, ou PDU (Protocol Data Unit). Nous revenons plus en détail sur ces primitives et unités de donnée un peu plus loin dans cette annexe.

Comme expliqué précédemment, le deuxième attribut des objets d'une couche est la sémantique de fonctionnalité. Ce concept désigne l'ensemble des procédures qui sont utilisées pendant la phase de transfert des données. Pour une association avec connexion, par exemple, ces procédures sont les suivantes :

- fragmentation-réassemblage
- concaténation-séparation
- données expresses
- remise en séquence

- réinitialisation
- contrôle de flux
- contrôle d'erreur

Le troisième attribut d'un service, protocole ou N-SAP d'une couche N est la syntaxe de codage. Il s'applique au codage des primitives de service et des PDU utilisées par la sémantique d'association. Ces syntaxes de codage permettent de décrire les entités rencontrées dans un réseau. La syntaxe la plus utilisée est ASN.1 (Abstract Syntax Notation 1), que nous introduisons dans cette annexe en même temps que la couche 6 du modèle de référence.

La sémantique d'association

La sémantique d'association propose deux types de dialogue entre les entités communicantes : le mode avec connexion (connection oriented) et le mode sans connexion (connectionless oriented).

La norme de base du modèle de référence opte pour le mode avec connexion, tandis que l'additif n° 1 à la norme retient le mode sans connexion. Dans ce dernier mode, les entités homologues ont une connaissance *a priori* des possibilités de communication communes. Les discussions actuelles pourraient aboutir à une intégration des deux modes dans les futures architectures NGN (Next Generation Network).

Le mode avec connexion

La norme de base ISO 7498 définit explicitement la mise en place d'une connexion pour les communications entre des entités de même niveau. Elle indique qu'une entité de niveau N ne peut émettre de bloc d'information qu'après avoir demandé à l'homologue avec lequel elle souhaite communiquer la permission de le faire.

Pour mettre en place une connexion, le protocole de niveau N émet donc un bloc d'information contenant une demande de connexion de niveau N. Le récepteur a le choix d'accepter ou de refuser la connexion par l'émission d'un bloc de données indiquant sa décision. Dans certains cas, la demande de connexion peut être arrêtée par le gestionnaire du service, qui peut refuser de propager la demande de connexion jusqu'au récepteur, par exemple par manque de ressources internes. Une demande d'ouverture de circuit virtuel de niveau 3, qui n'est rien d'autre qu'une connexion réseau, peut ainsi être stoppée dans un nœud intermédiaire si la mémoire est insuffisante ou si la capacité d'émission est dépassée.

La mise en place du mode avec connexion, permettant la communication entre entités homologues, se déroule en trois phases distinctes :

1. Établissement de la connexion.
2. Transfert des données de l'utilisateur d'une entité à l'autre.
3. Libération de la connexion.

L'avantage du mode avec connexion est évident pour la sécurisation du transport de l'information. Puisque les émetteurs et les récepteurs se mettent d'accord, l'ensemble de

l'activité du réseau est facilement contrôlable, tout au moins au niveau des nœuds extrémité. Au moment de l'ouverture d'une connexion, des paramètres peuvent de surcroît être passés entre l'émetteur et le récepteur pour équilibrer la transmission dans des limites admissibles par les deux extrémités. On parle en ce cas de négociation de la qualité de service, ou QoS (Quality of Service), laquelle s'effectue au moment de l'ouverture de la connexion. Pendant toute la durée de vie de la connexion, des paramètres peuvent être échangés entre les participants à la communication.

Le mode avec connexion présente cependant plusieurs difficultés, engendrées notamment par la lourdeur de la mise en place d'une connexion. Même pour n'envoyer que quelques octets, il faut mettre en place la connexion et discuter des valeurs des paramètres de service et, le cas échéant, de la qualité de service. S'il faut ouvrir une connexion à chaque niveau de l'architecture OSI, le temps d'émission de quelques octets est considérablement plus long que dans le mode sans connexion.

L'accès à des applications multipoint est par ailleurs délicat dans ce mode, puisqu'il faut ouvrir autant de connexions que de points à atteindre. Si, par exemple, on veut diffuser un fichier vers 1 000 utilisateurs distants, il est nécessaire d'ouvrir 1 000 connexions, c'est-à-dire d'émettre 1 000 demandes de connexion, et ce à tous les niveaux de l'architecture.

Le mode sans connexion

Dans le mode sans connexion, les blocs de données sont émis sans qu'il soit nécessaire de s'assurer au préalable que l'entité distante est présente. L'existence d'une connexion à l'un quelconque des niveaux de l'architecture est cependant nécessaire pour s'assurer que le service rendu n'est pas complètement inutile. Pour mettre en place une telle connexion, il faut utiliser les services des couches inférieures, ce qui implique nécessairement leur activité.

La principale difficulté d'une communication en mode sans connexion réside dans le contrôle de la communication, puisqu'il n'y a pas de négociation entre l'émetteur et le récepteur. Une station peut ainsi recevoir des données venant simultanément d'un grand nombre de stations émettrices, alors que, dans le mode avec connexion, la station réceptrice n'accepterait pas d'ouvrir autant de connexions. En raison de la difficulté à contrôler la communication, le gestionnaire du réseau doit souvent prendre plus de précautions dans une communication sans connexion que dans le mode avec connexion.

Le mode sans connexion est intéressant pour le transport de messages courts, tandis que celui avec connexion est plus adapté aux messages longs, à condition que les temps de mise en place et de libération des connexions soient négligeables par rapport à la durée de la communication. Comme expliqué précédemment, le mode avec connexion est privilégié dans la norme de base.

Si une connexion est réalisée à un niveau N, les niveaux supérieurs peuvent utiliser un mode sans connexion. Parmi les nombreuses applications qui peuvent utiliser le mode sans connexion, citons la messagerie électronique dans sa définition la plus large. La messagerie est le moyen d'émettre de l'information vers un utilisateur lointain dont on ne sait s'il est présent ou non. Lorsque le client n'est pas actif, il est remplacé par une boîte aux lettres. La connexion de session s'effectue avec la machine qui gère cette boîte aux lettres.

Quantité d'autres applications fonctionnent dans le mode sans connexion, notamment les suivantes :

- **Transfert de fichiers.** Il suffit de s'assurer que le représentant de l'utilisateur final est capable de mémoriser l'ensemble des données contenues dans le fichier.
- **Conférence répartie.** Différents clients mettent en commun des informations dans une boîte aux lettres spécialisée, accessible à l'ensemble des éléments du groupe. Cette application se satisfait très bien du mode messagerie.
- **Accès à une base de données distribuée.** Un utilisateur à la recherche d'informations d'un type non complètement spécifié émet sa demande en messagerie et obtient une réponse quelques heures plus tard.
- **Transactionnel.** Par essence, cette application fonctionne en mode avec connexion, mais elle peut aussi, dans le cas où le temps réel n'est pas nécessaire, se contenter d'un temps de réponse de quelques secondes au lieu d'une fraction de seconde. L'utilisation d'un mode sans connexion n'est alors pas contre-indiquée.

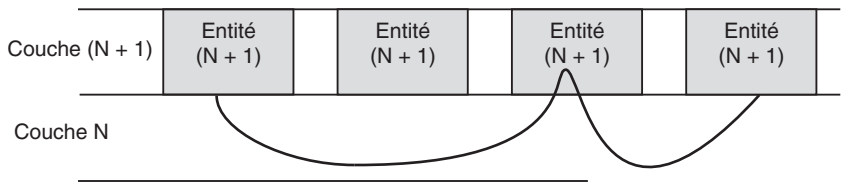
Dans une communication en mode sans connexion, les caractéristiques des unités de donnée doivent être connues à l'avance. À chaque émission, il faut spécifier toutes les informations de contrôle nécessaires pour que l'unité de donnée arrive à destination. En particulier, l'adresse complète de l'entité à joindre ainsi que celle de l'émetteur sont exigées dans le corps de l'unité de donnée. L'ensemble de ces informations peut représenter une longueur non négligeable par rapport à celle des informations à transmettre.

Pour que la communication puisse s'effectuer, il faut en outre une association préalable, provenant d'une connexion à un niveau supérieur de l'architecture, et une connaissance réciproque des deux entités homologues. Cette connaissance concerne les quatre éléments suivants :

- adresses des entités homologues ;
- nature du protocole accepté par les entités homologues ;
- disponibilité des entités homologues ;
- qualité de service offerte par le service N.

Comme dans le mode avec connexion, la communication entre deux entités d'une couche N peut s'effectuer par l'intermédiaire d'un relais de la couche N + 1, laquelle prend en charge les fonctionnalités nécessaires pour que le service N – 1 soit rendu entre les deux entités communicantes. La figure A.7 illustre ce relais.

Figure A.7
Relais en mode sans connexion



Choix d'un mode

Dans les couches de communication de l'architecture du modèle de référence autres que le niveau application, les deux modes sont possibles, le choix de l'un ou de l'autre dépendant des contraintes imposées par les protocoles considérés. En voici quelques exemples choisis aux différents niveaux de l'architecture :

- **Niveau 2.** La norme de base du niveau 2, HDLC (High-level Data Link Control) est en mode avec connexion. Au moment de l'ouverture, on définit les options de fonctionnement et la valeur des paramètres. Le protocole HDLC travaille en bipoint. Le cas particulier du sous-ensemble LAP-B du protocole HDLC, qui a été normalisé par le CCITT (Consultative Committee for International Telegraph and Telephone), est aussi en mode avec connexion. Les protocoles ATM et relais de trames sont de même en mode avec connexion. En revanche, pour les réseaux locaux dans lesquels la distance est faible entre les utilisateurs et où ces derniers sont tous connectés sur un même câble, le mode de base est sans connexion. On suppose en ce cas qu'il y a connexion à un niveau supérieur pour assurer l'activité des récepteurs. Le protocole LLC 1 (Logical Link Control 1), ISO 8802.2, qui est utilisé dans la plupart des réseaux commercialisés, est en mode sans connexion.
- **Niveau 3.** Le protocole IP (Internet Protocol) est sans connexion. On envoie les paquets IP sans demander son avis au récepteur. À l'inverse, le protocole X.25 du CCITT est en mode avec connexion. La raison de ce choix est compréhensible. Cette norme a surtout été mise en place pour les réseaux des opérateurs et des organismes publics de télécommunications. Dans un environnement national, il faut pouvoir assurer une qualité de service définie, et le mode avec connexion est beaucoup plus apte à satisfaire cette contrainte. En revanche, pour des environnements privés de réseaux locaux, le mode sans connexion est suffisant.
- **Niveau 4.** Le protocole TCP demande une connexion, tandis qu'UDP est sans connexion. La recommandation X.224, ou ISO 8073, utilise aussi un mode avec connexion. En règle générale, au niveau 4, il faut pouvoir assurer une qualité de service, laquelle doit être discutée au préalable entre l'émetteur et le récepteur. Autant donc se mettre en mode avec connexion. Si l'on sait que l'interlocuteur distant est toujours présent, on peut se satisfaire d'un mode sans connexion.

Au niveau de la session, le mode avec connexion est fortement recommandé dans la mesure où il faut s'assurer qu'une entité distante est bien présente pour récupérer l'information. Il existe bien une norme de session en mode sans connexion, mais les applications qui en bénéficient, comme la télévision diffusée, sont peu nombreuses.

Les deux modes sont comparés et discutés dans l'additif n° 1 à la norme ISO 7498.

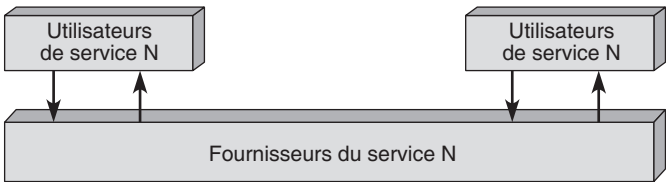
La sémantique de fonctionnalité

La sémantique de fonctionnalité fait référence aux propriétés qui doivent être mises en œuvre pour réaliser une communication. Nous allons commencer par examiner les propriétés d'une connexion point-à-point avant de nous pencher sur les différentes fonctionnalités que l'on peut y associer.

Propriétés d'une connexion point-à-point

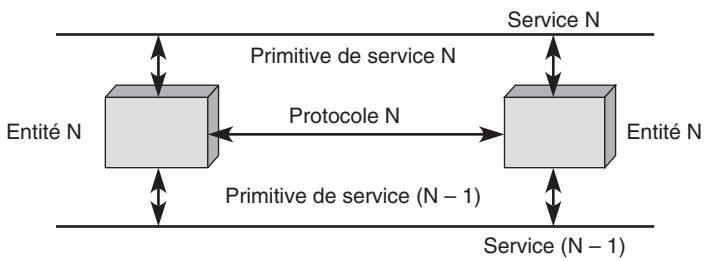
Un réseau en couches est défini par des utilisateurs d'un service N et par des fournisseurs du même service N, comme l'illustre la figure A.8.

Figure A.8
Modèle de service d'un réseau en couches



La figure A.9 illustre les différentes relations entre l'entité N (le logiciel ou le matériel qui gère le protocole de niveau N) et les services N et N – 1. Les entités N communiquent par le biais d'un protocole N.

Figure A.9
Interactions entre entités



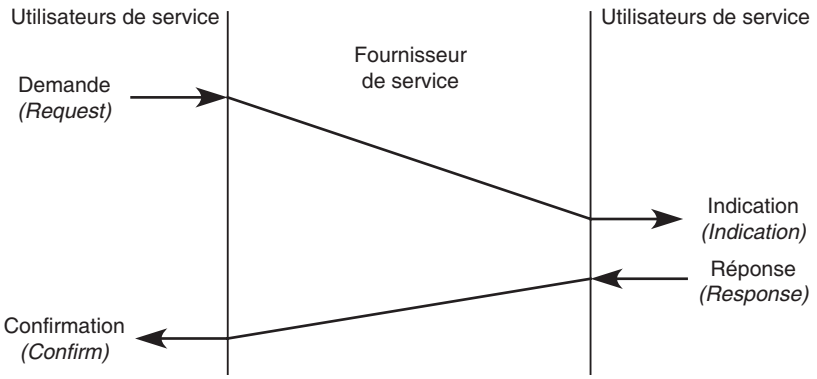
Quatre primitives de service sont définies pour permettre à un utilisateur de service de s'adresser à une entité ou à une entité de répondre à un utilisateur de service (*comme indiqué par les flèches verticales à la figure A.9*) :

- Les primitives de demande, par lesquelles un utilisateur de service appelle une procédure.
- Les primitives d'indication, par lesquelles l'entité destinataire est avertie qu'une procédure a été mise en route par l'entité émettrice sur son point d'accès au service ou que le fournisseur de service indique qu'il appelle une procédure.
- Les primitives de réponse, par lesquelles l'utilisateur distant du service N accepte ou refuse le service demandé.
- Les primitives de confirmation, qui indiquent l'acceptation ou le refus du service demandé qui a été fait au point d'accès au service N.

Les services N peuvent être obligatoires. Dans ce cas, le logiciel ou le matériel réalisant ces services doit être présent. Ils peuvent aussi être optionnels. L'implémentation physique de ces services par le fournisseur de service N n'est alors pas obligatoire. Enfin, les services peuvent être confirmés ou non, c'est-à-dire demander une confirmation explicite ou non du fournisseur de service vers l'utilisateur du service.

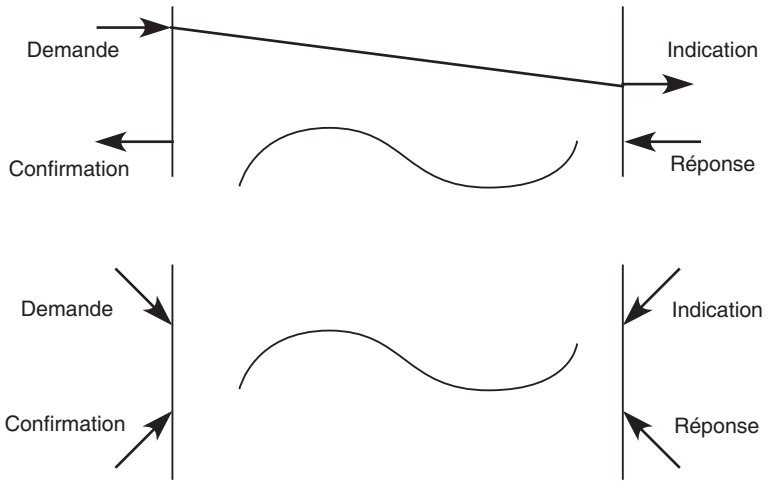
On peut représenter les quatre primitives de service sous la forme illustrée à la figure A.10.

Figure A.10
Primitives de service



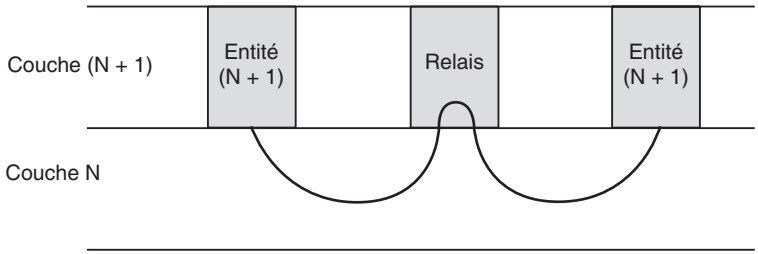
L'ordre temporel dans lequel les interactions aux deux points d'accès au service sont effectuées n'est pas obligatoirement la réponse avant la confirmation. Le fournisseur de service peut envoyer une confirmation de non-exécution avant la réponse définie, par exemple. On représente le chronogramme des ordres d'exécution temporels des primitives de l'une ou l'autre des façons illustrées à la figure A.11. Lorsqu'il n'y a pas de relation temporelle, un tilde est dessiné entre les utilisateurs de service.

Figure A.11
Chronogrammes de primitives de service



Pour échanger des informations entre deux entités du niveau N + 1, il faut établir entre elles une association dans la couche N en suivant un protocole N. Cette association définit une connexion N. Dans certains cas, la communication n'est pas directe et nécessite un relais, comme illustré à la figure A.12.

Figure A.12
Relais de niveau N + 1



Pour déterminer où se trouvent les entités avec lesquelles on souhaite communiquer et comment y arriver, les fonctions suivantes ont été ajoutées à la norme :

- Appellation, pour identifier une entité de façon permanente.
- Adresse N, pour indiquer où se trouve un point d'accès à des services N.
- Répertoire N, pour traduire l'appellation d'une entité N en l'adresse N – 1 du point d'accès aux services N – 1 auxquels elle est reliée.

La figure A.13 illustre ces fonctions ainsi que les correspondances possibles entre entités et points d'accès au service. L'identificateur d'extrémité de connexion N doit être unique dans le contexte d'un point d'accès à des services N. La mise en correspondance des adresses pour aller d'une entité d'application à une autre en passant par l'ensemble des couches peut se faire soit par un adressage hiérarchique, comme illustré à la figure A.14, soit par une gestion de tables.

Figure A.13
Correspondances entre entités et N-SAP

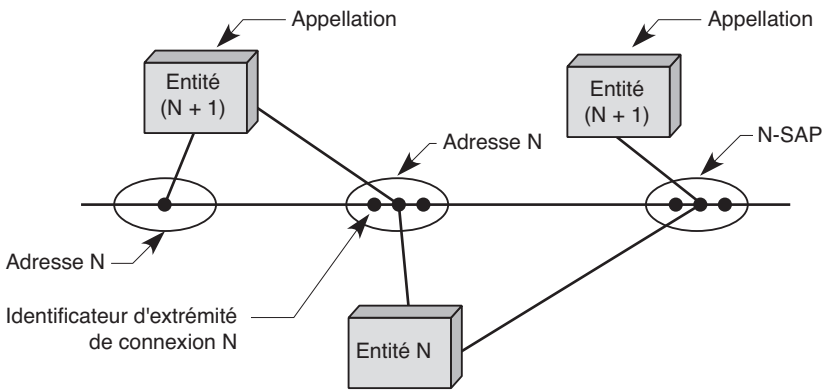
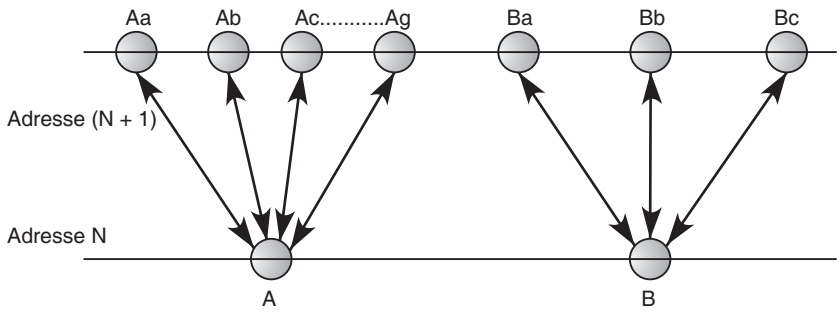
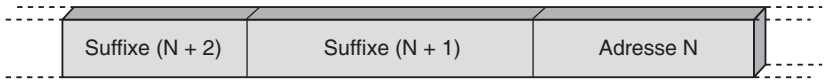


Figure A.14
Adressage hiérarchique



Dans le cas d'un adressage hiérarchique, l'adresse est composée de plusieurs parties, comme illustré à la figure A.15.

Figure A.15
Adresses hiérarchiques



À partir d'une adresse de niveau supérieur à N, il est possible de retrouver l'adresse N en enlevant les suffixes N + 1, N + 2, etc., qui sont des éléments d'adresse unique dans le contexte d'un point d'accès à des services N + 1, N + 2, etc.

L'adressage hiérarchique simplifie considérablement le routage des unités de donnée dans un réseau. Il est simple à mettre en œuvre, quoique le nombre d'octet à transporter soit généralement important et implique une surcharge pour les lignes de communication.

Les adresses de niveau 3 et de niveau 7 sont particulièrement importantes. L'adresse portée par la couche 3, que l'on appelle également adresse de niveau paquet, est située dans l'en-tête du paquet. Elle permet d'acheminer les paquets d'une extrémité à une autre du réseau. L'adresse utilisée dans la couche 7, ou adresse de niveau application, est située dans la zone de contrôle associée au niveau application. Elle permet de retrouver le processus qui, à l'intérieur du niveau application, a procédé à l'émission ou qui doit recevoir les données. L'adresse de niveau 3 peut être remplacée par une adresse de niveau 2 dans les réseaux qui ont adopté un transfert de niveau trame. L'adresse importante reste de niveau 3 si un paquet est transporté dans la trame mais devient de niveau 2 si la couche paquet est supprimée.

Une seconde méthode de mise en correspondance des adresses consiste à utiliser des tables d'adressage pour traduire les adresses N en adresses N – 1. La structure des adresses aux différents niveaux peut en effet se présenter de manière très différente. Certaines peuvent revêtir une forme hiérarchique, d'autres une forme géographique et d'autres encore une forme plate. La taille de ces tables peut rendre leur gestion délicate. Plus le nombre d'entrées dans une table est important, plus la surcharge de travail des nœuds de routage augmente.

L'adressage géographique

L'adressage géographique est un cas particulier de l'adressage hiérarchique dans lequel les parties de l'adresse sont dictées par la situation géographique de l'interface utilisateur. Autrefois, le réseau téléphonique utilisait un adressage totalement géographique, de telle sorte que l'adresse permettait de situer l'emplacement de l'utilisateur.

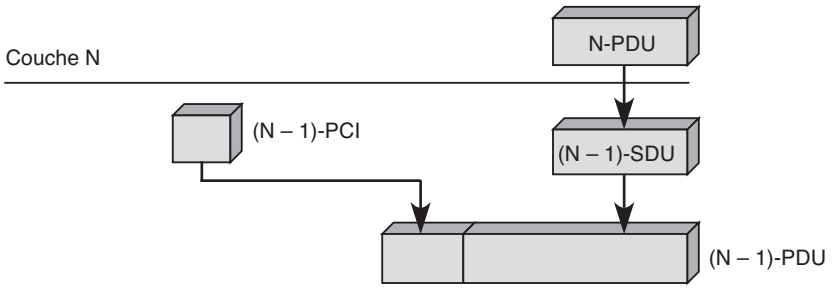
Aujourd'hui, même si la plupart des adresses téléphoniques sont encore hiérarchiques, le fait de garder son adresse téléphonique en déménageant détruit le contexte géographique. Les adresses Internet sont hiérarchiques mais non géographiques. Le nombre de niveaux hiérarchiques est de deux pour la première génération d'Internet, dite IPv4, et de huit pour la deuxième, IPv6.

Les unités de donnée

Une unité de donnée d'un service N, ou N-SDU (Service Data Unit), est un ensemble de données provenant de l'interface avec la couche N et devant être transportées sur une connexion N. Les informations de contrôle du protocole N, dites N-PCI (Protocol Control Information), proviennent d'entités N. Elles sont ajoutées, le cas échéant, à des SDU sur une connexion N – 1.

Les principales unités de donnée sont illustrées à la figure A.16.

Figure A.16
Unités de donnée

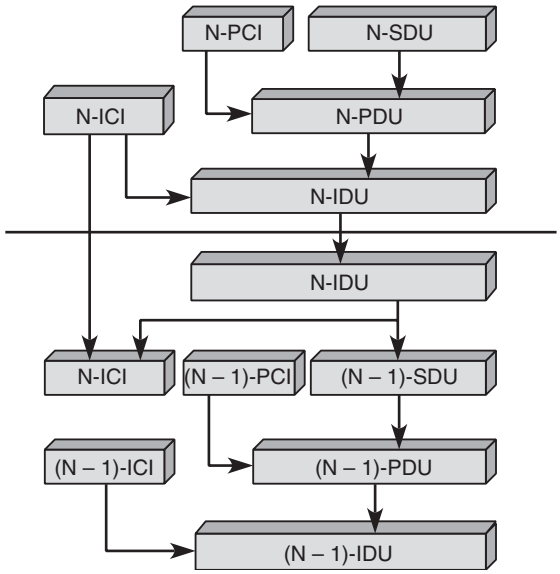


Les unités de donnée du protocole N, ou N-PDU (Protocol Data Unit), sont spécifiées par un protocole N. Elles consistent en informations de contrôle du niveau N et en informations provenant de une ou plusieurs unités de donnée de service. Pour coordonner le travail au même niveau, nous avons déjà rencontré les unités de donnée PCI. Pour contrôler la communication entre entités de niveau N + 1 et entités de niveau N, les informations nécessaires sont transportées dans des N-ICI (Interface Control Information). Ces informations de gestion peuvent être ajoutées aux données à transporter au travers de l'interface N, autrement dit aux N-PDU, pour donner naissance à des N-IDU (Interface Data Unit).

La figure A.17 illustre la structure d'ensemble des entités de transport de données et de contrôle.

Figure A.17

Structure d'ensemble des entités de transport de données et de contrôle

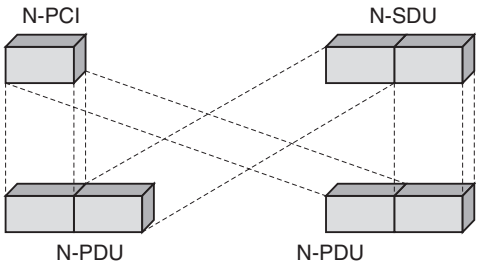


Les données utilisateur qui traversent l'interface de couche N peuvent être appelées données de l'interface N, ou N-IDU. Elles proviennent des données utilisateur N ou N-UD. Dans le cas le plus simple, lorsqu'il n'y a ni segmentation ni groupage, à une N-SDU correspond une seule N-PDU. En règle générale, les unités de donnée ont des longueurs déterminées par une valeur maximale et une valeur minimale, pouvant être 0 octet, et ce pour chaque protocole et chaque service. Le réseau doit découvrir la meilleure longueur possible des unités de donnée pour fonctionner de manière optimale, en coupant ou, au contraire, en recollant des morceaux. Nous examinons dans la suite de cette annexe les diverses possibilités de découpage et de regroupage proposées par la normalisation.

La fonction de segmentation-réassemblage est illustrée à la figure A.18. C'est la fonction accomplie par une entité N pour mettre en correspondance une unité de donnée du service N avec plusieurs unités de donnée du protocole N. Cette figure ne présente que le cas où une N-SDU est segmentée en deux parties. Dans la réalité, il peut y avoir un nombre de fragments beaucoup plus important. Le réassemblage est la fonction inverse de la segmentation.

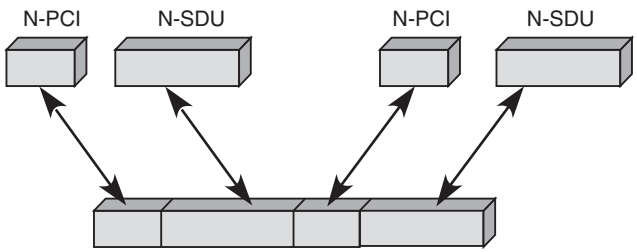
Figure A.18

Segmentation-réassemblage



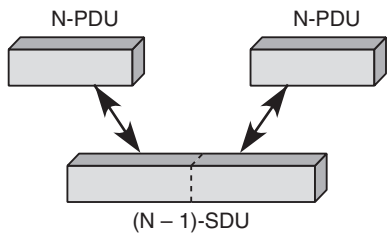
Le groupage-dégroupage est illustré à la figure A.19. Le groupage est la fonction accomplie par une entité N pour mettre en correspondance plusieurs unités de donnée du service N avec une unité de donnée du protocole N. Le dégroupage est la fonction inverse du groupage.

Figure A.19
Groupage-dégroupage



La concaténation-séparation est illustrée à la figure A.20. La concaténation est la fonction accomplie par une entité N pour mettre en correspondance plusieurs unités de donnée du protocole N avec une unité de donnée du service N – 1. La séparation est l'opération inverse. Au travers de l'interface, il n'est possible, entre deux couches, que d'effectuer une concaténation dans un sens et une séparation dans l'autre sens. Il n'est pas possible de couper une N-PDU en plusieurs morceaux, lesquels deviendraient des (N – 1)-SDU.

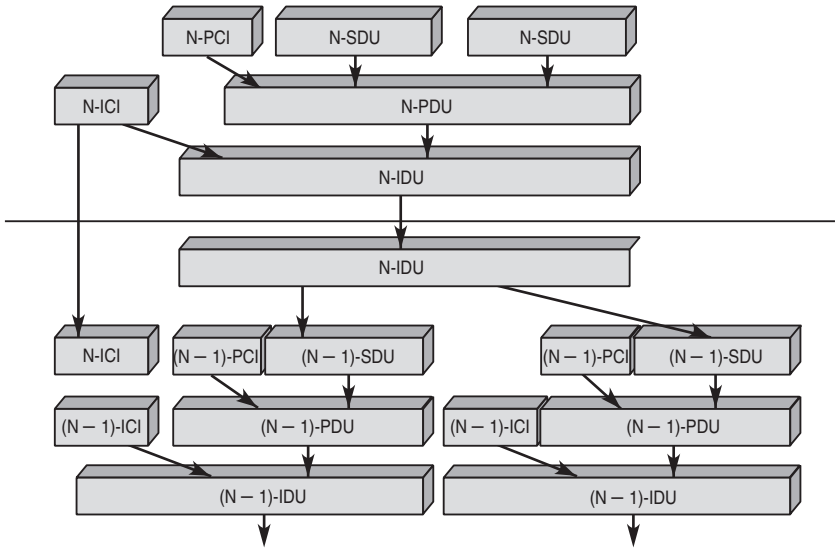
Figure A.20
Concaténation-séparation



La figure A.21 illustre la transmission de la figure A.17, mais en ajoutant une segmentation et une concaténation.

Figure A.21

Concaténation de niveau N suivie d'une segmentation de niveau N – 1

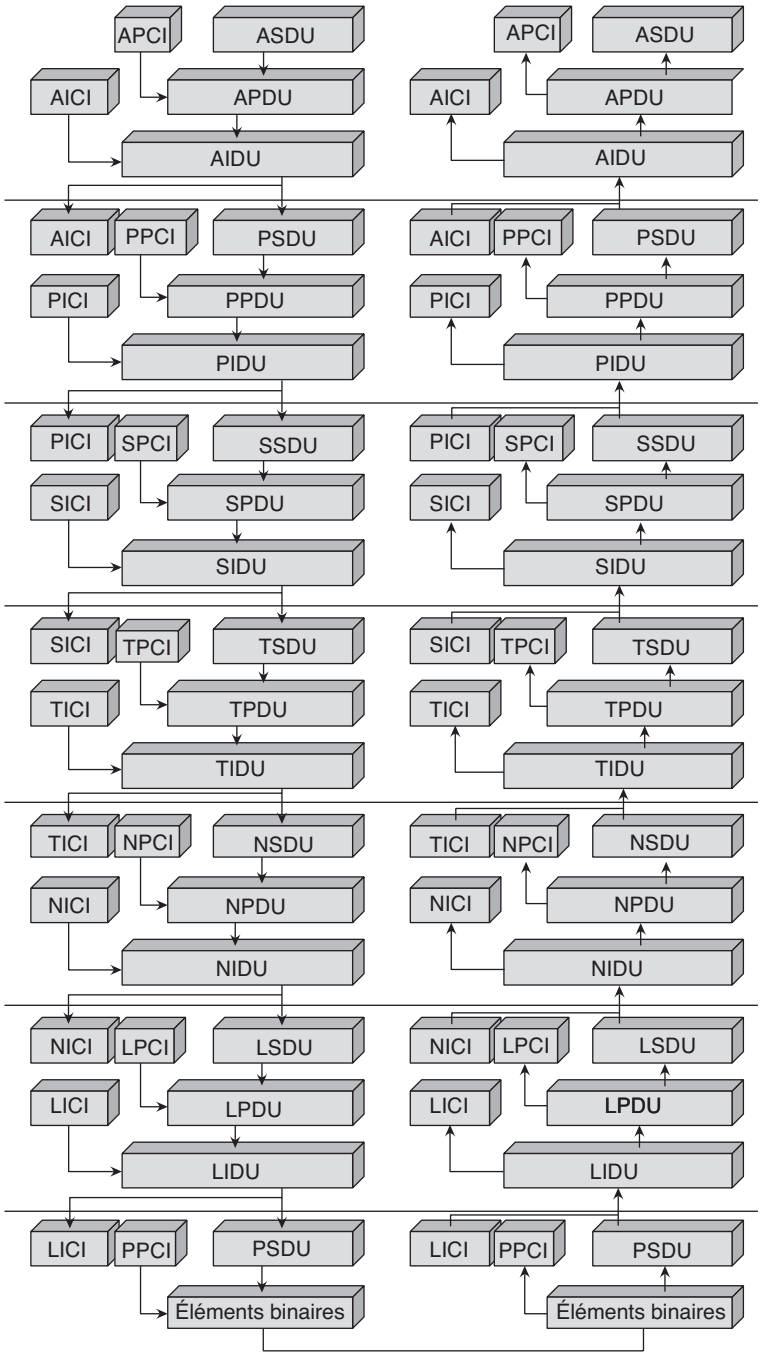


Nous avons employé jusqu'ici le numéro de la couche N pour indiquer la énième couche. Dans la réalité, on utilise une lettre pour désigner ce niveau. Pour chaque niveau du modèle de référence ces lettres sont les suivantes :

- P – Physique
- L – Liaison : LSDU, LPDU, LSAP
- N – Réseau : NSDU, NPDU, NSAP
- T – Transport : TSDU, TPDU, TSAP
- S – Session : SSDU, SPDU, SSAP
- P – Présentation : PSDU, PPDU, PSAP
- A – Application : ASDU, APDU, ASAP

La figure A.22 illustre les unités de donnée de l'ensemble de l'architecture en partant du principe qu'à chaque SDU correspond une PDU et *vice versa*. Dans cette représentation simplifiée, il n'y a ni segmentation-réassemblage, ni groupage-dégroupage, ni concaténation-séparation.

Figure A.22
Unités de donnée de l'architecture OSI



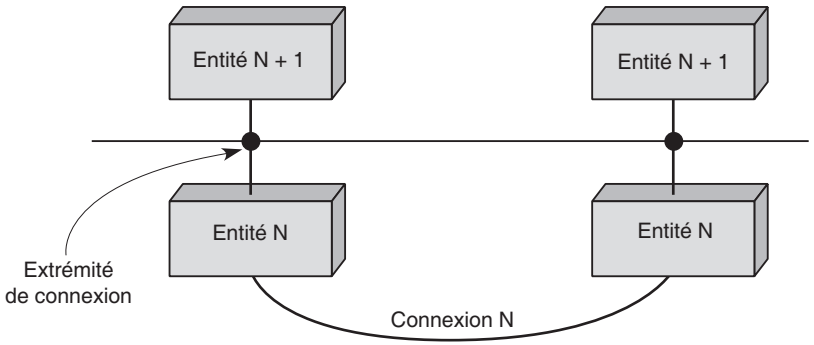
Les connexions

Chaque niveau de l'architecture du modèle de référence possède des fonctionnalités qui lui permettent d'appliquer le traitement approprié aux entités qui la traversent. Les plus importantes de ces fonctionnalités sont les connexions, qui mettent en relation les entités distantes, le contrôle de flux et le contrôle d'erreur.

Une connexion N est une association établie pour permettre la communication entre au moins deux entités N + 1 identifiées par leur adresse N. Une connexion N est donc un service offert par la couche N pour permettre l'échange d'informations entre des entités N + 1. Une connexion multipoint lie au moins trois entités N + 1.

Une connexion N possède au moins deux extrémités de connexion N, qui associent deux entités, comme l'illustre la figure A.23 (une extrémité de connexion est indiquée par un rond noir).

Figure A.23
Extrémités de connexion



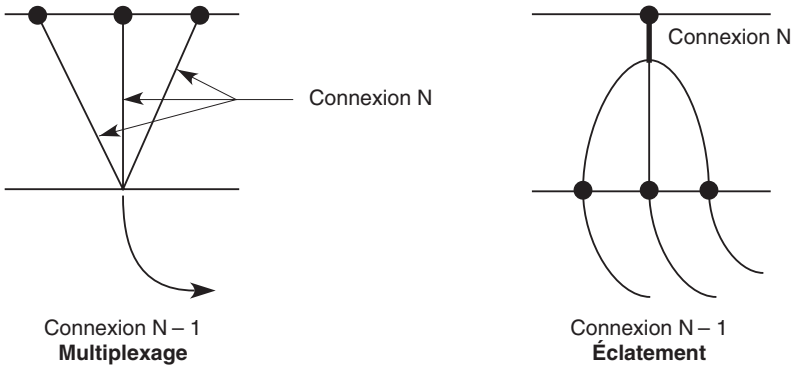
À une extrémité de connexion N correspond une adresse N. Pour qu'une connexion s'établisse, il faut que les deux entités qui veulent communiquer disposent des mêmes éléments de protocole et d'une connexion N – 1. Une fois les données utilisateur N transférées, il faut libérer la connexion. Il existe pour cela deux possibilités :

- Libération immédiate de la connexion, indépendamment du fait que toutes les données utilisateur sont ou non parvenues à destination.
- Libération négociée, qui laisse le temps de s'assurer que les données ont bien été transportées. Dans ce cas, les accusés de réception doivent être parvenus avant la véritable libération de la connexion.

Pour optimiser l'utilisation des connexions, il est possible de multiplexer plusieurs connexions N sur une même connexion N – 1 ou, inversement, d'éclater une connexion N sur plusieurs connexions N – 1, comme illustré à la figure A.24.

Pour mettre en place un multiplexage, une identification de la connexion N est nécessaire. Elle est multiplexée sur la connexion N – 1, de façon que chaque connexion N destination puisse retrouver les N-PDU des différentes connexions N émettrices. Cette identification est bien sûr différente des identificateurs d'extrémité de connexion N, qui sont liés au N-SAP. L'éclatement demande la remise en séquence des PDU, qui doivent être redonnées dans le bon ordre à l'extrémité de la connexion N.

Figure A.24
Multiplexage et éclatement



Contrôle de flux et contrôle d'erreur

Une autre fonctionnalité, que l'on rencontre dans la plupart des niveaux du modèle de référence, est le contrôle de flux. Son rôle est de cadencer l'envoi des PDU sur la connexion, de telle sorte que l'entité homologue puisse récupérer les informations à une vitesse lui convenant, sans perte d'information ni de temps. Un autre contrôle de flux a lieu sur l'interface entre deux couches. Ce contrôle est généralement d'autant plus facile à effectuer que les entités correspondantes sont plus rapprochées.

Sur une connexion N, il faut aussi être capable de prendre en charge les erreurs, tant celles en ligne, c'est-à-dire sur la connexion, que celles dues aux protocoles traversés, ou encore les pertes d'information par écrasement dans des mémoires intermédiaires. On utilise pour cela des accusés de réception,, qui font partie des informations de contrôle du protocole N-PCI. Le cas échéant, une notification d'erreur peut être envoyée à l'entité communicante pour lui signaler la perte d'information et la cause de cette perte. Une réinitialisation peut être demandée par une entité N pour que les deux entités N homologues repartent sur des bases connues.

L'architecture OSI

L'ISO (International Standardization Organization) a normalisé sa propre architecture sous le nom d'OSI (Open Systems Interconnection). L'architecture ISO est la première à avoir été définie, et ce de façon relativement parallèle à celle d'Internet. La distinction entre les deux est que l'architecture ISO définit formellement les différentes couches, tandis que l'architecture Internet s'applique à réaliser un environnement pragmatique.

La couche physique est complexe. De nombreuses normes décrivent la façon de coder et d'émettre les signaux physiques sur une ligne de communication. La couche trame fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, au maintien et à la libération des connexions entre entités de réseau, ainsi qu'au transfert des unités de donnée du service de liaison. C'est la norme ISO 8886, ou CCITT X.212, qui définit le service procuré par la couche 2.

Les autres normes importantes de l'architecture ISO sont les suivantes :

- ISO 3309 et 4335 pour la normalisation du protocole de liaison HDLC (High-level Data Link Control) ;
- ISO 3309, pour la structure des trames ou LPDU ;
- ISO 4335 et 7809, pour les éléments de procédure ;
- ISO 8471, pour la description de la classe en mode équilibré de HDLC ;
- ISO 7776, pour la description de la norme CCITT LAP-B dans un contexte ISO.

Le rôle de la couche paquet (niveau transfert) est, d'une part, de fournir les moyens d'établir, de maintenir et de libérer des connexions réseau entre systèmes ouverts et, d'autre part, de fournir les moyens fonctionnels et les procédures nécessaires pour échanger, entre entités de transport, des unités du service de réseau.

La normalisation de la couche 3 comporte les normes suivantes :

- ISO 8348, ou CCITT X.213, qui définit le service réseau.
- ISO 8208, ou CCITT X.25, qui définit le protocole réseau en mode avec connexion. Ce protocole est le plus souvent appelé X.25, et tous les grands réseaux publics du monde suivent cette recommandation.
- ISO 8473, qui définit le protocole de réseau en mode sans connexion, connu sous le nom d'Internet ISO. C'est une normalisation du protocole développé par le département de la Défense américain sous le nom d'IP (Internet Protocol).
- ISO 8878, ou CCITT X.223, qui décrit l'utilisation de X.25 pour obtenir le service réseau orienté connexion.
- ISO 8648, qui définit l'organisation interne de la couche réseau.
- ISO 8880, en quatre parties, qui définit les différentes combinaisons possibles de protocoles pour rendre un service de niveau 3 conforme à la normalisation.
- ISO 8881, qui permet l'adaptation du niveau 3 de X.25 sur un réseau local possédant un protocole de liaison de type LLC 1.

La couche message (niveau transport) doit assurer un transfert de données entre les entités de session. Ce transport doit être transparent, c'est-à-dire indépendant de la succession des caractères et même des éléments binaires transportés. La normalisation internationale provenant de l'ISO prévoit cinq classes de protocoles capables de satisfaire aux exigences de l'utilisateur.

Les différentes classes du niveau 4 vont de logiciels très simples, qui ne font que formater les données provenant du niveau supérieur et les déformater à l'arrivée, à des logiciels de communication complexes, qui reprennent l'ensemble des fonctionnalités des trois niveaux inférieurs. On peut y trouver une zone de détection d'erreur et des algorithmes de reprise sur erreur. Des redémarrages sur perte de message ou de paquet signalée par la couche inférieure font également partie des outils disponibles dans ces logiciels.

Les principales normes de cette couche sont les suivantes :

- ISO 8072, ou CCITT X.214, qui définit le service transport.

- ISO 8073, ou CCITT X.224, qui définit le protocole de transport orienté connexion et qui possède, comme nous l'avons vu, cinq classes sous-jacentes.
- ISO 8602, qui définit un protocole de transport en mode sans connexion.

Les trois couches supérieures correspondent exactement à celles décrites dans l'architecture du modèle de référence.

Les architectures multipoint

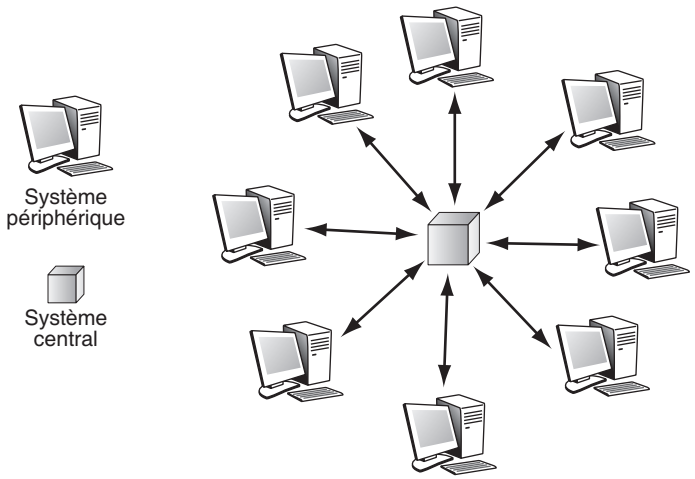
Les applications que l'on utilise classiquement sur un équipement terminal mettent en œuvre une communication point-à-point, c'est-à-dire que la communication part du micro pour aller rechercher l'information vers un seul autre point. Beaucoup d'autres applications font appel à la coopération de plusieurs processus. Par exemple, une recherche dans une base de données distribuée, dans laquelle les informations sont réparties sur plusieurs sites, fait appel à une demande simultanée d'informations vers plusieurs centres. Pour faire cette demande, l'application et toutes les couches de protocoles associées doivent gérer des multipoint. Cette façon de communiquer est plus performante que celle qui consiste à faire la demande à un premier site puis, une fois la réponse obtenue, à un deuxième, et ainsi de suite.

La mise en place d'une communication multipoint est évidemment plus complexe que celle d'une communication point-à-point simple. Avant de décrire ce que les normalisateurs ont retenu dans l'additif n° 2 à la norme ISO 7498-1, il est important de comprendre les deux possibilités extrêmes d'une communication multipoint.

Dans le cas le plus simple, il existe un système central et des systèmes périphériques. Seul le système central peut communiquer avec l'ensemble des sites périphériques, les systèmes périphériques ne pouvant communiquer qu'avec le site central. L'avantage de cette méthode est la grande simplicité des communications. La gestion de l'ensemble peut s'effectuer par le centre. Ce cas est illustré à la figure A.25.

Figure A.25

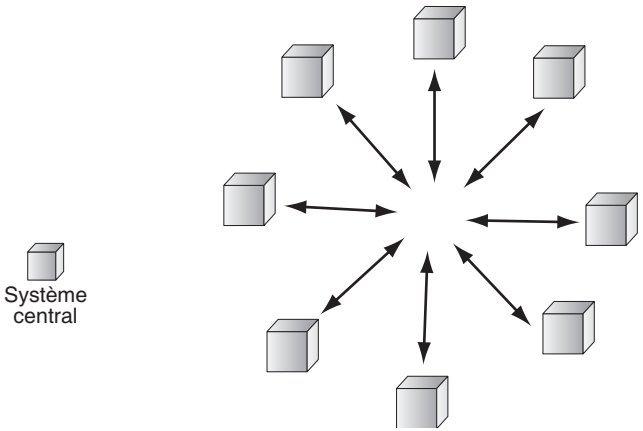
Système multipoint le plus simple



À l'opposé, le multipoint le plus complexe est celui dans lequel tout système est un système central, c'est-à-dire où chaque site peut communiquer directement avec tout autre site. On voit bien la complexité globale de cette configuration, puisque la gestion des échanges est totalement distribuée et que la coordination des systèmes est difficile à prendre en charge. Ce cas est illustré à la figure A.26.

Figure A.26

Système multipoint le plus complexe



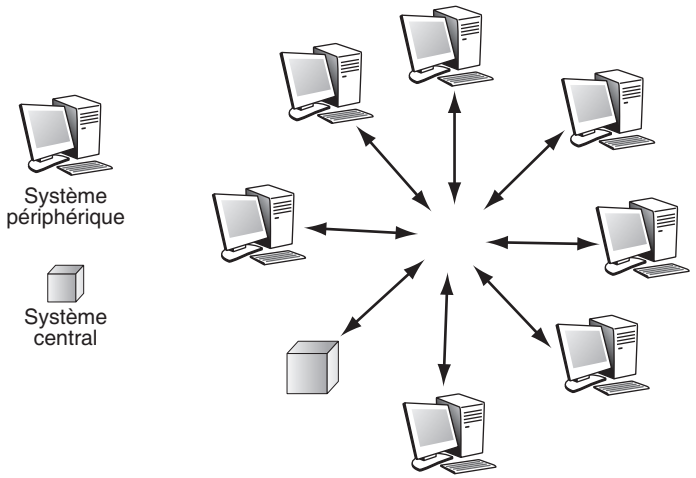
Entre ces deux configurations extrêmes, il existe toute une hiérarchie de possibilités. Les normalisateurs en ont retenu deux, la communication multipoint à centre mobile et la communication multicentre.

La communication multipoint à centre mobile est une légère amélioration du multipoint le plus simple : à un instant donné, il n'y a qu'un seul système central, mais ce site primaire peut varier dans le temps. Un système multipoint complexe est toujours équivalent à une succession de communications multipoint à centre mobile.

Cette configuration est illustrée à la figure A.27. Son inconvénient peut être sa relative lenteur lorsque le système multipoint veut faire du parallélisme.

Figure A.27

Communication multipoint à centre mobile

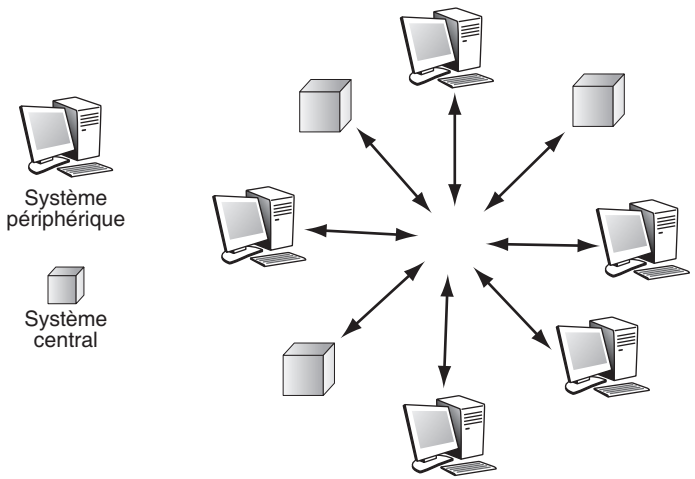


Dans la communication multicentre, si N sites participent à la réalisation de la communication multipoint, seulement M. sites au maximum peuvent se comporter comme un système central, M. étant généralement très inférieur à N.

Cette configuration est illustrée à la figure A.28, dans laquelle, sur les 8 sites du réseau, 3 sont des systèmes centraux et 5 des systèmes périphériques.

Figure A.28

Communication multicentre



B

Annexe du chapitre 4 (L'intelligence dans les réseaux)

Cette annexe concerne les réseaux intelligents, qui ont été définis dans les années 1990 pour permettre à de nouveaux services de télécommunications de se mettre en place en des laps de temps courts par rapport à ceux des années 1980. Ces réseaux intelligents sont aujourd'hui utilisés par les opérateurs pour introduire facilement de nouveaux services.

Les réseaux intelligents

L'expression « réseaux intelligents » concerne à une autre catégorie de réseaux, qui sont des réseaux qui peuvent s'adapter assez simplement à l'introduction d'un nouveau service. Ces réseaux sont totalement différents de ceux qui intègrent des agents intelligents.

Les architectures de réseau développées jusqu'à aujourd'hui ne permettent de prendre en compte que des services simples, ne faisant appel qu'à une seule application, tels les services de messagerie électronique, de transfert de fichiers, de traitement transactionnel, etc. Il est possible d'associer plusieurs applications pour réaliser un nouveau service en utilisant l'architecture mise en place dans la couche application. On peut ainsi transporter un document EDI (échange de données informatisé) dans un message électronique.

La complexité de la gestion et du contrôle des équipements de réseau s'accroît énormément dès lors que l'on sort du cadre du réseau et que l'on y intègre les applications. En effet, l'utilisateur désire avoir une vue globale du service qu'il demande, depuis son fonctionnement jusqu'à son coût, en passant par les problèmes de sécurité et de qualité de service. Le plus simple pour un utilisateur serait qu'il puisse définir exactement ce qu'il souhaite du réseau. Le rôle du réseau intelligent est justement de pouvoir s'adapter à la demande des utilisateurs.

Un premier exemple de service de réseau intelligent est le suivant : au début des années 1980, un grand utilisateur demande à son opérateur de mettre en place un service de renseignements téléphonique à destination de ses clients qui puisse, au moment le plus chargé, fournir un standard par département et, au moment le moins chargé, au milieu de la nuit, un seul standard répondant pour toute la France. Le client n'a aucune idée du numéro de téléphone à choisir en fonction de l'heure de la journée.

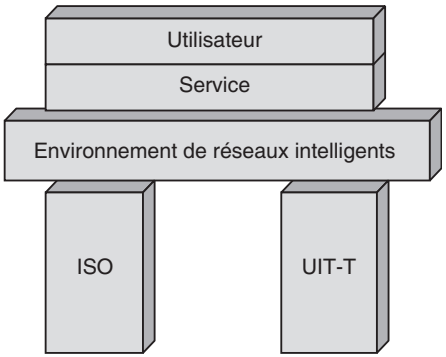
Ce service ne pouvait guère être mis en place à l'époque. Cependant, les opérateurs ont compris le message et ont lancé le numéro 800, ex-numéro vert en France. Ce numéro permet de diriger l'appel d'un client vers le standard le plus proche qui comporte une opératrice disponible. L'application 800 paraît simple. Elle a cependant demandé huit ans de développement. C'était le premier service intelligent à voir le jour. La raison de ce temps extrêmement long est due à l'impossibilité de programmer certains autocommutateurs pour leur dire que s'ils reçoivent un numéro qui commence par 800, ils doivent faire un travail très spécial, qui consiste à interroger une base de données pour trouver le numéro de téléphone à appeler.

Avec l'expérience retirée de la mise en place de ce service, les autocommutateurs sont devenus plus intelligents, et les concepts du réseau intelligent ont suivi. De nouveaux services intelligents, surtout associés à la téléphonie, sont nés, comme la facturation par carte de crédit et tous les numéros spéciaux qui existent aujourd'hui.

Le rôle d'un réseau intelligent est de mettre en place et d'adapter l'infrastructure du réseau de communication de façon à prendre en charge des fonctionnalités d'un nouveau service. Cette adaptation doit également déterminer l'environnement de contrôle et de gestion associé au réseau. De façon assez simpliste, on peut représenter le réseau intelligent comme une couche de protocoles située entre les ressources réseau et l'utilisateur, comme illustré à la figure B.1.

Figure B.1

Place du réseau intelligent dans l'architecture réseau



Pour introduire de façon correcte les différents composants logiciels et matériels nécessaires à la réalisation d'un réseau intelligent ou d'une architecture ayant les mêmes propriétés, il faut modéliser de façon efficace les fonctionnalités du réseau traité. Les

sections qui suivent décrivent le modèle de base du réseau intelligent avant de s'intéresser aux outils permettant de modéliser les fonctionnalités indispensables d'un tel réseau. Nous terminons par l'architecture TINA, que les opérateurs de télécommunications développent en ce sens.

INCM (Intelligent Network Conceptual Model)

Pour définir un réseau intelligent, il faut un modèle précisant l'architecture et les interfaces de référence. L'objectif d'un réseau intelligent étant de s'adapter à la demande de l'utilisateur, ces interfaces doivent permettre une adaptation simple des ressources du réseau. Un tel réseau est en fait intelligent grâce à ces interfaces.

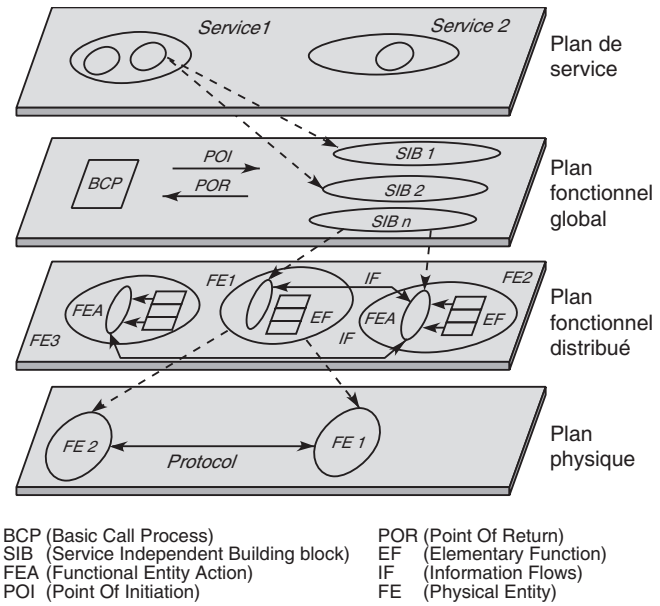
Le modèle conceptuel définissant l'architecture normalisée d'un réseau intelligent est aujourd'hui parfaitement défini. Il s'agit du modèle INCM (Intelligent Network Conceptual Model), qui peut être utilisé pour construire une architecture de réseau intelligent satisfaisant aux exigences suivantes :

- indépendance par rapport à la réalisation du service ;
- indépendance par rapport à la réalisation du réseau ;
- indépendance par rapport aux industriels ;
- indépendance par rapport à la technologie.

Le modèle INCM est illustré à la figure B.2. Il contient quatre couches, que nous allons décrire en détail.

Figure B.2

Plans de l'architecture du modèle de réseau intelligent



Le plan de service

Le plan de service concerne la définition des services que l'utilisateur peut demander. Ces services peuvent être plus ou moins complexes, mais il s'agit généralement d'une superposition de services élémentaires. Un service élémentaire est appelé SF (Service Feature). La demande de l'utilisateur peut rassembler plusieurs services élémentaires pour former un nouveau service. Le service élémentaire SF est réalisé par un module qui se situe dans la couche sous-jacente : le plan fonctionnel global.

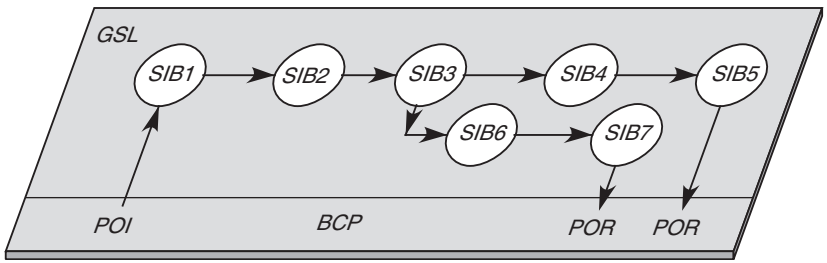
Le plan fonctionnel global

Le plan fonctionnel global contient les modules de base, ou SIB (Service-Independent Building). Ces modules doivent être considérés comme des blocs indépendants de la distribution. À ces blocs correspondent des services ou des parties de service. La distribution n'est prise en compte que dans le plan fonctionnel distribué, le réseau étant interprété comme une machine virtuelle.

Dans ce plan, le processus BCP (Basic Call Process) et les processus GSL (Global Service Logic) sont des SIB spécialisés. Les GSL permettent de chaîner les SIB entre eux pour réaliser un service. Le GSL décrit donc entièrement le service.

Le BCP est un SIB qui contient toutes les fonctionnalités permettant de gérer un appel. Cette gestion utilise deux types de points de synchronisation : les POI (Point Of Initiation) et les POR (Point Of Return). Les POI déterminent à quel moment du traitement il faut appeler le GSL et selon quels critères. Les POR définissent les points au niveau desquels le GSL peut réactiver le réseau pour continuer le processus de service. Ce processus est illustré à la figure B.3.

Figure B.3
Fonctionnement d'un processus GSL



Le GSL décrit un enchaînement linéaire d'exécution de SIB. Le parallélisme, c'est-à-dire la possibilité que plusieurs SIB soient exécutés en parallèle, ne devrait pas tarder. Ce parallélisme devrait apporter des améliorations à la définition de services futurs encore plus complexes. Enfin, dans l'exécution du GSL, plusieurs demandes de POR peuvent être engendrées entre deux POI, de façon à gérer, par exemple, divers événements lors du traitement d'appel.

Les SIB peuvent être extrêmement nombreux. En voici quelques exemples :

- Charge, qui définit les procédures de taxation.
- Compare, qui permet de comparer deux valeurs.

- Limit, qui limite le nombre d'appels à un service.
- Log Call Information, qui permet de stocker des informations sur l'appel en cours.
- Queue, qui permet de mettre un appel en attente.
- Screen, qui permet de vérifier la présence d'un identifiant.
- Service Data Management, qui permet de lire, de créer, d'ajouter ou de supprimer des données dans un fichier.
- Status Notification, qui permet de connaître l'état des ressources du réseau.
- Translate, qui traduit des données de l'utilisateur en termes accessibles au système.
- User Information, qui permet au système de correspondre avec un utilisateur.
- Verify, qui vérifie la syntaxe des informations émises par l'utilisateur.

Le plan fonctionnel distribué

Le plan fonctionnel distribué a pour rôle d'identifier les modules (et leurs relations) nécessaires à la réalisation du réseau intelligent. Ces modules possèdent des fonctions décrites dans la recommandation Q.1204 de l'UIT-T. La description de cette architecture est indépendante de sa réalisation. Celle-ci doit être très flexible, de façon à permettre l'introduction de nouvelles fonctionnalités, indispensables à l'extension des possibilités du réseau intelligent.

Une correspondance assez simple doit être réalisée entre les entités fonctionnelles du plan fonctionnel distribué et les modules SIB (Service-Independent Building) du plan fonctionnel global. Plus précisément, la réalisation de chaque SIB doit s'effectuer à l'aide d'au moins une unité fonctionnelle. Les fonctions de base de l'entité fonctionnelle sont gérées par des actions d'entité fonctionnelle, ou FEA (Functional Entity Action).

Construction d'une application intelligente

En ayant en tête cette représentation du modèle de réseau intelligent, il est possible de comprendre la construction d'une application intelligente.

Le client choisit les services élémentaires dont il a besoin pour réaliser son service global. Il définit ainsi dans le plan de service le service désiré. Une fois le service déterminé, le modèle lui indique les SIB dont il a besoin et l'ordre dans lequel il doit les mettre en œuvre. En d'autres termes, il construit, grâce aux briques de logiciel dont il dispose, le logiciel dont il a besoin pour réaliser son service. C'est le travail effectué dans le plan fonctionnel global.

Pour distribuer ce logiciel global sur le réseau, le client peut soit le distribuer dans tous les nœuds du réseau, soit le placer en un emplacement unique. Le rôle du plan fonctionnel distribué est d'effectuer la distribution du logiciel global. La dernière étape consiste à déterminer où implanter physiquement les briques logicielles.

Les entités fonctionnelles

Une entité fonctionnelle est un groupe unique de fonctions destinées à rendre un service. Une ou plusieurs entités fonctionnelles peuvent être situées sur une même entité physique. Deux entités fonctionnelles distinctes peuvent contenir des fonctions identiques. Les entités fonctionnelles communiquent entre elles par des flux d'information (Information Flow).

Les principales entités fonctionnelles sont les suivantes :

- CCAF (Call Control Agent Function), qui gère l'interface entre l'utilisateur et le réseau.
- CCF (Call Control Function), qui établit, manipule et relâche les appels des utilisateurs dans leur demande de service.
- SSF (Service Switching Function), qui est souvent associée au CCF et permet de réaliser la connexion entre un utilisateur et l'entité de contrôle du service (SCF).
- SCF (Service Control Function), qui contrôle le bon déroulement du module CCF lors de son exécution de sorte qu'il atteigne les entités fonctionnelles de service nécessaires à la réalisation du service demandé par l'utilisateur.
- SDF (Service Data Function), qui contient toutes les informations et fonctions nécessaires pour qu'une entité SCF ait accès en temps réel à un service de réseau intelligent demandé par l'utilisateur.
- SRF (Specialized Resource Function), qui contient des ressources spécifiques qui peuvent s'avérer nécessaires à un service de réseau intelligent.

Les entités fonctionnelles que nous venons de décrire servent à l'accès et à la mise en place du service dans un réseau intelligent mais n'ont pas de fonctionnalités correspondant au service. Il s'agit d'entités fonctionnelles communes, permettant de mettre en place le service.

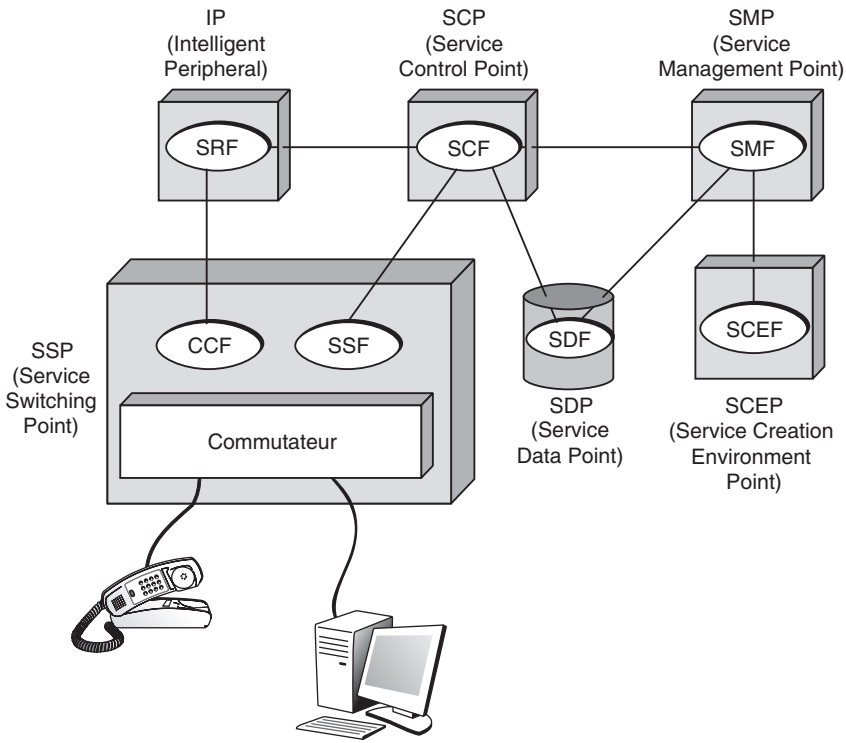
Les entités fonctionnelles suivantes servent, elles, à créer et gérer les services :

- SCEF (Service Creation Environment Function), qui permet la création de nouveaux services de réseau intelligent.
- SMAF (Service Management Agent Function), qui définit une interface entre le gestionnaire du service et la fonction de gestion SMF.
- SMF (Service Management Function), qui doit prendre en charge la gestion des services ouverts dans le cadre du réseau intelligent et coordonne les SCF et les SDF.

Les relations entre les entités fonctionnelles sont nombreuses. La figure B.4 en fournit un exemple simplifié. Elle schématise également des éléments physiques que nous allons aborder ci-après.

Figure B.4

Exemple de relations entre les entités fonctionnelles



Le plan physique

Le plan physique du modèle conceptuel de réseau intelligent identifie les différentes entités physiques et les interfaces entre ces entités. L'architecture du plan physique doit être en cohérence avec le modèle conceptuel INCM. Pour cela, cette architecture doit satisfaire aux exigences suivantes :

- À une entité fonctionnelle du plan fonctionnel distribué correspond une entité physique.
- Une entité fonctionnelle ne peut être découpée et correspondre à deux entités physiques. En d'autres termes, une entité fonctionnelle correspond à une entité physique ou à une partie d'une entité physique.
- Des copies d'une même entité fonctionnelle correspondent à des entités physiques différentes.
- Les entités physiques peuvent être regroupées pour former une architecture physique.
- Les entités physiques peuvent offrir des interfaces standards.
- Les entités physiques sont capables de développer des entités physiques fondées sur une correspondance avec des entités fonctionnelles, et ce avec des interfaces standards.
- Les industriels peuvent adapter leurs produits à de nouvelles technologies sans revoir les principes de l'architecture.

De nombreuses entités physiques ont été définies pour le réseau intelligent, notamment les suivantes :

- SSP (Service Switching Point). Ce sont les points d'accès des utilisateurs au réseau intelligent. Ils sont avant tout des points de commutation, qui se chargent des informations provenant des machines terminales. Les SSP peuvent communiquer avec les autres entités physiques, et en particulier avec les SCP. Un SSP contient une fonction de contrôle d'appel, ou CCF (Call Control Function), une fonction de service de commutation, ou SSF (Service Switching Function), et, si le SSP est un point d'accès utilisateur, une fonction d'agent de contrôle des appels, ou CCAF (Call Control Agent Function). D'autres fonctions plus spécialisées peuvent être disponibles dans un SSP, telles une fonction de ressources spécialisées, ou SRF (Specialized Resource Function), et une fonction de données de service, ou SDF (Service Data Function).
- SCP (Service Control Point). Contient les programmes de logique de service, ou SLP (Service Logic Programs), qui sont utilisés pour rendre le service demandé. Les SCP peuvent posséder des SLP identiques. Un SCP contient une fonction de contrôle de service, ou SCF (Service Control Function), et peut avoir une fonction de données de service, ou SDF (Service Data Function). Le SCP peut accéder à des données situées dans une autre entité physique, soit directement, soit par l'intermédiaire du réseau de signalisation. Le SCP est souvent connecté à des SSP pour traiter les demandes utilisateur qui nécessitent l'intervention du réseau intelligent. La connexion s'effectue par l'intermédiaire du réseau sémaphore.
- SDP (Service Data Point). Les SDP contiennent toutes les données qui seront utilisées par les programmes de logique de service (SLP). Un SDP comporte une fonction de données de service, ou SDF (Service Data Function). Il est possible d'accéder au SDP soit directement, par un SCP ou un SMP, soit par le réseau sémaphore.
- IP (Intelligent Peripheral). Les IP disposent de ressources spécifiques pour permettre une adaptation des commandes de service à la demande utilisateur. Ces ressources très générales incluent :
  - Les annonceurs, par exemple l'organe qui indique le nouveau numéro de téléphone d'un abonné qui a déménagé.
  - Des organes de synthèse de la parole.
  - Des organes de reconnaissance de la parole.
  - Des organes nécessaires à la réalisation d'une téléconférence.
  - Des organes pour intégrer des données venues de l'extérieur.
  - Des générateurs de tonalité.
  - Des tests en synthèse de la parole.
  - Des convertisseurs de protocole.

  Fonctionnellement, un IP contient une fonction de ressources spécifiques SRF (Specialized Resource Function) ou une fonction de contrôle d'appel CCF (Call Control Function). Ces deux fonctions permettent d'accéder aux ressources de l'entité physique IP à partir du SSP.

- AD (ADjunct). L'entité physique AD est fonctionnellement équivalente à celle de SCP. Elle contient les mêmes entités fonctionnelles. La spécificité de l'AD est d'être connecté directement à un SSP. L'interface entre les deux entités peut permettre de très hauts débits et générer de nouveaux services. Un AD peut être connecté à plusieurs SSP, et plusieurs AD peuvent être connectés au même SSP.
- SN (Service Node). Le SN sert à contrôler les services rendus par le réseau intelligent. Un SN communique directement avec un ou plusieurs SSP par le réseau sémaphore. Fonctionnellement, un SN peut contenir un SCF, un SDF, un SRF, un SSF et un CCF. D'une manière similaire à l'AD, la fonction de contrôle de service SCF d'un SN reçoit des messages du SSP, exécute les SLP et renvoie des messages au SSP. Les SLP peuvent être développés par l'environnement de création de nouveaux services.
- SSCP (Service Switching and Control Point). Cette entité physique est une combinaison des SCP et SSP dans un même nœud. Elle contient les fonctions SCF, SDF, CCAF et SSF.
- SMP (Service Management Point). Le SMP réalise les contrôles nécessaires à la gestion du service. Les exemples de fonctions que cette entité physique doit contrôler sont nombreux et vont de la gestion des bases de données de gestion, à la surveillance du réseau, en passant par les tests sur le réseau et la gestion du trafic, des anomalies, de la comptabilité, etc. Un SMP contient la fonction de gestion du service, ou SMF (Service Management Function), ainsi que, optionnellement, celle d'accès à la gestion du service, ou SMAF (Service Management Access Function) et celle d'environnement de création de service, ou SCEF (Service Creation Environment Function).
- SCEP (Service Creation Environment Point). Un SCEP permet de définir, de développer et de tester un nouveau service de réseau intelligent. Il peut charger le logiciel correspondant dans le SMP. Le SCEP contient la fonction d'environnement de création de services, ou SCEF. L'unité physique SCEP travaille directement avec l'unité SMP.
- SMAP (Service Management Access Point). L'unité physique SMAP permet à certains utilisateurs d'accéder directement à l'unité physique SMP. Un SMAP peut notamment constituer l'interface unique d'un utilisateur avec plusieurs SMP. Un SMAP contient une fonction d'accès à la gestion du service, ou SMAF. Les SMAP communiquent directement avec les SMP.

Modélisation des fonctionnalités

La mise en place d'un réseau intelligent requiert des outils informatiques avancés, tels que des techniques objet, des bases de données distribuées, des bases de connaissances, des techniques provenant de l'intelligence artificielle, etc. L'intelligence est presque absente des architectures que nous avons rencontrées à la section précédente. C'est là un paradoxe, même si une certaine intelligence primaire se cache dans cette adaptation.

Le temps nécessaire à l'introduction de nouveaux services intelligents a été jusqu'à présent très long et se compte en années. Par exemple, l'introduction du numéro vert ou des cartes téléphoniques a demandé de nombreuses années du fait qu'il fallait implanter de nouvelles commandes dans tous les commutateurs et points de gestion. L'introduction

des SIB et de l'infrastructure des réseaux intelligents va permettre de diviser par 10, voire par 100, ces temps de mise en œuvre.

Les techniques utilisées proviennent des architectures orientées objet, qui offrent une grande souplesse de mise en œuvre et une gestion simplifiée par la suite. Les bases de données distribuées forment également un thème clé pour le stockage des connaissances et des informations.

L'intelligence artificielle est à la base de très nombreux outils qui commencent à être utilisés dans le logiciel du réseau intelligent. En effet, les systèmes qui nous intéressent sont particulièrement complexes, et l'on ne sait plus aujourd'hui gérer cette complexité avec des machines centralisées de type séquentiel. Les corrélations entre événements sont telles que des systèmes à base de règles et de connaissances sont plus aptes à répondre aux problèmes de diagnostic et plus généralement aux demandes des systèmes de gestion. La distribution pousse vers une nouvelle direction : l'intelligence artificielle distribuée.

Par l'introduction du concept d'intelligence artificielle distribuée, on doit pouvoir parvenir à une automatisation de la mise en place de l'infrastructure associée au service. Ce type d'implémentation prend en compte la complexité due à la distribution des fonctionnalités. Des systèmes multiagents cognitifs peuvent aussi être introduits dans le plan fonctionnel global pour permettre de corréler, filtrer, diagnostiquer et prendre des décisions. Ce type d'environnement est présenté au chapitre 4.

ODP (Open Distributed Processing)

Cette section s'intéresse à la modélisation des fonctionnalités nécessaires pour réaliser un réseau distribué. À ce titre, nous examinons ODP et le modèle d'architecture G.805 de l'UIT-T.

L'architecture ODP propose un modèle très général, qui a pour objet de décrire la sémantique et l'architecture des systèmes répartis ouverts. Défini dans les normes ISO et UIT-T X.901, X.902 et X.903, ce modèle se fonde sur deux concepts de base, à savoir une distribution objet et une découpe des systèmes en « points de vue » (*voir plus loin*).

À la fin des années 1980, l'ISO s'est efforcé de dépasser la seule normalisation des protocoles de communication et a essayé d'organiser les protocoles dans un contexte plus vaste, celui d'un système distribué, mis en place dans le cadre d'une entreprise. Le rôle d'ODP est de normaliser les outils de conception et de gestion globale de la distribution des traitements dans l'univers réparti d'une entreprise.

L'ensemble des documents normatifs comprend quatre parties :

- La partie 1, non normative, regroupe les objectifs d'ODP, un aperçu d'ODP, les concepts clés et des éléments de base de l'architecture.
- La partie 2 contient le modèle descriptif. Ce modèle définit les concepts de la modélisation (objets, interfaces, états, interactions, etc.), les concepts de spécification (composition, décomposition, compatibilité, type, classe, etc.) et les concepts architecturaux (organisation, propriétés des objets, nommage, etc.).
- La partie 3 contient le modèle prescriptif. Celui-ci permet de caractériser un système ouvert à l'aide de techniques descriptives aptes à détecter si les contraintes définissant un système ODP sont satisfaites.

- La partie 4 décrit la sémantique architecturale, c'est-à-dire la manière dont les concepts de modélisation et le modèle prescriptif peuvent être représentés par une technique de description formelle.

Cinq points de vue, représentant autant d'approches d'un même problème — un point de vue apporte une description abstraite du système — ont été définis par les normalisateurs :

- Le point de vue Enterprise (entreprise) envisage la place du système distribué dans l'entreprise. Il concerne essentiellement l'utilisation du système distribué et la gestion de l'entreprise.
- Le point de vue Informational (information) concerne les informations manipulées par le système distribué et l'usage que l'on peut en faire.
- Le point de vue Computational (traitement) vise l'organisation fonctionnelle du système. En d'autres termes, il implique la définition des logiciels qui participent aux systèmes distribués.
- Le point de vue Engineering (ingénierie) est relatif à la distribution des ressources du système distribué, c'est-à-dire à la façon de construire le système distribué pour que les traitements puissent se faire dans les meilleures conditions possibles.
- Le point de vue Technology (technologie) concerne les choix d'implantation des composants physiques (matériels, logiciels, systèmes de gestion, protocoles, etc.).

L'architecture ODP s'appuie sur la notion d'objet. Un objet est caractérisé par un identificateur, un état et un comportement. L'accès à un objet s'effectue par des interfaces, qui déterminent les interactions entre l'objet et son environnement.

Dans ODP, on définit également les aspects d'un système. Ces aspects sont identifiés par les problèmes que doit résoudre le système de traitement réparti et existent généralement dans les différents points de vue. Deux catégories ont été définies, qui regroupent, d'une part, les aspects qui nécessitent la répartition (traitement, stockage et accès utilisateur) et, d'autre part, les aspects supportant la distribution (communication, identification, gestion et sécurité).

Des fonctions génériques ont aussi été définies pour la construction des systèmes ODP. Elles sont décrites selon les points de vue et regroupées en quatre classes : gestion, répertoire, sécurité et transparence.

Le modèle de référence ODP (RM-ODP) définit un ensemble de concepts architecturaux pour la construction d'un système ODP. Orientés objet, les systèmes ODP sont définis en terme d'interactions d'un ensemble de composants objets avec les interfaces identifiées. Des templates, ou « patrons », d'objets sont introduits pour décrire les contraintes en fonction desquelles les objets sont instanciés. Les objets résultant des templates sont organisés dans une famille de classes liées par la relation entre sous-classe et superclasse.

Le modèle G.805 et UML

Le modèle G.805 a été élaboré à la fin des années 1990 pour définir les principales fonctionnalités des réseaux. Il a pour rôle de représenter tous les types de réseaux et tous les protocoles associés.

Trois fonctions de base ont été identifiées : les fonctions de connexion, d'adaptation et de terminaison. Les fonctions de connexion concernent l'établissement de connexions entre deux points. Les fonctions d'adaptation correspondent à la mise en forme des données d'un utilisateur en vue de leur émission sur un réseau. Les fonctions de terminaison correspondent au contrôle et à la gestion effectués sur le service de transport du réseau. Outre ces principes fonctionnels, la recommandation G.805 introduit un ensemble de concepts pour modéliser les couches de protocoles, les différents niveaux d'abstraction et les entités de transport.

Les entités du processus de modélisation sont essentiellement les suivantes :

- Les sous-réseaux formés des points qui peuvent être connectés directement. Le mot sous-réseau remplace le mot réseau, trop générique.
- Les connexions de liens, qui représentent les connexions définies une fois pour toutes entre deux points.
- Les connexions de sous-réseaux, qui correspondent à des connexions pouvant être modifiées avec le temps.
- Les liens, qui correspondent à des capacités de transfert entre deux sous-réseaux.
- Les trails, qui correspondent à des connexions de bout en bout.
- Les points de connexion, qui forment les extrémités d'une connexion.
- Les points de terminaison, qui constituent les extrémités d'un trail.

Ces différentes fonctionnalités constituent un modèle complet permettant d'établir des architectures de réseau avec leurs fonctionnalités. Des extensions ont été réalisées à la fin des années 1990 pour que soit pris en compte l'aspect service, qui n'apparaît pas vraiment dans la modélisation de base. Contrairement au modèle ODP, la description n'est pas du tout orientée objet. Des sous-ensembles ont été déterminés pour la description d'architectures spécifiques, comme G.803, qui vise les architectures SDH (Synchronous Digital Hierarchy).

Décrire une architecture fonctionnelle est une chose, mais arriver à utiliser ces concepts simplement en est une autre. Pour cela, il faut unifier les notations. À cet égard, UML (Unified Modeling Language) constitue une réponse possible pour une notation unifiée acceptée par les industriels. Finalisée en 1999 par l'OMG (Object Management Group), la norme UML repose sur des concepts fondés sur un métamodèle, c'est-à-dire un modèle réalisé à partir des modèles de base, bien formalisés. UML s'appuie fortement sur C++ et non sur les nouveaux langages apportant une forte distribution, comme Java. Cependant, les outils UML offrent de nombreux moyens de génération vers les principaux langages de programmation.

TINA (Telecom Information Networking Architecture)

L'initiative TINA est plus large que le concept de réseau intelligent. Elle consiste à développer une plate-forme ouverte pour accueillir tous les types de services.

Le concept de réseau intelligent est né du besoin de développer une architecture globale capable d'appréhender l'ensemble des problèmes posés par la mise en place d'un nouveau service, depuis ceux à traiter par l'utilisateur jusqu'à ceux à traiter par le réseau. Tous les SIB doivent être les mêmes pour tous les opérateurs pour qu'un service puisse être accessible depuis tous les clients de tous les opérateurs. Il faut donc que tous les opérateurs désirant développer un réseau intelligent se mettent d'accord sur les composants divers et variés (service élémentaire, SIB, etc.) nécessaires à sa réalisation. Plusieurs initiatives ont été élaborées par différents types de groupements pour essayer de créer un consortium mondial capable d'imposer une vue uniforme du réseau intelligent.

Finalement, l'initiative qui a réellement lancé le mouvement pour développer un réseau intelligent sur la planète a été prise par des organes de normalisation, et plus particulièrement par l'UIT-T, qui a développé le modèle conceptuel du réseau intelligent INCM (Intelligent Network Conceptual Model), présenté à la première section de cette annexe.

Une cinquantaine d'opérateurs de télécommunications ont regroupé leur force pour donner naissance à l'architecture TINA (Telecommunications Information Networking Architecture). Le groupe TINA-C (TINA Consortium) a défini une architecture très générale, la plus ouverte possible, susceptible de prendre en charge tous les types de services large bande et multimédias, y compris les grands standards du monde des télécommunications, tels ODP (Open Distributed Processing), IN (Intelligent Network), TMN (Telecommunications Management Network) et CORBA (Common Object Request Broker Architecture).

L'architecture TINA est divisée en trois sous-ensembles : une architecture de traitement, une architecture de service et une architecture de gestion. Un service TINA est déterminé par des composants de service, qui sont des unités de logiciel, appelées objets de traitement. L'exécution de ces objets est réalisée par un environnement distribué d'exécution, le DPE (Distributed Processing Environment). Cet environnement s'appuie sur un noyau, le noyau DPE, et des services DPE.

Parmi les exemples de services DPE, citons les services rendus par des intermédiaires, appelés traders, les serveurs de noms, qui permettent d'identifier et de localiser les unités de logiciels nécessaires à l'exécution, les serveurs de sécurité et les serveurs de transactions.

L'architecture de traitement suit le modèle ODP. C'est une architecture orientée objet. Dans TINA, le composant de base, l'objet, est appelé USCM (Usage, Substance, Core, Management), car il est défini par les éléments suivants : un noyau (core), décrivant la nature de l'objet indépendamment de son utilisation et de sa gestion, un usage, décrivant son apparence pour l'utilisateur, une gestion (management), décrivant les opérations de gestion et de maintenance, et une substance, représentant sa dépendance vis-à-vis des autres composants du système.

Un autre principe de l'architecture de traitement est l'indépendance des composants logiciels vis-à-vis des services et de leur environnement distribué ainsi que vis-à-vis de la technologie déployée pour réaliser le système.

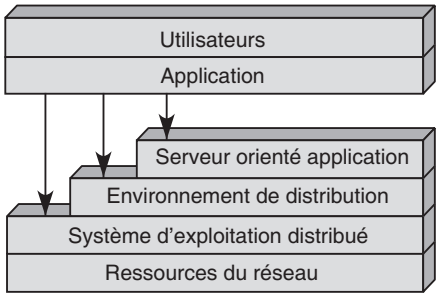
Le modèle d'interaction qui définit comment les composants peuvent interagir est décrit dans le document *TINA Computational Modeling Concepts*. Les interfaces sont spécifiées indépendamment du langage de programmation utilisé (GDMO, OMG IDL, OSF IDL). Pour réaliser les spécifications d'interface de TINA, une extension d'IDL (Interface Definition Language) a été développée sous le nom d'ODL (Object Definition Language).

L'architecture de service décrit le moyen de construire des services de tout type : accès, transport, gestion, information, etc. De nouveau, les services sont décrits indépendamment des moyens qui permettent leur mise en œuvre. L'architecture du réseau intelligent en est la base.

L'architecture de gestion décrit l'ensemble des services de gestion à mettre en œuvre pour administrer le système. L'architecture de base retenue pour la gestion est le TMN.

On peut définir TINA comme une architecture à six niveaux, comme illustré à la figure B.5.

Figure B.5
Architecture TINA

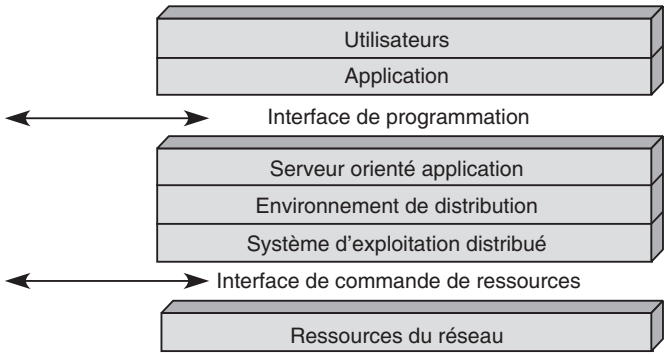


Le niveau le plus haut concerne l'utilisateur et sa vision dans l'entreprise du service qu'il souhaite obtenir. Le deuxième niveau s'intéresse au service lui-même : il en définit les objectifs. Le niveau 3, appelé Serveur orienté application (Application-Oriented Server), fournit un ensemble de ressources conceptuelles capables de répondre à la demande d'un nouveau service. Cette réponse est envisagée de façon centralisée, sans que sa réalisation effective sur un réseau entre en ligne de compte. Le niveau 4, ou Support de l'environnement distribué (Distribution Support Environment), prend le relais de la couche précédente pour réaliser de façon conceptuelle la distribution de la solution proposée par le niveau 3. Le niveau 5 doit établir avec le précédent une adéquation entre la distribution proposée au niveau conceptuel et sa prise en charge par le système d'exploitation distribué et le système d'interconnexion. Enfin, le dernier niveau se préoccupe des ressources physiques du réseau, lesquelles doivent être mises en place pour prendre en charge le nouveau service.

Entre le service et les couches sous-jacentes, les interfaces peuvent être multiples, suivant que le service demandé a déjà fait l'objet d'une réalisation partielle ou globale. Le cas le plus classique et le plus simple consiste à passer directement du service aux ressources distribuées lorsque l'infrastructure est déjà préparée à recevoir le service. À l'extrême inverse, il faut passer par le serveur orienté application lorsque le nouveau service n'est

pas répertorié dans les cas déjà réalisés. Dans cette architecture, les deux interfaces importantes sont celles illustrées à la figure B.6.

Figure B.6
Interfaces du réseau intelligent



L'interface la plus haute, ou interface de programmation, fait transiter la demande d'un nouveau service, c'est-à-dire la description de sa logique et de ses données associées. Les logiques permettront de bâtir, dans le niveau 3, des briques de base répondant aux besoins des services. Ces briques de base, ou SIB (Service-Independent Building), doivent être indépendantes les unes des autres et réutilisables. Il faut en outre que l'interface de programmation mette en place la demande de service et les SIB correspondants. Dans cette interface, on ne s'intéresse pas à la distribution. La correspondance est centralisée, ce qui facilite la relation service-logique de base.

La seconde interface, ou interface de commande de ressources, a pour fonction de mettre en correspondance la solution conceptuelle et sa réalisation au sein d'une architecture réelle distribuée. Cette réalisation s'effectue dans un environnement hétérogène. En d'autres termes, l'interface de commande de ressources doit disposer des ressources nécessaires à la réalisation du nouveau service.

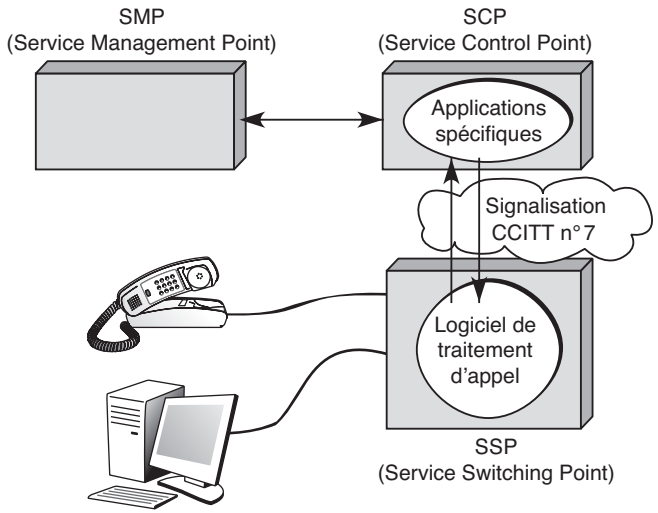
Réalisation d'un réseau intelligent

Plusieurs générations de réseaux intelligents ont été introduites pour tenir compte de la complexité croissante de l'environnement réseau.

La première génération, ou IN/1 (Intelligent Network/1), est assez simple : le client accède au point de commutation, appelé SSP (Service Switching Point), où un logiciel détecte s'il s'agit d'une demande de service dépendant du réseau intelligent. Le SSP prend également en charge le transfert de cette demande vers l'infrastructure du réseau intelligent. Si la réponse est positive, la demande est prise en compte par ce même logiciel, qui s'occupe de l'ouverture du circuit. La mise en place des ressources nécessaires s'effectue par l'intermédiaire du point de contrôle des services, ou SCP (Service Control Point). Celui-ci peut aussi s'adresser à un organe spécialisé, le système d'administration du service.

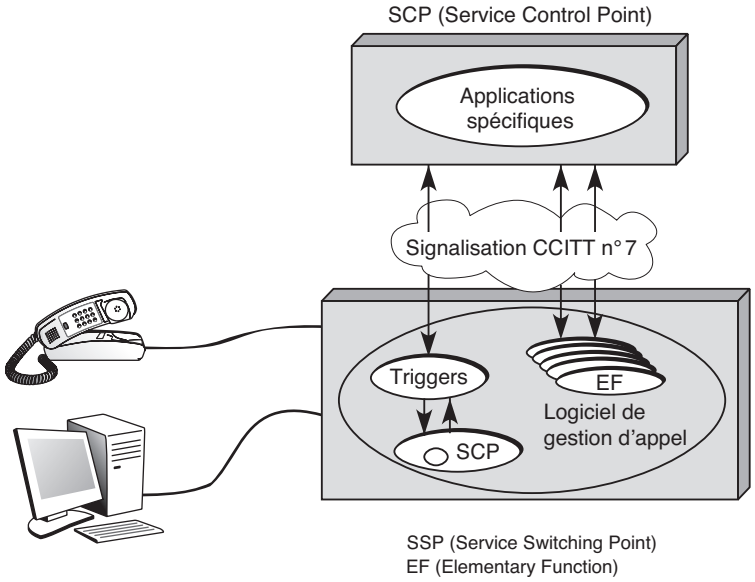
Cette première génération IN/1 est illustrée à la figure B.7.

Figure B.7
Architecture IN/1



Une première amélioration de cette architecture est illustrée à la figure B.8. Dans cette architecture, appelée IN1/+, apparaissent les fonctions élémentaires, ou EF (Elementary Function), qui forment les éléments de base dans les points d'accès au service. Ces éléments doivent être choisis ou adaptés à la prise en compte d'un nouveau service.

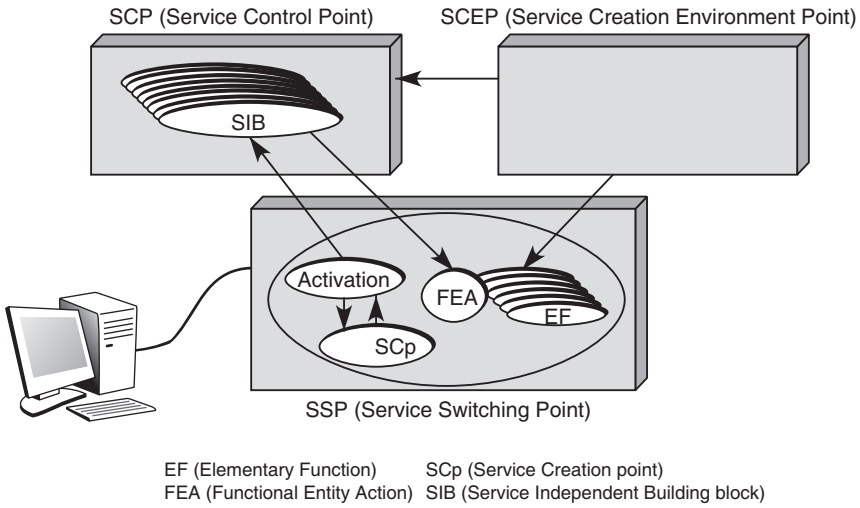
Figure B.8
Architecture IN/1+



Dans cette architecture IN1/+, à partir de la requête utilisateur de demande d'un nouveau service, la fonction trigger demande de l'aide au SCP, soit localement, soit à distance. À l'aide d'applications préspécifiées, le SCP peut renvoyer des ordres de mise en route ou d'adaptation des entités fonctionnelles. Les commandes-réponses entre le point d'accès et le point de contrôle des services s'effectuent par l'intermédiaire du réseau de signalisation. Ce réseau suit la recommandation CCITT n° 7 dans cette génération.

L'architecture IN/2, la plus évoluée aujourd'hui, est illustrée à la figure B.9.

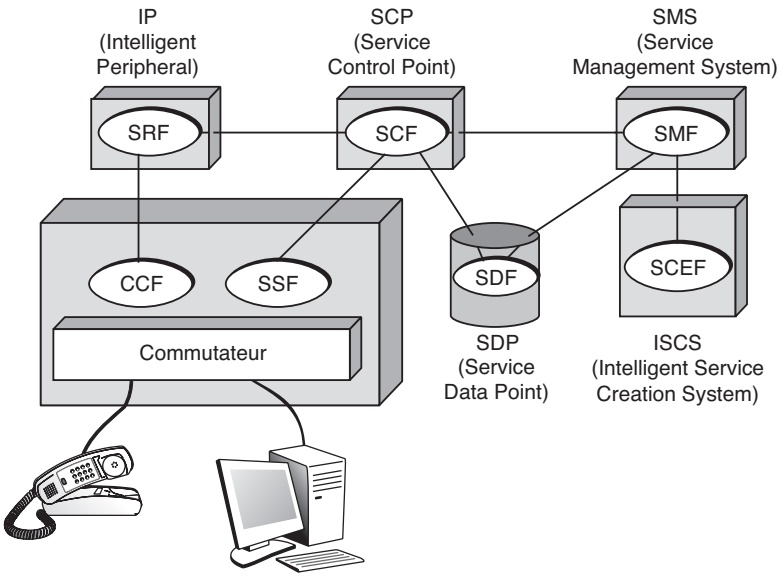
Figure B.9
Architecture IN/2



Cette architecture intègre les modules de base, ou SIB. Ce sont les modules rencontrés dans le plan fonctionnel global de l'architecture des réseaux intelligents. Les fonctions élémentaires EF sont coordonnées par des entités FEA (Functional Entity Action). Les regroupements de fonctions élémentaires permettent de mettre en place l'infrastructure physique pour desservir un nouveau service. Cette définition de l'architecture ressemble fortement à celle de la couche application du modèle de référence OSI, où les ASE (Application Service Element) sont coordonnés par des entités adaptées. Dans cette architecture IN/2, on trouve également un environnement de création de service, activé dès que le service ne peut être rendu par les SIB disponibles. Cet environnement, appelé SCE (Service Creation Environment), crée de nouveaux modules de base SIB et les fonctions élémentaires associées EF.

Les différents éléments de ces architectures peuvent être distribués de façons différentes. À la figure B.10, les différentes fonctions que nous avons rencontrées sont représentées avec les équipements physiques susceptibles de les accueillir. Les fonctions de contrôle de service sont incluses dans le point de contrôle des services (SCP).

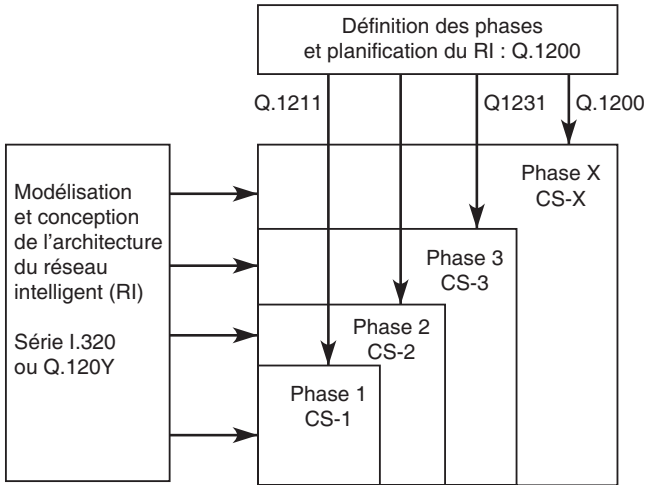
Figure B.10
Architecture matérielle de l'IN/2



Normalisation des réseaux intelligents

Les normes des réseaux intelligents sont parfaitement structurées. Elles se présentent sous la forme illustrée à la figure B.11. La série I.320/Q.120Y concerne la modélisation et les concepts de l'architecture des réseaux intelligents. Les différents niveaux sont référencés par la valeur Y. Plusieurs phases de réseaux intelligents sont prévues : les CS (Capability Set). Pour chaque ensemble, une série de normes sont introduites dans la recommandation Q.1200. Les recommandations Q.12XY concernent le niveau Y de l'ensemble X.

Figure B.11
Normalisation des réseaux intelligents



C

Annexe du chapitre 5 (Le niveau physique)

La première partie de cette annexe fait le point sur les contraintes d'installation du câblage et des systèmes de distribution. En particulier, elle détaille les environnements banalisés.

La deuxième partie de cette annexe présente l'architecture des commutateurs et décrit en détail les commutateurs Crossbar, Banyan, Knock-out, Lambdanet et ShuffleNet. Elle passe ensuite en revue différentes solutions de commutateurs ATM, dont l'objectif est de transférer des trames de longueur constante. Ces architectures sont à la base des commutateurs d'aujourd'hui.

Contraintes d'installation du câblage

Le choix de la distribution du câble est délicat. Les chemins que les câbles empruntent sont des supports généralement métalliques. Cela implique de nombreuses contraintes d'installation, parmi lesquelles la distance entre les équipements, la séparation entre les réseaux courant fort, tel le secteur électrique, et courant faible, comme l'informatique ou le téléphone.

Les chemins de câbles du réseau courant faible doivent être éloignés des sources de perturbation du réseau courant fort et éviter la proximité d'ascenseurs, de tubes fluorescents, de machines à café, etc.

De nombreux procédés existent pour la pose des câbles :

- Les plinthes, très utilisées dans l'environnement domestique pour les fils électriques, offrent une grande souplesse d'utilisation et d'installation des prises.
- Les faux plafonds, disposés à quelques dizaines de centimètres du plafond réel, permettent le passage des câbles et de la ventilation. Les câbles arrivent du faux plafond au poste de travail par des conduits verticaux, appelés potelets.

- Les faux planchers, ou planchers techniques, disposés à quelques dizaines de centimètres du sol, ont la même fonction que les faux plafonds.
- Les cloisons, etc.

Faux plafonds et faux planchers sont aussi appelés plénums. On peut utiliser le câblage sous-moquette avec des câbles plats. Des colonnes montantes sont utilisées pour faire passer les câbles d'un étage à un autre.

Les locaux techniques regroupant les concentrateurs, les passerelles et les autres matériels de transmission informatique peuvent, selon leur encombrement, contenir l'autocommutateur, si les réseaux téléphoniques et informatiques sont encore séparés. S'il y a lieu, ce regroupement doit être contrôlé afin d'éviter toute confusion possible.

Les locaux techniques peuvent être regroupés avec ceux destinés à recevoir les équipements de brassage et les sous-répartiteurs. La disposition de ces locaux doit être bien choisie. Ils doivent être faciles d'accès et suffisamment spacieux pour rendre aisée l'installation et la maintenance des liaisons et des équipements. Il faut y prévoir des dispositifs pour la climatisation, la ventilation, la sécurité et l'alimentation électrique de façon autonome et fiabilisée ainsi que la mise en place d'un téléphone de service. Leur emplacement doit également être judicieusement choisi, en fonction de la disposition des lieux à desservir.

Même si les locaux techniques peuvent être regroupés, il faut prévoir, pour des raisons de sécurité, des gaines différentes pour les réseaux courant faible et courant fort. Les chemins de câbles doivent aussi être protégés contre l'eau et le feu. Dans un souci de maintenance et d'évolution, un système d'étiquetage doit permettre une reconnaissance aisée des différents câbles.

Le câblage banalisé, ou structuré

Les problèmes de conception, de mise en œuvre et d'exploitation n'étant pas identiques suivant la taille des installations, on peut distinguer plusieurs types d'installations :

- **Grande entreprise.** Caractérisée par plusieurs centaines de postes de travail, des réseaux multiples et complexes et une structuration en zones desservies chacune par un sous-répartiteur.
- **Entreprise moyenne.** Comporte au maximum une centaine de postes de travail connectés à un répartiteur unique.
- **SOHO et résidentiel.** Marché globalement considérable mais diffus.

Les règles, normes de transmission, types de terminaux, ainsi que les composants de câblage, par exemple les prises RJ-45, les câbles en paires torsadées ou le brassage des équipements actifs, sont quasiment identiques pour les trois types d'installations. Les différences considérables entre elles viennent des systèmes de distribution, qui sont illustrés plus loin dans cette section.

Si le câblage des sites d'entreprise est désormais entré dans une phase de banalisation du fait de l'application des normes indiquées à la section suivante, celui des locaux d'habitation et des petits bureaux, ou SOHO, est encore relativement nouveau. Sa normalisation n'a été finalisée qu'en 2003 par le guide UTE C 90 483 et la nouvelle norme NF C 15-100. Il s'agit d'un marché considérable, deux fois plus important que celui des entreprises. En revanche, il est techniquement plus difficile, en raison de l'obligation de transmettre la TV en grade 3 sur des paires torsadées sur une bande de fréquences allant jusqu'à 862 MHz.

Ce nouveau marché est généré par l'avènement des réseaux haut débit et multimédias chez les usagers, et en particulier de l'ADSL, qui permet de distribuer simultanément le téléphone, l'accès Internet et les chaînes TV. Le problème reste de distribuer tous ces services là où ils sont utilisés, au salon, dans les chambres ou au bureau, voire d'y associer d'autres services, comme la hi-fi, la télésurveillance, les automatismes du logement, etc.

La normalisation

Avant l'avènement et la généralisation des normes ISO 11801, EN 50173, EIA/TIA 2002, IEEE 802.3, IEEE 802.11, etc., le marché était occupé par une multitude d'offres de câblage propriétaires. Les matériels d'un constructeur informatique ne pouvaient être supportés ou simplement garantis qu'avec le système de câblage de ce même constructeur. On trouvait donc une trentaine de câbles en paires torsadées, d'impédances 100, 110, 120 ou 150 Ω, à une, deux, quatre ou six paires, sans compter les câbles coaxiaux 50 Ω différents des câbles CATV 75 Ω.

L'époque des câblages exotiques est désormais révolue. Le câblage généré par les normes est devenu universel et international. Il permet d'interconnecter :

- tous les réseaux du marché ;
- tous les équipements actifs ou terminaux, en toute topologie (point-à-point, étoile, bus, arbre, etc.) ;
- tous les débits de transmission selon des modèles normalisés.

Fonctionnement du câblage banalisé

Le câblage banalisé consiste à disposer, partout où elles sont potentiellement utilisables, des prises RJ-45 (ISO 8877), elles-mêmes interconnectées à des répartiteurs ou sous-répartiteurs intégrant les équipements actifs de réseau, comme illustré aux figures C.1 et C.2.

Figure C.1

Bandeau de prises RJ-45, montable en rack 19 pouces, permettant la connexion des postes de travail

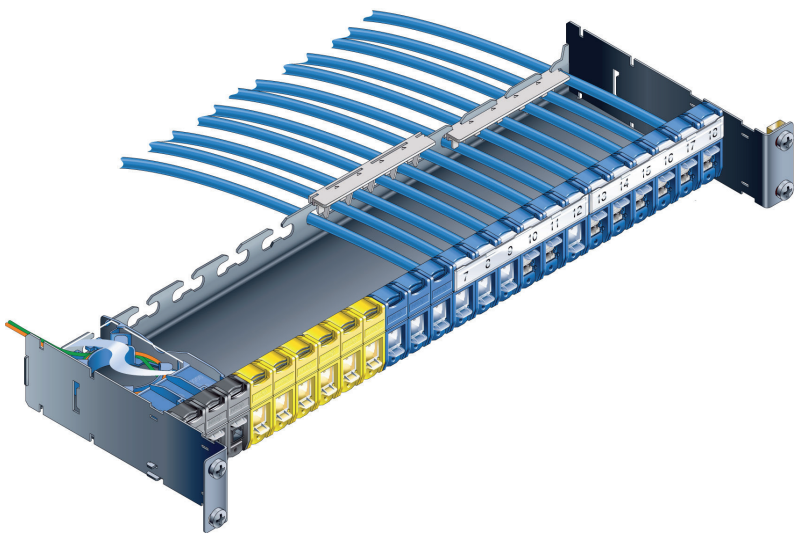


Figure C.2

Cordon de brassage RJ-45 interconnectant les équipements

Ce câblage est réalisé une fois pour toutes et devient une partie structurelle du bâtiment. Il permet de supporter tous les réseaux, tous les logiciels, tous les terminaux, sans qu'il soit nécessaire de repasser un seul câble.

Les liaisons quatre paires horizontales

Les liaisons quatre paires horizontales, aussi appelées capillaires, constituent l'essentiel du câblage banalisé puisqu'elles interconnectent tous les terminaux aux équipements de réseau actifs (*voir figure C.3*). Toutes les prises RJ-45 sont câblées de manière identique et répétitive aux deux extrémités du câble quatre paires, au niveau à la fois des postes de travail et des sous-répartiteurs. Une convention de raccordement immuable — 568 B est la plus courante — permet d'attribuer chaque fil du câble quatre paires à une borne définie des connecteurs RJ-45, comme l'illustre la figure C.4.

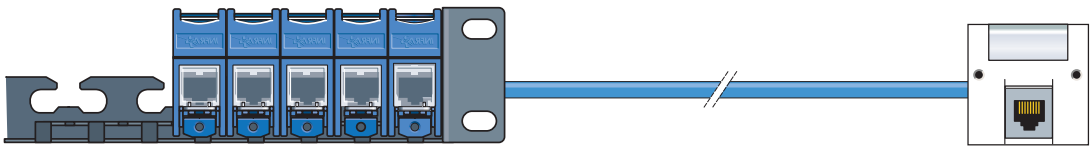
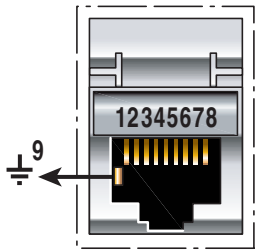


Figure C.3

Constitution d'une liaison quatre paires

Figure C.4

Vue en face avant d'un connecteur RJ-45 avec repérage de ses bornes



Le tableau C.1 donne la correspondance entre les paires et les bornes des connecteurs RJ-45 associés.

Tableau C.1 • Correspondance entre paires et bornes des connecteurs RJ-45

Nombre de bornes RJ-45 aux sous-repartiteurs	Couleur des fils des quatre paires	Nombre de bornes RJ-45 aux postes de travail
4 5	*Paire 1* Bleu Bleu/blanc	4 5
1 2	*Paire 2* Blanc/orange Orange	1 2
3 6	*Paire 3* Blanc/vert Vert	3 6
7 8	*Paire 4* Blanc/marron Marron	7 8

Critères de qualification des liaisons horizontales

Les normes laissent le choix entre plusieurs types de composants, qui diffèrent par leurs performances de transmission et leur immunité à l'environnement électromagnétique. Le tableau C.2 récapitule les performances et domaines d'application des principaux composants des liaisons horizontales.

Tableau C.2 • Performances des principaux composants des liaisons horizontales

Composant	Performance de transmission	Domaine d'application
Lien classe D Composant catégorie 5	100 MHz	- Téléphonie - LAN Ethernet 10BaseT
Lien classe E Composant catégorie 6	250 MHz	- Téléphonie - LAN Ethernet 100BaseT et 1000BaseT
UTP (Unshielded Twisted Pair), câble non blindé	Immunité moyenne aux perturbations électromagnétiques	- Environnement peu pollué, bâtiment incorporant des structures métalliques - Séparation courant fort-courant faible obligatoire (risque de foudre) - Pas de TV (5-862 MHz)
FTP (Foiled Twisted Pair), avec écran blindant l'ensemble du câble	Immunité forte aux perturbations électromagnétiques	- Environnement pollué, bâtiment incorporant des structures métalliques - Séparation courant fort-courant faible facultative

Il existe d'autres types de câbles, comme les câbles de catégories 7 et 8 ou les câbles SFTP (Shielded Foiled Twisted Pair), mais ils sont très marginaux.

Sans entrer dans le détail de la technologie des câbles, il est possible de se protéger des perturbations électromagnétiques de deux manières :

- En torsadant les paires de câbles UTP et FTP. En ce cas, à chaque demi-spire, le champ induit s'inverse et s'annule. C'est pour cette raison que l'on recommande d'éviter de détorsader les paires.
- En blindant les câbles et les connecteurs. Un écran mis à la terre est une protection peu coûteuse et très efficace.

Pour mémoire, les câbles SFTP comportent, comme les FTP, un écran général, voire une tresse, mais les paires sont écrantées individuellement. L'intérêt de ce câble réside surtout dans le blindage entre les paires, et non dans la protection électromagnétique par rapport à l'environnement. C'est là une des deux manières efficaces d'éviter que les paires ne se perturbent entre elles (diaphonie), l'autre étant, sur les UTP et les FTP, de fabriquer des paires à des pas de torsades différents.

Il est recommandé de choisir les câbles en paires torsadées les plus optimisés suivants :

- **Entreprise.** Catégorie 5 ou 6 FTP, écranté globalement.
- **Résidentiel.** Grade 3 SFTP, écranté globalement mais aussi paire par paire. La paire dédiée à la TV doit impérativement être écrantée.

Les rocades

Les rocades servent à interconnecter les sous-répartiteurs, ou SR, desservant chacun une zone du bâtiment, généralement un étage, avec un maximum de 200 prises RJ-45. Elles ne concernent que les grandes installations et sont généralement dédiées aux applications qu'elles supportent, telles que LAN, téléphonie, gestion technique du bâtiment, etc.

La figure C.5 illustre l'organisation d'une installation avec deux sous-répartiteurs. Une installation de 2 000 prises comporte au moins une dizaine de sous-répartiteurs. Sur la figure, des liaisons horizontales raccordent les terminaux des utilisateurs, et les équipements actifs sont de simples hubs.

On distingue plusieurs types de rocades en fonction des applications qui y circulent :

- **Rocade téléphonique.** Étoile de câbles multipaires reliant tous les SR à un répartiteur général téléphonique, ou RG, lui-même raccordé directement à l'autocommutateur téléphonique. Cette organisation peut être différente pour les très grands sites, dans lesquels des autocommutateurs avec satellite peuvent être répartis sur plusieurs bâtiments, ou pour la téléphonie sur IP.
- **Rocade informatique.** Leur rôle est d'interconnecter le réseau d'entreprise. Elles peuvent être constituées par de simples câbles quatre paires raccordés suivant les mêmes conventions que le câblage horizontal.

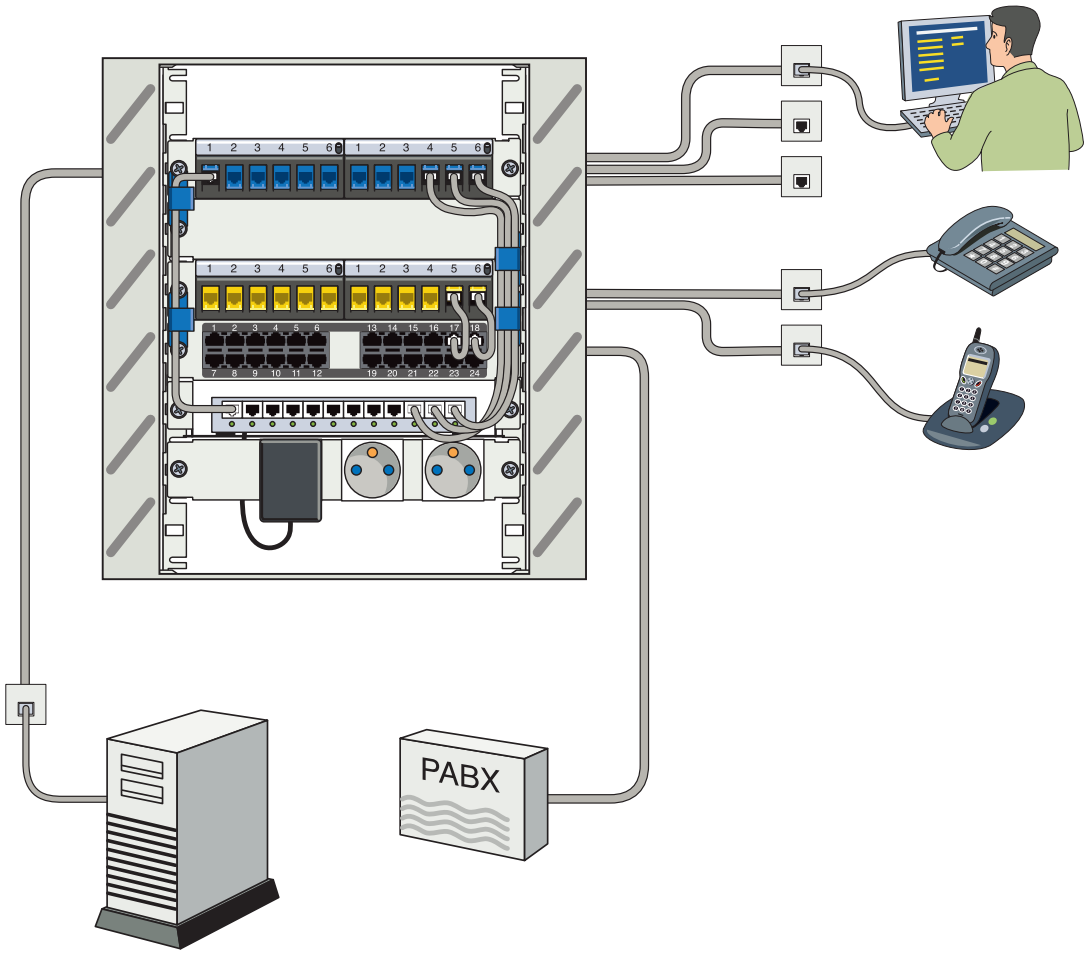


Figure C.5

Exemple d'organisation de deux sous-répartiteurs

- **Rocade optique.** Utilisées pour la connexion entre les bâtiments pour compenser la non-équipotentialité de leurs terres respectives, principalement pour les liaisons informatiques.
- **Rocade TV.** Constituées par un simple câble coaxial 75 Ω partant de la tête de réseau TV ou des sources audiovisuelles et aboutissant à chaque sous-répartiteur sur un distributeur actif TV. Il s'agit d'une sorte de hub destiné à transformer le signal coaxial entrant en signaux transportables sur les paires torsadées et brassables vers toutes les prises RJ-45. On peut donc, à partir des distributeurs TV, amener le signal TV analogique ou numérique sur toutes les prises RJ-45 de n'importe quel poste de travail, sans avoir besoin d'ajouter de câble CATV.

Raccordement des terminaux et des réseaux

Les normes et les usages déterminent sur quelles bornes du RJ-45 doivent se connecter les principaux équipements et réseaux du marché. Ces bornes sont récapitulées au tableau C.3.

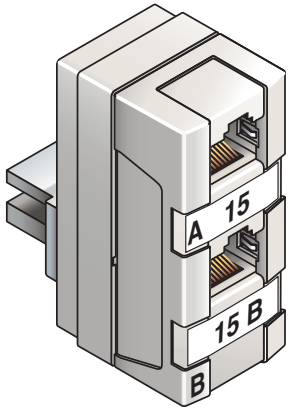
Tableau C.3 • Bornes de raccordement des équipements et réseaux

Équipement et réseau	Borne
Téléphonie une paire Téléphonie quatre paires	4-5 4-5 et 7-8
Ethernet 10 ou 100BaseT, micro-informatique, ADSL	1-2/3-6
Réseau fédérateur (backbone) 1000BaseT	Toutes les paires
TV/audiovisuel (5-862 MHz)	7-8
Terminaux écrans, hi-fi, enceintes actives, caméras, bus de terrain, etc.	Non défini

Il est possible de faire passer plusieurs réseaux sur des paires distinctes, par exemple le téléphone sur la paire 5-5 et Ethernet sur les paires 1-2 et 3-6. Dans ce cas, on utilise des duplicateurs à chaque extrémité de la liaison, comme illustré à la figure C.6.

Figure C.6

Exemple de duplicateur RJ-45



Les systèmes de distribution

Les systèmes de distribution déterminent les qualités organisationnelles des câblages banalisés. Ils reçoivent, outre les extrémités des câblages horizontaux et des rocades, les équipements actifs de réseau, tels que modems, hubs, routeurs, répéteurs, etc.

Les exemples suivants montrent les différences entre les systèmes de distribution spécifiques des trois types d'installations mentionnés précédemment :

- **Grande entreprise.** Comprend plusieurs centaines ou milliers de prises RJ-45, de nombreuses rocades et des équipements actifs divers (*voir figure C.7*).

Figure C.7

Armoire 19 pouces 42 U (Infra+)

- **Entreprise moyenne.** Comprend au maximum 200 prises RJ-45, aucune rocade, peu d'équipements actifs au format 19 pouces, voire aucun dans le cas d'une connexion à un ordinateur central de type AS400 (*voir figure C.8*).

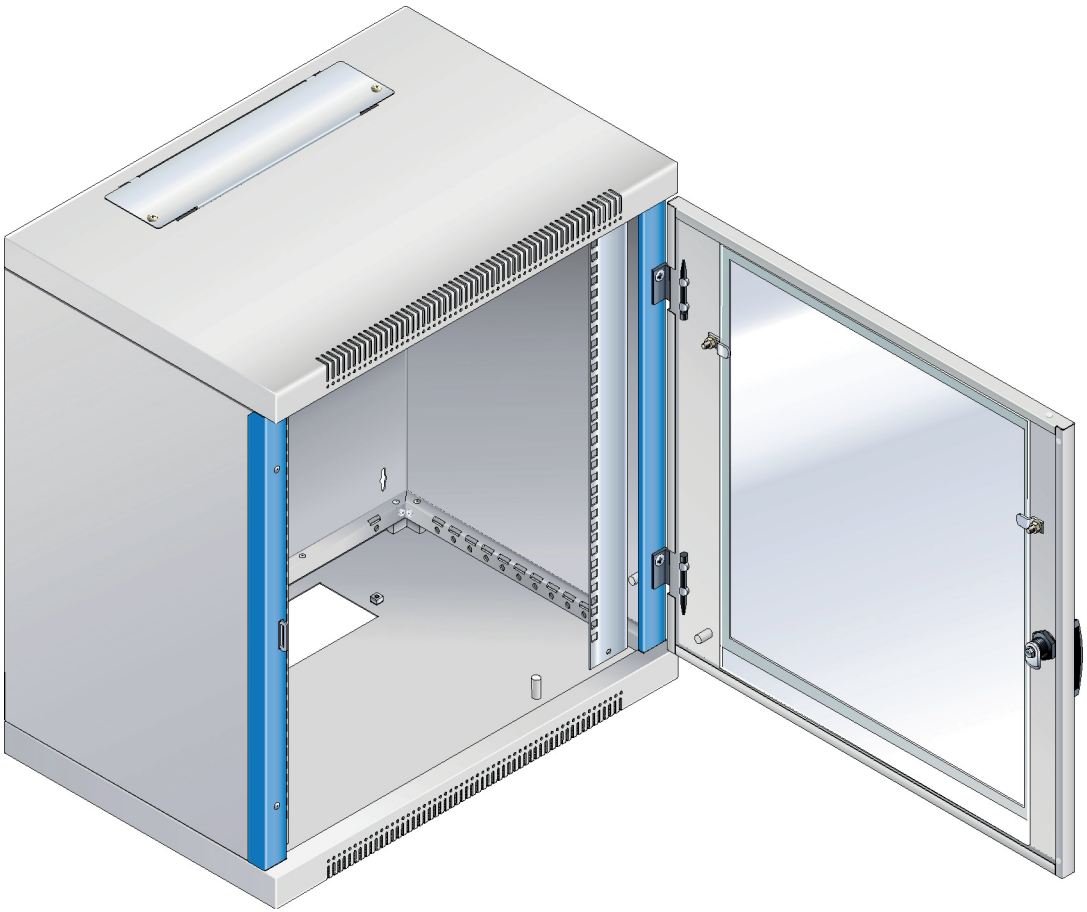


Figure C.8

Répartiteur pour petit site de 8 à 42 U (Infra+)

- **SOHO et résidentiel.** Comprend environ 8 à 24 prises RJ-45. Les équipements actifs sont de petit format (*voir figures C.9 et C.10*).

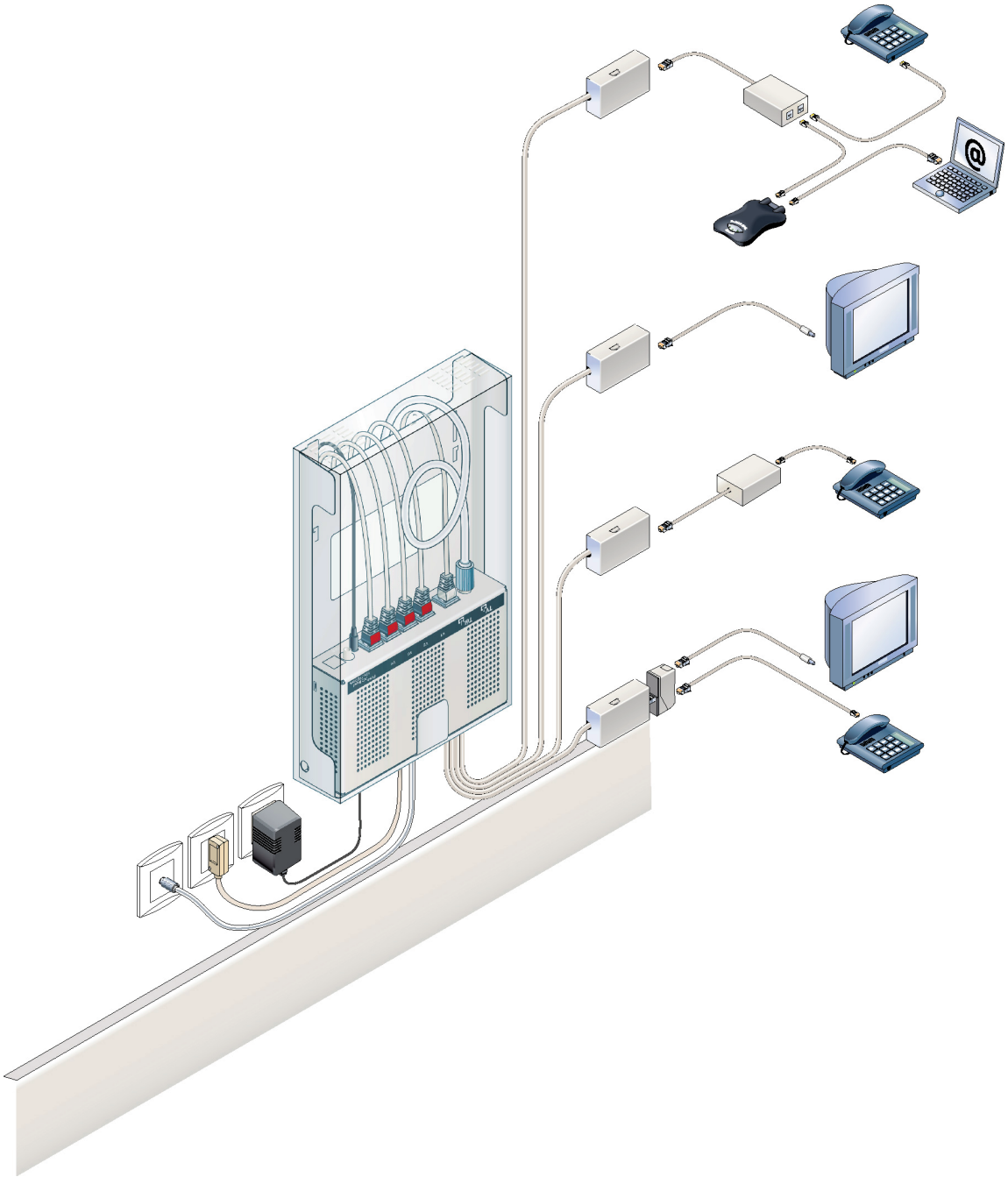


Figure C.9

Kit résidentiel SOLO (Casanova-sas) distribuant deux lignes téléphoniques, la TV et l'ADSL sur 8 prises RJ-45

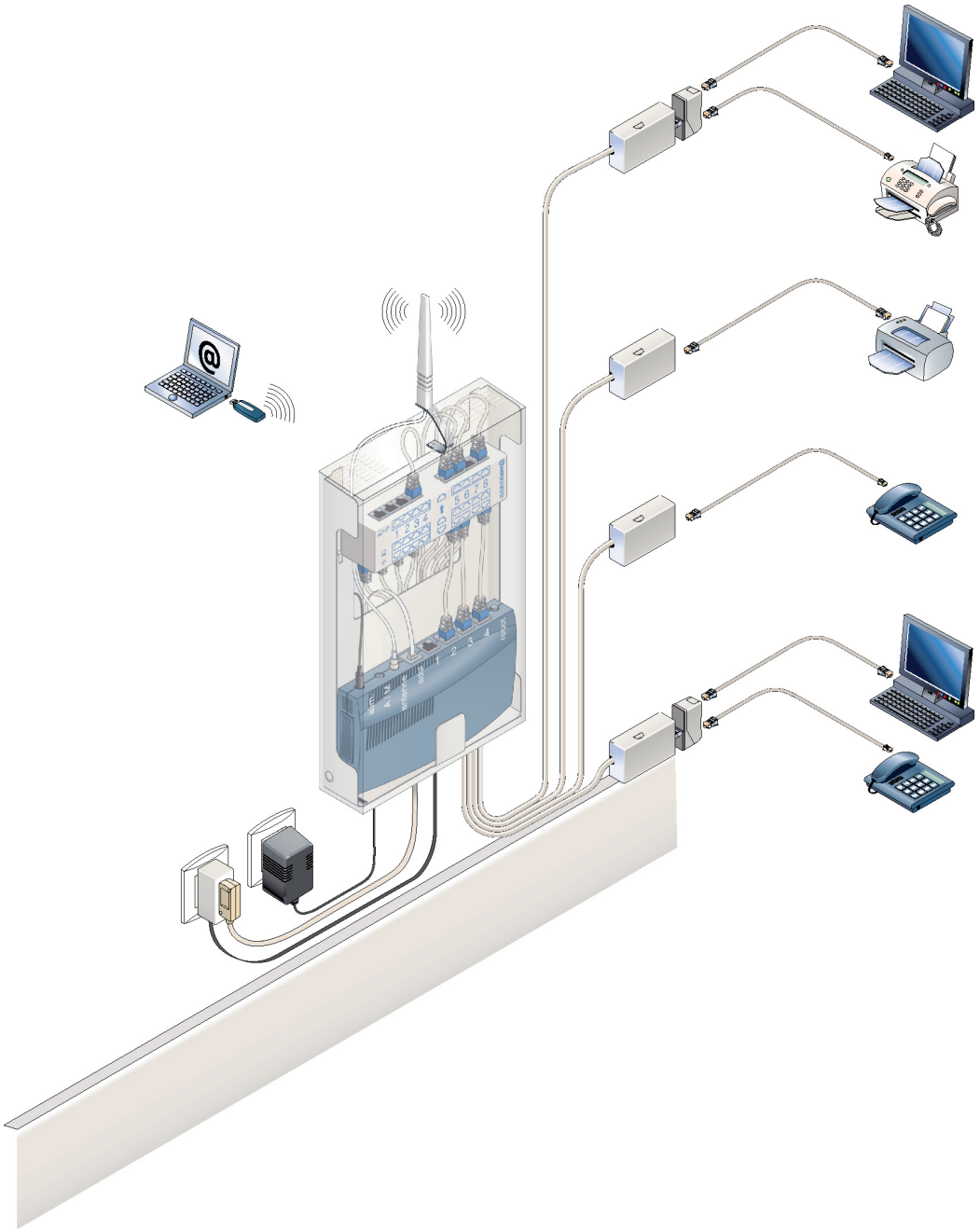


Figure C.10

Kit de bureau MINI OFFICE (Casanova-sas) distribuant deux lignes téléphoniques ou un micro-commutateur téléphonique, un réseau local 10-100BaseT, huit prises RJ-45, plus une option Wi-Fi

Recommandations pour réussir un câblage banalisé

Quelques règles sont nécessaires pour réussir un câblage banalisé, ou VDI (voix, données, images). Elles résultent de l'application des usages, du bon sens et des normes.

Les normes qui régissent le câblage actuel sont les suivantes :

- NF C15 -100 (électrique) ;
- NF C15 – 900 (cohabitation des réseaux) ;
- EN 50 173 ou ISO 11801 (câblage structuré) ;
- EN 90125 (TV/audiovisuel).

Dimensionnement

- Prévoir 30 à 50 % de prises en plus du besoin. Les prises en attente favoriseront la flexibilité des postes de travail.
- Densité des postes de travail : environ 1 pour 10 m^2.
- Poste de travail type : 2 prises RJ-45 et 3 à 4 prises 230 V.
- Nombre de prises RJ-45 par répartiteur : 200 au maximum. Au-delà, l'infrastructure devient ingérable (cordons de brassages trop longs et trop nombreux).
- Longueur du câblage horizontal : 90 m maximum (modèle de la norme). La longueur moyenne pour un câblage bien conçu doit être inférieure à 30 m. Mieux vaut prévoir 2 SR de 100 prises qu'un seul de 200 prises centralisé. Il en résulte un gain de main-d'œuvre et de câble de 35 % et un gain de performance de 50 %

CEM (compatibilité électromagnétique)

- Séparation courant fort/faible : obligatoire en UTP (30 cm entre les chemins de câbles, 5 cm pour les plinthes et chemins de câbles impérativement métalliques) et facultative en FTP pour des cheminements parallèles inférieurs à 5 m.
- Mise à la terre équipotentielle des SR, RG par tresse ou feuillard de section inférieure à 25 mm^2. Entre bâtiments ayant des terres différentes, la fibre optique est recommandée.

L'environnement électromagnétique est difficilement contrôlable. Il peut de plus se dégrader dans le temps du fait d'équipements radio de plus en plus nombreux, de matériels électriques défectueux, etc. Il est judicieux de privilégier les câbles FTP et les prises RJ-45 blindées.

Gestion

Il est important d'aérer les répartiteurs en intercalant des bandeaux passe-câbles entre les bandeaux de connexion ou actifs.

Au-delà de 200 postes de travail, il est nécessaire d'utiliser un système de gestion informatisé courant fort/faible. Un tel système permet la mémorisation des liaisons, des équipements actifs de réseau, des meilleurs cheminements et des disponibilités et fournit des statistiques, ainsi qu'une validation sous SNMP.

Le logiciel BMC de la société ARC offre, par exemple, les fonctionnalités suivantes :

- intégration directe des informations des testeurs dans la base de données du site ;
- ingénierie des réseaux (vision fédératrice des systèmes de communication) ;
- inventaire des liaisons, des réseaux et des équipements actifs raccordés ;
- gestion du câblage et des équipements actifs sous SNMP (bons de travaux, meilleur cheminement, etc.).

Contrôle et test du câblage

Le contrôle et le test sont indispensables car le câblage, une fois validé, ne doit jamais être suspecté en cas de dysfonctionnement éventuel de l'installation. Le contrôle dynamique n'est pas indispensable pour le résidentiel.

Contrôle électrique

Le contrôle électrique est réalisé systématiquement par l'installateur au moyen d'un testeur économique afin de vérifier que le câblage des paires sur les connecteurs est effectué correctement et que la continuité de la terre est assurée. Il s'effectue sur les RJ-45 depuis les SR. Des bouchons sont introduits à l'autre extrémité des câbles pour boucler les paires.

Un autre test permet de vérifier qu'il n'y a pas de court-circuit entre les paires et la terre (les bouchons doivent alors être retirés).

Test dynamique

Un test dynamique simule le fonctionnement des réseaux informatiques normalisés et mesure les paramètres fondamentaux de transmission, en fonction de la classe de câblage choisie :

- Classe E 250 MHz : composants catégorie 6 ;
- Classe D 100 MHz : composants catégorie 5.

Les testeurs de chantier sont des appareils sophistiqués, dont l'usage nécessite une formation spécifique. Ils permettent d'interpréter les résultats de test en fonction des valeurs mesurées suivantes :

- **Affaiblissement ou atténuation.** Cette valeur dépend de la longueur et de la qualité du câble. Elle doit être la plus faible possible.
- **Next.** Mesure la perturbation provoquée par le couplage d'une paire sur une autre. Cette valeur doit être la plus élevée possible.
- **ACR.** Résulte du calcul Next moins Atténuation. Cette valeur doit être la plus élevée possible.
- **Return Loss, ou affaiblissement de réflexion.** C'est la différence entre la puissance du signal émis et celle du signal réfléchi en raison des variations d'impédance du lien (connecteurs, mauvaise connexion, câble endommagé, etc.). Cette valeur doit être la plus élevée possible.

Le câblage

Le câblage des bureaux et des entreprises nécessite des sommes souvent importantes. Lors de l'évaluation de ce coût, il faut prendre en compte non seulement le support mais aussi les équipements situés aux deux extrémités du câble. Il faut en outre évaluer les besoins afin de sélectionner et d'installer le bon câble une fois pour toutes.

Divers paramètres interviennent quant au choix des composants d'un système de câblage, tels le coût, l'environnement, les contraintes particulières des utilisateurs, la fiabilité, l'évolutivité, etc. Il est impératif de caractériser dès le départ l'environnement dans lequel est déployé le réseau. Certains environnements industriels sont critiques et nécessitent des supports spécifiques. Un environnement bruyant, par exemple, peut requérir l'emploi de la fibre optique. Le réseau peut aussi être exposé à des perturbations électromagnétiques ou climatiques. La sécurité des informations est un autre élément à prendre en compte.

La population d'utilisateurs escomptée détermine le nombre de prises nécessaires pour dimensionner le système. Il faut en outre envisager les types de trafics destinés à être supportés et en évaluer le volume — il peut être important dans le cas de transport d'images numérisées, par exemple — afin d'avoir une idée précise du niveau de fiabilité des transmissions requis, le transfert de données étant très sensible aux erreurs de transmission, contrairement au transfert de voix numérisées.

La topologie du bâtiment est une autre contrainte à prendre en compte. Certains supports sont beaucoup plus maniables que d'autres — le rayon de courbure d'une fibre optique est inférieur à celui d'un câble coaxial, par exemple —, et l'utilisation d'une fibre optique ou d'une paire métallique souple peut être nécessaire dans des bâtiments où le chemin de câblage est quelque peu tortueux.

Les infrastructures de câblage se répartissent entre réseau courant faible pour le transport de l'information (téléphonie, informatique, multimédia) et réseau courant fort pour l'alimentation électrique. Le transport de l'information requiert une puissance très inférieure, de l'ordre du milliwatt, à celle nécessaire au fonctionnement des appareils électriques, qui est de l'ordre de dizaines ou de centaines de watts.

Pour l'implantation d'un réseau de distribution courant faible, il faut décider du chemin des câbles et de la technologie à utiliser de la façon la plus générique possible, indépendamment des types d'information, de matériel et d'utilisateur auxquels le réseau est destiné.

Le plan de câblage d'une entreprise est capital pour la bonne marche des réseaux que l'on souhaite y implanter. Les sections suivantes présentent les différents plans de câblage disponibles.

Le câblage départemental

Les réseaux départementaux, que l'on appelle aussi réseaux SOHO (Small Office/Home Office), ont une taille maximale de l'ordre de la centaine de mètres.

Le rôle du câblage départemental, ou capillaire, est de distribuer les informations vers l'ensemble des bureaux dans un environnement limité. Ces réseaux capillaires sont formés par le câblage sortant du répartiteur d'étage.

La normalisation du câblage départemental a choisi comme support physique quatre paires de fils torsadées distribuées en étoile depuis un local technique central. Cette topologie est illustrée à la figure C.11.

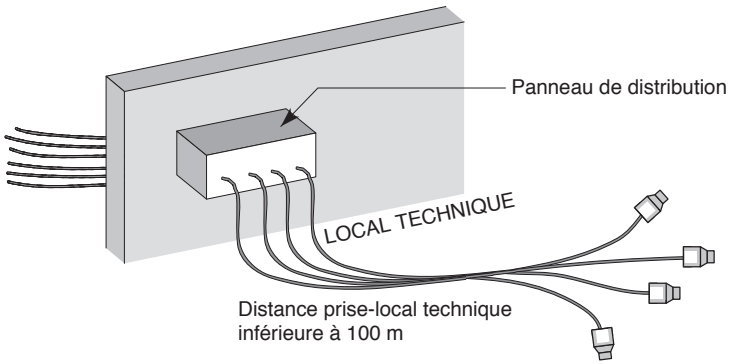


Figure C.11

Topologie du câblage départemental

La structure en étoile permet de desservir très facilement l'ensemble des pièces du département. On compte généralement une prise pour 6 m^2. Lors du précâblage d'un immeuble neuf, il faut câbler l'ensemble de la surface avec un nombre de prises suffisant pour ne pas avoir à tirer de nouveaux fils ultérieurement. En effet, lorsqu'on câble un immeuble, le coût à la prise est très bas, comparé au même câblage dans un immeuble ancien, où des travaux d'infrastructure sont nécessaires. Si le coût de la prise d'un précâblage dans un bâtiment neuf est de 75 à 150 euros en moyenne, il faut multiplier ces chiffres par dix pour un immeuble ancien sans infrastructure de câblage.

De plus en plus, les nouveaux bâtiments sont précâblés selon une structure identique à celle des câblages du réseau téléphonique à partir du répartiteur d'étage. Quelques différences doivent toutefois être signalées :

- Le câblage peut être banalisé : on utilise dans ce cas le câble pour y raccorder indifféremment un téléphone ou un équipement informatique.
- Le câblage peut être non banalisé : on raccorde les terminaux téléphoniques sur un câble de faible diamètre et les équipements informatiques sur un câble de meilleure qualité.
- Les câbles peuvent permettre de réaliser divers types de réseaux locaux capillaires. La qualité du câble est importante en cas de contrainte de distance. Pour les réseaux à 100 Mbit/s et à 1 Gbit/s, le câble doit être d'excellente qualité pour atteindre la centaine de mètres. Le mieux est de limiter la distance entre le local technique et la périphérie à 50 m et d'utiliser un câble métallique de bonne qualité.

Dans le câblage banalisé, aussi appelé structuré ou universel, la banalisation doit être totale, et la prise du terminal unique. Le choix penche généralement en faveur de la prise

normalisée ISO 8877, qui peut se décliner de différentes façons dans chaque pays. La norme de câblage française avec une prise RJ-45 universelle est NF C 15-100 (guide UTE C 90-483). Elle est également applicable au câblage résidentiel.

Tous les câbles arrivent sur un même répartiteur, et ce sont des cordons de connexion, ou jarretières, qui sont utilisés pour connecter, dans le local technique, l'arrivée du câble banalisé aux prises donnant accès au réseau téléphonique ou informatique. Les câbles utilisés sont identiques. En règle générale, on utilise quatre paires de fils torsadées pour être compatible avec la prise RJ-45, qui possède 8 broches, 4 pour les données et 4 pour la téléalimentation.

La non-banalisation permet de poser des câbles de qualités différentes entre l'informatique et la téléphonie. Par exemple, on peut utiliser deux paires de fils torsadées blindées de très bonne qualité pour la partie informatique et quatre paires de fils torsadées non blindées pour la partie téléphonique. Du fait de cette différence entre les deux câblages, les arrivées au répartiteur d'étage sont différentes : la partie informatique arrive sur un tableau de distribution informatique et la partie téléphonique sur un tableau de distribution téléphonique.

Rien n'empêche un utilisateur de demander la pose d'un câble spécifique de meilleure qualité que celui proposé par le constructeur, de façon à éviter tout problème d'adaptation à l'environnement. Une autre solution pour prendre en compte les caractéristiques de tous les types de réseaux locaux consiste à réduire la distance maximale entre le terminal et le tableau de distribution. Cette distance doit être suffisamment courte pour supporter les débits les plus importants des produits disponibles sur le marché.

Nous venons de voir que la topologie normalisée était de type étoile. Cependant, cette topologie en étoile n'est pas toujours adaptée à l'entreprise. D'autres topologies sont possibles, comme le bus ou la boucle.

La topologie en étoile

La topologie en étoile est évidemment parfaitement adaptée à la distribution des réseaux en étoile. Les câblages des autocommutateurs privés, ou PABX, sont conformes à cette topologie. Une difficulté peut toutefois surgir de l'inadéquation des câbles aux débits proposés par les autocommutateurs. Le système de câblage peut dater de nombreuses années et n'avoir été conçu que pour faire transiter un signal analogique à 3 200 Hz de bande passante, par exemple. L'inconvénient de cette topologie en étoile est la centralisation : si le centre est défaillant, tout le système risque de s'arrêter.

La topologie en bus

Largement répandue dans les réseaux locaux Ethernet, la topologie en bus présente de nombreux avantages, en particulier celui de pouvoir être passive, c'est-à-dire sans alimentation électrique. Les câbles associés peuvent être de différents types : paires de fils métalliques ou câble coaxial 50 ou 75 Ω. La fibre optique est mal adaptée à cette structure.

Les tronçons de câble, ou brins, peuvent être raccordés entre eux par des répéteurs. Un répéteur est un organe non intelligent, qui répète automatiquement vers un deuxième câble tous les signaux passant sur un brin, comme illustré à la figure C.12.

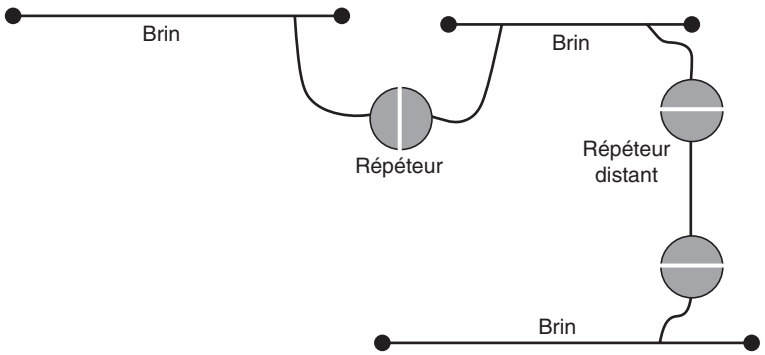


Figure C.12

Raccordement de brins par des répéteurs

Des répéteurs distants peuvent être reliés entre eux par un autre support de communication, comme la fibre optique.

La topologie en anneau

Sur une topologie en anneau, les coupleurs qui gèrent l'accès au support physique arrêtent l'information, c'est-à-dire mémorisent pendant un certain temps les informations passant sur la boucle. Plusieurs décisions doivent être prises, telles que déterminer si la trame doit être recopiée vers la prochaine station ou détruite dans le registre, si la valeur du jeton doit être modifiée ou non, si la trame doit être recopiée vers le coupleur, etc. Il faut donc couper le support physique et ajouter un registre à décalage, comme illustré à la figure C.13. Le registre à décalage mémorise les éléments binaires au fur et à mesure de leur arrivée. À la fin du décalage, ils sont émis sur la boucle en direction de la prochaine station. Le temps de réflexion pour prendre les décisions utiles est égal au temps des décalages et dépend donc du nombre de registres.

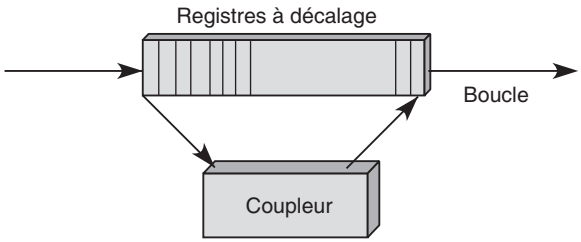


Figure C.13

Registre à décalage du jeton sur boucle

Le coupleur prend une copie de la trame dans le premier registre. Le nombre de décalages correspond au temps de réflexion du coupleur pour modifier une information ou

en introduire une nouvelle. L'incorporation de nouveaux bits ou l'effacement de certains s'effectue sur le dernier bit du registre à décalage.

Le registre à décalage est une structure active, qui doit être alimentée électriquement. Les supports physiques en boucle doivent donc nécessairement être secourus en cas de panne ou de défaut d'alimentation. Les deux grandes techniques utilisées en cas de défaillance sont le by-pass, ou dérivation, illustré à la figure C.14, et la structuration en étoile, détaillée plus loin.

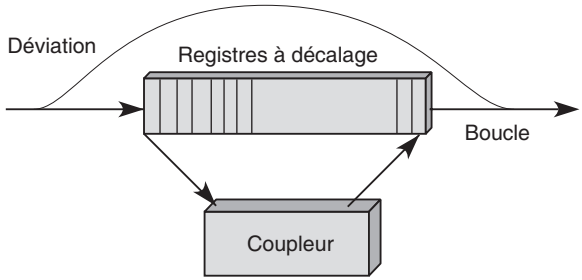


Figure C.14
Dérivation d'un coupleur

Le passage par un registre à décalage oblige à régénérer le signal à la sortie. C'est un avantage pour la portée totale du réseau mais un défaut du point de vue de la fiabilité. En particulier, l'utilisation d'un by-pass ne permet pas la régénération du signal, ce qui oblige à faire très attention à la portée maximale entre deux coupleurs. Si la portée maximale est de 200 m et que les coupleurs soient disposés tous les 100 m, il n'y a aucun problème lorsqu'un coupleur tombe en panne. En revanche, si deux coupleurs de suite sont en panne, le signal doit parcourir 300 m sans régénération. La distance est trop grande et provoque des dégradations importantes de la qualité de l'information transmise.

Pour éviter ces problèmes, il est possible de proposer une architecture en étoile pour une topologie en boucle. Si un coupleur tombe en panne, la boucle est refermée par l'intermédiaire d'un interrupteur sur le panneau de distribution. Cette solution n'est toutefois guère satisfaisante, puisqu'elle nécessite une intervention manuelle. Dans la réalité, derrière le panneau, on utilise un concentrateur, qui est relié par des jarretières aux prises terminales du câblage. En cas de panne d'un coupleur, le concentrateur est capable de reformer la boucle d'une façon totalement passive.

Pour connecter un utilisateur supplémentaire, on étend la boucle par une nouvelle connexion. L'intérêt de cette technique est qu'elle permet la mise hors circuit, d'une façon simple, de tout élément défaillant. De plus, aucun problème ne se pose au niveau de la répétition du signal, puisqu'on passe directement d'un coupleur au coupleur actif suivant. On peut donc déconnecter les machines et les coupleurs sur l'anneau sans aucun risque pour la qualité du signal.

La distribution en étoile autour du local technique est parfaitement adaptée à cette structure.

L'arbre actif

L'arbre est une configuration qui comporte des nœuds, ou hubs, et des branches. La figure C.15 illustre cette topologie, avec, au sommet, le nœud racine.

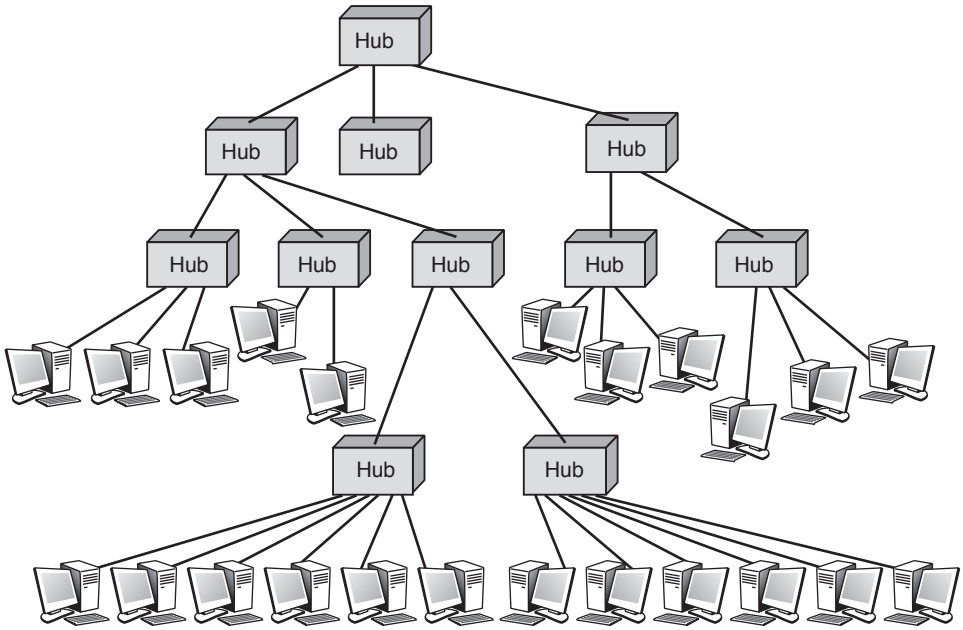


Figure C.15
Arbre actif

L'arbre actif est caractérisé par une structure arborescente. À chaque intersection correspond un hub alimenté électriquement, dont le rôle est de répéter, dans toutes les directions possibles, une copie du message qui arrive. Cette caractéristique permet, à partir de n'importe quelle station, d'atteindre toutes les autres. Elle se retrouve sur les structures en bus, dans lesquelles, lorsqu'un émetteur envoie de l'information, toutes les stations en prennent une copie au passage et la conservent si l'adresse du destinataire correspond à leur propre adresse. Dans la structure de l'arbre actif, on a exactement les mêmes propriétés : chacun reçoit une copie, et personne n'a à se soucier de savoir qui enlève le signal du câble comme sur une boucle, les signaux disparaissant automatiquement.

Les techniques d'accès correspondant à ce type de réseau en arbre sont identiques à celles des structures en bus, à savoir les techniques Ethernet. Les réseaux en arbre actif avec la technique d'accès Ethernet s'appellent des réseaux Starlan.

La structure en arbre actif est bien adaptée à la distribution en étoile, puisqu'il suffit de placer un hub dans le local technique et de relier, sur le tableau de distribution, les fils correspondant aux machines à raccorder. Plusieurs hubs peuvent être placés dans le même local technique si le nombre de sorties n'est pas suffisant sur un seul hub.

D'autres types de connexions sont possibles à partir d'une structure en arbre, en particulier le raccordement de stations terminales à un contrôleur de communication.

Dans cet exemple, il faut pouvoir connecter le câble de sortie du terminal, correspondant aux caractéristiques du terminal sur le câblage départemental, qui n'a pas forcément la même impédance. Il faut alors ajouter un élément intermédiaire, qui effectue l'adaptation entre les deux types de câbles. Cet élément s'appelle un balun (BALanced-UNbalanced). Ce balun peut être intégré au terminal lui-même.

Le câblage d'établissement

Le câblage d'établissement a pour fonction de raccorder entre eux les différents tableaux de distribution du niveau départemental. On peut envisager pour cela trois possibilités : les rocades, les réseaux locaux et les étoiles.

Les rocades

Les rocades relient les locaux techniques par des faisceaux de câbles. Ces câbles sont utilisés indépendamment les uns des autres, à la demande, pour former des liaisons entre les panneaux de distribution. En règle générale, les rocades sont formées d'un grand nombre de paires de fils : 25, 50, 100 paires ou beaucoup plus. La réalisation d'un réseau Starlan sur trois répartiteurs d'étage est illustrée à la figure C.16.

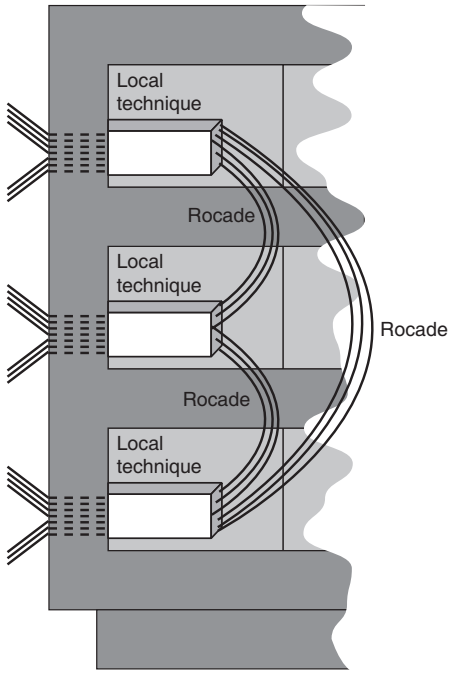


Figure C.16

Réseau Starlan sur trois répartiteurs d'étages

Les câbles de rocade peuvent être des fibres optiques, comme on en rencontre dans de nombreux systèmes de câblage.

Les réseaux locaux

Les réseaux locaux représentent la meilleure manière de relier les panneaux de distribution, puisqu'ils ne nécessitent pas le déplacement des jarretières et garantissent une excellente productivité. Parmi les solutions possibles, les sections suivantes présentent brièvement le bus, la boucle et l'étoile.

Les réseaux locaux en bus

Si cette architecture n'est guère adaptée au cadre départemental, elle l'est à celui de l'établissement, où la connexion des différents locaux techniques peut être effectuée en série sur un bus. Les réseaux Ethernet peuvent ainsi utiliser des vitesses de 1 à 10 Gbit/s pour relier des locaux techniques à très haut débit en bus.

Les réseaux locaux en boucle

Les réseaux locaux en boucle ont connu leur heure de gloire avec le Token-Ring d'IBM, à 16 puis 100 Mbit/s, et FDDI (Fiber Distributed Data Interface). Même s'il existe encore de telles structures dans les entreprises, elles sont en voie de disparition au profit des réseaux en bus et en étoile. Nous avons représenté un réseau local en boucle à la figure C.17.

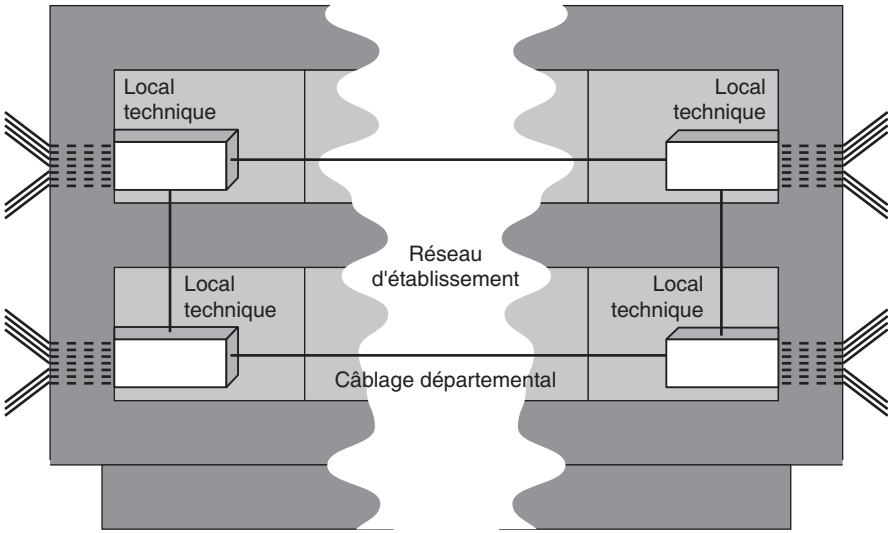


Figure C.17

Réseau d'établissement en boucle

Les réseaux d'établissement en boucle présentent une difficulté. La régénération des signaux ne s'effectue que dans les cartes coupleurs ajoutées aux machines à connecter.

Or les seules machines à connecter dans un réseau d'établissement sont les ponts de connexion des réseaux départementaux. Les régénérations sont effectuées lorsque le signal passe par ces ponts. Si un pont tombe en panne, ou s'il est déconnecté, il faut aller jusqu'au local technique suivant pour que le signal soit régénéré. C'est la raison pour laquelle il est conseillé de doubler les équipements au niveau de l'établissement ou de limiter la distance entre deux répartiteurs d'étage. Cette dernière solution permet au signal de revenir au premier pont ou d'aller au pont suivant.

Les réseaux locaux en étoile

La connexion entre les répartiteurs d'étage ou les tableaux de distribution peut s'effectuer grâce à des étoiles optiques partant d'un point central de l'entreprise. L'étoile peut être passive et répéter dans toutes les directions les informations qui lui proviennent sur une entrée. Pour éviter de diffuser sur tous les câblages raccordés une information destinée à un seul utilisateur, il faut ajouter des ponts dans les locaux techniques.

Dans la plupart des cas, l'étoile optique est un composant passif, générant une perte en ligne importante. Pour cette raison, il ne doit pas y avoir plus de 2 ou 3 étoiles optiques passives en série entre deux points de raccordement. La figure C.18 illustre une configuration utilisant une étoile optique.

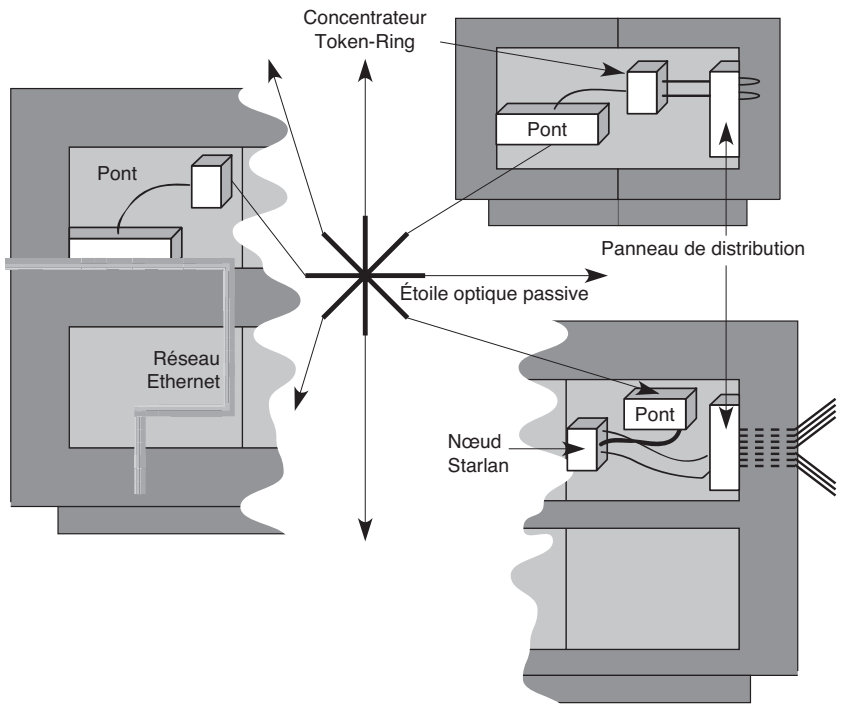


Figure C.18
Raccordement par étoile optique

Une deuxième possibilité, beaucoup plus classique, consiste à raccorder les répartiteurs par des faisceaux de câbles qui se dirigent vers un point central. C'est la technique utilisée pour le raccordement des panneaux de distribution téléphonique à un autocommutateur privé (PABX) ou des panneaux de distribution banalisés à un PABX multiservice. Cette structure de raccordement est illustrée à la figure C.19

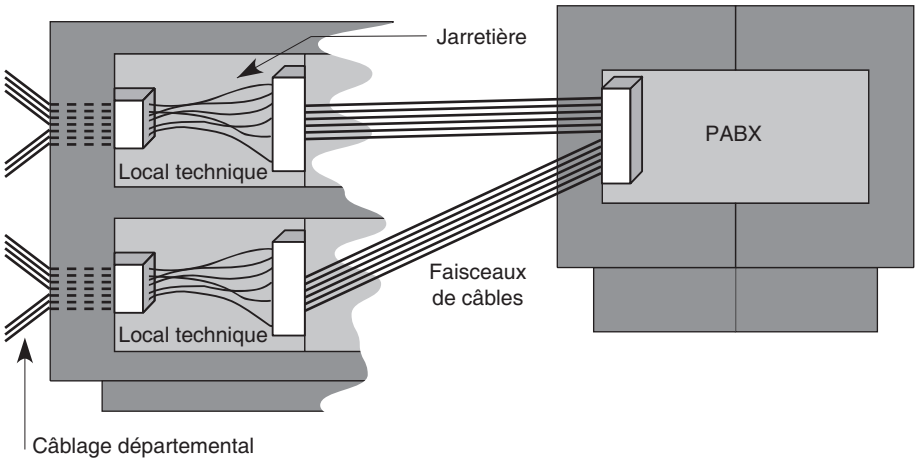


Figure C.19

Raccordement par faisceaux de câbles

Architecture des commutateurs

Les architectures des commutateurs sont assez semblables dans la plupart des technologies de commutation telles que ATM ou Ethernet commuté ainsi que dans le coeur de commutation des routeurs, c'est-à-dire dans l'élément central du routeur permettant le transfert d'un paquet d'une interface d'entrée vers une interface de sortie une fois le noeud suivant choisi. Comme la plupart des commutateurs sont de niveau 2, on parler de commutateur de trames, même s'il s'agit de façon sous-jacente de commutateur de paquets.

De nombreuses catégories d'architectures de commutateurs ont été proposées, et des types très variés de circuits VLSI (Very Large Scale Integration), les fameuses puces de silicium, ont été développés dans les laboratoires de recherche et chez les industriels. Les diverses publications issues de ces travaux distinguent trois types principaux d'architecture, comme nous l'avons vu au chapitre 2 : à mémoire partagée (*shared-memory*), à support partagé (*shared-medium*) et à division spatiale (*space-division*).

Étant donné les vitesses élevées des lignes de transmission modernes, les commutateurs doivent pouvoir transférer les trames à des débits extrêmement rapides, de l'ordre de cent

mille à un million de trames par seconde et par ligne d'entrée. La réalisation de tels commutateurs demande des composants à haute performance.

Les commutateurs doivent être capables de supporter des trafics tant homogènes que sporadiques. Par ailleurs, la qualité de service fournie par le réseau étant affectée par le délai de transfert de bout en bout et la probabilité de perte de trames, une différenciation des services est nécessaire. Les objectifs et critères de performance de cette différenciation peuvent toutefois être opposés, tels que la perte d'aucune trame, mais avec un temps de latence important, ou au contraire la perte de trame, mais avec un temps de traversée réduit. Un service de commutation avec priorité est donc essentiel pour que les différentes classes de services puissent coexister à l'intérieur d'un même commutateur.

Rôle et fonctionnalités des commutateurs

Un commutateur est un composant avec *n* entrées et *n* sorties qui achemine les paquets arrivant sur les entrées vers leur destination de sortie.

Le rôle d'un commutateur consiste à assurer les trois fonctions essentielles suivantes :

- analyse de l'en-tête de la trame et sa traduction ;
- commutation spatiale, ou routage ;
- multiplexage des trames sur la sortie requise.

Les données des utilisateurs sont transportées dans le champ de données des trames et transférées de manière asynchrone. Du fait de son comportement statistique et parce qu'un nombre important de flots peuvent partager la même liaison, le commutateur doit se synchroniser sur les instants d'entrée des trames dans le noeud. Le commutateur examine l'en-tête de chaque trame pour identifier la porte de sortie de la trame. Cette identification s'effectue soit par l'intermédiaire de la référence qui détermine le chemin, soit par l'adresse complète du destinataire dans le cas d'un routage. Il convertit la zone de supervision en un nouvel en-tête pour le noeud de commutation suivant, gère le routage et envoie des informations de contrôle et de gestion dans les réseaux associés.

Dans un commutateur ATM, la commutation s'effectue à partir du VCI (Virtual Channel Identifier) ou du VPI (Virtual Path Identifier) contenus dans l'en-tête de la cellule. Des mécanismes de contrôle de collision permettent aux trames provenant de différentes entrées d'accéder à la file d'attente d'un même multiplex, qui n'est autre qu'une voie de communication prenant en charge plusieurs flux simultanément. Les trames sont commutées individuellement, l'horloge interne du commutateur travaillant à un rythme correspondant au temps de transmission d'une trame ATM. Par exemple, si la ligne de communication la plus rapide a un débit de 10 Gbit/s, la durée de la transmission d'une trame ATM est de 42,4 ns. Dans ce cas, le commutateur est rythmé à la cadence d'une décision toutes les 42,4 ns.

Les commutateurs Ethernet ont a prendre en charge des trames un peu plus longues, de 64 octets à 1 500 octets. Le temps de traitement étant identique que la trame soit courte ou longue, on comptabilise la performance d'un commutateur par le nombre de trames

émises par seconde. Bien sûr, il faut tenir compte de la longueur moyenne des trames pour déterminer la vitesse des lignes de sortie.

La réalisation d'un commutateur peut s'effectuer de diverses façons. Dans tous les cas, il faut créer une fonction de stockage, qui peut se trouver à l'entrée, à la sortie ou le long de la chaîne de commutation. À l'intérieur du commutateur, diverses techniques de routage peuvent être mises en oeuvre : circuit virtuel, autoroutage ou datagramme. Deux des principales fonctions assurées par le commutateur correspondent au routage et à la mémorisation des trames. Des fonctions optionnelles, telles que le recouvrement d'erreur ou le contrôle de flux, peuvent être éventuellement implémentées dans les commutateurs.

Un commutateur doit satisfaire à de nombreuses contraintes, notamment les suivantes :

- très haut débit ;
- faible délai de commutation ;
- très faible taux de perte de trames ;
- gestion des applications multicast (communication multipoint) ;
- modularité et extensibilité ;
- faible coût d'implémentation.

De plus, un commutateur moderne doit être pourvu de fonctions de distribution et de gestion des priorités.

Les catégories de commutateurs

De nombreux auteurs ont tenté de mettre un peu d'ordre dans la prolifération des propositions de structure des commutateurs. Nous adoptons dans ce livre une classification qui recouvre les architectures de la quasi-totalité des commutateurs et repose sur cinq critères d'architecture :

- architecture interne en fonction du nombre d'étapes élémentaires ;
- type de liaison à l'intérieur du commutateur ;
- technique de commutation interne ;
- contrôle interne du commutateur ;
- position des mémoires et blocages internes.

Les architectures internes se différencient par le nombre d'étapes à traverser. Une étape peut être considérée comme un bloc monolithique traversé en une seule tranche de temps. Plus le nombre d'étapes est faible, plus le temps de réponse est court.

La liaison à l'intérieur du commutateur peut être dédiée ou statistique. Pour les liaisons dédiées, les trames vont d'une porte d'entrée vers une porte de sortie en transitant toujours par le même chemin. Dans le cas statistique, toute trame est apte à emprunter une liaison quelconque à l'intérieur du commutateur. Le routage est déterminé par un algorithme de contrôle.

Le tableau C.4 récapitule ces cinq catégories de commutateurs et leurs propriétés.

Tableau C.4 • Critères de classification des commutateurs

Architecture interne	Liaison interne	Commutation interne	Contrôle du commutateur	Mémoire et blocage
Nombre d'étapes à parcourir	Liaison dédiée Liaison statistique	Répartition dans l'espace Répartition dans le temps	Algorithme de gestion des ressources ; routage, contrôle de flux	Position des mémoires dans le commutateur Possibilité de blocage interne

Les techniques de commutation interne peuvent se classer en deux grandes catégories : par répartition dans l'espace et par répartition dans le temps. Dans le premier cas, plusieurs chemins parallèles peuvent être mis en place pour véhiculer les trames, tandis que, dans le second, les trames se partagent les ressources dans le temps. Pour simplifier la présentation, nous supposerons qu'avec la répartition dans le temps, toutes les trames transitent par une même liaison interne, liaison nécessairement statistique. Dans la réalité, il peut y avoir superposition des deux techniques de commutation : plusieurs liaisons sont possibles, et, sur ces liaisons, il peut y avoir un multiplexage temporel.

Les algorithmes de gestion des ressources permettent le contrôle du commutateur. Ces algorithmes concernent, entre autres, le routage des trames et les contrôles de flux et de congestion.

Blocage et mémorisation

À l'intérieur du commutateur, il peut être nécessaire de mémoriser des trames lorsqu'un phénomène de blocage se produit, c'est-à-dire quand deux trames entrent en compétition pour obtenir une même ressource. Il faut alors mettre une trame en attente. Les mémoires peuvent se situer à l'entrée, à la sortie ou en différents points à l'intérieur du commutateur.

Les différents types de blocages

Comme nous venons de le voir, il existe des commutateurs avec blocage et d'autres sans blocage. On distingue trois types de blocages, le blocage interne, le blocage en sortie et le blocage en tête de file :

- Blocage interne. Ce blocage survient lorsque plusieurs trames veulent accéder à la même liaison interne. Des conditions de non-blocage ont été spécifiées pour un réseau Banyan (*voir plus loin dans ce chapitre*). Un réseau Banyan est non bloquant si les entrées actives x1, x2,… xk et leurs sorties respectives y1, y2,… yk satisfont les relations suivantes :
  - Les sorties sont monotones, c'est-à-dire que $y_1 < y_2 < \ldots < y_k$ ou $y_1 > y_2 > \ldots > y_k$.
  - Les entrées sont concentrées, c'est-à-dire que toute entrée comprise entre deux entrées actives est active.
- Blocage en sortie. Comme il n'y a pas de coordination entre les trames qui arrivent en fonction de leur destination, les trames qui parviennent dans la même tranche de temps peuvent être destinées à une même sortie et donc aboutir à un conflit en sortie.

- Blocage en tête de file, ou HOL (Head Of Line). Ce blocage intervient dans les files d'entrée du commutateur. Considérons deux files d'entrée avec des trames en tête de file entrant en conflit pour une même sortie. Une de ces trames est acceptée pour le routage interne vers la sortie, tandis que les autres sont bloquées. Cette technique impose la contrainte suivante : les trames situées dans la file d'attente derrière les trames bloquées ne peuvent être transmises vers leur sortie, même si elles sont destinées à des sorties non conflictuelles.

Placement des mémoires

Le placement des mémoires tampons, ou buffers, pour stocker les trames et les moyens permettant de résoudre les contentions en sortie affecte à la fois les performances et la complexité des commutateurs.

La figure C.20 illustre les différents placements de mémoires envisageables.

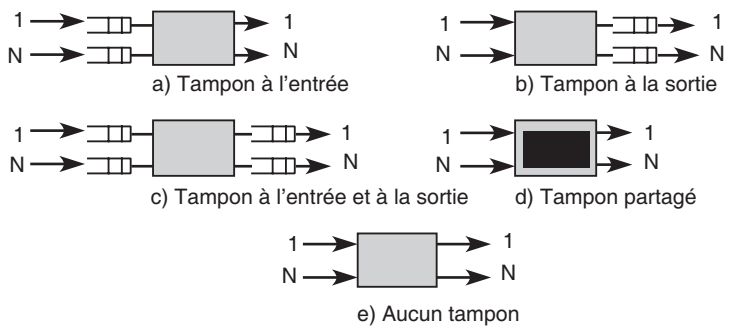


Figure C.20

Placement des mémoires tampons dans les commutateurs

Les architectures avec mémoire tampon à l'entrée permettent à toute nouvelle arrivée d'être placée dans ces mémoires, résolvant de ce fait les problèmes de contention. Les trames en tête de chaque file essaient d'accéder aux liaisons de sortie. Les trames sélectionnées sont délivrées aux ports de sortie, tandis que les autres restent en tête de file pour un nouveau tour d'arbitrage. Le problème majeur de cette architecture est le blocage en position de tête, qui limite le débit.

Les architectures utilisant une file partagée ne rencontrent pas ce type de blocage. Les trames qui se présentent en entrée sont directement transmises au commutateur, et la résolution de contention pour le port de sortie a lieu avant le transport de la trame. Les trames bloquées restent dans le commutateur et sont recyclées vers leur port, où elles sont resynchronées avec l'ensemble des nouvelles arrivées.

Concernant le taux de perte de trames, les commutateurs à mémoire partagée présentent les meilleures performances. En effet, chaque adresse de la mémoire partagée peut être allouée temporairement à n'importe quel port de sortie, et non à un port de sortie particulier. De la sorte, la limite maximale de longueur de chaque file, et notamment des files

de sortie, peut être étendue jusqu'au débordement de la mémoire partagée, réduisant de ce fait le taux de perte des trames.

Les architectures avec mémoires tampons en sortie utilisent des chemins parallèles pour accéder aux ports de sortie. Cela autorise la délivrance de multiples trames simultanément pour chaque destination. Les mémoires tampons situées à chaque port de sortie stockent les trames en attendant l'accès aux liaisons de transmission.

Exemples de commutateurs

Les sections qui suivent présentent les commutateurs les plus connus en fonction des critères que nous avons introduits à la section précédente.

Le commutateur Crossbar

L'un des commutateurs les plus simples se construit en reprenant les concepts des premiers autocommutateurs Crossbar téléphoniques, qui remontent à plusieurs dizaines d'années. Les commutateurs Crossbar électroniques, et non plus mécaniques, font toujours partie, au début des années 2010, des petits commutateurs les plus vendus.

La figure C.21 illustre le fonctionnement de trois types de commutateurs Crossbar.

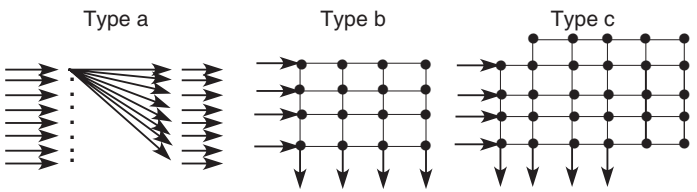


Figure C.21
Commutateurs Crossbar

Sur la figure, les flots qui entrent dans les commutateurs Crossbar sont représentés par les flèches de gauche et ceux qui sortent par les flèches de droite pour le type a et par les flèches du bas pour les types b et c. Le rôle de ces commutateurs est d'acheminer des flots de trames arrivant sur l'une des entrées vers une des sorties. Dans les types b et c, les points noirs représentent des commutateurs élémentaires permettant à une trame de se diriger vers trois sorties au choix, une sortie vers le haut, une sortie droit devant et une sortie vers le bas. Arrivé aux bords du commutateur, il ne peut y avoir que deux sorties au choix, voire une seule.

Le commutateur Crossbar illustré à la partie gauche de la figure (type a) permet, à partir de toute entrée, d'aller directement à toute sortie. De mécaniques au début du siècle, les relais sont devenus électroniques à partir des années 1980. Le commutateur Crossbar de base de type a ne comporte qu'une étape : une trame entrant dans le Crossbar va directement à la ligne de sortie. Entre la porte d'entrée et la porte de sortie, la liaison est dédiée ; la commutation est répartie dans l'espace, et le routage est fixe. Si deux trames se dirigent en parallèle vers une même porte de sortie, des mémoires sont nécessaires soit à la porte d'entrée, soit à la porte de sortie. De ce fait, il n'y a pas de blocage interne au commutateur.

Il existe des commutateurs Crossbar beaucoup plus complexes, dont l'architecture est profondément modifiée. Par exemple, la partie centrale de la figure C.21 (type b) décrit un commutateur qui permet de mettre en place une ou plusieurs voies entre l'entrée et la sortie. Dans ce cas, il faut n^2 points de connexion pour n entrées et n sorties du commutateur. Un seul chemin peut être envisagé entre une entrée et une sortie. Plusieurs chemins distincts sont disponibles grâce aux commutateurs élémentaires. Ces commutateurs n'empêchent pas les collisions potentielles entre les trames sur les chemins internes. Il faut donc stocker les trames dans des mémoires en entrée et mettre en place un mécanisme écoulant un maximum de trames en parallèle. Une autre possibilité consiste à placer des mémoires à chaque point de jonction, ce qui augmente d'autant le nombre d'étapes à franchir en interne.

En se servant des cinq critères que nous avons introduits précédemment dans cette annexe, un commutateur Crossbar avec mémoires se définit par un nombre d'étapes dépendant de la route et des ports d'entrée et de sortie, des liaisons statistiques, une commutation dans l'espace, un routage dynamique et des mémoires intermédiaires nécessaires pour éviter les blocages internes.

On peut modifier le commutateur en agrandissant le nombre de commutateurs élémentaires afin de permettre un plus grand nombre de parcours et d'éviter les collisions. À chaque collision potentielle, la trame est détournée de son chemin direct et doit, soit tourner à gauche, soit aller tout droit. En faisant tourner la trame trois fois à gauche, on finit par retrouver le chemin de départ. On peut se représenter le commutateur comme modélisant les rues de Manhattan, à New York, et la trame comme étant une voiture. Dans Manhattan, pour simplifier la circulation, il est interdit de tourner sur sa gauche, de façon à ne pas couper les flux de circulation. Pour prendre une direction à gauche dans un carrefour, il faut aller tout droit et tourner trois fois à droite. Les commutateurs que nous examinons s'appellent des commutateurs Manhattan pour rappeler cette analogie et la possibilité pour une trame de prendre des chemins détournés pour arriver à la sortie choisie. Un commutateur Manhattan est illustré à la partie droite de la figure C.21 (type c).

Les caractéristiques comparées des trois architectures Crossbar sont indiquées au tableau C.5.

TABLEAU C.5 • Caractéristiques des commutateurs Crossbar

	Architecture interne	Liaison interne	Commutation interne	Contrôle du commutateur	Mémoire et blocage
Crossbar (fig 26.5.a)	1 étape	Liaison dédiée	Répartition dans l'espace	Routage fixe	Pas de blocage interne
Crossbar (fig 26.5.b)	*n* étapes	Liaisons statistiques	Répartition dans l'espace	Routage dynamique	Blocage interne résolu par des mémoires
Crossbar (fig 26.5.c)	*n* étapes	Liaisons statistiques	Répartition dans l'espace	Routage spécifique	Blocage interne résolu par le routage

Le commutateur Banyan et ses extensions

Le commutateur de base qui semble rassembler le plus de suffrages est le commutateur Banyan, illustré à la figure C.22. Ce commutateur 8x8 possède huit files d'entrée et huit files de sortie. Sur la figure, les trames à commuter se présentent sur la gauche et doivent ressortir sur l'une des huit files de sortie indiquées sur la droite de la figure.

Ce commutateur est construit avec douze commutateurs élémentaires, un commutateur élémentaire étant ici un commutateur possédant deux entrées et deux sorties, ce que l'on appelle encore un commutateur 2x2. Ce commutateur comporte trois étages, un étage étant représenté par la traversée d'un commutateur élémentaire 2x2. En d'autres termes, la trame qui se présente sur l'une des huit entrées doit traverser trois commutateurs élémentaires pour atteindre une sortie.

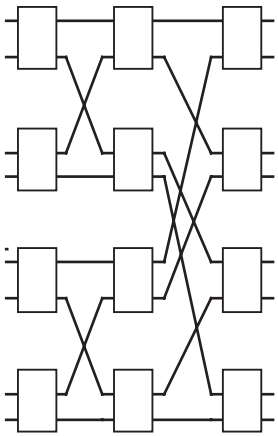


Figure C.22

Commutateur Banyan

La figure C.23 illustre la construction d'un commutateur Banyan. À partir des deux premières entrées, celles du haut à gauche, on accède aux huit sorties en utilisant des commutateurs élémentaires à deux entrées et deux sorties. On obtient à l'étape a de la figure C.23 un commutateur 2x8, qui possède deux entrées et huit sorties. À l'étape b, on ajoute deux nouvelles entrées et un commutateur élémentaire, qui prend en charge ces deux nouvelles entrées. On relie ce commutateur élémentaire aux entrées libres des commutateurs élémentaires du deuxième étage de l'étape a, ce qui permet de construire un commutateur 4x8. L'étape c permet de passer à un commutateur 6x8 et l'étape d à un commutateur Banyan 8x8 complet.

Avec un étage de commutateurs élémentaires, on accède à 2 sorties depuis 2 entrées. Avec deux étages, on accède à 4 sorties depuis 4 entrées, et, plus généralement, avec n étages, on accède à 2^n sorties depuis 2^n entrées, ce qui constitue un avantage par rapport au Crossbar, le nombre de commutateurs élémentaires utilisés pour réaliser le commutateur global étant beaucoup plus petit.

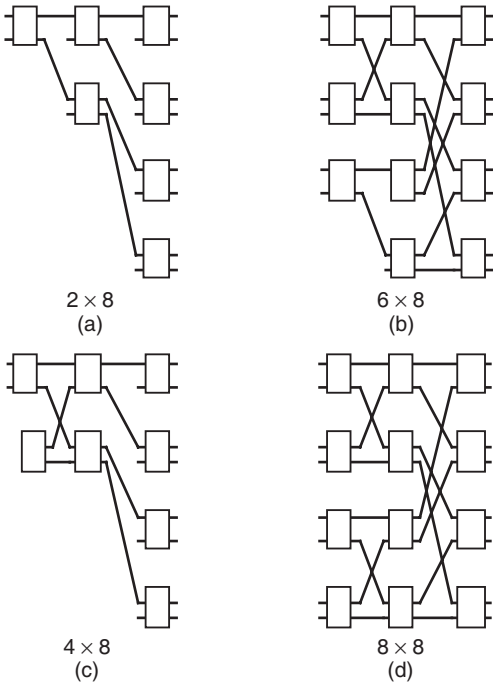


Figure C.23
Étapes de construction d'un commutateur Banyan

Deux types de collisions entre trames peuvent se produire :

- Deux trames qui convergent vers la même sortie.
- Deux trames qui empruntent la même voie à l'intérieur d'un commutateur élémentaire.

Comme à chaque couple entrée-sortie ne correspond qu'un seul chemin, il n'est pas possible d'éviter la collision en changeant de chemin. De nouveau, pour éviter ces deux types de collisions, on peut ajouter des mémoires à l'entrée, à la sortie ou dans tous les commutateurs élémentaires intermédiaires.

Les commutateurs de base

Au moins trois possibilités sont utilisées comme éléments de base pour les commutateurs que l'on trouve dans le commerce :

- plusieurs commutateurs Banyan en série ;
- commutateur Batcher Banyan ;
- commutateur Knock-out.

Commutateurs Banyan en série

Pour deux commutateurs en série, il y a m façons d'aller de l'émetteur au récepteur, si m est le nombre d'entrées et de sorties. Si k commutateurs sont en série, mk^{-1} chemins

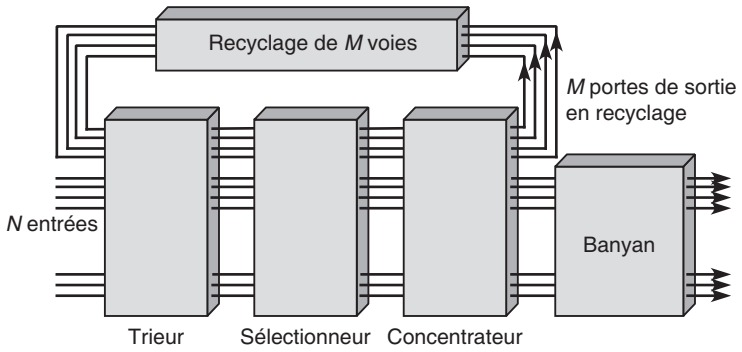
peuvent être envisagés. Néanmoins, cela ne résout pas directement les problèmes de collisions en sortie et rallonge le délai de transit.

Commutateur Batcher Banyan

Dans un commutateur Batcher Banyan, les trames qui entrent en collision en sortie sont recyclées suivant le principe illustré à la figure C.24. Le premier commutateur Banyan (trieur) permet de changer de ligne, et le deuxième (sélectionneur) d'opérer une sélection parmi les trames qui ont la même direction et qui entreraient en collision sur la ligne de sortie. Ensuite, le concentrateur permet de diriger la trame soit vers le dernier commutateur Banyan, et donc d'atteindre la ligne de sortie, soit de l'envoyer vers l'une des entrées d'un commutateur de recyclage de type MxM permettant de réintroduire la trame en début de cycle. Le choix de recycler une trame est pris dès que la ligne de sortie sur laquelle doit se rendre la trame est saturée. Une trame peut donc tourner dans le commutateur tant que la ligne de sortie est saturée.

Figure C.24

Fonctionnement du commutateur Batcher Banyan



Commutateur Knock-out

Dans le commutateur Knock-out illustré à la figure C.25, à partir d'une ligne d'entrée, les trames sont diffusées vers l'ensemble des interfaces de sortie. Dans l'interface de sortie, un Banyan à *n* entrées permet de faire converger les trames qui se dirigent vers la sortie *n*.

Si plusieurs trames se présentent sur le même commutateur élémentaire, l'une d'elles est mise en attente de telle sorte qu'une seule trame sorte vers *n*. Le commutateur interne à l'interface de sortie est illustré à la figure C.26.

Figure C.25

Fonctionnement du commutateur Knock-out

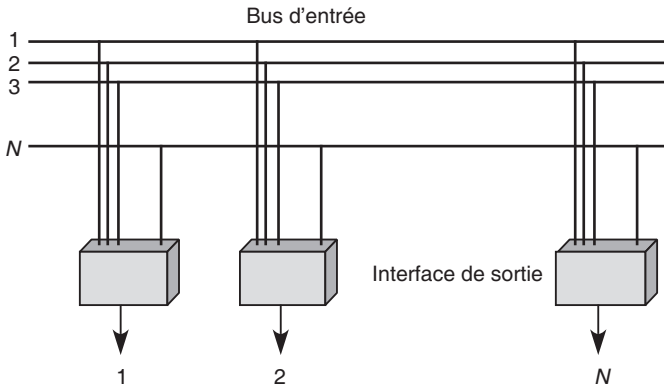
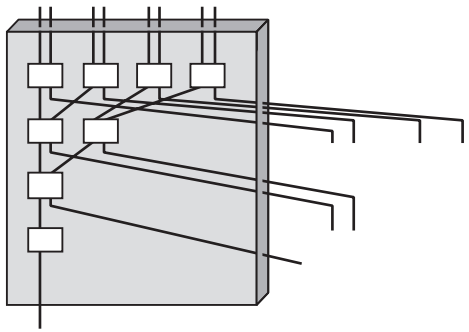


Figure C.26

Commutateur d'interface d'un Knock-out



Autres commutateurs

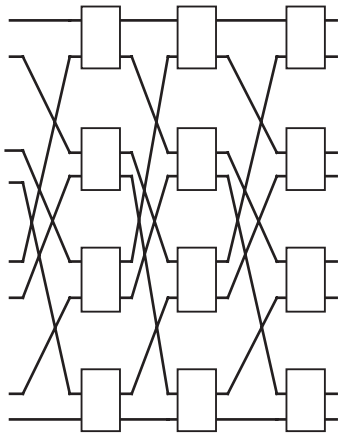
Pour compléter la description des commutateurs actuels, on peut noter que, dans un réseau Banyan, si huit trames arrivent aux huit entrées simultanément, il n'y a qu'une seule possibilité de sortie pour que le parallélisme soit complet. Dans le réseau Banyan, cette possibilité est la suivante :

1 1 ; 2 5 ; 3 3 ; 4 7 ; 5 2 ; 6 6 ; 7 4 ; 8 8.

On peut imaginer d'autres commutateurs, avec des parallélismes différents (commutateurs Δ, Ω, etc.), dans lesquels les chemins suivis par les huit trames arrivant sur les huit entrées sont différents de ceux qui existent dans le commutateur Banyan. Le commutateur Ω permet l'identité, c'est-à-dire que la trame qui se présente sur l'entrée numéro 1 sort par la sortie numéro 1, la trame qui arrive en même temps sur l'entrée numéro 2 sort par la sortie numéro 2, et ainsi de suite. Le commutateur Ω est illustré à la figure C.27.

En prenant, par exemple, la troisième entrée à partir du haut et en suivant toujours tout droit dans les commutateurs élémentaires, on se retrouve sur la troisième ligne de sortie. À la énième ligne d'entrée correspond la énième ligne de sortie.

Figure C.27
Fonctionnement d'un commutateur Ω



Ce commutateur Ω présente toutefois l'inconvénient de ne plus permettre un routage aussi simple que le Banyan, où l'adresse de sortie autorise, lorsqu'elle est codée en binaire, le routage de la trame : avec un 0, on va vers le haut, et avec un 1 on va vers le bas. L'adresse de sortie 010 est atteinte si la trame est routée vers le haut puis vers le bas puis vers le haut pour terminer, et ce quelle que soit l'entrée. L'avantage global de ce système est de permettre le parallélisme des flux de trames à travers le commutateur.

Aujourd'hui, un regain d'intérêt se fait jour pour les techniques de commutation utilisant un bus partagé, car les progrès technologiques permettent de concevoir des bus atteignant des capacités de transport de plusieurs centaines de gigabits par seconde.

Le tableau C.6 recense les caractéristiques des différents commutateurs provenant de la source Banyan en fonction des cinq critères que nous avons retenus pour la définition d'un commutateur au début de ce chapitre.

Tableau C.6 • Caractéristiques des commutateurs de type Banyan

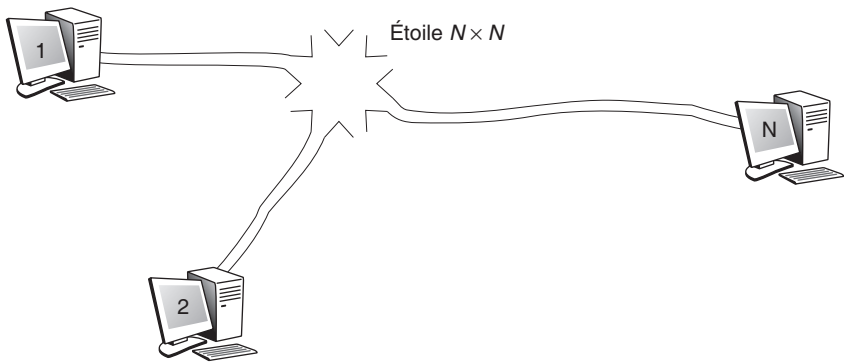
	Architecture interne	Liaison interne	Commutation interne	Contrôle du commutateur	Mémoire et blocage
Banyan élémentaire	1 étape	Liaisons dédiées	Répartition dans l'espace	Autoroutage	Pas de blocage interne
Banyan avec mémoire	*m* étapes	Liaisons dédiées	Répartition dans l'espace	Autoroutage dynamique	Pas de blocage résolu par des mémoire
Batcher Banyan	1 étape (*n* étapes si *n* rebouclages)	Liaisons statistiques	Répartition dans l'espace	Routage spécifique	Blocage interne résolu par le routage
Knock-out	1 étape	Liaisons dédiées	Répartition dans l'espace	Autoroutage	Blocage interne résolu par des mémoires internes

D'autres types de commutateurs de trames sont incarnés par le Lambdanet et le ShuffleNet. Ces deux commutateurs utilisent de la fibre optique avec du multiplexage en longueur d'onde, plusieurs faisceaux lumineux étant véhiculés en parallèle dans le cœur de la fibre optique.

Le Lambdanet

La figure C.28 illustre le fonctionnement d'un commutateur Lambdanet. À partir d'un émetteur, on envoie sur un sous-canal des trames diffusées par une étoile passive centrale vers des sous-canaux correspondant aux nœuds connectés. Pour 16 nœuds au total, il y a une voie aller et 16 voies de retour entre un nœud et l'étoile optique. Toutes ces voies sont multiplexées en longueur d'onde dans une fibre optique monomode. Chaque voie atteint un débit de 10 Gbit/s si nécessaire. Cette technique facilite la diffusion et le multipoint, mais elle est coûteuse. En particulier, les machines terminales doivent avoir 16 récepteurs distincts pour recevoir sur les 16 longueurs d'onde en même temps.

Figure C.28
Fonctionnement du commutateur Lambdanet



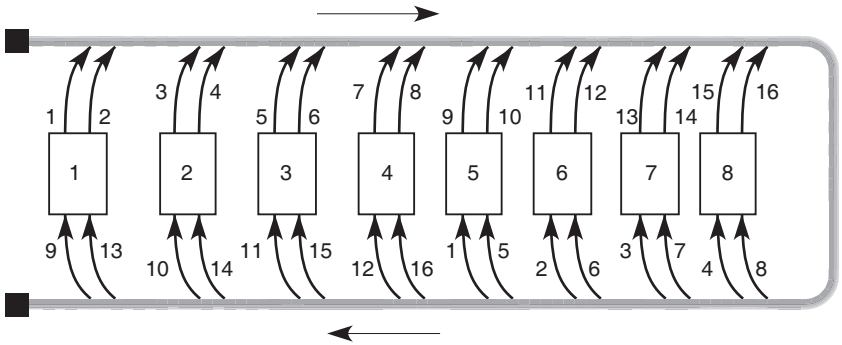
Le commutateur Lambdanet se caractérise par une étape, une liaison dédiée, une commutation spatiale, pas de contrôle *a priori*, des mémoires en sortie et pas de blocage.

Le ShuffleNet

Le commutateur ShuffleNet essaie de concilier les méthodes précédentes par des nœuds intermédiaires de commutation. Pour aller d'un point à un autre point, il faut généralement passer par un ou plusieurs nœuds intermédiaires, comme illustré à la figure C.29.

Figure C.29

Structure physique du ShuffleNet

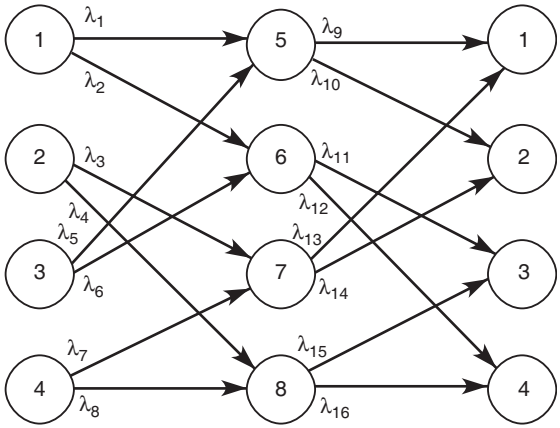


L'avantage de cette technique est d'avoir plusieurs chemins utiles en cas de panne. Ces chemins ont une longueur variable. S'il y a trop d'embouteillage, on peut toujours prendre un autre chemin, certes plus long, pour atteindre le destinataire. Le support est une fibre qui prend en charge 16 canaux multiplexés en longueur d'onde. Sur la figure, pour aller d'un nœud quelconque à un autre nœud, il faut passer au maximum par 3 nœuds intermédiaires. Par exemple, pour aller du nœud 1 au nœud 3, le nœud 1 émet sa trame vers la sortie 2 ; celle-ci arrive au nœud 6, qui l'envoie vers la sortie 11, ce qui permet au nœud 3 de recevoir l'information. L'avantage de cette technique est de n'avoir à chaque nœud que deux émetteurs et deux récepteurs et de disposer de plusieurs chemins pour aller d'un nœud à un autre.

Le commutateur ShuffleNet se caractérise par plusieurs étapes, une liaison statistique, une commutation spatiale, un contrôle à l'entrée pour optimiser le chemin et des mémoires dans les nœuds intermédiaires pour éviter les blocages.

Un commutateur ShuffleNet peut aussi être réalisé par le maillage illustré à la figure C.30. Une trame entrant par le nœud 1 et sortant par le nœud 3 doit être émise par le nœud 1 sur la longueur d'onde $2(\lambda_2)$ jusqu'à la porte 6, qui retransmet la trame sur la longueur d'onde $11(\lambda_{11})$ jusqu'à la porte 3. Nous pouvons vérifier sur la figure que, partant du nœud 1, la trame arrive bien au nœud 3 après avoir suivi le chemin que nous venons d'indiquer. Il est bien sûr possible de trouver d'autres chemins pour aller du nœud 1 au nœud 3. Par exemple, en partant du nœud 1 sur la longueur d'onde 1, la trame arrive sur le nœud 5, qui envoie la trame sur la longueur d'onde 10, ce qui lui permet d'arriver au nœud 2. À partir de ce nœud, en se replaçant à droite de la figure, nous pouvons envoyer la trame sur la longueur d'onde 4, ce qui lui permet d'arriver au nœud 8, et, enfin, en utilisant la longueur d'onde 15, l'envoyer au nœud 3. Le chemin suivi comporte quatre étapes au lieu de deux dans le choix précédent. Ce deuxième choix n'est cependant pas inutile si le nœud 6 tombe en panne.

Figure C.30
Structure logique du ShuffleNet



Les techniques que nous venons de décrire sont à la base d'un grand nombre d'architectures de commutateurs actuellement commercialisées. Elles sont fondées sur une répartition dans l'espace. Une génération de commutateurs totalement différente, fondée sur la répartition dans le temps, est analysée à la section suivante.

Les commutateurs à répartition dans le temps

Les architectures à base de Crossbar ou de Banyan utilisent une répartition dans l'espace, qui privilégie l'affectation de voies parallèles pour effectuer le transport des trames entre les portes d'entrée et de sortie. Une autre grande solution consiste à travailler avec une répartition dans le temps, ce que l'on appelle encore répartition statistique, puisque la répartition des trames dans les tranches de temps se fait de façon statistique. C'est la raison pour laquelle on appelle ces commutateurs à répartition dans le temps des commutateurs temporels statistiques.

Dans ces commutateurs, le support physique est commun à l'ensemble des chemins, un découpage dans le temps permettant d'affecter les communications à tour de rôle. Bien évidemment, des solutions mixtes se sont développées, dans lesquelles un commutateur à répartition dans l'espace commence par proposer de multiples chemins entre une entrée et une sortie. Sur chaque chemin, un multiplexage temporel statistique permet ensuite à plusieurs communications de passer simultanément.

L'inconvénient majeur des techniques de répartition dans le temps est l'obligation d'utiliser un bus commun d'une capacité de transport égale à la somme des vitesses des voies d'accès, ce qui représente un coût important. Les commutateurs ATM temporels statistiques commercialisés par de grands équipementiers incarnent toutefois des solutions acceptables du point de vue du coût.

Commutateurs ATM temporels statistiques

Comme expliqué précédemment, les commutateurs temporels statistiques doivent posséder un bus par lequel transitent toutes les trames. Cette contrainte est très forte : pour 64 entrées avec une interface T_B à 155,52 Mbit/s, qui est l'interface de base normalisée pour les réseaux large bande, le débit du bus doit être de 10 Gbit/s. Le commutateur ATM que nous décrivons ci-après utilise un bus de très grande largeur, d'exactement 424 fils pour les données, une valeur qui correspond à la taille d'une cellule (424 bits). Si le débit de chaque fil est de 100 Mbit/s, on obtient une capacité de transport de 42,4 Gbit/s pour le commutateur. Les deux architectures que nous décrivons reposent, pour la première, sur un support en boucle et, pour la seconde, sur un support en bus.

Architecture en boucle

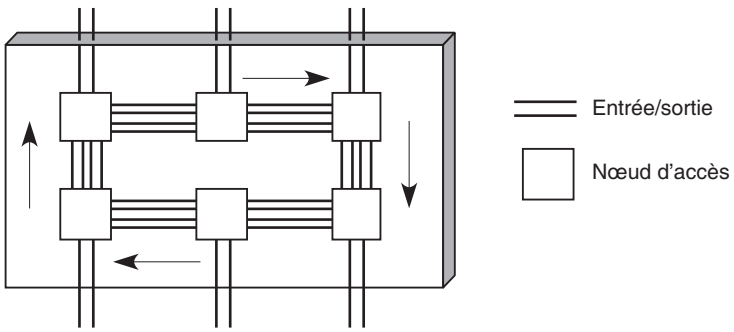
La boucle possède 424 lignes, ce qui permet de transporter les cellules en parallèle. Deux lignes supplémentaires sont réservées à la synchronisation et à la supervision. La vitesse de chaque ligne détermine une unité de temps. Si nous supposons une vitesse de 100 Mbit/s, l'unité de temps qui représente la durée d'une transmission est $y = 10$ ns. Pour entrer sur la boucle, un arbitrage est nécessaire. Nous proposons ici d'utiliser une insertion en parallèle, qui peut être considérée comme un arbitrage distribué. Cette solution est implémentée dans de nombreux commutateurs temporels statistiques sous des formes parfois légèrement différentes.

La cellule est introduite et retirée du support par l'émetteur. Cette solution permet de prendre en charge le multipoint ou la diffusion d'une cellule, les nœuds intermédiaires n'ayant qu'à réaliser une copie de la cellule lors de son passage.

Le support physique illustré à la figure C.31 est constitué de 6 portes d'entrée-sortie, qui donnent naissance à 6 nœuds internes sur la boucle. Entre ces nœuds, une boucle comportant 424 fils est constituée pour transporter les cellules en parallèle. Dans un nœud, un processus de sérialisation-parallélisation a lieu pour transmettre la cellule en série sur la porte d'entrée-sortie et en parallèle sur le bus interne. Cette partie du commutateur est décrite plus en détail dans l'encadré « L'architecture en bus ». Nous nous intéressons ici au transport de la cellule d'une porte d'entrée à une porte de sortie, en supposant que la parallélisation a été effectuée.

Figure C.31

Support physique du commutateur ATM temporel statistique



La cellule est transmise en parallèle, la synchronisation s'effectuant par un signal spécifique sur le fil supplémentaire. Comme la distance est particulièrement petite entre les nœuds d'accès au support, qui se trouvent tous soit sur la même carte physique, soit sur le même circuit imprimé, la synchronisation ne pose aucun problème. Le temps de transmission de la cellule sur le support physique est très court, puisque la transmission s'effectue en parallèle. De plus, dans chaque nœud du support physique, le signal n'a que deux registres à traverser.

L'accès au support physique est détaillé à la figure C.32. Il utilise deux registres parallèles dont les temps de remplacement sont variables et s'adaptent aux contraintes. Ces deux registres garantissent l'absence de collision sur le support.

Soit T_e = 10 ns le temps de remplacement maximal du registre correspondant au temps de transmission d'une cellule. Ce temps de remplacement pouvant en fait être variable, nous supposons ici que les valeurs 2, 4... à 10 ns sont possibles. Ce temps de remplacement dépend de l'activité du nœud, comme nous le verrons plus loin.

Le signal SYO (SYnchronization Out) est transformé en signal SYI (SYnchronization In) sur le fil de synchronisation. Ce signal permet de lire le contenu du registre d'entrée. Il faut noter qu'il n'y a pas d'horloge synchronisée entre les nœuds du support physique.

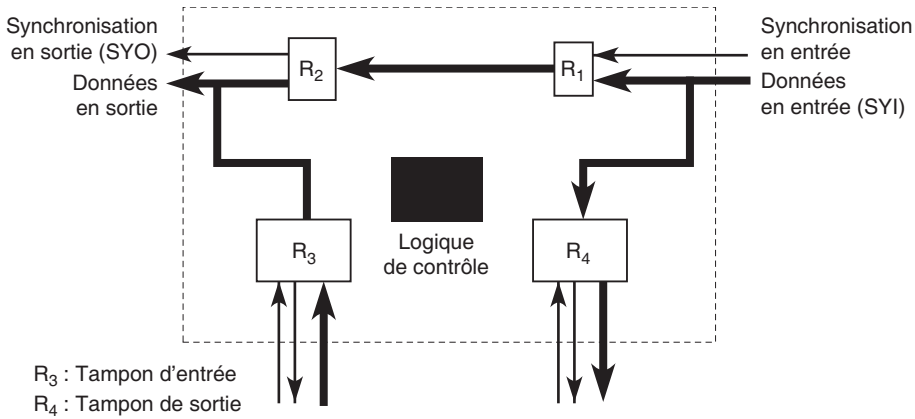


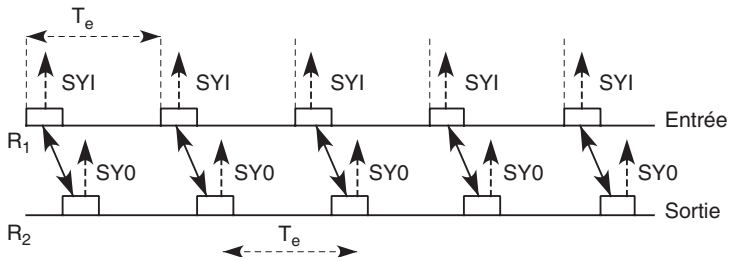
Figure C.32

Architecture du nœud d'accès au support physique

Transit d'une cellule

Différents cas de figure peuvent se produire dans le nœud d'accès. Une cellule peut transiter dans un nœud sans que celui-ci soit concerné par l'émission ou la réception. Ce passage est illustré à la figure C.33. La cellule est stockée dans chaque registre pendant un temps minimal, soit 10 ns dans notre exemple, si le nœud n'est pas dans un état d'insertion. Si le temps de remplacement des registres est supérieur à cette valeur, il faut réduire le plus possible le temps pendant lequel la cellule reste dans les deux registres.

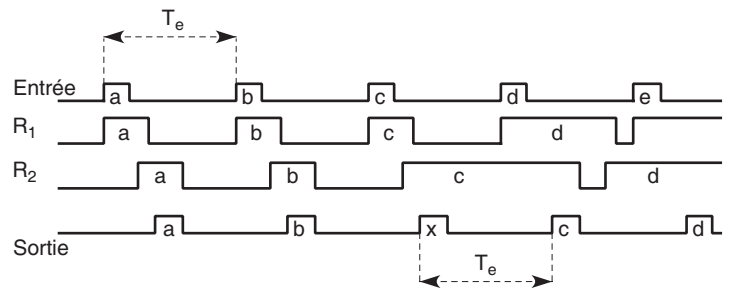
Figure C.33
Transit dans un nœud



Insertion d'une cellule

Lorsque le registre R_3 d'émission est plein, la cellule contenue au sommet est insérée sur la boucle juste après la transmission. Si une cellule arrive de la boucle, elle est retardée dans le registre R_1 car la plus petite valeur possible du temps de remplacement est utilisée, mais sans qu'il y ait collision avec la cellule qui vient d'être insérée. Comme illustré à la figure C.34, la cellule *x* est insérée, ce qui retarde la cellule c, qui doit rester un temps de 50 ns dans les registres R_1 et R_2 avant d'être émise.

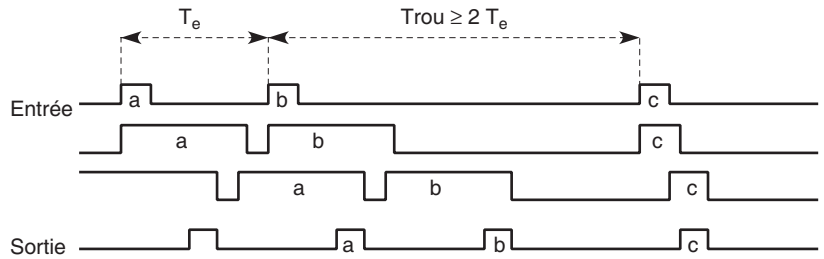
Figure C.34
Insertion d'une cellule



Une fois qu'une cellule est émise, il n'est pas possible d'en transmettre une nouvelle tant que les registres R_1 et R_2 ne retrouvent pas leur état (illustré à la figure C.35). Pour atteindre cette position, deux possibilités se présentent :

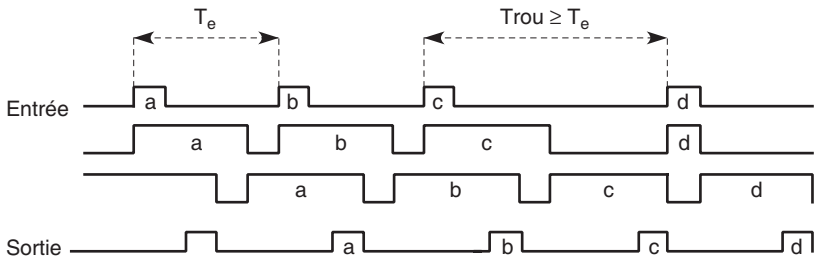
- Attendre un trou suffisamment grand entre deux cellules qui se présentent dans le nœud. Ce cas est illustré à la figure C.35.
- Attendre qu'une cellule insérée par ce même nœud revienne après un tour de boucle. Lors de son prélèvement du support, le nœud revient à son état de base.

Figure C.35
Retour en position de base



Grâce aux registres dont les temps de remplacement sont variables, il est possible de récupérer facilement des trous, qui, sinon, resteraient inemployés. Cette récupération est illustrée à la figure C.36.

Figure C.36
Récupération d'un trou sur le support



Les performances de ce commutateur à répartition dans le temps sont bien adaptées aux contraintes des flux ATM grâce à une très grande flexibilité de l'arbitrage distribué du support physique. Tout d'abord, chaque porte du commutateur possède un débit minimal garanti, que nous appelons débit synchrone. Au minimum, une cellule peut être émise durant tous les intervalles de temps égaux au délai de propagation sur la boucle. Dans notre exemple, le temps maximal pour traverser un nœud est de 100 ns. En supposant le délai de propagation négligeable et 64 portes d'entrée-sortie, le temps de propagation maximal sur la boucle est de 6,4 µs. On en déduit que toutes les 6,4 µs, 48 octets d'informations peuvent être pris en charge, ce qui donne un débit minimal de 60 Mbit/s par porte. Le total des débits minimaux est de 3,84 Gbit/s. Cela représente exactement la moitié de la capacité utile du support. Les autres 3,84 Gbit/s peuvent être distribués de façon asynchrone aux différentes portes du commutateur.

Au moins deux possibilités de gestion de la bande asynchrone peuvent être définies :

- Outre son accès synchrone, une porte peut émettre dans les trous du support. Une fois qu'une cellule a pu être émise sur le support, la porte peut conserver le débit supplémentaire qui lui est donné par cette cellule. Il faut dans ce cas qu'à chaque retard de la cellule supplémentaire une nouvelle cellule soit émise immédiatement pour ne pas perdre le trou qui a été conquis.
- Interdire au nœud qui a conquis un trou supplémentaire de le réutiliser immédiatement.

Dans le premier cas, la porte possède un débit complètement garanti et synchrone, tandis que, dans le second, la bande supplémentaire est équitablement répartie entre les nœuds actifs.

D'après les simulations effectuées pour comprendre le comportement d'un tel commutateur ATM, la seconde solution est satisfaisante et s'adapte bien au trafic par à-coups que l'on rencontre dans les réseaux ATM. Nous avons également noté que les bandes passantes synchrones non utilisées sont récupérées par les autres portes en cas de nécessité. Cela se comprend très bien eu égard au temps de transit sur la boucle. Si nous supposons que 32 stations sur 64 sont inactives, le temps de transit d'une cellule sur la boucle est de 3,84 µs — les temps de passage sont de 20 ns dans les stations inactives. Le débit synchrone des stations actives devient donc de 100 Mbit/s.

Architecture en bus

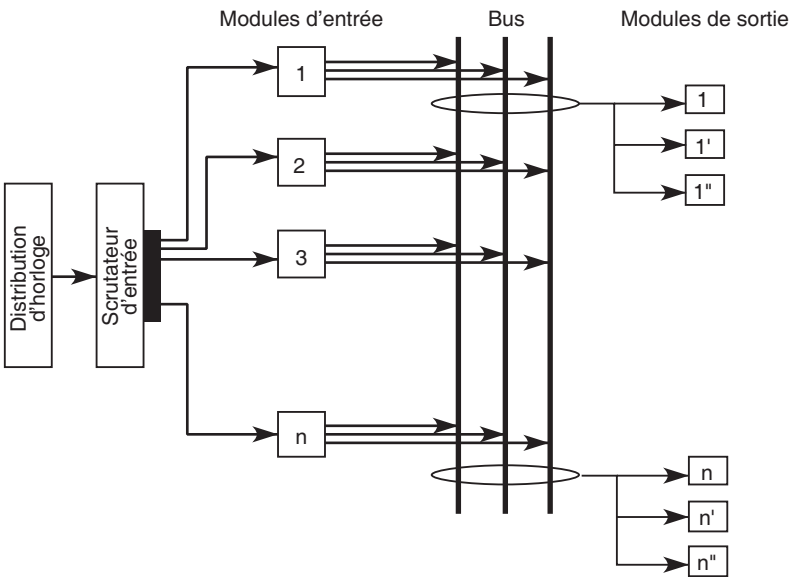
L'idée de cette architecture est de remplacer le support physique en boucle par une architecture en bus. La topologie en bus présente l'avantage de ne pas se préoccuper du prélèvement des informations qui transitent sur le support physique.

Dans ce nouveau commutateur, un scrutateur d'entrée dispose séquentiellement l'information provenant des *n* portes d'entrée sur le bus. En fonction de l'adresse des destinataires, la cellule est véhiculée ou non vers les portes de sortie. Le système est conçu de façon que, à chaque changement d'information sur le bus, une mémoire soit toujours disponible sur chaque sortie pour recevoir la cellule. Une mémoire de sortie doit impérativement être libérée entre deux pas successifs de scrutation en entrée, ce qui suppose un nombre de mémoires suffisant en sortie et un contrôle entre les entrées et les sorties.

La figure C.37 illustre le scrutateur d'entrée, les modules d'entrée et de sortie et un distributeur d'horloge.

Figure C.37

Schéma de fonctionnement d'un commutateur temporel statistique en bus



Le scrutateur d'entrée a pour fonction de prendre l'information contenue dans la porte d'entrée et de la déposer sur le bus, en synchronisation avec un signal d'horloge. Lors du top d'horloge suivant, une nouvelle entrée est scrutée, et sa cellule est insérée sur le bus.

Le rôle du module de sortie est d'extraire l'information qui lui est destinée et de la charger en parallèle dans le registre de sortie. Celui-ci est composé de 424 bits plus un bit PI (Presence Information). Tous les registres de sortie reçoivent le contenu du bus, mais seuls sont sélectionnés ceux qui correspondent au décodage d'adresse. Chaque sortie dispose d'un distributeur d'adresses, de telle sorte que, dès qu'une mémoire de sortie est chargée, une nouvelle mémoire libre est connectée.

D

Annexe du chapitre 6 (Le niveau trame)

Cette annexe détaille le protocole HDLC, qui a été des années durant le modèle des protocoles de liaison. Aujourd'hui, il n'est quasiment plus utilisé directement, mais reste un modèle de référence. Nous examinons ensuite les divers protocoles de liaison des réseaux Ethernet LLC (Link Logical Control).

HDLC (High-level Data Link Control)

En 1976, l'ISO normalise une procédure de communication entre deux ordinateurs sous le nom de HDLC (High-level Data Link Control). C'est la naissance du premier protocole standardisé de niveau liaison. D'autres protocoles moins puissants étaient jusqu'alors utilisés. Ils étaient du type « envoyer et attendre », l'émission d'une trame étant suivie d'une période d'attente de l'acquittement de la part du récepteur. La génération HDLC procède par anticipation : l'attente de l'acquittement n'empêche pas la transmission des trames suivantes.

Pour les besoins de transmission sur les liaisons des réseaux des opérateurs, l'UIT-T a repris un sous-ensemble de la norme HDLC, la partie concernant le mode équilibré. Cette procédure a pris au départ le nom de LAP (Link Access Protocol) et comportait des options particulières. Après des mises à jour en 1980 et en 1984, la procédure a été appelée LAP-B (Link Access Protocol-Balanced). La lettre B peut aussi indiquer le canal B du RNIS. C'est la procédure adaptée au niveau 2 du RNIS pour les canaux en mode circuit de type B. Cette norme a été complétée par le LAP-D (Link Access Procedure for the D-channel), associé au canal D du RNIS. Avant d'examiner plus en détail le protocole LAP-B, indiquons qu'il existe une possibilité normalisée de travailler en mode

multiliaison grâce au multiplexage de plusieurs protocoles LAP-B en mode équilibré sur une seule liaison.

Nous allons analyser le fonctionnement du protocole LAP-B, qui est aussi le protocole le plus courant dans le monde HDLC. Les deux autres protocoles décrits dans HDLC travaillent en mode maître-esclave, ce qui veut dire qu'une extrémité de la liaison dirige l'autre côté. La structure de la trame LAP-B est illustrée à la figure D.1.

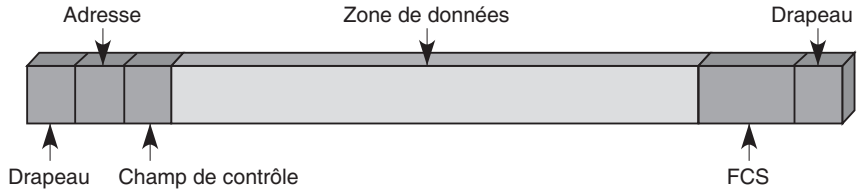


Figure D.1
Trame LAP-B

La trame LAP-B est composée d'une suite d'éléments binaires et d'un drapeau en début et en fin de trame de la forme 01111110.

Pour être certain qu'il n'existe pas de suite identique dans les données transportées, une technique, appelée insertion de 0, a été normalisée. Elle consiste à insérer automatiquement un 0 après cinq 1. Au niveau du récepteur, le 0 est supprimé dès que la valeur binaire 1 est reçue cinq fois de suite et que ces cinq bits sont suivis de la valeur 0. Cette démarche est illustrée dans les quatre transformations suivantes, très faciles à mettre en œuvre :

- 0111110 devient 01111100
- 01111110 devient 111111010
- 01111111 devient 011111011
- 011111110 devient 0111110110

La trame LAP-B comporte également un champ de contrôle et un champ d'adresse.

Les trois types de trames suivants ont été définis :

- trame I (Information) ;
- trame S (Supervision) ;
- trame U (Unumbered, ou non numérotée, ou encore trame de gestion).

Les trames U permettent de mettre en place les mécanismes nécessaires au bon fonctionnement du protocole. Les trames I portent les données provenant de la couche supérieure. Au nombre de trois, les trames S permettent le transport des commandes : la trame RR (Receive Ready) porte les acquittements qui ne sont pas émis dans une trame I, la trame RNR (Receive Not Ready) donne un contrôle de flux de niveau trame en demandant à

l'émetteur de stopper les envois jusqu'à réception d'une nouvelle trame RR spécifiant le même numéro et la trame REJ (Reject) correspond à une reprise sur erreur en cas de détection d'anomalie. La norme HDLC de base offre une quatrième possibilité, la trame SREJ (Selective Reject), qui ne demande la retransmission que de la seule trame en erreur.

Le champ de contrôle du protocole HDLC

Trois structures ont été définies pour le champ de contrôle (*voir tableau D.1*). Elles sont utilisées pour effectuer le transfert de trames d'information, numérotées ou non, de trames de supervision numérotées et de trames de commande non numérotées :

- **Structure de transfert de l'information (trame I).** La trame I permet d'effectuer le transfert de l'information. Les fonctions de N(S) et P/F sont indépendantes, chaque trame I contenant un numéro d'ordre N(S), un numéro d'ordre N(R), qui peut ou non accuser réception d'autres trames I à la station réceptrice, et un élément binaire P/F, qui peut être mis à 1 ou à 0.
- **Structure de supervision (trame S).** La trame S sert à réaliser les fonctions de commande de supervision de la liaison, comme l'accusé de réception, la demande de retransmission ou la demande de suspension temporaire de transmission. Les fonctions de N(R) et P/F sont indépendantes, chaque trame de structure S contenant un numéro d'ordre N(R), qui peut ou non accuser réception d'autres trames I à la station réceptrice, et un élément binaire P/F, qui peut être mis à 1 ou à 0.
- **Structure non numérotée (trame U).** La trame U est utilisée pour effectuer les fonctions de commande de la liaison et pour le transfert d'informations non numérotées. Cette structure ne doit pas contenir de numéro d'ordre mais comprendre un élément binaire P/F, qui peut être mis à 1 ou à 0. Cinq positions d'élément binaire modificateur sont disponibles, ce qui permet de définir jusqu'à 32 fonctions de commande et 32 fonctions de réponse supplémentaires.

Tableau D.1 • Formats du champ de contrôle (les numéros sont exprimés modulo 8)

Format du champ de contrôle	Élément binaire du champ de contrôle							
	1	2	3	4	5	6	7	8
Format I	0	N(S)			P	N(R)		
Format S	1	0	S	S	P/F	N(R)		
Format U	1	1	M	M	P/F	M	M	M

N(S)	numéro de séquence en émission (l'élément binaire 2 = élément binaire de poids faible).
N(R)	numéro de séquence en réception (l'élément binaire 6 = élément binaire de poids faible).
S	élément binaire de la fonction de supervision
M	élément binaire de la fonction de modification
P/F	élément binaire d'invitation à émettre lorsqu'il provient d'une commande ; élément binaire final lorsqu'il provient d'une réponse (1 = invitation à émettre/fin).
P	élément binaire d'invitation à émettre (1 = invitation à émettre)

Paramètres du champ de contrôle de HDLC

Les numéros, ainsi que les autres valeurs transportées dans les champs de contrôle, sont limités par la longueur du champ dans lequel ils sont notés. Si le champ est de 8 bits, la valeur varie de 0 à $2^8 - 1$, c'est-à-dire 255. Plus le champ est grand, plus la numérotation sans repasser par la valeur 0 est longue. La longueur du champ donne le modulo de comptage.

Modulo

Si *a* est un entier quelconque et *n* un entier strictement positif, nous écrivons *a* mod *n* pour représenter le reste dans {0,... , *n* – 1} obtenu en effectuant une division de *a* par *n*. Par exemple, 28 mod 12 = 4. Dans cet exemple, 12 est le modulo de comptage.

Numérotation

Chaque trame I doit recevoir un numéro d'ordre, qui peut prendre des valeurs allant de 0 à modulo – 1, correspondant au modulo de congruence des numéros d'ordre. Le modulo est égal à 8 ou à 128. La numérotation parcourt le cycle complet. Les formats du champ de commandes et réponses de modulo 8 sont indiqués au tableau D.2. Les formats du champ de commande de modulo 128 sont simplement une extension sur 2 octets du champ de contrôle.

Tableau D.2 • Formats du champ de commandes et réponses de modulo 8

Format	Commande	Réponse	Codage								
			1	2	3	4	5	6	7	8
Transfert d'information	I (information)		0	N(S)			P	N(R)		
Contrôle	RR (prêt à recevoir) RNR (non prêt à recevoir) REJ (rejet)	RR (prêt à recevoir) RNR (non prêt à recevoir) REJ (rejet)	1 1 1	0 0 0	0 1 0	0 0 1	P/F P/F P/F	N(R) N(R) N(R)		
Non numéroté	SABM (mise en mode asynchrone équilibré)		1	1	1	1	P	1	0	0
	DISC (déconnexion)		1	1	0	0	P	0	1	0
		UA (accusé de réception non numéroté)	1	1	0	0	P	1	1	0
		DM (mode déconnecté)	1	1	1	1	F	0	0	0
		FRMR (rejet de trame)	1	1	1	0	F	0	0	1

Le nombre maximal de trames I numérotées en séquence dans la station primaire ou secondaire en attente d'acquittement, c'est-à-dire pour lesquelles il n'y a pas eu d'accusé

de réception, ne doit jamais excéder le modulo des numéros d'ordre moins un. Cette restriction empêche toute ambiguïté dans l'association des trames I transmises avec les numéros d'ordre pendant le fonctionnement normal ou pendant les reprises en cas d'erreur.

Le nombre de trames I en attente d'acquittement peut être également limité par la capacité de stockage de la station de données, c'est-à-dire par le nombre de trames I qui peuvent être stockées pour la transmission ou la retransmission en cas d'erreur. Toutefois, le rendement optimal de la liaison ne peut être obtenu que si la capacité minimale de stockage de trames de la station de données est égale ou supérieure au délai de transmission aller-retour.

Variables d'état et numéros d'ordre

Chaque station de données doit maintenir de façon indépendante une variable d'état lors de l'émission V(S) et de la réception V(R) des trames I qu'elle transmet et reçoit :

- **Variable d'état à l'émission V(S).** Désigne le numéro d'ordre de la trame I suivante à transmettre en séquence. Cette variable peut prendre des valeurs comprises entre 0 et modulo – 1, correspondant au modulo de congruence des numéros d'ordre des trames, la numérotation parcourant le cycle complet. La valeur de la variable d'état à l'émission doit être augmentée d'une unité pour chaque trame I consécutive transmise mais ne doit pas dépasser la valeur de N(R) de la dernière trame reçue de plus de modulo moins un.
- **Numéro d'ordre à l'émission N(S).** Seules les trames I contiennent la valeur N(S), qui est le numéro d'ordre à l'émission des trames transmises.
- **Variable d'état à la réception V(R).** Désigne le numéro d'ordre de la prochaine trame I à recevoir en séquence. Cette variable d'état à la réception peut prendre des valeurs comprises entre 0 et le modulo – 1, qui correspond au modulo de congruence des numéros d'ordre des trames, la numérotation parcourant le cycle complet. La valeur de la variable d'état à la réception doit être augmentée d'une unité pour chacune des trames I reçues sans erreur et en séquence, le numéro d'ordre à l'émission N(S) devant être égal à la variable d'état à la réception.
- **Numéro d'ordre à la réception N(R).** Toutes les trames I et S doivent contenir la valeur N(R), qui indique le numéro d'ordre N(S) de la prochaine trame I attendue, à l'exception de la trame de supervision de rejet sélectif (SREJ), l'élément binaire P/F étant dans ce cas à 0. Avant de transmettre une trame I ou S, le N(R) doit être rendu égal à la valeur courante de la variable d'état à la réception. Le N(R) indique que la station transmettant le N(R) a reçu correctement toutes les trames I numérotées jusqu'à N(R) – 1.

Les figures D.2 à D.4 illustrent quelques exemples de fonctionnement du protocole et de la numérotation des trames.

Figure D.2
Transfert des données

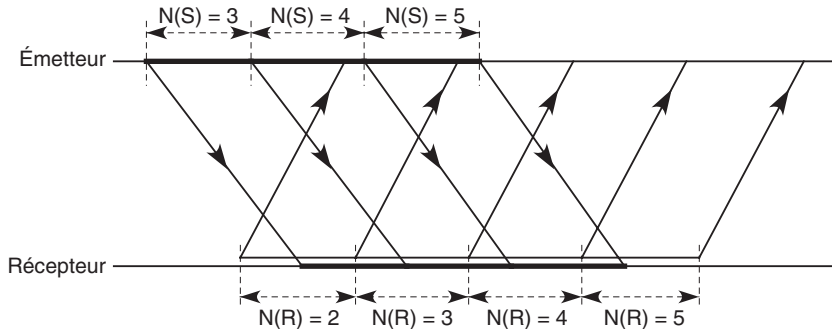


Figure D.3
Acquittements regroupés

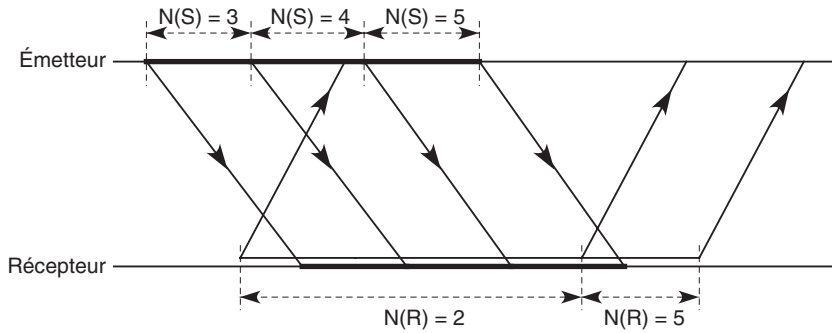
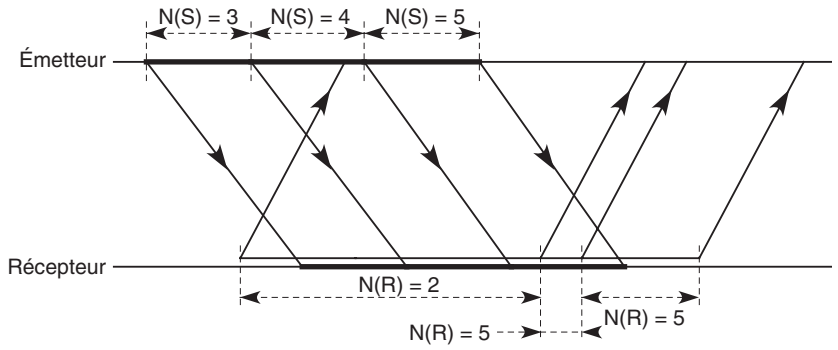


Figure D.4
Acquittements multiples



Commandes du champ de contrôle

Pour fonctionner correctement, le protocole doit émettre et recevoir des ordres de l'autre extrémité. Ces ordres s'exercent par le biais de valeurs, qui sont transportées dans le champ de contrôle. Regardons dans un premier temps les commandes disponibles dans HDLC.

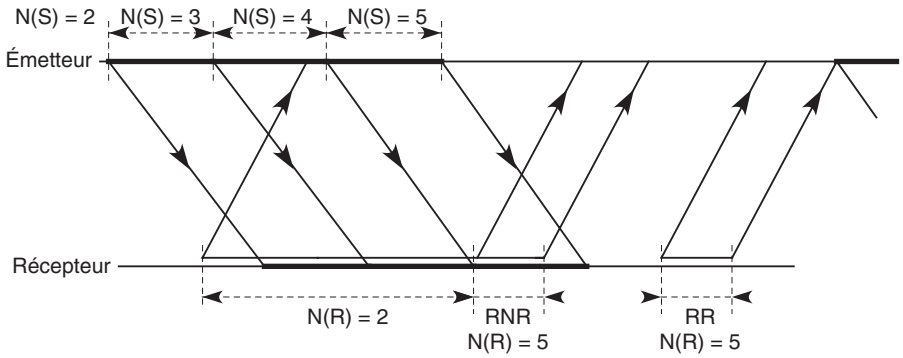
Commande et réponse RR

La trame de supervision RR, ou prêt à recevoir, doit être utilisée par l'émetteur pour indiquer qu'il est prêt à recevoir une trame I ou accuser réception des trames I reçues précédemment et dont le numéro de séquence est inférieur ou égal à N(R) – 1. Une trame RR peut être utilisée pour indiquer la fin d'un état d'occupation qui a été signalé auparavant par l'émission d'une trame RNR par cette même station (émetteur ou récepteur distant). Outre l'indication de l'état de l'émetteur, la commande RR, avec l'élément binaire P positionné à la valeur 1, peut être utilisée par l'émetteur pour demander l'état du récepteur distant.

Commande et réponse RNR

La trame de supervision RNR, ou non prêt à recevoir, est utilisée par l'ETTD (équipement terminal de transmission de données) pour indiquer un état d'occupation, c'est-à-dire une incapacité momentanée à accepter des trames I supplémentaires. La trame RNR accuse réception des trames I dont le numéro de séquence est inférieur ou égal à N(R) – 1. Elle ne doit pas accuser réception de la trame I numérotée N(R), ni d'aucune autre trame I qui pourrait éventuellement être reçue à sa suite, les acceptations de ces trames I étant indiquées dans des échanges ultérieurs. Le fonctionnement de la trame RNR est illustré à la figure D.5. Outre l'indication de l'état de l'émetteur, la commande RNR, avec l'élément binaire P positionné à 1, peut être utilisée par l'émetteur pour demander l'état du récepteur distant.

Figure D.5
Utilisation de la trame RNR



Commande et réponse REJ

La trame de supervision REJ, ou de rejet, doit être utilisée par l'émetteur pour demander la retransmission de trames I numérotées à partir de N(R). La trame REJ accuse réception des trames I dont le numéro de séquence est inférieur ou égal à N(R) – 1. Les trames I suivantes, en attente de transmission initiale, peuvent être transmises à la suite de la ou des trames I retransmise. Pour une liaison donnée, une seule trame REJ peut être émise à la fois. La commande REJ doit être annulée à la réception d'une trame I dont le numéro de séquence N(S) est égal au numéro N(R) spécifié dans la trame REJ.

Une trame REJ peut être utilisée par une station pour indiquer sa sortie d'un état d'occupation qu'elle avait signalé par la transmission antérieure d'une trame RNR. Outre

l'indication de l'état de l'émetteur, la commande REJ, dont l'élément binaire P a la valeur 1, peut être employée par l'émetteur pour demander l'état du récepteur distant.

Erreur sur le numéro de séquence N(S)

Le champ d'information de toutes les trames I reçues par le récepteur dont le numéro N(S) n'est pas égal à la variable d'état en réception V(R) doit être ignoré. Une condition d'exception apparaît lorsqu'une trame I reçue contient un numéro N(S) qui n'est pas égal à la variable d'état en réception. Le récepteur n'accuse pas réception, autrement dit n'incrémente pas sa variable d'état en réception, de la trame I qui a causé l'erreur de séquence, ni d'aucune autre trame I qui pourrait la suivre, avant d'avoir reçu une trame I comportant le numéro N(S) correct.

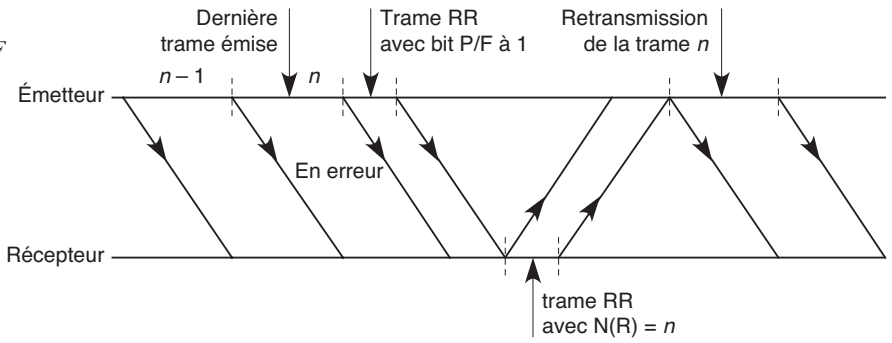
Un récepteur qui reçoit une ou plusieurs trames I comportant des erreurs de séquence ou des trames de supervision RR, RNR et REJ doit accepter l'information de commande contenue dans le champ N(R) et l'élément binaire P ou F afin d'exécuter les fonctions de commande de la liaison. Il doit, par exemple, accepter de recevoir des accusés de réception de trames I précédemment émises par l'émetteur et répondre, l'élément binaire P étant positionné à 1. Les moyens spécifiés ci-après doivent être disponibles pour déclencher la retransmission de trames I perdues ou erronées, suite à l'apparition d'une condition d'erreur sur le numéro de séquence N(S).

Reprise par le bit P/F

La reprise par le bit P/F se fonde sur un cycle de point de reprise. Pour l'ETTD, un cycle de point de reprise commence au moment de la transmission d'une trame de commande, avec l'élément binaire P positionné à 1. Elle prend fin soit lors de la réception d'une trame de réponse avec un élément binaire F positionné à 1, soit lorsque la fonction de temporisation de réponse s'achève, le temporisateur T1 ayant été déclenché au moment de l'émission de la trame comportant le bit P = 1.

Par la transmission d'une trame I, RR, RNR ou REJ avec l'élément binaire P positionné à 1, l'émetteur réclame une réponse sous la forme d'une trame de supervision avec l'élément binaire F positionné à 1. Au moment de la réception de cette trame, il commence la retransmission de toutes les trames I non acquittées et possédant un numéro de séquence inférieur à la valeur qu'avait la variable d'état en émission V(S) au moment où la trame de commande avec l'élément binaire P positionné à 1 a été transmise (*voir figure D.6*).

Figure D.6
Reprise par le bit P/F

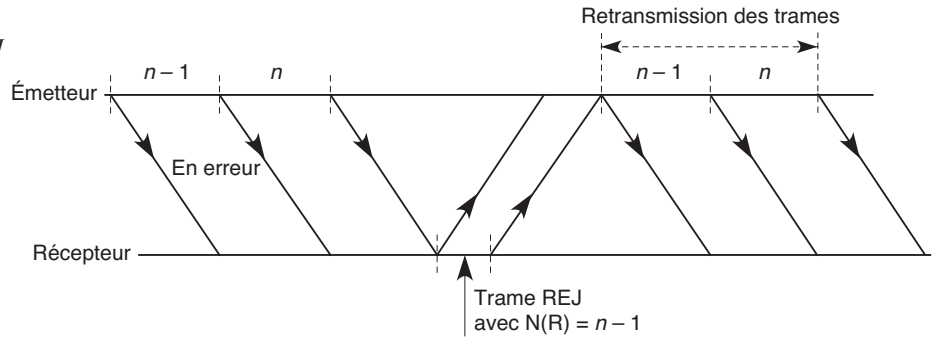


Reprise par REJ

La trame REJ doit être utilisée par un récepteur pour déclencher une reprise, ou retransmission, à la suite de la détection d'une erreur de séquence N(S).

On ne doit établir qu'une seule condition d'exception « REJ envoyée », issue du récepteur à un instant donné. Il faut annuler les conditions d'exception « REJ envoyée » lors de la réception de la trame I requise. Une trame REJ peut être retransmise un nombre de fois déterminé par le protocole, si la condition d'exception de REJ n'est pas annulée par le temporisateur T1 suite à la transmission d'une trame REJ (*voir figure D.7*).

Figure D.7
Reprise par REJ



L'émetteur recevant une trame REJ en provenance d'un récepteur distant déclenche la retransmission séquentielle de trames I, en commençant par celle comprenant le même numéro N(R) que celui contenu dans la trame REJ. Les trames retransmises peuvent comprendre un numéro N(R) et un élément binaire P mis à jour, par conséquent différents de ceux contenus dans les trames I transmises à l'origine. L'ETTD commence la retransmission avant ou pendant la transmission de la nouvelle tranche de commande, avec l'élément binaire P positionné à 1.

La retransmission suite à une trame REJ doit être interdite par l'émetteur dans les deux cas suivants :

- La retransmission de l'ETTD commençant par une trame particulière se produit par l'intermédiaire du point de reprise (*voir plus haut*).
- Une trame REJ est reçue de l'ETCD avant la fin du cycle de point de reprise suivant, cycle qui amorcerait également la retransmission de cette même trame (telle qu'elle est identifiée par le numéro N(R) dans la trame REJ).

Nous décrivons dans la suite de l'annexe quelques trames de gestion (trame U) utilisées en mode LAP-B.

Commandes de mise en mode asynchrone équilibré (SABM) et équilibré étendu (SABME)

La commande non numérotée SABM (Set Asynchronous Balanced Mode) est utilisée pour placer l'ETCD ou l'ETTD appelé dans l'état de transfert de l'information en mode

asynchrone équilibré (LAP-B). Dans ce mode, tous les champs de commandes et de commandes-réponses doivent s'étendre sur une longueur d'un octet.

La commande non numérotée SABME (Set Asynchronous Balanced Mode Extended) a les mêmes fonctions que la commande SABM, mais les champs de commandes et de commandes-réponses numérotées doivent maintenant avoir une longueur de 2 octets, et les réponses non numérotées une longueur de 1 octet.

Commande de déconnexion (DISC)

La commande non numérotée DISC (Disconnect Command) est utilisée par l'ETTD pour demander que prenne fin le mode préalablement établi. Elle sert à informer l'ETCD-ETTD distant, récepteur de la commande DISC, que l'ETTD émetteur de la commande DISC suspend son fonctionnement. Il n'est pas permis d'inclure un champ d'information dans la commande DISC. Avant d'exécuter la commande, l'ETCD-ETTD distant, récepteur de la commande DISC, exprime l'acceptation de la commande DISC en envoyant un accusé de réception non numéroté (UA). L'ETTD émetteur de la commande DISC passe à la phase de déconnexion lorsqu'il reçoit l'accusé de réception UA.

Réponse d'accusé de réception non numérotée (UA)

La réponse non numérotée UA (Unnumbered Acknowledgement) est utilisée par l'ETTD pour accuser réception des commandes non numérotées SABM-SABME et DISC et les accepter. Il n'est pas permis d'inclure un champ d'information dans la réponse UA. L'émission d'une réponse UA doit indiquer la sortie d'un état d'occupation qui avait été signalé auparavant par la même station par l'émission d'une trame RNR.

Réponse en mode déconnecté (DM)

La réponse en mode déconnecté, DM, est utilisée par l'ETTD pour signaler un état dans lequel l'ETTD est logiquement déconnecté de la liaison et se trouve dans la phase de déconnexion. La réponse DM peut être émise dans cette phase pour demander une commande de mise en mode. Si elle est déjà émise, elle peut répondre à la réception d'une commande de mise en mode informant l'ETCD-ETTD distant que l'ETTD se trouve toujours en phase de déconnexion et ne peut exécuter la commande de mise en mode. Il n'est pas permis d'inclure un champ d'information dans la réponse DM.

Réponse de rejet de trame (FRMR)

La réponse FRMR (Frame Reject) est utilisée par l'ETTD pour indiquer une condition d'erreur ne pouvant être récupérée par la retransmission de la trame identique par l'ETCD-ETTD distant. Cela revient à dire que l'une au moins des conditions suivantes qui résultent de la réception d'une trame valide doit être satisfaite :

- Réception d'un champ de commande ou de commande-réponse non défini ou non mis en œuvre.
- Réception d'une trame I dont le champ d'information dépasse la longueur maximale déterminée.

- Réception d'un N(R) non valide.
- Réception d'une trame comprenant un champ d'information qui n'est pas permis ou la réception d'une trame de supervision de longueur incorrecte (comprenant de 32 à 39 éléments binaires inclusivement).

Un N(R) non valide est défini comme un N(R) qui pointe vers une trame I émise auparavant et acquittée ou vers une trame I non encore émise, qui n'est pas la trame I suivante en séquence ou en attente de transmission. Un N(R) valide doit être contenu dans l'intervalle compris entre le numéro de séquence en émission le plus faible N(S) de la ou des trame non encore acquittée et la valeur en cours de la variable d'état en émission de l'ETTD.

Un champ d'information doit être joint à cette réponse et fournir la raison de l'émission de la réponse FRMR. Ce champ suit immédiatement le champ de commande et consiste en 3 octets (fonctionnement de base modulo 8) ou en 5 octets (fonctionnement étendu modulo 128).

LAP-F

Le protocole LAP-F (Link Access Protocol-Frame) est né avec le relais de trames, conçu pour améliorer les performances des réseaux issus de la recommandation X.25 de l'UIT-T. Cette dernière s'étant révélée trop lourde et donc incapable d'accroître les débits, il a fallu en rechercher une simplification.

L'idée mise en œuvre a consisté à supprimer le niveau paquet et à faire redescendre les fonctionnalités de ce niveau dans le niveau trame. Le protocole LAP-B a évolué pour devenir le protocole LAP-F, caractérisée par le remplacement de la zone d'adresse par une zone destinée à accueillir une référence de commutation, le DLCI (Data Link Connection Identifier).

Le champ DLCI de base a été étendu par l'adjonction d'un deuxième octet puis d'un troisième, dans lesquels 6 et 7 bits sont dévolus à l'allongement du champ DLCI. La structure de la trame LAP-F est illustrée à la figure D.8.

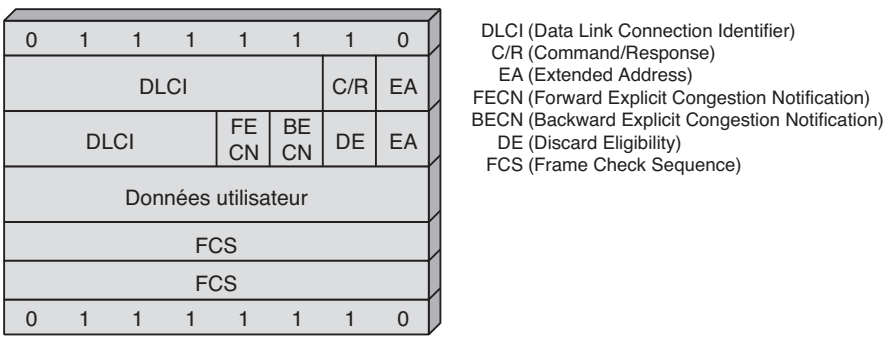


Figure D.8

Structure de la trame LAP-F

Les trames LLC

Les réseaux locaux (LAN) ont des particularités assez différentes des réseaux étendus (WAN). Ils sont d'abord multipoint. Cela revient à dire que toutes les stations peuvent être atteintes à partir d'un coupleur. La prise en compte du multipoint a poussé l'ISO à normaliser un protocole de niveau trame spécifique pour les réseaux locaux. Le travail a été effectué en grande partie par le groupe 802.2 de l'IEEE. La norme correspondante reprise par l'ISO porte la valeur ISO 8802.2 et est appelée LLC (Logical Link Control).

En réalité, il n'y a pas une norme LLC mais trois : LLC 1, LLC 2 et LLC 3, chacune adaptée à un mode de fonctionnement spécifique. Lors de l'élaboration de la norme de base LLC 1, souvent appelée LLC pour des raisons historiques, le faible taux d'erreur résiduelle au sommet de la couche 1 a été pris en compte. Puisqu'il était inutile de mettre en œuvre une technique de reprise sur erreur, la norme LLC 1 n'en possède pas. Enfin, pour prendre en compte plus facilement le multipoint, le protocole est exploité dans un mode sans connexion.

Le protocole LLC 1 est assez simple et comporte peu de fonctionnalités. Une zone de contrôle d'erreur a été introduite dans la trame afin de vérifier que les erreurs sont en nombre négligeable. Lorsqu'une trame en erreur est détectée, elle est détruite, de façon à éviter que des informations erronées soient utilisées. Le taux d'erreur résiduelle peut ne plus être négligeable après ces destructions. Puisque le niveau liaison n'a pas la possibilité d'effectuer les reprises nécessaires, un niveau supérieur de l'architecture doit s'en occuper. C'est le niveau message qui effectue la reprise, et plus spécifiquement le protocole TCP.

La norme LLC 2 est issue d'une constatation simple : si le nombre d'erreur en ligne n'est pas négligeable, plutôt que de repousser le problème de la correction au niveau message (couche 4), il est préférable d'effectuer directement la reprise sur erreur au niveau trame (couche 2). Pour sécuriser l'acheminement des données, la norme LLC 2 spécifie un protocole de niveau trame en mode avec connexion. Avec la reprise sur erreur et le mode avec connexion, LLC 2 dispose de toutes les fonctionnalités de la norme HDLC.

La norme LLC 3 provient d'un constat particulier du monde industriel. Si une trame est erronée et doit être renvoyée, on peut se poser la question de sa validité et de son utilité, surtout si elle est renvoyée après un temps assez long. La procédure LLC 3 est une norme sans connexion, mais avec une possibilité de reprise sur erreur laissée à l'initiative de l'émetteur, qui peut ainsi récupérer les trames dont les temps critiques ne sont pas dépassés.

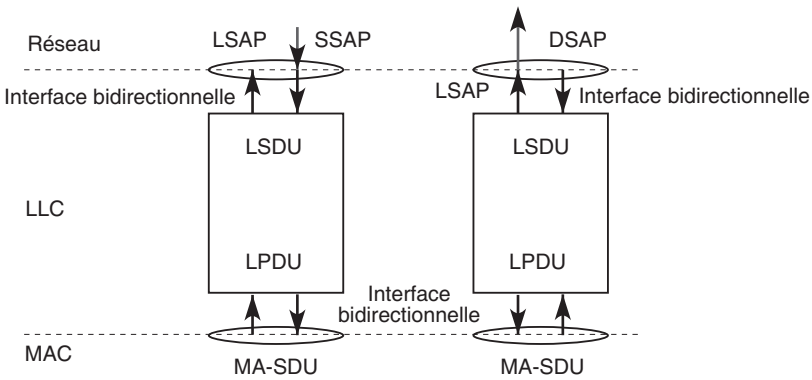
La couche LLC offre un service de niveau paquet, ou couche 3 (ISO 8802.2). Des primitives de service permettent de demander ce service au travers de LSAP (Link Service Access Point).

En mode sans connexion, les extrémités d'une connexion, ou portes d'accès au service, sont désignées de la façon suivante :

- DSAP (Destination Service Access Point), ou point d'accès au service destination.
- SSAP (Source Service Access Point), ou point d'accès au service source, qu'il ne faut pas confondre avec le point d'accès au service de session.

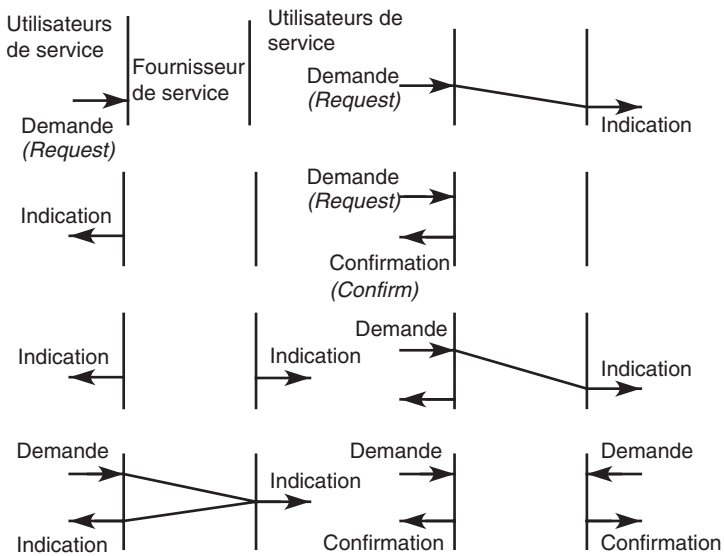
Les interfaces des couches réseau et MAC avec la couche LLC sont illustrées à la figure D.9.

Figure D.9
Interfaces de la couche LLC



Les primitives de contrôle des interactions entre la couche réseau et la couche LLC sont représentées à la figure D.10.

Figure D.10
Primitives de contrôle LLC



Différences entre les normes LLC et HDLC

Les protocoles LLC et HDLC comportent globalement les mêmes normes et les mêmes formats de trame, mais avec les six différences fondamentales suivantes :

- Comme la trame HDLC dans son mode étendu, la trame LLC comporte deux champs d'adresse sur 7 bits (*voir figure D.11*). Le bit supplémentaire du premier octet indique une adresse multipoint ou de diffusion :

  1 : adresse multipoint. Si le champ d'adresse porte la valeur 7, c'est une diffusion.

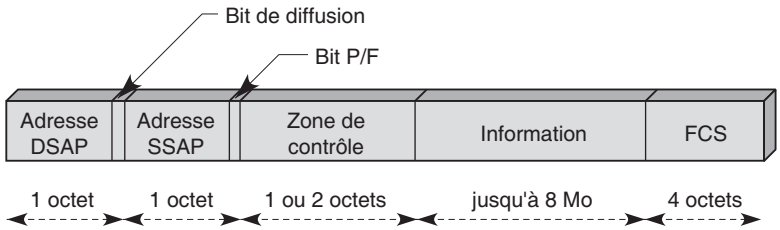
  0 : adresse individuelle. La valeur 0 dans le champ d'adresse indique le service de gestion du niveau MAC.

- Le dernier bit du deuxième octet indique une commande ou une réponse. Il travaille à peu près comme le bit P/F de HDLC :

  1 : indique une réponse.

  0 : indique une commande.

Figure D.11
Format de la trame LLC



- La zone de contrôle est généralement sur deux octets, avec une numérotation des trames sur 7 bits, ce qui permet une anticipation de 127 trames. La numérotation sur 3 bits n'est pas interdite.
- LLC n'utilise que le mode ABM (Asynchronous Balanced Mode), ou mode équilibré. Les trames de gestion SABM et DISC sont utilisées pour établir et libérer la connexion dans le protocole LLC 2. Le mode sans connexion de LLC 1 et LLC 3 supporte la trame de gestion UI.
- Les protocoles LLC se servent d'un multiplexage sur les points d'accès au service MAC.
- Deux trames de gestion spécifiques de LLC 3 ont été définies pour prendre en charge le service avec acquittement, mais sans connexion.

E

Annexe du chapitre 7 (Les niveaux paquet et message)

La première partie de cette annexe détaille l'adressage ISO, qui n'est plus utilisé mais qui sert toujours de modèle pour de nombreuses solutions d'adressage. Elle passe également en revue le protocole X.25, qui a été très important durant les années 1980 et 1990. Les plus grands réseaux du monde ont utilisé ce standard, comme le réseau français Transpac.

La seconde partie de l'annexe détaille de façon plus formelle le niveau message de l'architecture OSI. Elle présente ensuite le standard OSI pour la couche 4, qui n'est plus utilisé, mais qui reste une bonne approche pour comprendre ce que l'on peut attendre d'une couche message. Enfin, nous présentons brièvement l'équivalent de la couche message dans le monde des réseaux ATM.

L'adressage ISO

Donnons tout d'abord quelques définitions de la norme d'adressage ISO de base :

- Une appellation est un identificateur permanent d'une entité.
- Le domaine d'appellation est le sous-ensemble de l'espace d'appellation de l'environnement OSI.
- Le nom de domaine est un sous-ensemble de l'espace d'appellation dans l'environnement OSI. Les couches OSI sont des domaines d'appellation.
- Une appellation locale est une appellation unique à l'intérieur d'un domaine d'application.
- Une appellation globale est une appellation unique à l'intérieur de l'environnement OSI. Elle comprend deux parties : un nom de domaine et une appellation locale.

- Une adresse N est un identificateur indiquant où se trouve un point d'accès à des services N.

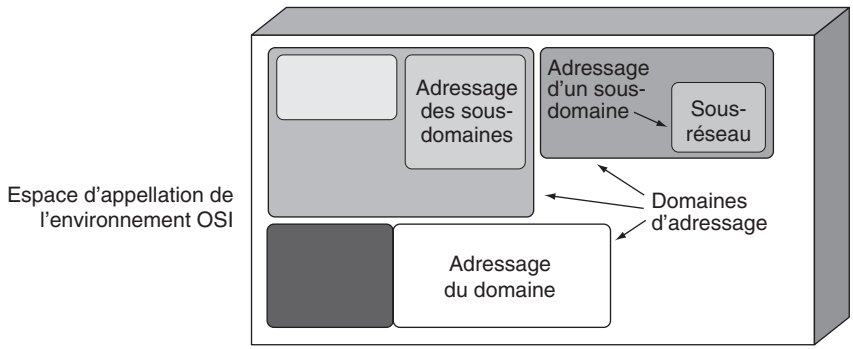
Un suffixe N est un élément d'adresse N unique dans le contexte d'un point d'accès à des services N. Pour que le système d'adressage fonctionne correctement, il faut que chaque utilisateur et chaque application puissent connaître de façon naturelle l'identité des objets à joindre. À cet effet, les entités de niveau réseau et de niveau application peuvent posséder un ou plusieurs nom (appelé titre par les organismes de normalisation). Des correspondances permettent de passer du nom d'une entité au point d'accès qui y mène. Pour obtenir une adresse de niveau N, il faut ajouter un sélecteur ou un suffixe à l'adresse du (N – 1)-SAP sous-jacent (*voir l'annexe A*).

Pour arriver à une concordance de tous ces principes, l'ISO a identifié les besoins suivants :

- définir de manière non ambiguë un ensemble de types pour les objets utilisés dans le contexte de l'OSI ;
- assigner des noms aux occurrences d'objets appartenant à ces types ;
- informer les autres participants des enregistrements effectués.

Pour chacun de ces types, une autorité d'enregistrement, internationale ou nationale, est nécessaire afin de déterminer les noms des objets appartenant au monde OSI. Les autorités d'enregistrement de plus haut niveau sont les organismes de normalisation. La figure E.1 illustre la situation globale des domaines d'adressage.

Figure E.1
Domaines d'adressage



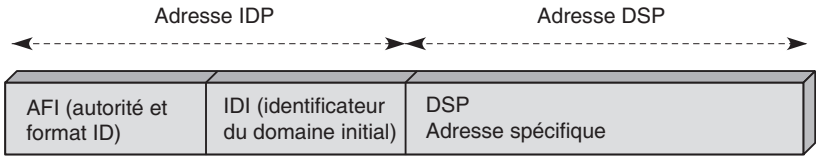
Structure des adresses ISO

La structure des adresses réseau est normalisée dans le document ISO 8348 (additif n° 2). Deux champs sont nécessaires :

- le domaine initial, ou IDP (Initial Domain Part) ;
- l'adresse spécifique, ou DSP (Domain Specific Part).

Cette structure est illustrée à la figure E.2.

Figure E.2
Format des adresses ISO



Le champ IDP est lui-même divisé en deux parties :

- Le champ AFI, qui indique l'autorité et le format utilisé.
- Le champ IDI d'identification du domaine initial. Plusieurs codes sont prédéfinis pour ce champ :

  36 ou 52 indique une adresse d'ETTD selon la norme X.121 (voir plus loin dans ce chapitre), codée en décimal. L'adresse est globale ou locale suivant le suffixe (36 : globale, 52 : locale).

  37 ou 53 indique une adresse d'ETTD selon la norme X.121, codée en binaire.

  38 indique une adresse d'ETCD selon la norme X.121, codée en décimal.

  39 indique une adresse d'ETCD selon la norme X.121, codée en binaire.

  40 ou 54 indique une adresse télex en décimal.

  41 ou 55 indique une adresse télex en binaire.

  42 ou 56 indique une adresse téléphonique en décimal.

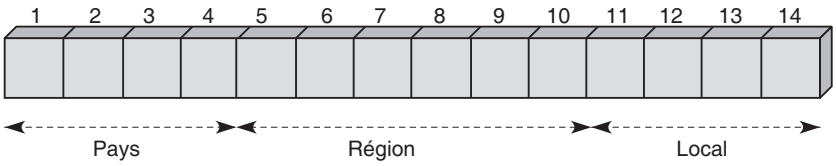
  43 ou 57 indique adresse téléphonique en binaire.

  44 ou 58 indique une adresse RNIS en décimal.

  45 ou 59 indique une adresse RNIS en binaire.

Le sous-adressage utilisé pour les réseaux de données longue distance est normalisé par le document X.121. Ce texte permet de déterminer les valeurs des champs IDP et DSP. La structure de cette adresse est illustrée à la figure E.3. Cette adresse tient sur 14 demi-octets, que nous avons numérotés de 1 à 14 ; deux demi-octets supplémentaires peuvent servir à des extensions. Sur un demi-octet, on peut représenter un chiffre décimal. L'adressage s'effectue dans ce cas sur 14 chiffres décimaux. Il est évident que ce choix est plus pénalisant que si la valeur avait été codée en binaire, prenant ainsi moins de place.

Figure E.3
Structure de l'adressage X.121



Les trois premiers demi-octets contiennent le code d'un pays. Au quatrième demi-octet correspond un numéro de réseau à l'intérieur du pays. Comme les grands pays ont plus de dix réseaux internes, plusieurs numéros sont donnés pour un même pays :

- 310 à 329 pour les États-Unis ;
- 302 à 307 pour le Canada ;
- 234 à 238 pour la Grande-Bretagne ;
- 208 à 212 pour la France.

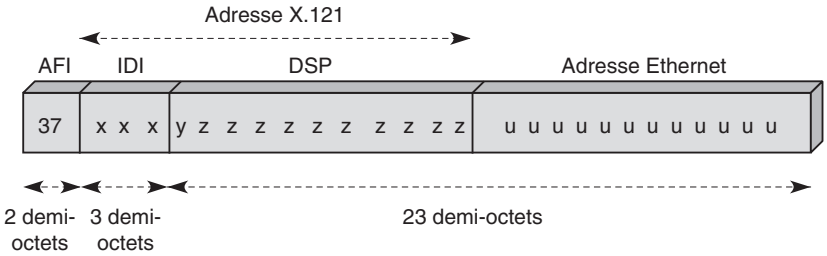
Pour les États-Unis, comme 20 numéros ont été spécifiés, il peut y avoir jusqu'à 200 sous-réseaux directement adressables.

Les demi-octets restants sont affectés à l'adresse dans le pays. Ils peuvent être découpés en deux tranches de 7 et 3 demi-octets, les sept premiers indiquant l'adresse du commutateur auquel le client est rattaché et les trois derniers l'adresse locale.

La figure E.4 illustre l'exemple d'un terminal OSI connecté à un réseau local de type Ethernet que l'on atteint *via* une passerelle connectée à un réseau X.25. L'adresse de ce terminal comporte le champ AFI, le champ X.121 et l'adresse Ethernet.

Figure E.4

Adresse d'un terminal OSI se comportant en ETTD distant



Le protocole X.25

Adopté en septembre 1976 par le CCITT, le protocole X.25, ou ISO 8208, résulte de l'expérience accumulée sur différents réseaux à commutation de paquets. Proposé au départ par quatre grands organismes, les PTT françaises, leur homologue britannique, TCTS (Trans Canada Telephone System) au Canada et Telenet Communication Corps aux États-Unis, il a été implémenté, entre autres, sur les réseaux publics de ces quatre compagnies sous la forme de Transpac, EPSS, Datapac et Telenet.

Les sections qui suivent décrivent en détail les fonctionnalités, la structure et le fonctionnement du protocole X.25.

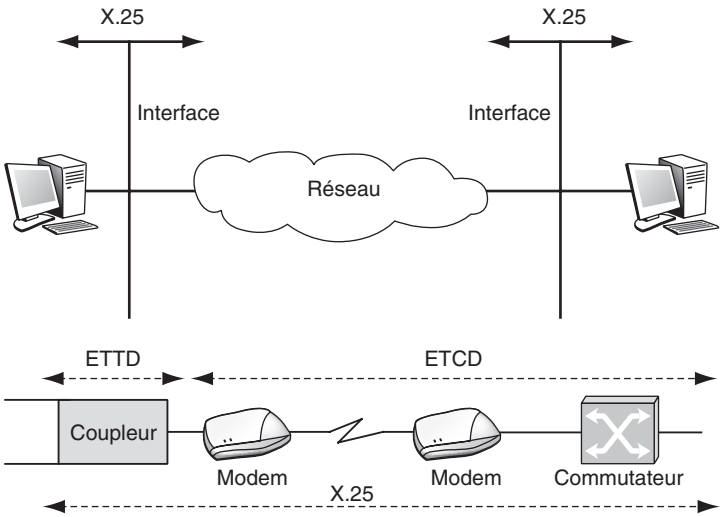
Caractéristiques de X.25

Le protocole X.25 en lui-même contient les trois premières couches de protocole. Le niveau physique provient principalement de la norme X.21. Le niveau trame est constitué par le protocole LAP-B, un sous-ensemble de la norme HDLC, présentée à l'annexe D. Ici, c'est le niveau paquet de la norme X.25 qui nous intéresse.

La recommandation X.25 précise un protocole définissant l'interface entre un ETTD et un ETCD pour la transmission de paquets. X.25 est donc en premier lieu une interface

locale entre un équipement informatique connecté au réseau et le réseau lui-même (*voir figure E.5*).

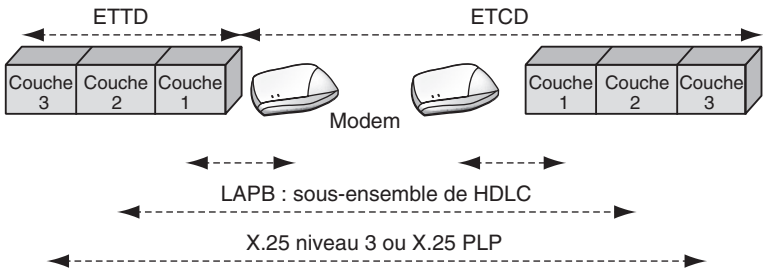
Figure E.5
Implémentation du protocole X.25



La définition de X.25 a été étendue pour prendre en compte des transmissions sur les interfaces soit d'entrée du réseau, entre la machine de l'utilisateur (ETTD) et l'équipement d'accès de l'opérateur (ETCD), soit de la machine de l'utilisateur à la machine distante (ETTD à ETTD).

Les trois premières couches du modèle de référence de l'architecture des réseaux informatiques sont prises en compte par X.25 (*voir figure E.6*).

Figure E.6
Niveaux et couches du protocole X.25

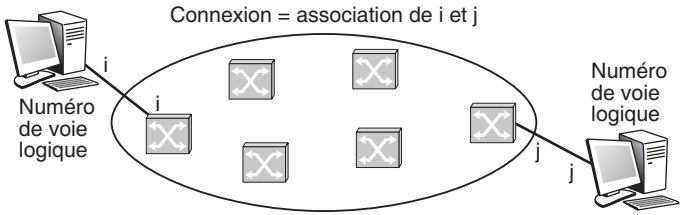


La recommandation X.25 du CCITT définit les types de paquets et leur format mais ne spécifie pas comment certaines informations de contrôle doivent être interprétées. En particulier, la fenêtre de contrôle de flux peut être interprétée au niveau local entre l'ETTD et l'ETCD ou au niveau global entre l'ETTD émetteur et l'ETTD récepteur. Ces imprécisions donnent naissance à des réseaux très différents les uns des autres.

X.25 utilise le mode avec connexion. La connexion est une association bidirectionnelle entre l'émetteur et le récepteur. En plus de cette connexion, l'ensemble des réseaux X.25

utilise un mode circuit virtuel, sans que ce soit une obligation de la norme. De ce fait, X.25 multiplexe sur la couche 2 les circuits virtuels passant par la même liaison. La connexion entre deux adresses extrémité s'exprime par une correspondance entre deux références, appelées voies logiques, comme illustré à la figure E.7.

Figure E.7
Connexion X.25



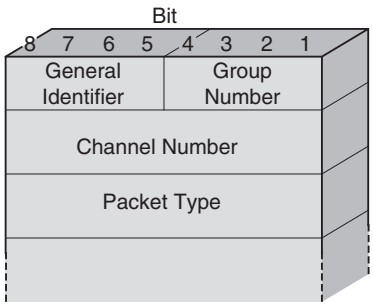
Le niveau paquet de X.25 permet un maximum de 16 groupes de 256 voies logiques entre un ETTD et un ETCD. L'en-tête du paquet contient un champ de 4 bits qui identifie le groupe et un champ de 8 bits pour le numéro de la voie logique. 4 095 voies logiques — la voie 0 joue un rôle particulier — sont donc utilisables sur une entrée. L'ETTD et l'ETCD partagent le même numéro de voie logique lors de la formation de la connexion.

On profite de la mise en place de la connexion pour réaliser un circuit virtuel, qui s'établit lors du routage du paquet d'appel. Ce circuit virtuel est emprunté par l'ensemble des paquets d'un même message. Le numéro de voie logique joue également le rôle d'une référence. L'ouverture du circuit virtuel peut s'accompagner d'allocations de ressources pour assurer le contrôle de flux et garantir le séquencement des paquets dans le réseau.

Format des paquets X.25

Le format général des paquets X.25 se présente sous la forme illustrée à la figure E.8.

Figure E.8
Format des paquets X.25



La zone identificateur de type de paquet (Packet Type) permet de déterminer la fonction du paquet. Elle ressemble à la zone de supervision de HDLC pour le contrôle de la

connexion réseau. Le tableau E.1 répertorie les différents types de paquets rencontrés dans le protocole X.25.

Tableau E.1 • Types de paquets d'un environnement X.25

Type de paquet	Zone identificateur du type de paquet							
	8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
Paquet d'appel/Appel entrant *CALL REQUEST/INCOMING CALL*	0	0	0	0	1	0	1	1
Communication acceptée/Communication établie *CALL ACCEPTED/CALL CONNECTED*	0	0	0	0	1	1	1	1
Demande de libération/Indication de libération *CLEAR REQUEST/CLEAR INDICATION*	0	0	0	1	0	0	1	1
Confirmation de libération *CLEAR CONFIRMATION*	0	0	0	1	0	1	1	1
Paquet de données *DATA PACKET*	X	X	X	X	X	X	X	1
Demande d'interruption *INTERRUPT REQUEST*	0	0	1	0	0	0	1	1
Confirmation d'interruption *INTERRUPT CONFIRMATION*	0	0	1	0	0	1	1	1
Paquet RR *RECEIVE READY*	X	X	X	0	0	0	0	1
Paquet RNR *RECEIVE NOT READY*	X	X	X	0	0	1	0	1
Paquet REJ *REJECT*	X	X	X	0	1	0	0	1
Demande de réinitialisation/Indication de réinitialisation *RESET REQUEST/RESET INDICATION*	0	0	0	1	1	0	1	1
Confirmation de réinitialisation *RESET CONFIRMATION*	0	0	0	1	1	1	1	1
Demande de reprise/Indication de reprise *RESTART REQUEST/RESTART INDICATION*	1	1	1	1	1	1	0	1
Confirmation de reprise *RESTART CONFIRMATION*	1	1	1	1	1	1	1	1
Les bits X indiquent des informations de contrôle contenues dans le champ identificateur.								

Des paquets de diagnostic et d'enregistrement complètent cette panoplie de paquets.

La connexion X.25

La connexion entre deux utilisateurs et le circuit virtuel mis en place pour acheminer les paquets sur cette connexion permettent la circulation des données de contrôle et les informations utilisateur. La figure E.9 illustre les différentes phases de la vie d'un circuit virtuel, que nous explicitons dans les sections suivantes.

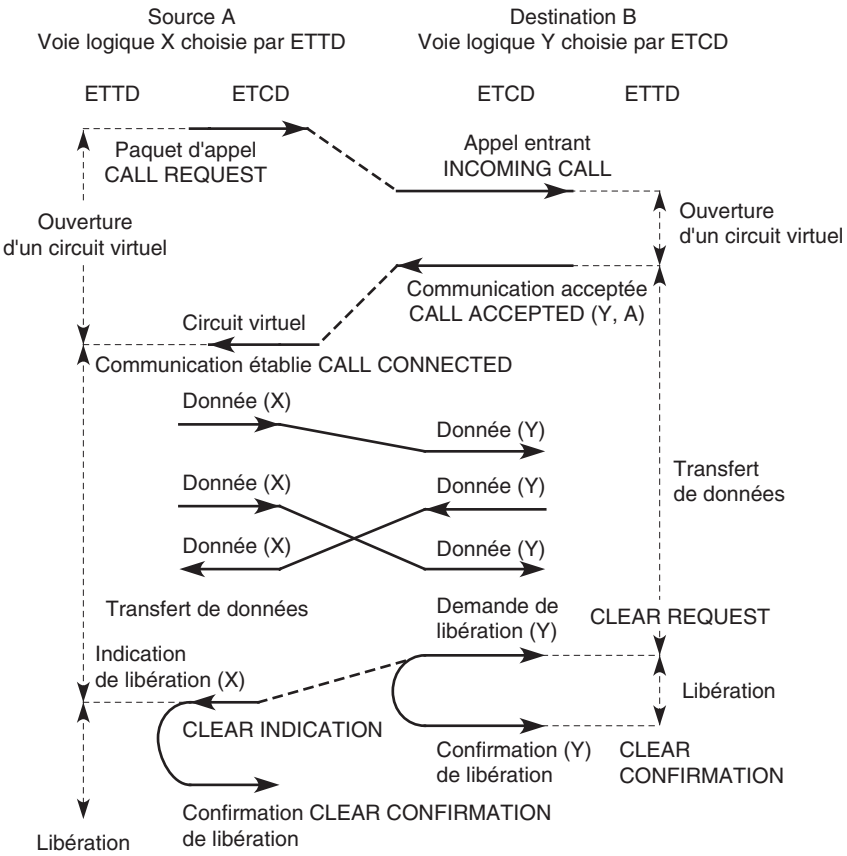


Figure E.9

Phases de la vie d'un circuit virtuel

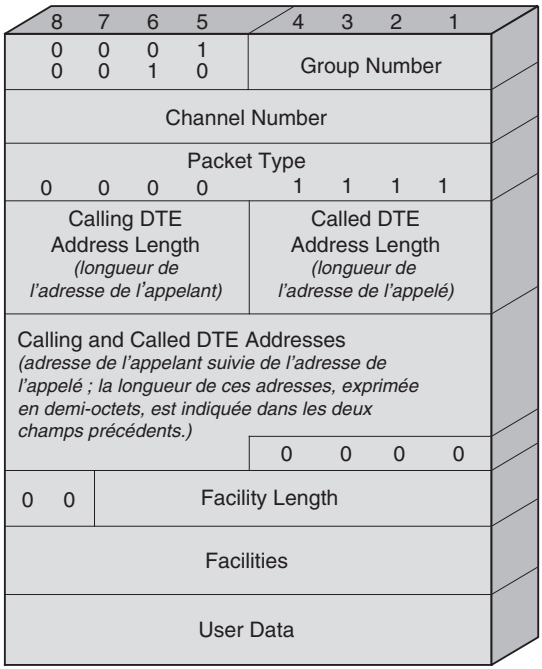
Ouverture et fermeture d'une connexion

Un utilisateur qui veut transmettre des paquets doit au préalable ouvrir une connexion et, en règle générale, un circuit virtuel. Pour ce faire, il émet une demande d'ouverture (CALL REQUEST). Le paquet contient le numéro de la voie logique obtenu par l'utilisateur (le plus grand disponible) et l'adresse réseau des abonnés (demandé et demandeur). Cette dernière est inscrite dans un champ dont la longueur, variable, est spécifiée par un champ

de quatre bits en nombre de demi-octets (*voir figure E.10*). La recommandation X.121 normalise l'adresse sur 14 demi-octets. Comme le champ est de 4 bits, il permet d'obtenir une longueur de 16 demi-octets.

Figure E.10

Paquet d'appel (CALL REQUEST) et appel entrant (INCOMING CALL)



Le paquet contient un premier champ indiquant les options de contrôle du circuit virtuel et un second, de 64 octets au maximum, destiné à l'utilisateur. Ce dernier peut utiliser ce champ pour préciser, entre autres, des adresses complémentaires, si l'adresse du récepteur est un réseau local ou un autocommutateur privé, et des mots de passe.

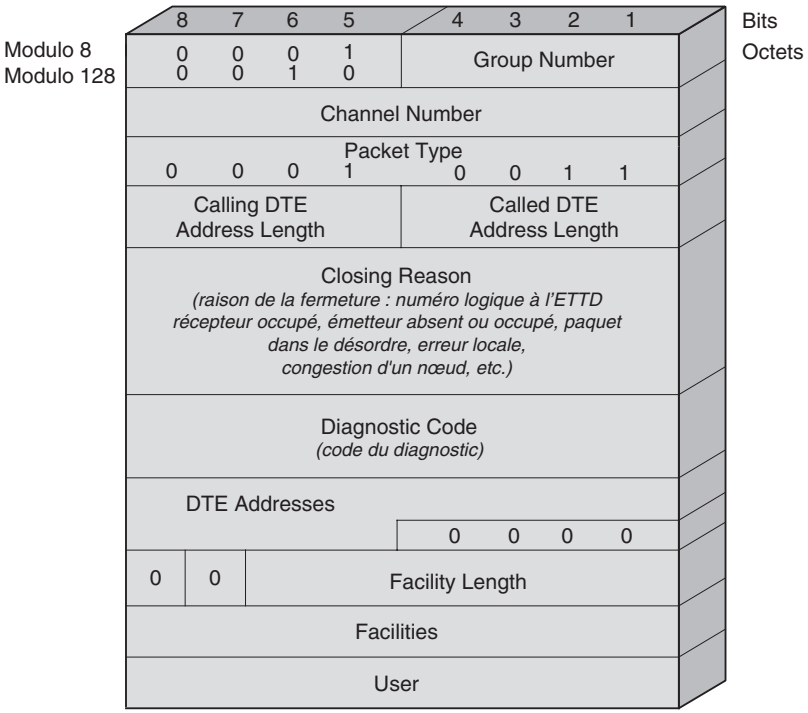
Lorsqu'il arrive à l'ETCD destinataire, le paquet d'appel capte le plus petit numéro de voie logique pour éviter la collision avec une demande d'ouverture de circuit virtuel qui pourrait arriver sur l'ETCD après avoir réservé le même numéro de voie logique sur l'ETTD, la demande entrante étant alors prioritaire. Si le récepteur accepte la communication, il retourne un paquet communication acceptée (CALL ACCEPTED). Sinon, il envoie une demande de libération (CLEAR REQUEST).

L'émetteur ou le récepteur peut mettre fin au circuit virtuel en envoyant une demande de fermeture (DTE INTERRUPT et DCE INTERRUPT), qui est acquittée au niveau local.

Le paquet de libération (DTE INTERRUPT CONFIRMATION et DCE INTERRUPT CONFIRMATION) peut contenir la raison de la demande : numéro logique à l'ETTD récepteur occupé, émetteur absent ou occupé, paquet dans le désordre, erreur locale, congestion d'un nœud, etc. Le format des trames de demande de libération et d'indication de libération est illustré à la figure E.11.

Figure E.11

Format des trames de demande de libération et d'indication de libération

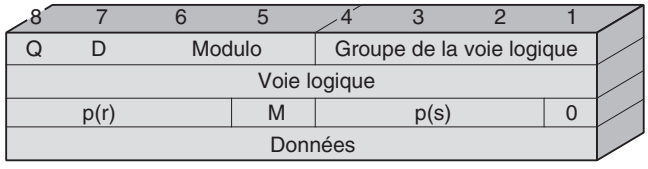


L'octet 5 indique le diagnostic et contient des informations supplémentaires. Les 256 possibilités sont utilisées et sont explicitées dans la norme CCITT ou ISO.

La figure E.12 illustre le format des paquets de données.

Figure E.12

Format des paquets de données



La phase de transfert

Une fois la phase d'ouverture effectuée, le circuit virtuel passe à la phase de transfert des paquets de l'utilisateur. Cette phase se termine par une demande de fermeture, qui démarre la phase de fermeture du circuit virtuel et de la connexion.

Les paquets de données sont transférés sur un circuit virtuel permanent ou commuté. Les numéros p(s) et p(r) servent pour le contrôle de flux. Comme nous l'indiquerons par la suite, il n'est pas précisé dans la norme à quoi s'appliquent les fenêtres : voie logique ou circuit virtuel. La valeur p(s) précise le numéro du paquet envoyé, tandis que p(r) indique le numéro du prochain paquet attendu par le récepteur. Ce dernier autorise l'émetteur à

envoyer plusieurs autres paquets selon l'ouverture de la fenêtre. Bien sûr, l'émetteur et le récepteur gardent en mémoire des numéros v(s) et v(r) analogues à ceux de HDLC.

Le bit Q indique que le paquet transporte des données qualifiées (Qualified Data). L'avis X.25 ne spécifie pas la nature des données qualifiées, mais l'intention sous-jacente est de distinguer les données de l'utilisateur des données de contrôle provenant de la couche supérieure. Si Q = 1, la zone de données transporte des messages de contrôle de la couche 4. C'est une signalisation dans la bande. Ce bit est notamment utilisé pour contrôler les PAD (Packet Assembler Disassembler), qui permettent la connexion de terminaux asynchrones sur un réseau X.25.

Le bit D précise la portée des acquittements. Si D = 0, le contrôle de flux s'effectue localement, et le champ p(r) est positionné par l'ETCD local. Si D = 1, le contrôle de flux est de bout en bout, et p(r) provient de l'ETTD récepteur. Le standard X.25 originel n'autorisait que la valeur D = 0. Plusieurs réseaux internationaux qui ont adopté la norme X.25 ne permettent pas au bit D d'être égal à 1.

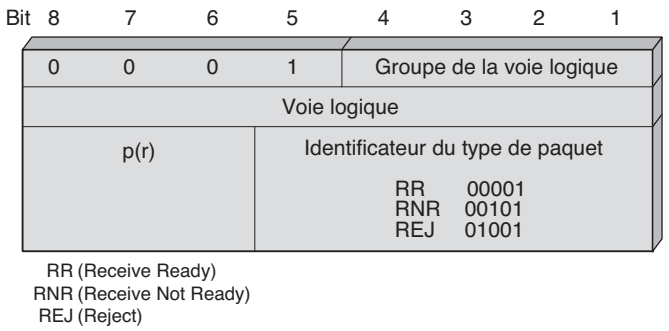
Dans l'identificateur général, les deux bits modulo indiquent le modulo de la séquence des numéros de paquet. Si c'est la suite 01, la numérotation est effectuée modulo 8 ; si la suite 10 est affichée, le modulo est en mode étendu porté à 128. Dans ce dernier cas, le champ de supervision est étendu à deux octets. Le bit M indique, s'il est à 1, que la NPDU fait partie d'une NSDU qui a été fragmentée et qu'il faut regrouper ces données avec celles du paquet précédent. Un 0 indique qu'il s'agit du dernier fragment du message.

La fenêtre qui gère l'avancement des compteurs p(r) et p(s) sert au contrôle de flux, le contrôle des erreurs étant assuré au niveau 2. Cette fenêtre limite le nombre de paquets circulant entre ses deux extrémités. Malheureusement, les extrémités de la fenêtre ne sont pas définies dans la norme, et deux interprétations très différentes régissent les implémentations de X.25. La compréhension de cette fenêtre peut être de bout en bout, c'est-à-dire de l'ETTD émetteur jusqu'à l'ETTD récepteur. Généralement, elle est interprétée comme locale entre l'ETTD et l'ETCD. Le contrôle de flux s'effectue dans ce dernier cas sur la voie logique et non plus sur le circuit virtuel. Les deux extrémités d'un circuit virtuel peuvent être gérées par des fenêtres distinctes, avec des longueurs de paquet différentes.

Les paquets utilisés par le contrôle de flux sont comparables à ceux de HDLC. Il s'agit des paquets RR, RNR et REJ, dont les formats sont illustrés à la figure E.13.

Figure E.13

Format des paquets de contrôle



Le paquet RR (Receive Ready) sert d'accusé de réception lorsque le récepteur n'a rien à transmettre. Il acquitte tous les paquets dont les numéros précèdent p(r). Le paquet RNR (Receive Not Ready) indique que le nœud qui l'envoie ne peut, pour des raisons diverses, recevoir de nouveaux paquets. Ce paquet RNR acquitte tous les paquets précédant celui numéroté p(r). Le récepteur détruit automatiquement tous les paquets qui lui parviennent. L'émetteur attend de recevoir un paquet RR doté du numéro p(r), indiquant que le prochain paquet attendu par le récepteur est celui numéroté p(r), pour reprendre sa transmission. C'est un contrôle de flux de ce type qui est utilisé dans le relais de trames.

Seul l'ETCD utilise le paquet REJ pour demander, à la suite d'un problème, la retransmission de tous les paquets à partir du numéro p(r). En effet, le paquet ne contient pas de bloc de contrôle d'erreur, et l'ETCD ne peut détecter les erreurs qui auraient été laissées par la couche inférieure. Ce sont les erreurs sur les déséquencements ou les pertes de paquets qui sont prises en compte à ce niveau.

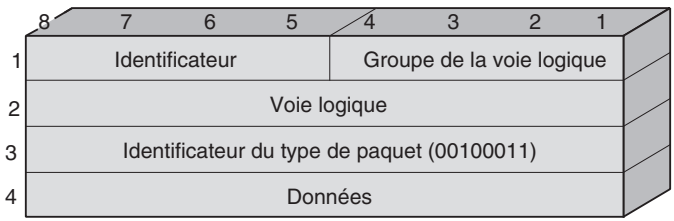
La longueur des paquets est spécifiée au moment de la demande d'ouverture du circuit virtuel. Le maximum recommandé par la norme est de 128 octets, mais les valeurs 16, 32, 256, 512, 1 024 ou même 255 octets sont permises. La longueur peut correspondre à un nombre quelconque d'octet, même non entier, si le tout est inférieur à la longueur maximale. Si la fenêtre de contrôle est locale, le nombre maximal d'octet d'un paquet peut être différent à chacun des bouts. À l'intérieur du réseau lui-même, les paquets peuvent être fragmentés ou réassemblés.

Les paquets de demande d'interruption

Les paquets de demande d'interruption ne sont pas soumis au contrôle de flux et n'ont donc pas de numéro p(s). Ils peuvent être envoyés lorsque la fenêtre de contrôle est atteinte. Ce sont en quelque sorte des paquets prioritaires pouvant transporter un octet de données. La figure E.14 illustre le format de ces paquets.

Figure E.14

Format des paquets d'interruption



Les demandes d'interruption sont acquittées par des paquets de confirmation d'interruption. Une seule demande peut circuler sur la voie logique. Les paquets de confirmation d'interruption comportent seulement 3 octets, et l'identificateur du type de paquet (troisième octet) est 00100111.

Les paquets de réinitialisation et de reprise

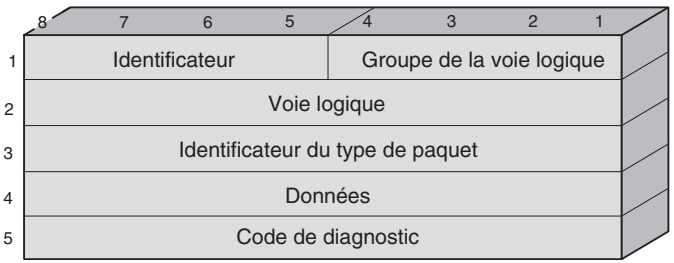
La procédure de réinitialisation permet de remettre le circuit virtuel dans un état connu, et ce dans les deux directions à la fois, c'est-à-dire de l'émetteur vers le récepteur et du

récepteur vers l'émetteur. En outre, elle détruit les paquets et les demandes d'interruption qui pourraient se trouver dans le circuit. Les compteurs p(s) et p(r) sont remis à 0. Une réinitialisation peut être demandée par chacun des deux bouts, généralement suite à une erreur de séquence ou suite à une erreur indiquée par la couche inférieure. Les réinitialisations sont acquittées au niveau local.

La reprise est une réinitialisation de tous les circuits virtuels en parallèle. Le format de ces paquets est illustré à la figure E.15.

Figure E.15

Format des paquets de réinitialisation et de reprise



Le niveau message

L'architecture OSI n'est plus utilisée aujourd'hui, mais l'étude de son niveau message est intéressante à plus d'un titre. Elle donne un exemple de ce que pourrait être un niveau message bien étudié et explicite les fonctionnalités qu'il faut faire entrer dans toute couche complète de niveau 4.

Le protocole de transport doit pouvoir s'adapter à la demande de service de l'utilisateur et à la qualité de service fournie par les trois premières couches de l'architecture. Pour bien comprendre ces caractéristiques, les normalisateurs ont classé les services réseau en trois grandes catégories :

- Le type A représente un service de réseau qui possède un taux acceptable d'erreur résiduelle et un taux acceptable d'incident signalé par la couche réseau. L'exemple classique souvent proposé est celui d'une architecture utilisant le protocole LAP-B, qui garantit généralement que le taux d'erreur résiduelle est bas et acceptable, et le protocole X.25 au niveau réseau, qui assure un taux tolérable d'incident signalé. Cette architecture peut ne pas être classée dans le type A si l'utilisateur demande un service réseau d'une qualité supérieure.
- Le type B est déterminé par un taux acceptable d'erreur résiduelle, mais un taux inacceptable d'incident signalé. Dans cette catégorie, on peut placer un réseau qui posséderait un protocole de niveau trame avec une reprise sur correction d'erreur et un protocole de niveau paquet simplifié, comme IP. Cette architecture peut également se trouver dans une autre catégorie, suivant le service demandé par l'utilisateur.
- Le type C représente les réseaux qui ont un taux d'erreur résiduelle inacceptable. Un réseau qui possède un protocole de niveau trame sans reprise sur erreur dans un réseau

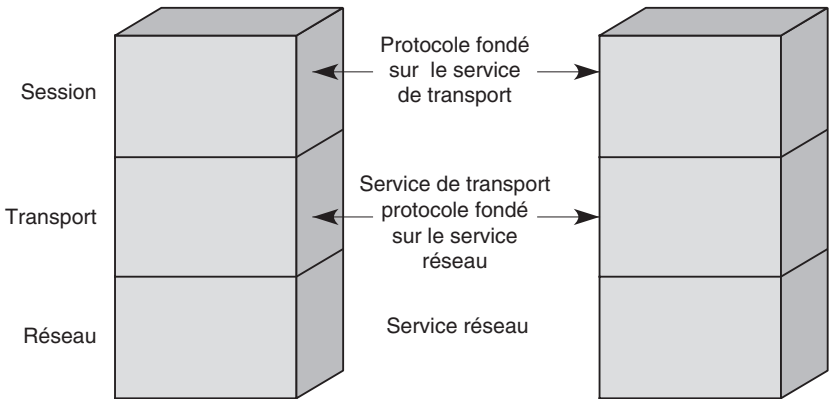
de mauvaise qualité surmonté par un niveau paquet sans possibilité de reprise, comme le protocole IP, peut être classé dans cette catégorie.

Suivant le type du service réseau et la qualité que l'utilisateur souhaite pour le service de transfert, on détermine le protocole de transport à choisir. Le protocole de transport normalisé par l'ISO et l'UIT-T contient cinq classes, numérotées de 0 à 4, qui permettent de s'adapter aux demandes de l'utilisateur.

La relation classique que l'on observe entre la couche transport et les couches situées au-dessus et en dessous est illustrée à la figure E.16.

Figure E.16

Relations entre les couches dans le modèle OSI



La couche transport doit assurer un transfert transparent des données entre utilisateurs du service de transport. Les principales fonctionnalités de ce service sont les suivantes :

- choix d'une qualité de service ;
- indépendance par rapport aux ressources fournies par les trois couches inférieures ;
- contrôle de bout en bout de la communication ;
- adressage du service de transport.

Le protocole AAL

AAL (ATM Adaptation Layer) est un troisième exemple de protocole de niveau message. Il s'agit de la couche d'adaptation à l'ATM, qui se charge de l'interface avec les couches supérieures. Cet étage est lui-même subdivisé en deux niveaux, l'un prenant en compte les problèmes liés directement à l'interfonctionnement avec la couche supérieure et l'autre ceux concernant la fragmentation et le réassemblage des messages en cellules.

Le rôle de cette couche est de transporter de bout en bout des messages dont le format est spécifié, leur taille maximale ne pouvant dépasser 64 Ko, comme dans Internet. Ce bloc doit être découpé en petits fragments de 48 octets pour entrer dans la cellule ATM. Ce découpage peut en fait descendre en dessous de 48 octets, par exemple 47 voire 44 octets, pour récupérer des octets de supervision dans la partie donnée.

Dans la couche AAL, quatre classes de services, 1, 2, 3 et 4, ont été définies, auxquelles correspondent quatre classes de protocoles. Cette subdivision a été modifiée en 1993 par le regroupement des classes 3 et 4 et par l'ajout d'une nouvelle classe de protocoles, la classe 5, qui définit un transport de données simplifié. Enfin, en 2000, la classe 2 a été transformée, ce qui a conduit à la définition de trois classes, 1, 2 et 5 :

- **Classe 1.** Correspond à une émulation de circuit, c'est-à-dire à la mise en place d'un circuit virtuel susceptible de transporter ce qui proviendrait d'un circuit et de redonner en sortie le même circuit. On se sert de cette classe pour transporter la parole téléphonique non compressée. Les opérateurs télécoms classiques ont des protocoles de ce type pour desservir toutes les demandes de circuit.
- **Classe 2.** Correspond au transport d'une information qui serait de type circuit au départ mais que l'on aurait compressée de telle sorte que le débit devienne variable. Cette classe transporte des applications comportant des contraintes de synchronisation, comme la classe A, mais avec un débit variable. On y trouve toutes les applications de parole téléphonique et de vidéo compressée. L'UMTS, en particulier, a choisi cette solution pour le transport de ses voies de parole.
- **Classe 5.** Permet de faire tout transiter sans ajouter de fonction supplémentaire, sauf éventuellement un contrôle d'erreur.

Le niveau message de l'architecture OSI

L'architecture OSI n'est plus utilisée aujourd'hui, mais l'étude de son niveau message est intéressante à plus d'un titre. Elle donne un exemple de ce que pourrait être un niveau message bien conçu et explicite les fonctionnalités qu'il faut faire entrer dans toute couche complète de niveau 4.

Le protocole de transport doit pouvoir s'adapter à la demande de service de l'utilisateur et à la qualité de service fournie par les trois premières couches de l'architecture. Pour bien comprendre ces caractéristiques, les normalisateurs ont classé les services réseau en trois grandes catégories :

- Le type A représente un service de réseau qui possède un taux acceptable d'erreur résiduelle et d'incident signalé par la couche réseau. L'exemple classique souvent proposé est celui d'une architecture utilisant le protocole LAP-B, qui garantit généralement que le taux d'erreur résiduelle est bas et acceptable, et le protocole X.25 au niveau réseau, qui assure un taux également tolérable d'incident signalé. Cette architecture peut ne pas être classée dans le type A si l'utilisateur demande un service réseau d'une qualité supérieure.
- Le type B est déterminé par un taux acceptable d'erreur résiduelle, mais un taux inacceptable d'incident signalé. Dans cette catégorie, on peut placer un réseau qui posséderait un protocole de niveau trame avec une reprise sur correction d'erreur et un protocole de niveau paquet simplifié, comme IP. Cette architecture peut également se trouver dans une autre catégorie, suivant le service demandé par l'utilisateur.
- Le type C représente les réseaux qui ont un taux d'erreur résiduelle inacceptable. Un réseau qui possède un protocole de niveau trame sans reprise sur erreur dans un réseau

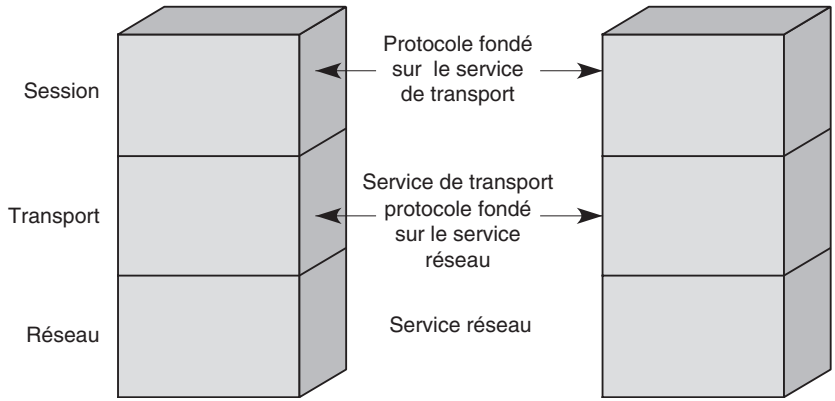
de mauvaise qualité surmonté par un niveau paquet sans possibilité de reprise, comme le protocole IP, peut être classé dans cette catégorie.

Suivant le type du service réseau et la qualité que l'utilisateur souhaite pour le service de transfert, on détermine le protocole de transport à choisir. Le protocole de transport normalisé par l'ISO et l'UIT-T contient cinq classes, numérotées de 0 à 4, qui permettent de s'adapter aux demandes de l'utilisateur.

La relation classique que l'on observe entre la couche transport et les couches situées au-dessus et en dessous est illustrée à la figure E.17.

Figure E.17

Relations entre les couches dans le modèle OSI



La couche transport doit assurer un transfert transparent des données entre utilisateurs du service de transport. Les principales fonctionnalités de ce service sont les suivantes :

- choix d'une qualité de service ;
- indépendance par rapport aux ressources fournies par les trois couches inférieures ;
- contrôle de bout en bout de la communication ;
- adressage du service de transport ;
- possibilité de mettre en place une connexion de transport capable de prendre en charge des TSDU et des TSDU expresses.

La connexion de transport est mise en œuvre classiquement par les primitives DEMANDE DE CONNEXION DE TRANSPORT et RÉPONSE À UNE DEMANDE DE CONNEXION DE TRANSPORT, l'émission des octets de données et enfin les indications de fin de TSDU.

La qualité de service est une des exigences du service de transport. Cette qualité de service, ou QoS, est négociée entre les utilisateurs et le fournisseur du service de transport. Cette négociation s'effectue par l'intermédiaire des primitives DEMANDE, INDICATION, RÉPONSE À UNE DEMANDE et CONFIRMATION DE CONNEXION DE TRANSPORT.

Les paramètres de qualité de service que l'on peut négocier sont les suivants :

- délai d'échec d'établissement d'une connexion de transport ;
- probabilité d'échec d'établissement d'une connexion de transport ;

- débit sur la connexion ;
- temps de transit ;
- taux d'erreur résiduelle ;
- probabilité de rupture de la connexion ;
- probabilité d'incident de transfert ;
- délai de libération de connexion ;
- probabilité d'échec d'une libération de connexion.

Nous allons détailler les trois paramètres les plus importants, à savoir le débit, le temps de transit et le taux d'erreur résiduelle.

Le débit moyen représente la cadence de transfert durant la vie de la connexion. Le débit maximal correspond à la cadence maximale à laquelle la connexion de transport peut prendre en charge les TSDU. La valeur du paramètre débit peut être définie à partir d'une séquence d'au moins deux TSDU arrivées correctement à destination. C'est le nombre d'octet de données utilisateur qui a pu être transféré divisé par le temps qui s'est écoulé entre la première et la dernière DEMANDE DE TRANSFERT DE DONNÉES DE TRANSPORT correspondant aux octets de données. Pour l'autre sens de la connexion, on considère le nombre d'octet de données entre la première et la dernière INDICATION DE TRANSFERT DE DONNÉES DE TRANSPORT. Si l'on se place sur un temps relativement court, correspondant à l'envoi de deux TSDU, on obtient un débit instantané qui peut s'approcher du débit maximal. Au contraire, sur une longue séquence de TSDU, on obtient le débit moyen.

Le temps de transit est le temps qui s'écoule entre une DEMANDE DE TRANSFERT DE DONNÉES DE TRANSPORT et L'INDICATION DE TRANSFERT DE DONNÉES DE TRANSPORT correspondante. Ce temps n'est valable que pour les TSDU dont le transfert s'est effectué correctement. Cette valeur varie énormément suivant les politiques de contrôle de flux et d'acquittement utilisées dans les différents niveaux de protocoles qui doivent être traversés.

Pour obtenir le taux d'erreur résiduelle, il faut calculer le rapport du nombre total de TSDU correctement remises à la couche supérieure sur le nombre total de TSDU transférées puis retrancher ce rapport de 1. Les erreurs peuvent provenir de TSDU perdues, incorrectes ou en surnombre. À partir de cette valeur, on peut déduire la qualité du service rendu. Cette valeur intéresse davantage le fournisseur de services que l'utilisateur. En effet, le taux d'erreur résiduelle classiquement défini est assez différent, puisque c'est le nombre de bit erroné reçu par le destinataire sans qu'il s'en aperçoive. Cette dernière valeur donne à l'utilisateur une idée du nombre d'erreur qui n'a pu être détectée et qui peut perturber le déroulement correct de l'application.

Les unités de données (TPDU) du protocole de transport

- CR (Connection Request) : TPDU de demande de connexion ;
- CC (Connection Confirm) : TPDU de confirmation de connexion ;
- DR (Disconnect Request) : TPDU de demande de déconnexion ;

- DC (Disconnect Confirm) : TPDU de confirmation de déconnexion ;
- DT (Data) : TPDU de données ;
- ED (Expedited Data) : TPDU de données expresses ;
- AK (Data Acknowledge) : TPDU d'accusé de réception de données ;
- EA (Expedited Acknowledge) : TPDU d'accusé de réception de données expresses ;
- RJ (Reject) : TPDU de rejet ;
- ER (Error) : TPDU d'erreur.

Le service de transport en mode avec connexion (ISO 8073 ou X.224)

La norme X.224 du CCITT normalise le service qui doit être rendu par le niveau message. Elle définit les cinq classes de protocoles suivantes, qui s'adaptent aux services rendus par les trois couches inférieures et à la qualité de service éventuellement demandée par l'utilisateur :

- **Classe 0.** Représente le minimum nécessaire à la réalisation d'un service de transport. C'est la classe de base.
- **Classe 1.** Classe de base, à laquelle on a ajouté une reprise sur erreur au cas où celle-ci serait signalée par la couche 3.
- **Classe 2.** Classe de base, à laquelle on a ajouté une possibilité de multiplexage et de contrôle de flux.
- **Classe 3.** Offre les possibilités des classes 1 et 2.
- **Classe 4.** Permet, outre les possibilités précédentes, de détecter les erreurs et d'effectuer les reprises nécessaires pour les corriger.

À ces différentes classes, il faut ajouter les options négociées lors de l'établissement de la connexion.

La classe 0

La classe 0 doit pouvoir, avec un minimum de fonctionnalités, se placer au-dessus du service réseau. C'est la classe de base, qui assure la mise en place des connexions de transport. La connexion de transport correspond, dans ce cas, à la connexion réseau. L'établissement s'effectue grâce à la TPDU CR (Connection Request) et à la TPDU CC (Connection Confirm).

Les TPDU comportent trois paramètres : l'adresse (ID) du point d'accès au service de transport, ou TSAP (Transport Service Access Point), de l'entité appelante, l'adresse (ID) du TSAP de l'entité appelée et la taille de la TPDU proposée. Il n'est pas possible d'avoir quelques octets de données utilisateur. Les données utilisateur sont transportées dans la TPDU DT (Data) *via* la procédure de segmentation-réassemblage.

La libération de la connexion utilise en règle générale les TPDU DR (Disconnect Request) et les DC (Disconnect Confirm). Lorsqu'une extrémité reçoit une INDICATION

DE DÉCONNEXION DE RÉSEAU ou une INDICATION DE RÉINITIALISATION DE RÉSEAU, la connexion de transport est automatiquement libérée. Pour les classes de protocoles de transport autres que 0 et 2, ces indications entraînent l'appel d'une procédure de reprise sur erreur. Le traitement des erreurs de protocole est effectué par la TPDU ER (Error), qui utilise les paramètres CAUSE DU REJET et TPDU NON VALIDE, ainsi que par la TPDU DR (Disconnected Request), qui porte le code de la cause de l'erreur.

Pour établir une connexion de transport, une entité de transport envoie une TPDU CR (Connection Request) à l'autre extrémité, qui répond par une TPDU CC (Connection Confirm). Toutes les informations et tous les paramètres nécessaires au fonctionnement des entités de transport doivent être échangés ou négociés au cours de l'échange des primitives d'ouverture. En particulier, chaque entité de transport choisit une référence sur 16 bits, qui permet d'identifier la connexion de transport. Lorsque la connexion est libérée, on peut geler la référence — pour un certain temps — afin que les TPDU qui n'offrent plus d'intérêt soient ignorées. Les références source et destination permettent de différencier les deux extrémités de la connexion.

Au cours de l'échange d'information, il est possible de recourir aux adresses indiquant les points d'accès au service de transport si les adresses réseau sont insuffisantes. Pour les classes de protocoles comportant un contrôle de flux, la valeur du crédit, c'est-à-dire le nombre de TPDU qui peut être envoyé sans acquittement, est indiquée explicitement. Ce n'est pas le cas dans la classe 0. La négociation de la classe de protocoles est également effectuée au cours de l'ouverture. L'émetteur propose une classe préférée et des classes de repli le cas échéant. La demande et la réponse doivent être compatibles avec les valeurs normalisées récapitulées au tableau E.2.

Par exemple, si la classe préférée est 4 et que la classe de repli soit 3, le récepteur peut choisir entre les classes 4, 3 et 2. Si l'émetteur ne précise aucune classe de repli, le récepteur a le choix entre les classes 4 et 2. Plusieurs classes de repli peuvent être proposées. Si la classe préférée est toujours 4 et que les classes de repli proposées soient 3 et 0, les classes possibles sont 0, 2 et 4, c'est-à-dire l'union des classes possibles correspondant aux classes de repli 0 et 3.

Tableau E.2 • Valeurs des classes de repli normalisées

Format du champ de contrôle	Élément binaire du champ de contrôle							
	1	2	3	4	5	6	7	8
Format I	0	N(S)			P	N(R)		
Format S	1	0	S	S	P/F	N(R)		
Format U	1	1	M	M	P/F	M	M	M

N(S)	numéro de séquence en émission (l'élément binaire 2 = élément binaire de poids faible).
N(R)	numéro de séquence en réception (l'élément binaire 6 = élément binaire de poids faible).
S	élément binaire de la fonction de supervision
M	élément binaire de la fonction de modification
P/F	élément binaire d'invitation à émettre lorsqu'il provient d'une commande ; élément binaire final lorsqu'il provient d'une réponse (1 = invitation à émettre/fin).
P	élément binaire d'invitation à émettre (1 = invitation à émettre)

La taille des TPDU se négocie au cours de la mise en place de la connexion. L'émetteur propose une taille maximale, et le récepteur peut accepter cette valeur ou demander une valeur comprise entre 128 octets et la taille maximale proposée. La taille maximale autorisée est de 8 192 octets, sauf en classe 0, où le maximum est de 2 048 octets. Mis à part la classe 0, pour laquelle seul le format normal est utilisé, de façon à permettre une numérotation de TPDU sur 7 bits, il est possible de choisir le format étendu, qui autorise une numérotation sur 31 bits.

Pour associer les TPDU aux connexions de transport, une procédure définie dans la norme permet d'utiliser des numéros de référence. Toutes les TPDU de toutes les classes de protocoles portent les numéros de référence source ou destination. Les paramètres RÉFÉRENCE DESTINATION et RÉFÉRENCE SOURCE sont utilisés pur cela. Ils identifient la connexion de transport au niveau de l'entité destinataire et de l'entité expéditrice. Pour la classe 0, une connexion de transport correspond à une connexion réseau, et les NSDU sont considérées comme constituant les TPDU, et *vice versa*. Dans les autres classes, des procédures de séparation et de concaténation peuvent être utilisées. Le paramètre RÉFÉRENCE DESTINATION sert à identifier la connexion de transport.

À partir de cet ensemble de fonctionnalités minimales, nous voyons que la classe 0 est apte à fonctionner sur un service réseau complet, puisqu'elle n'apporte aucune fonctionnalité supplémentaire. L'avantage d'une telle solution est son extrême simplicité, qui offre des performances optimales.

La classe 1

Outre les fonctionnalités de la classe de base, la classe 1 ajoute la possibilité de reprise sur erreur et un ensemble de procédures optimisant l'utilisation des ressources sous-jacentes. La connexion de transport s'effectue comme pour la classe 0.

Le transport de données utilise la segmentation et une numérotation des TPDU pour pouvoir effectuer un contrôle de flux ou une reprise sur une TPDU erronée. Dans la TPDU DT, on trouve un paramètre Numéro de TPDU. Cette numérotation s'effectue de façon classique : on ajoute 1 au numéro de la TPDU précédente. Lorsqu'une TPDU est réexpédiée, elle doit avoir le même numéro que la première émise. Dans le cas du format normal, le champ de numérotation demande 7 bits, ce qui permet une numérotation modulo 2^7. Le format étendu requiert un champ de numérotation de 31 bits, ce qui permet une numérotation modulo 2^{31} (cette option n'existe pas dans la classe 0). Grâce à la numérotation, le réassemblage peut être facilement effectué.

La classe 1 permet d'émettre des données expresses. L'envoi d'une TPDU ED (Expedited Data) doit être confirmé par une TPDU d'accusé de réception de données expresses, la TPDU EA (Expedited Acknowledge), qui doit être unique sur la connexion. Les acquittements s'effectuent un à un. La possibilité d'utiliser des données expresses doit être négociée au cours de la mise en place de la connexion. Les libérations des connexions de transport s'effectuent de la même façon que pour la classe 0.

Outre les fonctionnalités décrites dans la classe 0, plusieurs fonctionnalités additionnelles sont disponibles dans la classe 1, notamment les suivantes :

- **Réaffectation après incident.** La réaffectation après incident permet une reprise à la suite d'une déconnexion signalée par le fournisseur du service réseau. Cette procédure s'applique lors d'une indication de déconnexion réseau. Deux temporisateurs sont utilisés :
  - TTR (Time to Try Resynchronization), ou temporisateur d'essai de réaffectation-resynchronisation ;
  - TWR (Time to Wait Resynchronization), ou temporisateur d'attente d'exécution de réaffectation-resynchronisation.

  Le TTR est utilisé par l'entité appelante. Sa valeur maximale normalisée ne peut excéder deux minutes moins la somme du délai maximal de propagation de déconnexion et du temps de transit maximal. Cette valeur peut être indiquée dans la TPDU CR de demande de connexion. La valeur du temporisateur TWR doit être supérieure à la somme de TTR, du délai maximal de propagation de déconnexion et du temps de transit maximal.

  Lorsqu'une indication de déconnexion réseau se présente alors que le temporisateur TTR n'est pas arrivé à échéance, on affecte la connexion de transport à une connexion différente, puisqu'on effectue une procédure de resynchronisation. Si le temporisateur TTR arrive à échéance, on considère que la connexion de transport est libérée.
- **Resynchronisation.** La resynchronisation permet de rétablir l'état normal de la connexion de transport, soit après une réinitialisation, soit à la suite d'une réaffectation. L'une des deux possibilités suivantes est réalisée : si le temporisateur TTR arrive à échéance, la connexion de transport est considérée comme libérée. Dans les autres cas, après avoir armé le temporisateur TTR, il faut, si nécessaire, réexpédier une TPDU CR, DR, ED ou RJ (Reject) ou attendre l'arrivée d'une TPDU avant la fin du temporisateur TWR puis envoyer à ce moment la réponse correcte. Le cas le plus classique est celui de l'envoi d'une TPDU RJ (Reject) dont le paramètre numéro de YR-TU (numéro de séquence en réponse) est celui de la prochaine TPDU attendue.
- **Gel de référence.** Le gel de référence permet de ne pas réaffecter le numéro de référence d'une connexion à une nouvelle connexion de transport tant que des TPDU correspondant à une connexion libérée risquent de circuler.

La classe 2

La classe 2 reprend les caractéristiques de la classe 0 et la plupart de celles de la classe 1, à l'exception des reprises sur erreur signalées à l'aide de la TPDU RJ. Elle permet d'effectuer en outre un multiplexage-démultiplexage et un contrôle de flux explicite.

Le multiplexage-démultiplexage permet à plusieurs connexions de transport d'utiliser la même connexion réseau pour optimiser les ressources des couches sous-jacentes. Pour effectuer le multiplexage, on concatène plusieurs TPDU correspondant à des connexions distinctes en une seule NSDU, qui est transférée par la couche réseau. À l'autre extrémité, on sépare la NSDU en plusieurs TPDU. Les connexions de transport correspondantes sont reconnues par les numéros de référence.

Pour le contrôle de flux, les TPDU sont numérotées dans le format normal (modulo 2^7) ou étendu (modulo 2^{31}). Au cours de l'établissement de la connexion, un crédit est envoyé dans la TPDU CR ou la TPDU CC. Ce crédit, qui peut être égal à 0, donne le nombre maximal de TPDU qu'il est possible de transmettre sans que les acquittements homologues soient arrivés. La fenêtre correspondant à ce crédit est augmentée chaque fois qu'une TPDU AK (Acknowledgement) revient à l'émetteur portant l'acquittement de une ou plusieurs TPDU DT. Dans le cas de la classe 2, la valeur du crédit est fixe et ne peut être modifiée au cours de la vie de la connexion (il en va différemment dans la classe 4).

La classe 3

La classe 3 couvre les possibilités des classes 0, 1 et 2. Nous ne décrivons ici que ses fonctionnalités additionnelles les plus importantes.

Une extrémité de la connexion peut effectuer à tout moment une reprise sur erreur en émettant une TPDU RJ (Reject). Cette TPDU demande à l'autre extrémité de réemettre toutes les TPDU à partir de celle qui est notée mais peut aussi demander de réduire le nombre de crédit alloué à l'autre extrémité ou, ce qui revient au même, de réduire la fenêtre indiquant le nombre de TPDU pouvant être émise vers lui. Le numéro de la trame YR-TU ne peut être qu'égal au plus grand des numéros déjà reçus + 1. Les nouvelles TPDU non en séquence ne sont pas admises, ce qui implique de la part de la couche réseau de remettre les NSDU dans l'ordre.

Dans le cadre du contrôle de flux, une réduction de crédit à travers une TPDU RJ peut engendrer la réception d'une TPDU qui ne se trouve plus dans la fenêtre gérée par l'émetteur. Cette possibilité ne doit pas être considérée comme une erreur de protocole. De même, au cours d'une reprise, des acquittements de TPDU émis avant l'arrivée de la demande de reprise RJ peuvent être pris en compte par l'émetteur, ce qui permet au récepteur de ne retransmettre que les TPDU qui n'ont pas été acquittées correctement.

La classe 4

C'est la classe la plus complète. Elle reprend toutes les fonctionnalités des quatre précédentes et comporte la possibilité de détecter les erreurs et d'effectuer des reprises à partir de cette détection. De même, les TPDU perdues, dupliquées ou hors séquence sont prises en compte dans les opérations de récupération. Des fonctionnalités supplémentaires sont disponibles en cas de défaillance du service réseau. Lors de ces reprises, la classe 4 utilise des procédures spécifiques, qui demandent la mise en place de temporisateurs.

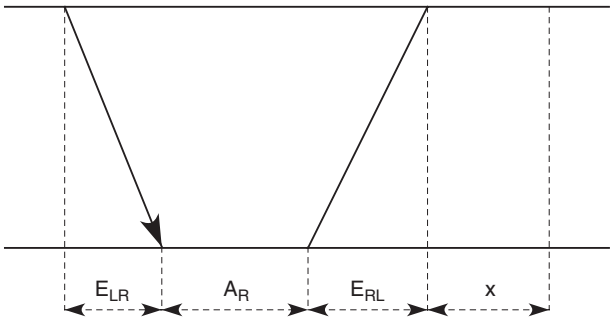
Les paramètres temporels utilisés en classe 4 sont définis dans la norme. Le tableau E.3 récapitule les symboles, noms et définitions exacte de ces valeurs.

Tableau E.3 • Paramètres temporels utilisés en classe 4

Symbole	Nom	Définition
M_{LR}	Durée de vie de NSDU, sens local-distant *(MAXIMUM TRANSIT DELAY)*	Temps maximal pouvant s'écouler entre l'expédition d'une NSDU par une entité de transport locale et la réception d'une copie de celle-ci par une entité distante
M_{RL}	Durée de vie de NSDU, sens distant-local *(MAXIMUM TRANSIT DELAY)*	Temps maximal pouvant s'écouler entre l'expédition d'une NSDU par une entité de transport distante et la réception d'une copie de celle-ci par une entitéde transport locale
E_{LR}	Temps de transit max. prévisible, sens local-distant *(EXPECTED MAXIMUM TRANSIT DELAY)*	Temps de transit acceptable pour l'ensemble des NSDU, à l'exception d'une faible fraction d'entre elles, transmises depuis l'entité de transport locale vers une entité de transport distante
E_{RL}	Temps de transit max. prévisible, sens distant-local *(EXPECTED MAXIMUM TRANSIT DELAY)*	Temps de transit acceptable pour l'ensemble des NSDU, à l'exception d'une faible fraction d'entre elles, transmises depuis une entité de transport distante vers l'entité de transport locale
A_L	Délai d'accusé de réception de l'entité locale *(ACKNOWLEDGEMENT TIME)*	Temps maximal pouvant s'écouler entre la réception par l'entité locale d'une TPDU provenant de la couche réseau et l'expédition de l'accusé de réception correspondant
A_R	Délai d'accusé de réception de l'entité distante *(ACKNOWLEDGEMENT TIME)*	Comme A_L, mais concerne l'entité distante.
T1	Délai de réexpédition de l'entité locale *(LOCAL TRANSMISSION TIME)*	Temps maximal d'attente, par l'entité locale, de l'accusé de réception d'une TPDU avant de réexpédier celle-ci
R	Délai de persistance *(PERSISTANCE TIME)*	Temps maximal pendant lequel l'entité de transport locale continue d'expédier une TPDU avec demande d'accusé de réception.
N	Nombre max. de réexpéditions *(MAXIMUM NUMBER OF TRANSMISSION)*	Nombre maximal de réexpéditions par l'entité de transport locale d'une TPDU avec demande d'accusé de réception.
L	Délai min. de réutilisation d'une référence d'un numéro de séquence *(BOUND ON REFERENCES AND SEQUENCE NUMBERS)*	Temps maximal écoulé entre l'expédition d'une TPDU et l'arrivée d'un accusé de réception de cette TPDU
I	Délai d'inactivité *(INACTIVITY TIME)* Note : ce paramètre est nécessaire pour se protéger des erreurs non signalées.	Délai au terme duquel une entité de transport qui ne reçoit aucune TPDU décide de lancer la procédure de libération pour mettre fin à la connexion de transport.
W	Délai de réexpédition d'informations de contrôle de fenêtre *(WINDOW TIME)*	Temps maximal d'attente d'une entité de transport avant de réexpédier des informations de contrôle de fenêtre actualisées.

Le temporisateur T1 illustré à la figure E.18 est défini par $T1 = E_{LR} + E_{RL} + A_R + x$. Son importance est capitale pour déterminer les performances du protocole. La valeur x, qui a été ajoutée dans T1, représente le délai de traitement local d'une TPDU. Le délai A_R dépend de la discipline d'acquittement des TPDU et du fonctionnement du récepteur. E_{LR} et E_{RL} représentent les délais de propagation aller-retour.

Figure E.18
Fonctionnement du temporisateur T1



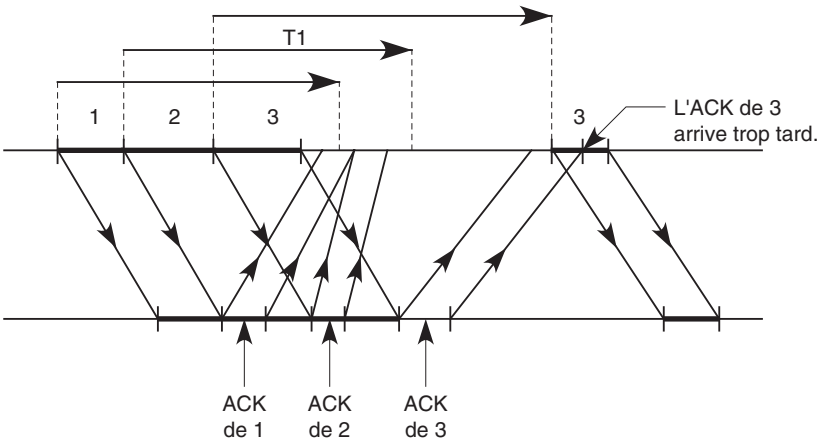
Comme dans la classe 4, on suppose que le taux d'erreur résiduelle est inacceptable. Chaque TPDU non acquittée est retransmise à l'échéance du temporisateur T1. On n'utilise pas d'acquittement négatif, puisqu'il n'est pas certain que les acquittements négatifs arrivent effectivement à l'émetteur.

Fonctionnement du temporisateur T1

On peut utiliser le temporisateur T1 de deux façons différentes :

- À chaque TPDU, on associe un temporisateur T1 au moment de son émission. À expiration de ce délai, la TPDU est réémise et le temporisateur T1 réinitialisé. Ce cas de figure est illustré à la figure E.19.

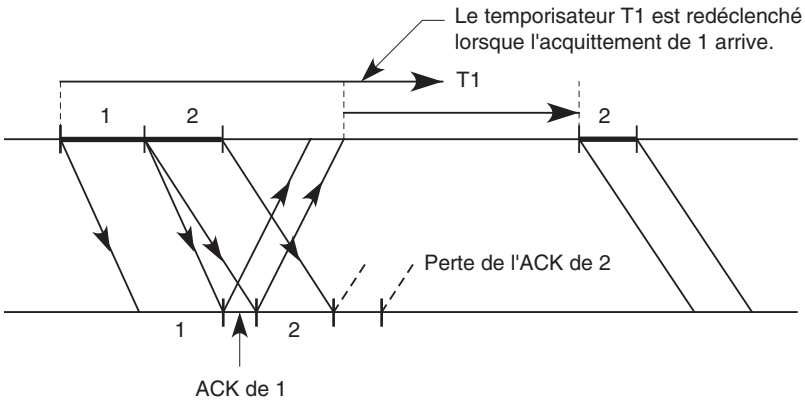
Figure E.19
Exemple où la TPDU 3 est réémise à la suite de l'échéance du temporisateur T1



- Un seul temporisateur est associé à la connexion de transport. Lors de l'émission d'une TPDU, le temporisateur T1 est armé s'il ne l'est déjà. S'il est en cours, l'émission d'une TPDU ne modifie rien. À réception d'un acquittement attendu, le temporisateur T1 est réarmé. Il est arrêté lors de la réception de la dernière TPDU attendue. Lorsque le temporisateur arrive à échéance, les TPDU non acquittées sont réémises. Ce cas de figure est illustré à la figure E.20.

Figure E.20

Reprise sur le temporisateur T1 lorsque celui-ci est affecté à une connexion de transport



La première solution permet de réémettre plus rapidement des TPDU erronées ou perdues mais exige davantage du logiciel, qui doit gérer autant de temporisateurs que de TPDU émises.

Un délai de persistance, R, est également utilisé : c'est le temps maximal pendant lequel l'entité de transport locale continue de réémettre les TPDU non acquittées. Si *N* émissions est la valeur que l'on se fixe pour arrêter les retransmissions d'une même TPDU, on prend R = *N* T1 + X, où X est une valeur fixe à déterminer localement et qui tient compte des délais internes pour réémettre la TPDU après expiration du temps T1.

La valeur de T1 est difficile à déterminer puisque l'émetteur peut avoir du mal à connaître la politique d'acquittement des TPDU. L'entité distante peut très bien attendre le temps A_R avant d'émettre l'acquittement, mais elle peut aussi le faire immédiatement. De plus, les temps de transit peuvent être très différents suivant le parcours des TPDU sur la connexion réseau. Enfin, le contrôle de flux du service réseau peut générer une attente de la TPDU dans l'émetteur local lorsque le temporisateur T1 arrive à échéance. Il est donc très difficile de contrôler le temps passé dans les logiciels exécutés sur les machines terminales.

Les TPDU de classe 4 peuvent porter une zone de détection d'erreur, appelée total de contrôle, mais ce n'est pas une obligation. L'algorithme qui est déroulé peut être adapté au type d'erreur attendu sur les connexions de transport. La norme définit l'algorithme ci-après, dont les paramètres sont transportés par les TPDU CR et DT. La valeur *L* représente le nombre d'octets de la TPDU et a_i la valeur de l'octet de position *i*.

Le premier octet du total de contrôle b_1 est déterminé par :

$$\sum_{i=1}^{L} a_i + b_1 = 0 \text{ (modulo 255)}$$

Le second octet du total de contrôle b_2 est déterminé par :

$$\sum_{i=1}^{L} i a_i + b_2 = 0 \text{ (modulo 255)}$$

Cette technique de détection d'erreur est extrêmement simple et peut être implémentée sans difficulté dans l'entité de transport. En revanche, elle ne détecte pas l'insertion de 0 en fin de TPDU.

La classe 4 se distingue encore par des échanges d'information supplémentaires lors de l'ouverture de la connexion. Comme pour les classes 1, 2 et 3, 32 octets de données utilisateur peuvent être transportés. Le délai d'accusé de réception, ainsi que les paramètres du total de contrôle et la possibilité d'ajouter des paramètres de sécurité définis par l'utilisateur sont transportés lors de l'ouverture.

Les tableaux E.4 et E.5 récapitulent les mécanismes utilisés dans le protocole X.224. Le tableau E.4 décrit certains éléments de procédure qui ne sont pas repris en détail au tableau E.5. Ce dernier précise, pour les cinq classes du protocole X.224, les mécanismes disponibles.

Le tableau E.6 recense les TPDU valides pour chaque classe et le code des TPDU. La suite *xxxx* est indique la valeur du crédit pour les classes 2 à 4. Cette valeur est de 0000 pour les classes 0 et 1. La suite *zzzz* indique la valeur du crédit en classes 2 à 4. Cette valeur est de 1111 en classe 1.

Tableau E.4 • Éléments de procédure disponibles dans les diverses classes X.224

x	Procédure faisant partie de la classe
m	Procédure négociable, mais dont l'équipement doit toujours permettre la mise en œuvre.
0	Procédure négociable, dont la possibilité de mise en œuvre par l'équipement est optionnelle.
ao	Procédure négociable, dont la mise en œuvre par l'équipement est optionnelle et dont l'utilisation dépend de sa disponibilité de la part du service de réseau.
(1)	Non applicable en classe 2 quand l'option Non utilisation du contrôle de flux explicite a été choisie.
(2)	L'utilisation du multiplexage peut conduire à une dégradation de la qualité du service dans le cas où l'option Non utilisation du contrôle de flux explicite a été choisie.
(3)	Cette fonction est offerte en classe 4 mais utilise des procédures différentes de celles qui ont été décrites dans le texte.

Tableau E.5 • Affectation des éléments de procédure dans chaque classe X.224

Mécanisme de protocole	Variante				
	0	1	2	3	4
Affectation à une connexion réseau	x	x	x	x	x
Transfert de TPDU	x	x	x	x	x
Segmentation et réassemblage	x	x	x	x	x
Concaténation et séparation		x	x	x	x
Établissement de connexion	x	x	x	x	x
Refus de connexion	x	x	x	x	x
Libération normale (implicite)	x	x	x	x	x
Libération sur erreur (explicite)	x	x	x	x	x
Association de TPDU à des connexions de transport	x	x	x	x	x
Numérotation de TPDU DT Normale Étendue		x	m(1) 0(1)	m 0	m 0
Données exprès Normale réseau Étendue réseau		m ao	x(1)	m	m
Réaffection après incident		x		x	(3)
Rétention jusqu'à accusé de réception de TPDU Confirmation réception AK	ao m		x	x	
Resynchronisation		x		x	(3)
Multiplexage et démultiplexage			x(2)	x	x
Contrôle de flux explicite			m	x	x
Total de contrôle					m
Gel de référence		x		x	x
Retransmission après temporisation					x
Remise en séquence					x
Détection d'inactivité					x
Traitement d'erreurs de protocole	x	x	x	x	x
Éclatement et recombinaison					x

Tableau E.6 • Codes des TPDU X.224

TPDU	0	1	2	3	4	Code
CR (Connect Request) : demande de connexion	x	x	x	x	x	1110 xxxx
CC (Connect Confirm) : confirmation de connexion	x	x	x	x	x	1101 xxxx
DR (Disconnect Request) : demande de déconnexion	x	x	x	x	x	1000 0000
DC (Disconnect Confirm) : confirmation de déconnexion		x	x	x	x	1100 0000
DT (DaTa) : données	x	x	x	x	x	1111 0000
ED (Expedited Data) : données exprès		x	NF	x	x	0001 0000
AK (data AcKnowledge) : accusé de réception de données		NRC	NF	x	x	0110 zzzz
EA (Expedited data Ack) : accusé de réception de données exprès		x	NF	x	x	0010 0000
RJ (ReJect) : rejet		x		x		0101 zzzz
ER (TPDU Errror) : erreur de TPDU	x	x	x	x	x	0111 0000

NF : non disponible quand l'option Non utilisation du contrôle de flux explicite a été adoptée.
NRC : non disponible quand l'option Confirmation de réception a été adoptée.

F

Annexe du chapitre 8 (Les réseaux de niveau physique)

Cette annexe revient sur la transmission des trames ATM et sur les supports physiques qui ont été fortement utilisés sur les supports plésiochrones. Elle aborde ensuite une interface de signalisation du monde de la fibre optique avant de terminer par la technique PON (Passive Optical Network), qui est utilisée par de nombreux grands opérateurs sur la boucle locale.

Transmission des trames ATM

La transmission de trames ATM illustre ce qui se passe dans la couche 2 lorsque la longueur de la trame est constante. La trame ATM est également appelée *cellule* pour bien dénoter ce cas particulier. L'en-tête des cellules contient une zone de 1 octet ayant pour rôle de protéger les 4 octets de supervision précédents. Il s'agit de la zone HEC (Header Error Control). Elle permet de détecter les erreurs de transmission et d'effectuer automatiquement la correction si le nombre d'erreur est limité à un. Lorsque les erreurs arrivent de façon aléatoire, la plupart du temps avec une probabilité très faible, le taux d'erreur est excellent. Il arrive que le taux d'erreur s'emballe lorsqu'une forte perturbation des signaux en cours de transmission se produit dans un laps de temps très court, générant une succession de cellules en erreur. C'est la raison pour laquelle on préfère, dès que l'on découvre plus de deux erreurs sur une même cellule, que le HEC devienne détecteur plutôt que correcteur de l'erreur, puisqu'il y a toutes les chances pour que la zone d'information soit erronée.

Le HEC permet également de délimiter des cellules. Le récepteur est constamment à la recherche des 4 octets, correspondant à la zone HEC. Dès qu'il trouve une séquence

qui satisfait le HEC, il vérifie que les zones correspondantes des cinq cellules suivantes sont également correctes. Si tel est le cas, le récepteur passe en mode synchronisé. S'il ne réussit pas à cadrer le HEC avec les cinq cellules suivantes, il reste dans un état non synchronisé. Il faut sept détections consécutives d'erreur pour considérer que le cadrage est perdu. Les valeurs 5 et 7 sont valables pour une transmission synchrone. Pour une transmission asynchrone, ces valeurs sont définies respectivement à 6 et 8.

L'adaptation au débit synchrone de la liaison permet de synchroniser les horloges de l'émetteur et du récepteur, de sorte que les bits émis à la vitesse de l'horloge de l'émetteur puissent être récupérés exactement au bon moment par le récepteur. Ces deux fonctions dépendent du support physique utilisé pour transmettre la trame.

L'acheminement des cellules ATM par l'intermédiaire de trames SONET ou SDH est surtout réservé aux opérateurs et aux grands réseaux. Deux solutions s'imposent actuellement : celle du transport des trames sur les lignes exploitées par les opérateurs et celle fondée sur le transport direct de la trame sur le support physique, sans aucune trame sous-jacente. La solution la plus simple pour une mise en œuvre rapide consiste à utiliser des liaisons PDH (Plesiochronous Digital Hierarchy). En Europe, il est possible d'acheminer les cellules sur des liaisons à 2 et 34 Mbit/s, suivant les recommandations G.804 et G.832 de l'UIT-T. Les cellules sont insérées dans le corps des trames qui circulent toutes les 125 µs. Un adaptateur est nécessaire à cette insertion afin d'ajuster la transmission des cellules à la vitesse de l'interface et à insérer des cellules vides pour maintenir la synchronisation.

L'interface standard de l'ATM

Le standard le plus classique de l'ATM correspond à un débit de 155 Mbit/s. Grâce au codage 8B/10B, qui utilise 10 bits pour transporter 8 bits de l'utilisateur, le débit peut atteindre 194,4 Mbit/s. La gestion du support physique est effectuée par des cellules OAM (Operation And Maintenance). On trouve une cellule de gestion après vingt-six cellules d'information transmises par l'émetteur. Le débit réel ATM descend de ce fait à 149,76 Mbit/s.

Les supports plésiochrones

Pour parvenir au multiplexage simultané de plusieurs paroles téléphoniques sur un même circuit, les Américains ont adopté un standard permettant de multiplexer 24 voies de 64 Kbit/s sur un support à 1 544 Kbit/s. Ce canal est nommé DS-1. Les Européens ont répondu à cette technique par le canal E-1, un multiplexage de 30 canaux de parole sur un support à 2 048 Mbit/s. À partir de ce multiplexage de base, toute une hiérarchie a été définie, qu'elle soit multiple du canal de base, comme dans le cas européen, ou un peu plus complexe, comme dans le cas américain, en raison d'une zone de supervision dépendant du débit.

Ces hiérarchies sont appelées PDH (Plesiochronous Digital Hierarchy). La hiérarchie européenne est la suivante :

- E-1 = 2 Mbit/s
- E-2 = 8 Mbit/s
- E-3 = 34 Mbit/s
- E-4 = 140 Mbit/s
- E-5 = 565 Mbit/s

La hiérarchie américaine est assez semblable mais moins régulière. Elle ne correspond pas à un multiple du canal de base, car les bits de synchronisation ne sont pas proportionnels au nombre de voies transportées. La racine *plesio* de *plesiochronous* vient du grec et signifie presque.

Les supports physiques étant passés en mode numérique, une hiérarchie spécifique a dû être développée sous le nom de SDH (Synchronous Digital Hierarchy) en Europe et de SONET (Synchronous Optical Network) en Amérique du Nord. Cette nouvelle hiérarchie prend toujours en compte la numérisation de la parole avec un échantillonnage toutes les 125 µs, mais elle est complètement synchrone. Une trame, d'une longueur dépendant de la vitesse, est émise toutes les 125 µs. SONET et SDH sont les deux techniques utilisées pour acheminer des transmissions numériques aussi différentes que la parole et les données. Cette technique peut donc transporter tous les types de paquets ou de trames, trame ATM, paquet IP, trame Ethernet, etc.

SONET est une interface standardisée par l'ANSI (American National Standards Institute), l'organisme de normalisation nord-américain. Son rôle était au départ d'introduire un très grand nombre de voies téléphoniques sur un même support physique de façon à relier entre eux les réseaux de deux opérateurs.

SDH est une généralisation de SONET normalisée par l'UIT-T, qui donne une définition de la zone de données qui traverse l'interface beaucoup plus précise que celle introduite dans SONET. Cette zone de données porte le nom de *container*.

La hiérarchie plésiochrone

Le standard PDH, en français hiérarchie plésiochrone, c'est-à-dire presque synchrone, a été défini par les organismes de normalisation s'occupant du téléphone pour faire transiter simultanément sur une même ligne physique plusieurs voies téléphoniques. Les termes « presque synchrone » indiquent que cette hiérarchie travaille en synchrone. Cependant, l'instant de départ de la communication est asynchrone. En d'autres termes, la communication est synchrone, une fois l'instant de départ décidé.

Des canaux de différents débits ont été définis :

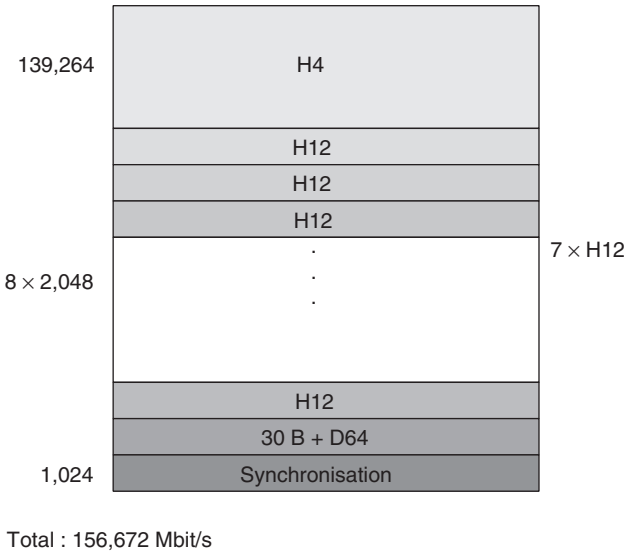
- B : canal circuit à 64 Kbit/s, qui correspond à une voie téléphonique.
- H_0 : canal circuit à 384 Kbit/s, ce qui représente une superposition de 6 canaux B.
- H_{11} : canal circuit à 1 472 Kbit/s, c'est-à-dire une superposition de 23 canaux B.
- H_{12} : canal circuit à 1 920 Kbit/s, c'est-à-dire une superposition de 30 canaux B.
- H_2 : canal à 6,312 Mbit/s ou 8,448 Mbit/s.
- H_3 : canal à 32,064 Mbit/s ou 34,368 Mbit/s ou 44,736 Mbit/s.

- H_4 : canal à 97,728 Mbit/s ou 139,264 Mbit/s.

Une autre solution, qui a été développée sans être normalisée, consiste à superposer différentes catégories de circuits. En particulier, le multicircuit illustré à la figure F.1 a souvent été cité comme une référence pour l'intégration de services à très haute vitesse. Ce multicircuit est une superposition de dix circuits : un circuit H4, sept circuits H12 et deux canaux B. On a ajouté à cette superposition de circuits un canal D, canal multipoint en commutation de paquets, et un canal de synchronisation. Au total, il y a donc douze circuits qui doivent transiter simultanément sur le multicircuit.

Figure F.1

Exemple de canal multicircuit pour l'intégration de services à très haute vitesse



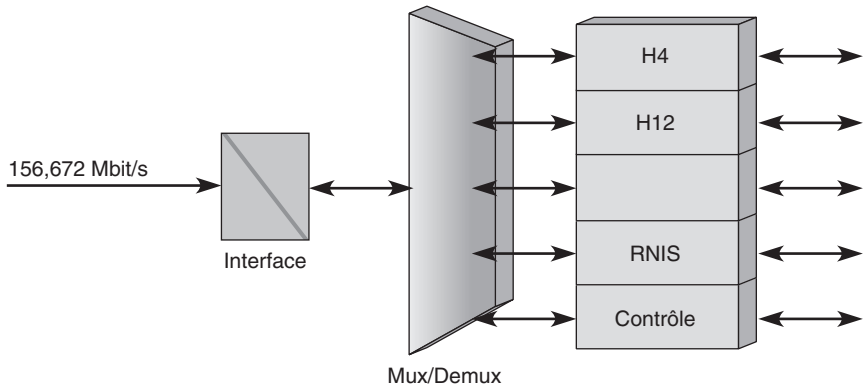
La difficulté principale de ce multicircuit réside dans la gestion du circuit multipoint. Il faut développer une interface unique avec l'utilisateur susceptible de multiplexer les données provenant des différentes sources et de les démultiplexer dans le sens opposé.

La figure F.2 illustre ce multiplexage. Sur la voie de droite arrive un flot à 156,672 Mbit/s. Ce flot doit être décomposé en dix sous-flots, plus des informations de contrôle et de synchronisation. Dans le sens contraire, les douze flots qui arrivent simultanément sur le multiplexeur doivent trouver leur place sur la liaison à 156,672 Mbit/s. Cela implique une mise en série des éléments binaires. En d'autres termes, les bits arrivant en même temps sur le multiplexeur doivent se placer les uns derrière les autres.

La gestion du multiplexage des canaux est complexe, ce qui occasionne la perte d'une partie de la bande passante pour des raisons autres que la transmission des données. La commutation multicircuit est la technique utilisée dans le RNIS bande étroite. Dans l'interface de base, on fournit à l'utilisateur deux canaux B à 64 Kbit/s, qui doivent être partagés entre les différents équipements terminaux de l'utilisateur : combiné téléphonique, PC, fax, terminal vidéotex, etc.

Figure F.2

Exemple de multiplexage-démultiplexage



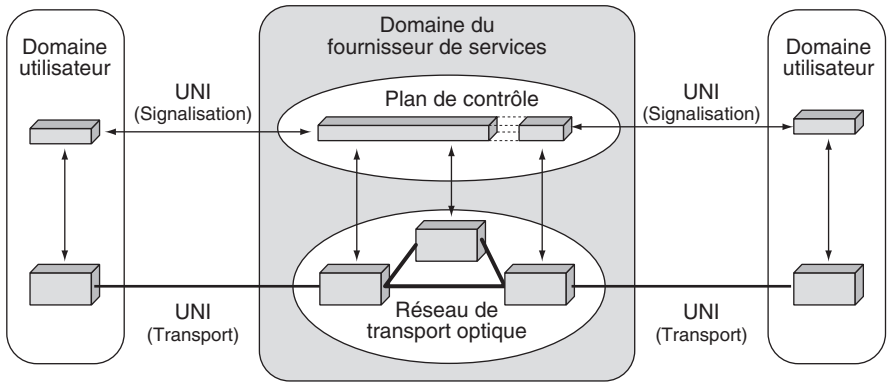
La signalisation OIF (Optical Internetworking Forum)

Si les opérateurs de télécommunications ont tous adopté la technique DWDM pour le cœur de leur réseau, le contrôle des grands réseaux reste une affaire délicate. Pour le moment, la solution trouvée est essentiellement liée au surdimensionnement.

L'interconnexion de deux réseaux d'opérateurs distincts pose problème à cause de leurs systèmes de contrôle respectifs, qui sont généralement incompatibles. Une solution possible à ce problème consiste à adopter MPLS (MultiProtcol Label-Switching) et GMPLS (Generalized MPLS) pour uniformiser les processus de gestion. L'OIF (Optical Internetworking Forum) propose d'ailleurs sous le nom d'OIF UNI 1.0 une signalisation pour les réseaux optiques permettant d'établir une connexion optique dynamiquement en utilisant la procédure de signalisation de GMPLS. Cette signalisation est illustrée à la figure F.3.

Figure F.3

Introduction d'une signalisation OIF UNI entre le service et l'utilisateur



En plus de la signalisation, les spécifications de l'UNI contiennent deux autres fonctionnalités destinées à simplifier la gestion du réseau optique. La première concerne un mécanisme de découverte des voisins, qui permet aux deux extrémités d'une fibre

optique de s'identifier et de construire une carte complète du réseau. La seconde est un mécanisme de découverte des services disponibles dans le réseau optique. Globalement, l'interface UNI simplifie le fonctionnement du réseau optique, engendrant une baisse sensible des coûts de contrôle et de gestion.

L'interface permettant la signalisation OIF UNI est une révolution dans le monde des interfaces, en ce qu'elle autorise la mise en place d'une connexion adaptée à l'application.

EPON (Ethernet Passive Optical Network)

Une nouvelle direction de développement a vu le jour avec la migration de la technologie Ethernet vers les réseaux métropolitains et étendus. La trame Ethernet est de fait une des plus efficaces qui soit, avec son préambule simple, qui permet de reconnaître facilement le début de la trame. De plus, les vitesses des coupleurs Ethernet s'étalant de 10 Mbit/s à 10 Gbit/s, il est facile de trouver la bonne valeur pour un réseau de type métropolitain.

Une raison supplémentaire à l'adoption de la trame Ethernet pour les longues distances réside dans l'utilisation massive de cartes coupleurs Ethernet dans les entreprises. Aujourd'hui, plus de 98 % des réseaux d'entreprise sont de type Ethernet. Les cartes coupleurs génèrent une trame Ethernet, et il semble naturel de garder cette trame tout au long du chemin plutôt que de la transformer en d'autres trames avant de revenir à la trame Ethernet dans le réseau d'arrivée.

Le transfert de trames Ethernet présente un dernier avantage car il peut être de type routé ou commuté. Pour la commutation, il suffit de considérer l'adresse Ethernet comme une référence associée à la route menant à la carte coupleur portant cette adresse et d'y ajouter une vraie référence, le shim-label.

La technologie PON (Passive Optical Network) a été définie pour réaliser des boucles locales sur fibre optique. C'est une technique point-à-multipoint sans élément actif, c'est-à-dire alimenté électriquement. Elle offre une large couverture à haut débit et une maintenance réduite, puisqu'il n'y a pas d'élément actif. La normalisation de la technologie EPON est effectuée par le groupe IEEE 802.3ah. Ce groupe vise plusieurs objectifs, dont celui d'introduire Ethernet dans la boucle locale sous le nom d'EFM (Ethernet in the First Mile). L'allocation de bande passante s'effectue par le biais d'un algorithme spécifique, développé par les équipementiers, en utilisant la méthode d'accès TDMA (Time Division Multiple Access), qui définit des slots à l'intérieur d'une longueur d'onde.

Un EPON permet d'émettre des trames Ethernet à partir d'unités de réseau optique, ou ONU (Optical Network Unit), vers une tête de réseau, ou OLT (Optical Line Termination). La tête de réseau est connectée à un FAI pour permettre l'émission des paquets IP encapsulés dans les trames Ethernet.

La figure F.4 illustre une architecture d'EPON en boucle.

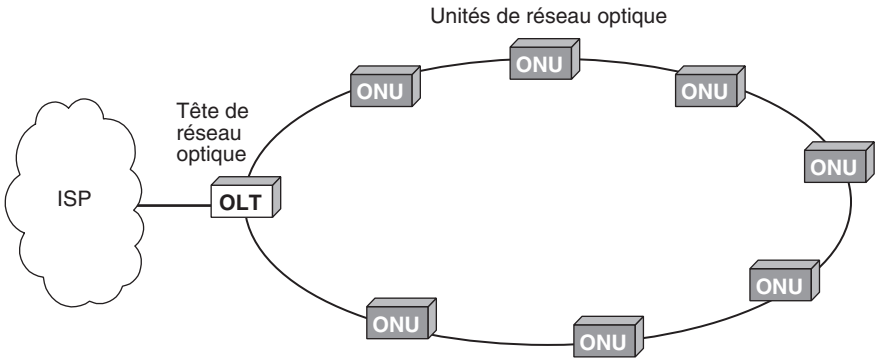


Figure F.4
Architecture d'un EPON

Le standard FSAN (Full Service Access Network) définit un réseau d'accès en fibre optique qui utilise la technologie ATM. Un GPON utilise une technique très similaire, mais avec des trames OTN à la place de trames ATM.

Les commutations par burst et par paquet

Les réseaux optiques que nous avons décrits jusqu'ici utilisent essentiellement une commutation en longueur d'onde. Les paquets utilisent un circuit construit entre un point d'entrée et un point de sortie soit en utilisant la même longueur d'onde tout le long du chemin, soit en changeant de longueur d'onde dans certains nœuds intermédiaires. Cette solution de type circuit n'est pas très efficace pour le transport des données. En effet, les débits qui transitent dans les circuits correspondent à la superposition des débits provenant de groupes d'utilisateurs multiplexés et se présentent donc sous une forme très irrégulière. Les débits transportés par les réseaux sont de surcroît de plus en plus variables dans le temps. De plus, la proportion du débit représentée par la parole téléphonique est en diminution, ce qui enlève encore un peu plus de régularité au trafic que les opérateurs ont à traiter lorsqu'il n'y a que des conversations téléphoniques à transporter.

Pour éviter cette mauvaise utilisation, on a développé des réseaux optiques capables de commuter non plus des longueurs d'onde mais des paquets. Les paquets sont commutés dans un commutateur optique vers une porte de sortie où on leur attribue une couleur disponible pour les émettre. L'inconvénient de cette solution est le nombre de paquets, qui se comptent en milliard par seconde, à traiter dans de gros commutateurs. Le coût de traitement optique étant très important, il est aujourd'hui difficile d'imaginer la date de sortie de tels commutateurs.

Une autre idée s'est développée, consistant à trouver le moyen de traiter de très gros paquets, appelés *bursts*. La commutation par burst n'est rien d'autre qu'une commutation de paquets avec de très gros paquets. À la vitesse de plusieurs gigabits par seconde,

la commutation d'un burst peut demander un temps de l'ordre de quelques dizaines à quelques centaines de microsecondes. À une vitesse de 10 Gbit/s, un burst de 100 µs correspond à 1 Mbit de données. On rassemble donc les données à transporter en paquets de l'ordre de 1 Mbit, puis on met en place un circuit pendant le temps de la transmission.

Appelée OBS (Optical Burst Switching), cette technique devrait bientôt être proposée par quelques équipementiers spécialisés dans la fibre optique. Plusieurs solutions pour réaliser la commutation par burst ont été testées sous les noms de TAG (Tell And Go), TAW (Tell And Wait), JIT (Just In Time) et JET (Just Enough Time).

Dans le TAG (*voir figure F.5*), lorsque le burst est prêt à être envoyé, un message d'établissement de connexion, ou message SETUP, est émis dans le réseau. Ce message SETUP ouvre le circuit, lequel se referme après le passage du dernier octet du burst. Pour que cette solution soit acceptable, il faut que le réseau soit très peu chargé et que les temps de mise en place du circuit soient négligeables.

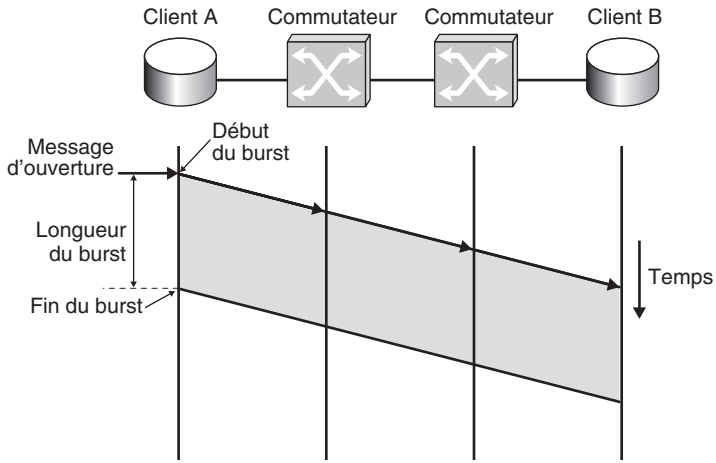


Figure F.5

Commutation par burst TAG

Dans le TAW (*voir figure F.6*), un message SETUP prend le temps nécessaire pour mettre en place le circuit puis envoie un message de confirmation d'ouverture avant que le burst soit émis. Cette méthode est acceptable si le temps d'ouverture du circuit est négligeable par rapport au temps de transmission du burst.

Les méthodes JIT et JET permettent toutes deux de s'approcher d'un fonctionnement optimal. Le message d'établissement SETUP est émis avec un temps d'avance sur le burst lui-même de telle sorte que le circuit soit ouvert au moment exact où le burst se présente (*voir figure F.7*).

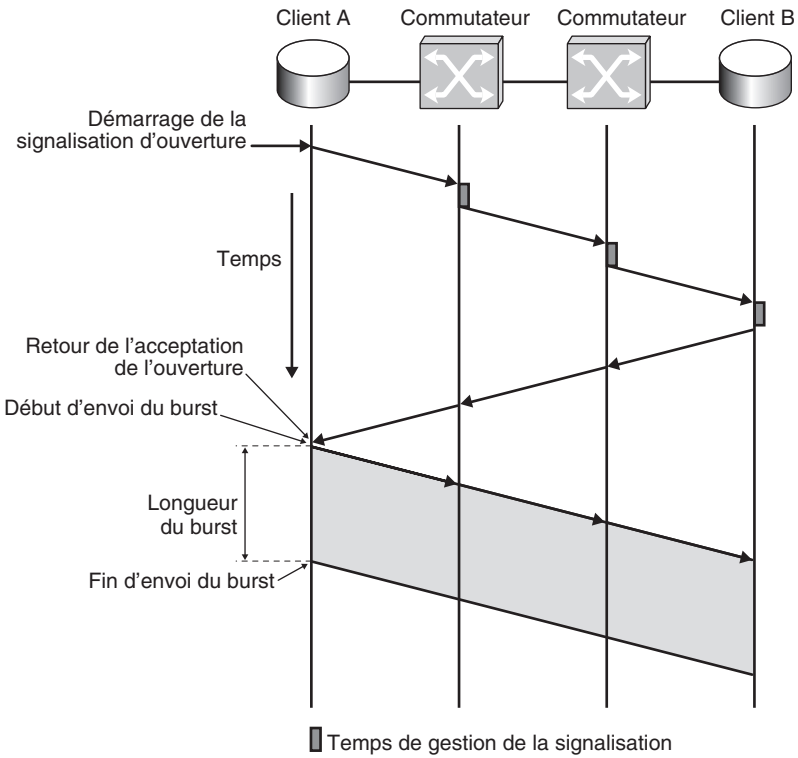


Figure F.6

Commutation par burst TAW

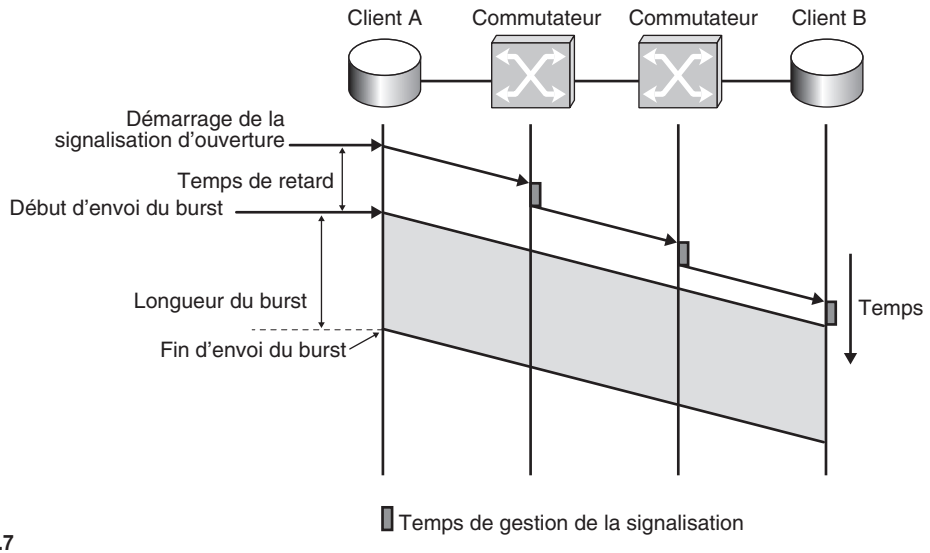


Figure F.7

Commutation par burst JIT et JEN

La difficulté de cette méthode est de déterminer le temps de latence avant le départ du burst. Plusieurs propositions ont été effectuées pour limiter ce temps au minimum, les deux techniques JIT et JET se distinguant par ce calcul. Il faut à tout prix éviter la destruction du burst par manque de réservation dans un nœud intermédiaire, comme l'illustre la figure F.8.

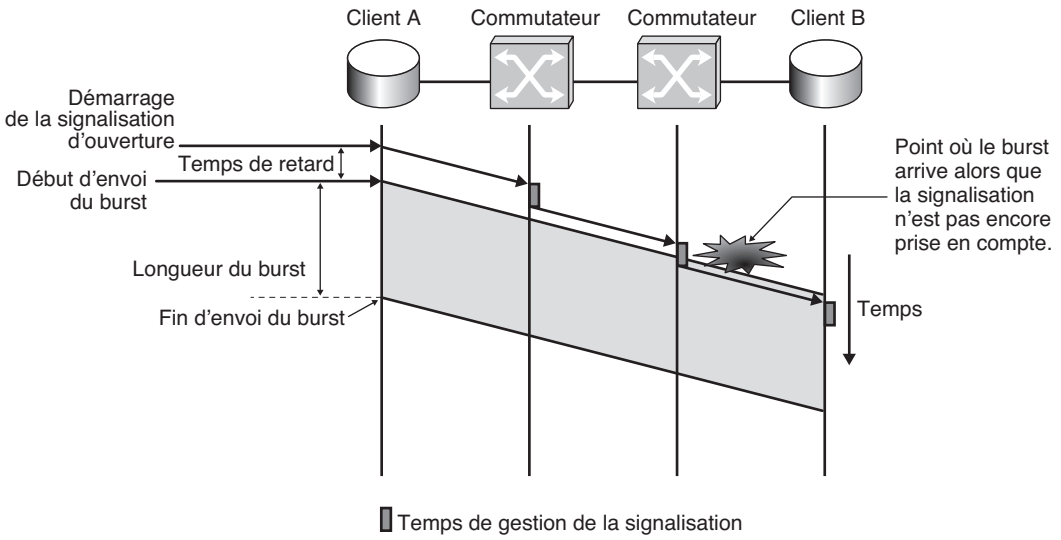


Figure F.8

Destruction du burst par manque de réservation

La commutation de paquets optiques devrait succéder à la commutation de burst en diminuant le burst jusqu'à la taille d'un paquet. La difficulté reste toujours l'impossibilité ou presque de mémoriser un paquet optique. On peut tout au plus utiliser un rouleau de câble optique pour mémoriser un paquet, mais il est impossible d'aller plus loin. La difficulté sera donc d'ouvrir une voie de communication pour le passage d'un paquet optique. Seule une signalisation extrêmement rapide sera capable de réaliser ce type de transfert.

RPR (Resilient Packet Ring)

Les réseaux Ethernet présentent généralement une topologie sous forme de bus ou d'arbre, qui ne facilite pas les reconfigurations en cas de panne. Quand il est possible d'utiliser une méthode commutée, la boucle est une meilleure technologie, et c'est pourquoi elle a été choisie par de nombreux réseaux métropolitains, notamment SONET/SDH.

RPR propose une nouvelle solution de réseau métropolitain en boucle permettant de réagir rapidement en cas de panne d'un tronçon de la boucle et d'offrir de très hauts débits, allant jusqu'à 10 Gbit/s par boucle. Son avantage sur SONET/SDH réside dans son prix de revient beaucoup plus bas, du fait des composants utilisés.

Limitations de SONET et d'Ethernet dans les techniques de boucle

SONET est essentiellement conçu pour des communications point-à-point en commutation de type circuit, comme la parole téléphonique. La figure J.9 illustre l'accès d'une station vers les autres stations. On peut constater que SONET permet d'aller directement de l'émetteur au récepteur. Chaque circuit se voit allouer une capacité de transmission déterminée. Si la quantité d'information à émettre est inférieure à la valeur allouée, ce qui n'est pas utilisé est perdu.

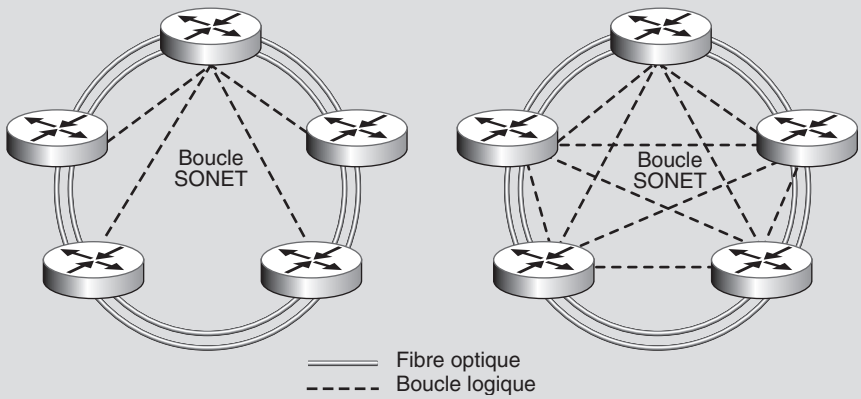


Figure F.9

Topologie de SONET

SONET n'est donc pas adapté aux transferts de trames asynchrones et irrégulières. De plus, les applications multipoint ne sont pas prises en compte de façon intrinsèque car il faut autant de circuits que de points à atteindre. Pour protéger SONET contre les incidents et permettre une reconfiguration simple, la bande passante réellement utilisée est de l'ordre de 50 %. À l'inverse, Ethernet est bien adapté aux flots asynchrones et aux applications multipoint mais très mal aux flots synchrones.

La figure F.10 illustre la topologie en anneau qu'il est possible de mettre en place dans Ethernet. On transmet la trame Ethernet d'un nœud vers un autre nœud. Lorsqu'on atteint le dernier commutateur de la chaîne, la trame repart vers l'origine sur une ligne qui va en sens contraire.

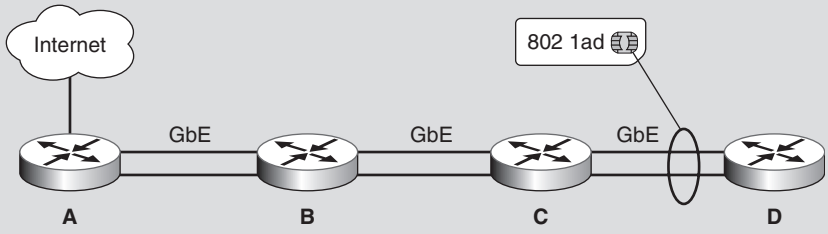


Figure F.10

Boucle Ethernet

Les techniques Ethernet utilisent l'algorithme du Spanning-Tree, présenté en détail au chapitre 5, pour réaliser le routage des trames. Cet algorithme est trop lent pour la reconfiguration lors de la circulation

de paroles téléphoniques. En effet, il faut compter un minimum de 500 ms pour remettre en place le nouveau routage, contre 50 ms au maximum pour une boucle SONET. C'est la raison de l'adoption dans RPR d'une solution en boucle, mais avec une technique de transfert dans les nœuds qui ne provient pas de la commutation, à la différence de SONET.

La méthode d'accès à la boucle doit être capable de gérer les milliers d'utilisateurs d'une boucle métropolitaine sans perte de temps sur la boucle. Avec la nouvelle technique d'accès partagée au support physique bien adaptée au monde métropolitain et aux réseaux de grande capacité possédant des milliers de clients, il est possible d'obtenir des réseaux métropolitains à temps de reconfiguration court et acceptable pour les voies de communication téléphoniques à tarifs compétitifs.

Le nœud du réseau RPR n'est pas un commutateur mais un équipement d'insertion de paquets, comme nous allons le voir. Les paquets vont d'un équipement RPR à un autre. Ils forment un flux de paquets transitant sur la boucle à laquelle sont connectés les équipements RPR. Un équipement RPR possède *N* files d'attente correspondant à des niveaux de priorité. La file prioritaire est servie jusqu'à ce qu'elle soit vide, après quoi la file 2 prend le relais, et ainsi de suite. Le service s'effectue de la façon suivante : lorsqu'un équipement RPR veut émettre sur la boucle, il met le paquet arrivant de la boucle dans un registre à décalage, qui n'est autre qu'une mémoire supplémentaire dans laquelle les éléments binaires entrent par un côté et ressortent par l'autre ; il émet alors le paquet en attente dans la file d'attente puis le paquet mis en attente dans le registre à décalage. Cette solution est schématisée à la figure F.11.

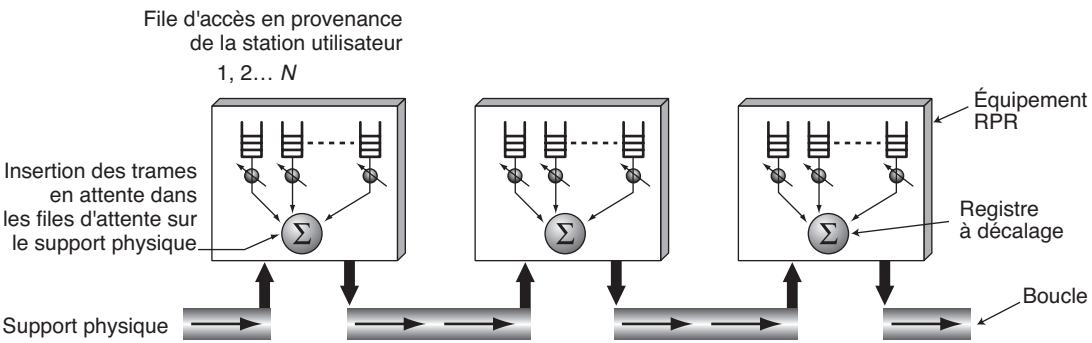


Figure F.11

Boucle fonctionnelle de la technique RPR

Tant que la boucle est pleine, c'est-à-dire tant que les registres d'insertion sont utilisés, une station ne peut plus émettre. Il faut donc enlever une trame, et c'est ce que l'on fait lorsque la trame revient à son émetteur. Un nœud a pour cela trois fonctions : ADD, qui insère une trame lorsque cela est possible, DROP, pour prélever une trame qui a fini son tour de boucle, et PASS, pour laisser passer une trame dans le registre.

Le multicast est inhérent à la technologie des registres à décalage puisque le nœud émetteur n'envoie qu'une seule trame, qui est recopiée en cas de diffusion à l'ensemble des nœuds de transfert lors du parcours du message. La topologie utilisée est en boucle, mais, pour des raisons de reconfigurabilité, elle est doublée par deux boucles contrarotatives. Cette boucle est illustrée à la figure F.12.

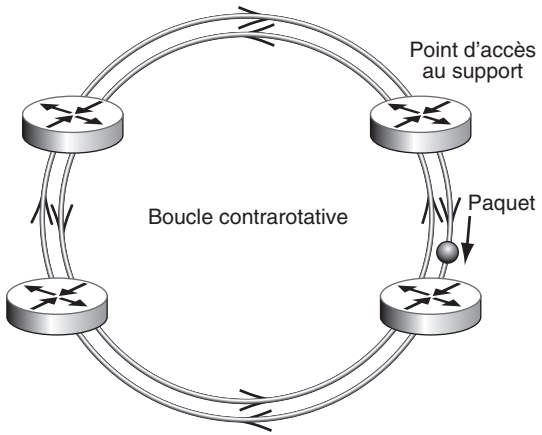


Figure F.12
Boucle contrarotative de RPR

Le support physique peut être de différents types entre deux nœuds si nécessaire.

La reconfiguration RPR

L'un des points fort de l'architecture RPR réside dans sa reconfigurabilité en moins de 50 ms, qui permet de prendre en compte des voies téléphoniques. Cette reconfiguration s'effectue en inversant le sens de la communication sur la boucle. Lorsque la double fibre optique est coupée (*voir figure F.13*), des interrupteurs sont déclenchés dans les nœuds entourant la fibre optique coupée. Ces interrupteurs permettent de refaire une boucle unique en remplacement de la double boucle.

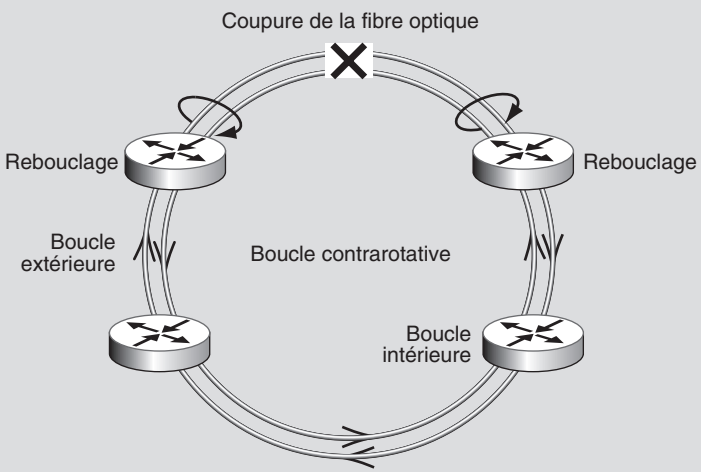


Figure F.13
Double boucle contrarotative de RPR

Un autre avantage de la topologie en boucle est qu'elle permet d'implémenter un algorithme d'accès attribuant des droits égaux à tous les utilisateurs. La technique d'accès par registre permet à chaque utilisateur d'obtenir le débit maximal disponible sur le réseau sans se restreindre à la valeur du circuit ouvert, à la différence de SONET.

Si une application demande une diffusion ou un multipoint, le support en boucle permet de prendre aisément en compte cette demande puisque la trame émise sur la boucle est prélevée par l'émetteur après un tour de boucle. Les stations participant au multipoint ont donc toute latitude pour prélever une copie au passage.

La différence entre la boucle RPR et la boucle SONET est illustrée à la figure F.14. Dans le cas de SONET, les trames sont émises sur un circuit allant directement de l'émetteur au récepteur et dont la capacité a été réservée à l'avance. Dans RPR, les trames sont émises sur la boucle avec un débit au moins égal au débit de la boucle divisé par le nombre de stations connectées, voire davantage si toutes les stations ne sont pas actives. Les ressources sont totalement partagées par l'ensemble des utilisateurs.

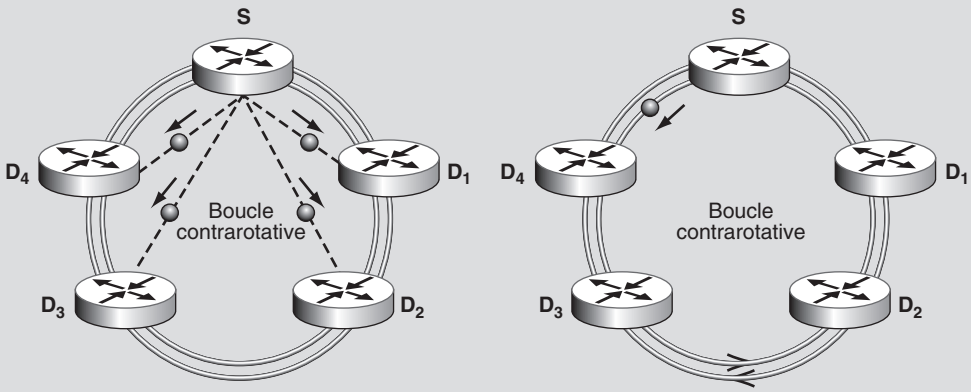


Figure F.14

Comparaison des boucles SONET (à gauche) et RPR

En comparaison des techniques de type circuit, dans lesquelles il faut souvent attendre un mois en moyenne pour pouvoir disposer du circuit, RPR se distingue par la rapidité avec laquelle il est possible d'offrir une capacité de transmission à un utilisateur. Dans SONET, il faut activer des mécanismes de réservation de slots déterminés pour arriver à la capacité de transmission réclamée par l'utilisateur. Dans RPR, étant donné que le trafic d'un nœud est connu à l'avance, l'opérateur sait immédiatement si le débit demandé est acceptable pour l'infrastructure du réseau.

Même si SONET permet d'effectuer la réservation de ressources par le biais d'un automate, la mise en place du circuit et son optimisation réclament du temps et des logiciels d'ingénierie de trafic.

Les applications de RPR

RPR permet de mettre en place de nombreux services, à commencer par ceux d'un fournisseur de services métropolitains, parfois appelé MSP (Metro Service Provider), ILEC (Incumbent Local Exchange Carrier), CLEC (Competitive Local Exchange Carrier) ou BLEC (Building Local Exchange Carrier). Il peut en outre remplacer les opérateurs de modems câble ou ADSL dont la fonction est de proposer des accès haut débit à Internet, car la technologie RPR est parfaitement adaptée à cette demande. La figure F.15 illustre ce que pourrait être un tel réseau métropolitain.

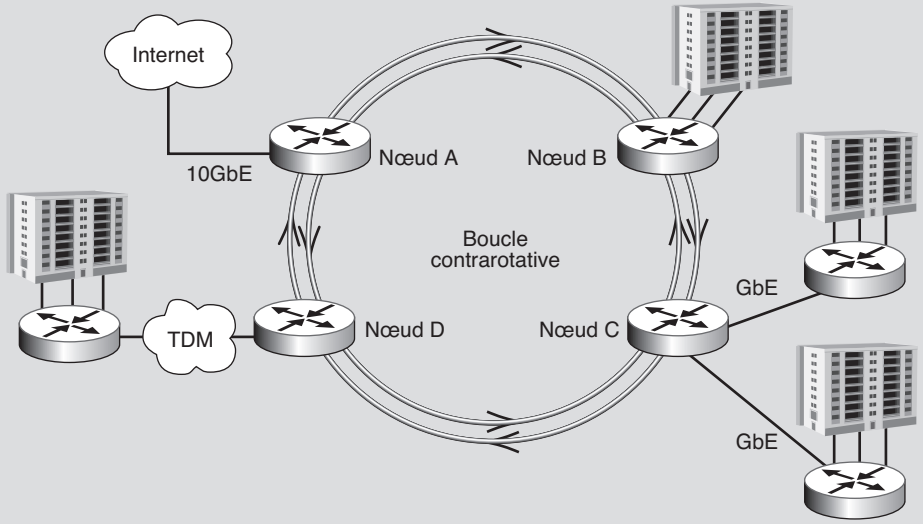


Figure F.15

Réseau métropolitain à base de technologie RPR

Grâce à RPR, chaque utilisateur se voit attribuer un débit variable, dont la borne maximale est connue, ce qui garantit une très grande souplesse d'exploitation. Un SLA (Service Level Agreement) peut être négocié pour le débit et le temps de transit dans le réseau. Un temps de reconfiguration de moins de 50 ms est acceptable puisque aucune station ne peut monopoliser la bande passante. De plus, la technologie RPR étant très proche d'Ethernet, un couplage avec les réseaux Ethernet des entreprises est simple à mettre en œuvre, quel que soit le débit, qui peut aller de 10 Mbit/s à 10 Gbit/s.

IEEE 802.17

Le groupe de normalisation de RPR est l'IEEE 802.17, chargé d'introduire les concepts Ethernet dans les réseaux métropolitains et étendus. Plus de 300 sociétés participent à cette normalisation. Le protocole IEEE 802.17 doit être parfaitement compatible avec les protocoles 802.1D, 802.1Q et 802.1f. La trame émise sur le support physique étant du même type que la trame Ethernet, la compatibilité avec Ethernet est complète. Le groupe de travail IEEE 802.17b a été monté pour encore améliorer la première norme en permettant une meilleure réutilisation des trames RPR.

L'utilisation intensive de la trame Ethernet semble une solution simple permettant de faire baisser les prix des connexions à des niveaux impossibles à atteindre avec les technologies de type SONET.

G

Relais de trames et ATM

La normalisation des réseaux ATM, à la fin des années 1980, avait pour ambition de proposer une solution capable de remplacer tous les autres réseaux et de permettre le passage de la parole téléphonique et de toutes les applications à fortes contraintes de temps réel. Cette solution a pris pour nom la commutation de cellules afin de la différencier de la commutation de trames classique.

Avant l'ATM, le relais de trames peut être vu comme une solution pré-ATM puisque assez similaire mais pas avec toutes les possibilités de qualité de service de l'ATM.

Cette annexe présente d'abord le relais de trames en tant que solution pré-ATM puis examine la commutation de cellules ATM avant de décrire l'architecture générale des réseaux ATM et les protocoles qui y sont mis en œuvre.

Le relais de trames

Le relais de trames a pris la succession du protocole X.25 en faisant descendre la commutation du niveau 3 au niveau 2. Dans le même temps, il a été doté de nouvelles fonctionnalités qui l'apparentent à une technologie pré-ATM, notamment la possibilité de garantir une qualité de service. Les sections qui suivent examinent ces fonctionnalités.

La commutation de niveau trame

L'objectif d'une commutation de niveau trame est d'améliorer les performances de la commutation de niveau paquet, comme X.25, en diminuant le nombre de niveaux de l'architecture à traverser à chaque nœud. En plaçant la commutation au niveau trame

de l'architecture, on n'est pas obligé de décapsuler la trame pour retrouver le paquet. En effet, dans un transfert de paquets, on attend de recevoir correctement une trame, avec des retransmissions potentielles. Une fois la trame décapsulée, on examine le paquet pour déterminer la direction dans laquelle on va l'émettre.

La commutation implique la mise en place d'un chemin ou circuit virtuel, qui est appelé liaison virtuelle dans le relais de trames puisque nous sommes au niveau 2. Des références placées dans la structure de la trame sont utilisées pour commuter les trames. Sans signalisation préalable, la liaison virtuelle est permanente, et les références sont posées une fois pour toutes pour toute la période d'abonnement.

Dans le relais de trames, les abonnements sont généralement effectués sur une base mensuelle. Ces liaisons permanentes peuvent être considérées comme des liaisons spécialisées, ou circuits, attribuées par un opérateur et mises en place à la demande d'un utilisateur pour aller à un point précis. Les ressources y sont affectées une fois pour toutes, et seules les deux extrémités peuvent les utiliser.

L'avantage d'un circuit virtuel permanent est de ne pas utiliser les ressources du réseau lorsque les deux utilisateurs sont silencieux, à l'exception des tables de commutation, lesquelles restent ouvertes en permanence.

Le relais de trames peut être considéré comme un cas particulier de commutation de trames, doté de simplifications supplémentaires permettant de gagner encore en débit. Les simplifications se trouvent principalement dans les algorithmes de reprise sur erreur et dans les contrôles de flux, qui ne sont effectués que dans les points extrémité. Dans le relais de trames, les contrôles d'erreur et de flux sont reportés aux extrémités de la connexion. Cette simplification du travail des nœuds intermédiaires est très importante puisqu'il n'y a plus à mettre en œuvre d'algorithmes complexes. On considère que l'on gagne en performance au moins un ordre de grandeur — multiplication par 10 du débit — pour une puissance d'équipement donnée par rapport à l'équivalent en commutation de paquets. Le débit de base du relais de trames est de 2 Mbit/s contre 64 Kbit/s dans une commutation de paquets de type X.25 avec des nœuds de même complexité.

La normalisation du relais de trames

La commutation de trames et le relais de trames ont été normalisés par l'ANSI et l'UIT-T dans le cadre du RNIS. La recommandation I.122 (Framework for Providing Additional Packet Mode Bearer Services) introduit les éléments de base. La principale recommandation technique se trouve dans le document Q.922 et figure également dans la recommandation I.441 ou dans le document T1.618 de l'ANSI. Elle limite à 2 Mbit/s le débit de cette technique de commutation. Dans les faits, rien n'empêche d'aller beaucoup plus vite. Cette limitation peut s'expliquer par le manque de visibilité à long terme de cette technique au moment de sa normalisation. En effet, la technique de transfert recommandée à l'époque étant l'ATM, le relais de trames n'était envisagé que comme une étape transitoire, capable de combler un trou de quelques années entre la commutation de paquets et la commutation de cellules ATM.

Un autre organisme, le Frame Relay Forum, ou FR Forum, a eu un impact important sur le relais de trames. Né du regroupement de quatre constructeurs, DEC, Northern Telecom, Cisco Systems et Stratacom, le FR Forum a surtout repris les recommandations de l'UIT-T, en modifiant parfois quelques éléments mais sans toucher aux principes de base. La différence principale avec la norme réside dans l'utilisation du relais de trames indépendamment du RNIS.

Deux modes, dénommés FR1 et FR2, sont décrits dans la normalisation. Dans le mode FR1, le contrôle de flux et la reprise sur erreur sont laissés à la charge de l'équipement terminal. Dans le mode FR2, ils sont effectués aux extrémités du réseau.

On peut considérer le relais de trames comme une amélioration décisive de la recommandation X.25, puisqu'il simplifie considérablement le travail des nœuds intermédiaires. Malgré cette simplification, on retrouve les mêmes services de transport de l'information, mais avec des capacités de transport bien supérieures.

Le relais de trames est bien adapté au transfert de fichiers de gros volume, aux applications interactives par bloc, comme les applications graphiques de CAO (conception assistée par ordinateur) ou d'images, ou encore au transport de voies haute vitesse multiplexant un grand nombre de voies basse vitesse.

La commutation de trames pure a rapidement été remplacée par le relais de trames dans les réseaux des opérateurs et est aujourd'hui inusitée pour le transport de données. Nous la présentons toutefois en premier de façon à conserver l'ordre chronologique d'introduction de ces techniques.

La commutation de trames (Frame Switching)

Comme expliqué précédemment, dans la commutation de trames, les trames sont transportées d'un bout à l'autre du réseau sans avoir à remonter au niveau paquet. Il faut utiliser un protocole de niveau trame suffisamment puissant pour permettre l'acheminement des trames en ne tenant compte que des informations de supervision disponibles dans la structure de la trame. En particulier, un adressage de niveau trame doit remplacer l'adressage de niveau paquet. De plus, les fonctions du niveau 2 doivent être maintenues.

Dans la commutation de trames et dans le relais de trames, il est nécessaire de retrouver les grandes fonctionnalités du niveau paquet, comme l'adressage, le routage et le contrôle de flux, reportées au niveau trame. Pour effectuer le transfert, on utilise l'adresse du niveau trame sans remonter au niveau paquet, contrairement à ce que préconise le modèle de référence. Cet adressage sert à ouvrir le circuit virtuel sur lequel les trames sont commutées. Le nom exact de ce circuit virtuel est liaison virtuelle, comme nous l'avons vu dans l'introduction de cette annexe, puisque nous sommes au niveau 2. Nous revenons un peu plus loin sur le problème de l'adressage et de la mise en place des références.

L'architecture d'un réseau à commutation de trames est illustrée à la figure G.1. Cette figure montre que les nœuds de commutation intermédiaires ne possèdent que les deux premières couches de l'architecture du modèle de référence, à savoir la couche physique et la couche liaison utilisant le protocole Q.922 normalisé par l'UIT-T. Q.922 est le protocole

de niveau trame qui est mis en œuvre dans les réseaux à commutation de trames. Ce protocole utilise la trame LAP-F, que nous décrivons dans une section ultérieure.

Dans les nœuds de commutation, on cherche la référence de niveau 2 autorisant la commutation de la trame vers le destinataire. La zone de détection d'erreur portée par la trame est examinée à chaque nœud du réseau. En cas de détection d'erreur, une demande de retransmission est lancée, et la trame est retransmise à partir du nœud précédent.

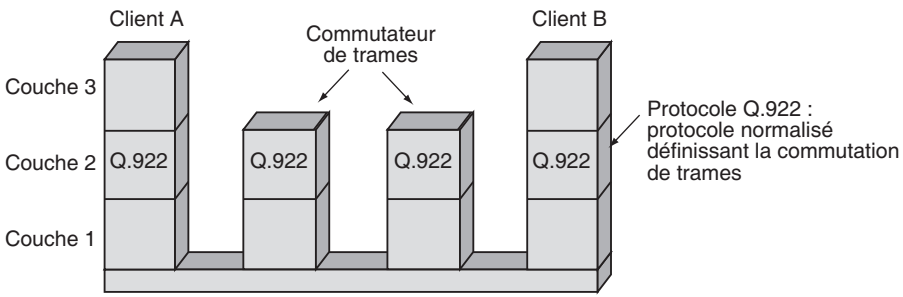


Figure G.1

Commutation de trames

Fonctionnement du relais de trames (Frame Relay)

Le relais de trames apporte une simplification supplémentaire à la commutation de trames. Dans les nœuds intermédiaires, les trames sont vérifiées grâce à une zone de détection d'erreur et détruites si une erreur est détectée. En revanche, il n'y a pas d'algorithme pour effectuer la récupération de la trame perdue. Les nœuds de commutation ne prennent donc en charge que les trames valides. La retransmission des trames erronées est effectuée par le nœud de sortie du réseau en demandant une retransmission à l'autre extrémité du réseau.

Cette solution permet de simplifier énormément les nœuds intermédiaires et d'atteindre des capacités de transmission se chiffrant en mégabit par seconde. Elle n'est toutefois viable que si le taux d'erreur est faible puisque les retransmissions sont beaucoup plus lentes que dans une reprise de nœud à nœud, comme cela se produit dans un transfert de niveau 3.

La normalisation du relais de trames s'appuie sur l'avis Q.922 de l'UIT-T et plus particulièrement sur le noyau de base de cette recommandation, Core Q.922. On utilise les fonctionnalités complètes de la recommandation aux extrémités de la connexion et celles du noyau dans les nœuds intermédiaires.

Les grandes fonctionnalités normalisées par cette recommandation sont les suivantes :

- Délimitation, alignement et transparence des trames.
- Multiplexage et démultiplexage des trames à l'aide du champ de référence.

- Inspection de la trame pour vérifier qu'elle possède un nombre entier d'octet avant insertion ou après extraction des 0 intégrés pour la transparence.
- Inspection de la trame pour vérifier qu'elle n'est ni trop courte, ni trop longue.
- Demande de retransmission dans les éléments extrémité de la connexion.
- Fonction de contrôle de flux de bout en bout.

Les deux dernières fonctions ne font pas partie du noyau et ne sont donc entreprises qu'aux extrémités de la connexion.

Le relais de trames a pour rôle de diminuer au maximum le temps passé dans les commutateurs en n'effectuant qu'un travail minimal, en l'occurrence l'examen de la zone de détection d'erreur et de la référence de niveau 2 et l'émission de la trame vers le nœud suivant.

Le relais de trames possède deux plans, c'est-à-dire deux réseaux logiques multiplexés sur un même réseau physique : le plan utilisateur et le plan de contrôle. Le plan utilisateur gère l'acheminement des trames qui transportent des données utilisateur tandis que le plan de contrôle se charge des trames qui transportent de la signalisation.

L'architecture du relais de trames en ce qui concerne le plan utilisateur est illustrée à la figure G.2. Nous verrons plus loin l'architecture pour les informations de supervision et de gestion. Dans cette figure, le niveau paquet est conservé aux deux extrémités et ce qui symbolise le relais de trames c'est la disparition d'une partie de la couche 2, correspondant aux reprises sur erreur, dans les nœuds intermédiaires. La partie de la couche 2 qui reste provient de la norme Q.922 de l'UIT-T et plus précisément le noyau de cette couche. La partie complémentaire de Q.922 se retrouve dans les nœuds extrémité. Cette partie complémentaire peut éventuellement être remplacée par une autre procédure spécifiée par l'utilisateur.

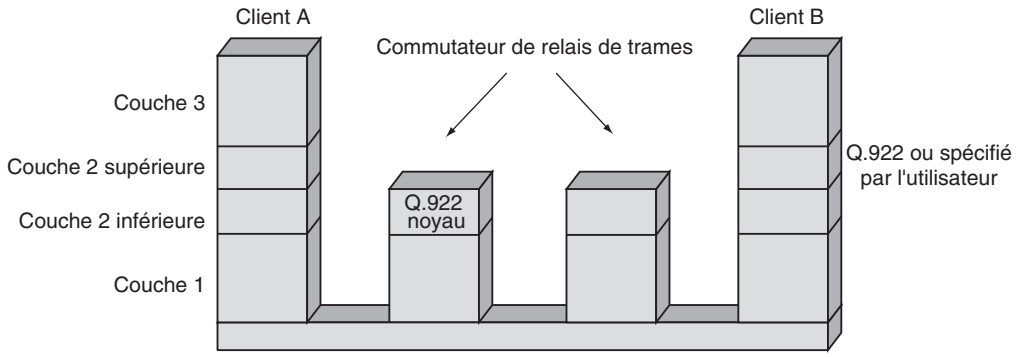


Figure G.2

Architecture du plan utilisateur du relais de trames

Le noyau de la recommandation Q.922, ou Q.922 Core, décrit les fonctions de base, la délimitation de la trame, la transparence par rapport aux délimiteurs, le multiplexage des

trames sur les liaisons physiques par un numéro de référence, appelé DLCI (Data Link Connection Identifier), la vérification du nombre d'octet, qui doit être un entier, et la vérification de la longueur totale de la trame.

La figure G.3 illustre l'architecture complète du relais de trames au niveau extrémité, c'est-à-dire les plans utilisateur et contrôle. La mise en place de la liaison virtuelle s'effectue en dehors du plan utilisateur par un plan spécifique, le plan de contrôle. La supervision du réseau en relais de trames doit être assurée par un environnement distinct de celui du réseau utilisateur, même si l'infrastructure de ce dernier est utilisée.

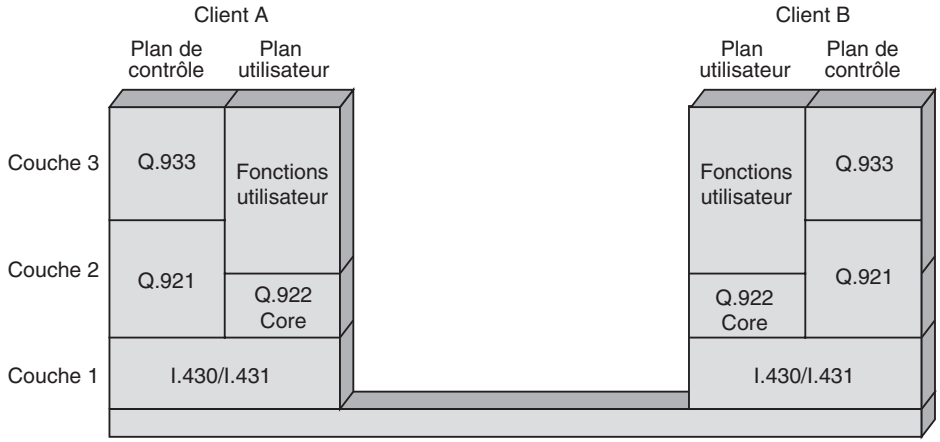


Figure G.3

Architecture complète du relais de trames

L'avis Q.922 de l'UIT-T

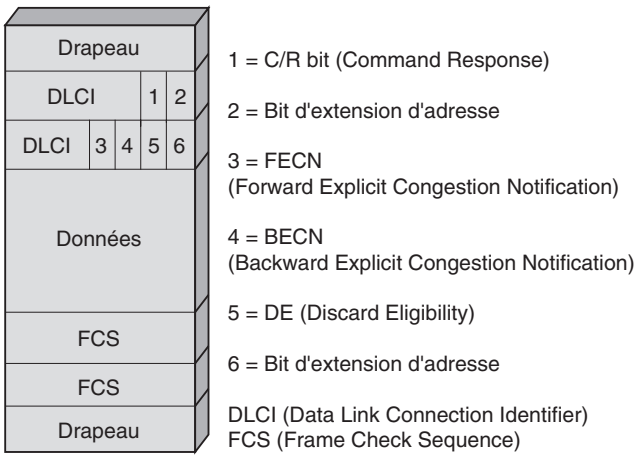
Le format de la trame véhiculée dans le relais de trames est illustré à la figure G.4. Cette trame correspond à celle du LAP-D légèrement modifiée pour tenir compte du contexte du relais de trames. La zone DLCI remplace les zones SAPI (Service Access Point Identifier) et TEPI (Terminal End Point Identifier), à l'exception des bits 3, 4 et 5. La zone de données peut atteindre 4 096 octets. Le drapeau est le même que dans la norme HDLC : 01111110. On utilise la procédure d'insertion de 0 en présence de la succession 011111, afin d'éviter de retrouver la valeur du drapeau à l'intérieur de la trame.

Dans le LAP-F (Link Access Protocol-Frame), la référence est spécifiée dans la zone DLCI. Ce champ compte 6 bits + 4 bits = 10 bits. Il peut donc y avoir jusqu'à $2^{10} = 1\,024$ valeurs pour le DLCI. Cette quantité est notoirement insuffisante si l'on veut réaliser des réseaux un tant soit peu complexes et encore plus insuffisante si l'on considère un contexte national dans lequel on souhaite que les réseaux en relais de trames aient assez de références pour permettre un grand nombre de liaisons virtuelles. C'est la raison pour laquelle deux extensions supplémentaires, de 1 ou 2 octets, ont été effectuées pour le relais de trames, aboutissant à des références sur 16 ou 23 bits. Dans le premier cas, un

troisième octet d'adressage est ajouté. Sur cet octet, 6 bits sont dédiés à l'extension de longueur de la référence. Dans le deuxième cas, un quatrième octet est ajouté, 7 de ses bits concernant l'extension de la longueur de la référence. Le huitième bit des octets 3 et 4 indique si un octet de supervision supplémentaire est à prendre en considération. Les octets d'extension se trouvent soit au milieu des deux octets de base, soit derrière eux.

Figure G.4

Format de la trame du relais de trames

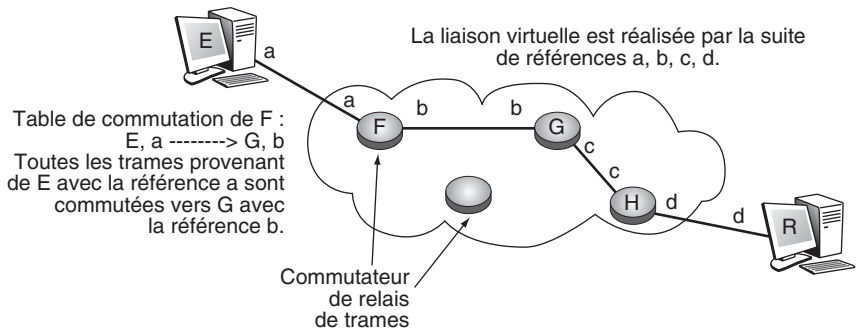


Le transfert des trames vers le nœud suivant s'effectue grâce à la valeur transportée dans le champ DLCI. La valeur du DLCI est modifiée lors de la traversée de chaque nœud. La nouvelle valeur de la référence se trouve dans la table de commutation. L'acheminement de la trame s'effectue par le chaînage des références DLCI. Les trames d'un même client allant de la machine terminale d'émission à la machine terminale de réception doivent toujours suivre un même chemin, à savoir la liaison virtuelle.

Lorsqu'un client veut émettre une suite de trames, il commence par mettre en place une liaison virtuelle. Cette dernière se réalise par l'intermédiaire d'une signalisation passant par le plan de contrôle lorsque la connexion est commutée ou l'utilisation des références placées sur une base mensuelle lorsque la liaison virtuelle est permanente. La figure G.5 illustre une liaison virtuelle déterminée par la succession des numéros DLCI a, b, c et d.

Figure G.5

Liaison virtuelle dans le relais de trames



Le commutateur de trames change la valeur du DLCI au passage, suivant les indications fournies par la table de commutation.

La procédure de commutation des trames sur la liaison virtuelle est en tout point similaire à la commutation de niveau paquet sur le circuit virtuel de la recommandation X.25.

Le contrôle de flux

Dans les premières versions du relais de trames, le contrôle de flux était pratiquement éliminé. Avec l'accroissement de la taille de ces réseaux, il a fallu ajouter un certain nombre d'éléments capables de réguler les flux. Les solutions retenues reposent sur un accord entre l'utilisateur et l'opérateur quant au débit moyen à respecter, ou CIR (Committed Information Rate), qui définit un flux à ne dépasser que sous certaines conditions. On définit aussi un CBS (Committed Burst Size), qui, pour le temps *T,* précise la quantité d'informations maximale à transporter sans dépasser le seuil garanti CIR : CBS = CIR × *T.*

Comme le relais de trames procède selon une méthode statistique, l'utilisateur a le droit de dépasser par moments le débit CIR. Cependant, ces dépassements peuvent mettre l'opérateur en difficulté, puisqu'il n'a réservé de ressources que pour la valeur garantie. C'est la raison pour laquelle l'autorisation de dépassement est accompagnée d'une indication relative aux données en surplus et spécifiée dans la trame. Cela permet à l'opérateur, en cas de difficulté dans son réseau, de détruire les données supplémentaires. Il n'y a donc pas de garantie de service pour les données en surplus.

Les dépassements peuvent se faire suivant un additif au contrat de base, par la détermination d'un débit maximal, ou EIR (Excess Information Rate), et d'une valeur nommée EBS (Excess Burst Size). Si l'utilisateur dépasse le seuil CIR, l'opérateur laisse entrer les données supplémentaires jusqu'à la valeur EIR, ces valeurs étant indiquées par la mise à 1 d'un bit du champ de la trame, le bit DE (Discard Eligibility). La valeur 1 du bit DE correspond aux données en excès. Cette indication a aussi pour signification que la trame peut être détruite par l'opérateur, suite à des problèmes de congestion du réseau.

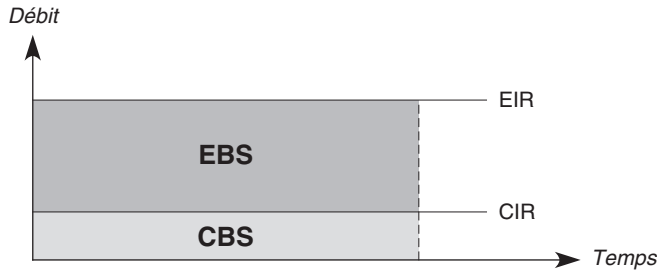
La valeur EBS indique la quantité d'information supplémentaire que l'opérateur transmet lorsque le seuil CIR est dépassé. Pour le temps *T,* cette quantité est définie par (EIR – CIR) × *T.*

En résumé, le dépassement de la valeur de base CIR est accepté par le réseau jusqu'à une limite maximale définie dans le contrat de trafic par la valeur EIR. Au-delà de cette limite, les trames sont détruites à l'entrée du réseau. La figure G.6 illustre ces différents paramètres de contrôle de flux.

Le contrôle de flux effectué par le contrat de trafic est complété par des notifications effectuées aux extrémités et spécifiées dans les trames elles-mêmes. Les deux notifications possibles sont :

- FECN (Forward Explicit Congestion Notification)
- BECN (Backward Explicit Congestion Notification)

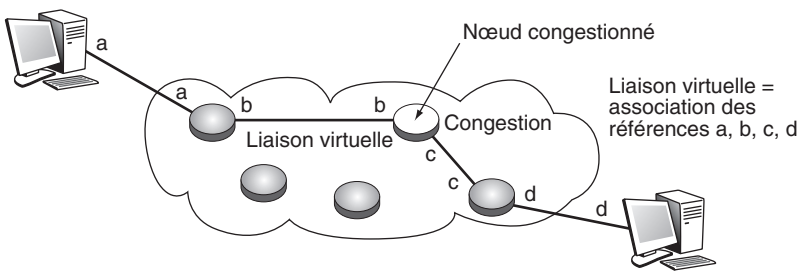
Figure G.6
Paramètres du contrôle de flux dans le relais de trames



Supposons qu'un nœud soit en période de congestion. Cette congestion est déterminée par des seuils définis par l'opérateur. Lorsqu'une trame passe par un nœud congestionné, elle est marquée soit par le bit FECN = 1, soit par le bit BECN = 1, suivant la direction de la trame, vers le récepteur ou l'émetteur. La notification vers l'avant correspond à un avertissement envoyé au récepteur pour l'informer que le réseau comporte un point saturé. La seconde notification repart vers l'émetteur pour lui indiquer qu'il serait souhaitable qu'il diminue provisoirement son débit.

Les normes ne donnent aucune indication sur l'usage effectif de ces notifications. Cependant, l'unité de raccordement, ou FRAD (Frame Relay Access Device), peut réduire son débit tout en avertissant les couches supérieures. La figure G.7 fournit un exemple de liaison virtuelle passant par un nœud congestionné notifiant la surcharge à ses extrémités. Le problème posé par cette notification collective vient de la demande effectuée à toutes les machines extrémité de réduire leur trafic, indépendamment des connexions fautives.

Figure G.7
Liaison virtuelle avec point de congestion



La commutation de cellules ATM

Une première caractéristique importante des réseaux ATM est qu'on utilise le mode avec connexion pour la transmission des cellules. Une cellule n'est transmise que lorsqu'un circuit virtuel est ouvert, ce circuit virtuel étant marqué à l'intérieur du réseau par des références précisées dans les tables de commutation placées dans chaque nœud traversé. Nous verrons à la fin de cette annexe comment mettre en place ce circuit virtuel grâce au réseau de signalisation.

Deux interfaces ont été définies dans le monde ATM suivant que la cellule provient de l'extérieur du réseau ou passe d'un nœud de commutation à un autre à l'intérieur du réseau :

- L'interface NNI (Network Node Interface), qui se situe entre deux nœuds du réseau.
- L'interface UNI (User Network Interface), qui est utilisée pour entrer dans le réseau ou pour en sortir.

Ces deux noms d'interface, UNI et NNI, sont maintenant utilisés dans la plupart des réseaux, mêmes s'ils ne sont pas ATM.

Les références destinées à permettre la commutation des trames ATM sont composées de deux numéros : le numéro VCI (Virtual Channel Identifier), ou identificateur de voie virtuelle, et le numéro VPI (Virtual Path Identifier), ou identificateur de conduit virtuel. Ces numéros permettent d'identifier le circuit virtuel entre deux nœuds. Nous parlons de circuit virtuel, car c'est la terminologie utilisée dans l'ATM, bien que nous ayons affaire à une liaison virtuelle puisque le niveau ATM est un niveau trame.

La référence d'un circuit virtuel comporte donc deux parties : le numéro de conduit virtuel (*virtual path*) et le numéro de voie virtuelle (*virtual channel*). La différence entre ces deux valeurs est explicitée un peu plus loin.

ATM étant en mode avec connexion, avant toute émission de cellule, une connexion doit être mise en place. Pour cela, une association entre les références d'entrée et de sortie du réseau doit être définie. Cette technique est déjà utilisée dans les réseaux X.25.

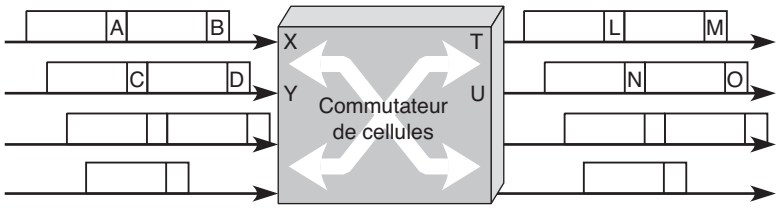
Le routage de la cellule de supervision, qui met en place le circuit virtuel, est effectué par des tables de routage, lesquelles déterminent vers quel nœud est envoyée la cellule de supervision avec l'adresse du destinataire final. Cette cellule de supervision détermine pour chaque nœud l'association entre le port d'entrée et le port de sortie. Ces associations sont regroupées dans la table de commutation.

La figure G.8 illustre l'association effectuée entre la référence et le port d'entrée dans un nœud de commutation et la référence et le port de sortie de ce même commutateur. Par exemple, si une cellule se présente à la porte d'entrée X avec la référence A, elle est transmise à la sortie T avec la référence L. La deuxième ligne du tableau de commutation constitue un autre exemple : une cellule qui entre sur la ligne X avec la référence B est envoyée vers la sortie U, accompagnée de la référence N de sortie.

Des connexions multipoint sont prévues dans la normalisation. Il suffit d'associer à une ligne et à une référence en entrée plusieurs lignes et des références en sortie. Les références permettant de commuter les cellules sont appelées, comme nous l'avons vu, VCI et VPI pour ce qui concerne la voie et le conduit. Dans un commutateur ATM, on commute une cellule en utilisant les deux références. Dans un brasseur, on ne se sert que d'une seule référence, celle du conduit. Par exemple, on peut commuter un ensemble de voies virtuelles en une seule fois en ne se préoccupant que du conduit. Dans ce cas, on a un brasseur de conduit, ou cross-connect, et l'on ne redescend pas au niveau de la voie virtuelle.

Figure G.8

Commutation des cellules dans un nœud de commutation



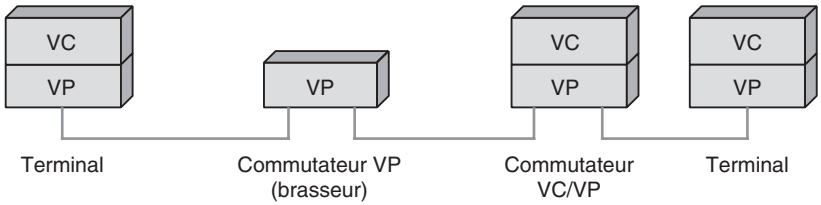
Les trames arrivant sur la porte d'entrée X avec la référence A sont dirigées sur la sortie T avec la référence L.

Ligne d'entrée	Référence d'entrée	Ligne de sortie	Référence de sortie
X	A	T	L
X	B	U	N
Y	C	T	M
Y	D	T	O
.			

La figure G.9 illustre un circuit virtuel avec un commutateur ATM et un brasseur.

Figure G.9

Circuit virtuel avec brasseur et commutateur ATM



Dans un brasseur de conduits, on commute simultanément toutes les voies virtuelles à l'intérieur du conduit. On a donc intérêt à regrouper les voies virtuelles qui vont vers la même destination de façon à les intégrer dans un même conduit. Cela simplifie grandement les problèmes de commutation à l'intérieur du réseau. La figure G.10 illustre, de façon assez symbolique, un même conduit partagé par un ensemble de voies. Le long du conduit, des brasseurs VP peuvent se succéder.

Figure G.10

Multiplexage de VC dans un VP

Longueur de la cellule ATM

La longueur de la zone de données, de 48 octets, est le résultat d'un compromis passé entre les Européens, qui souhaitaient 32 octets, et les Américains, qui désiraient 64 octets. Ce compromis a bien entendu un sens, que nous expliciterons.

La très faible longueur de la cellule est aussi explicable par une autre raison. Prenons l'exemple de la transmission de la parole téléphonique, qui demande une liaison à 64 Kbit/s. C'est une application isochrone qui possède deux contraintes :

- Une synchronisation très forte des données : un octet part de l'émetteur toutes les 125 µs, et les octets doivent être remis au codeur-décodeur de l'autre extrémité toutes les 125 µs.
- Un délai de propagation qui doit rester inférieur à 28 ms si l'on veut éviter les problèmes liés à la transmission de signaux sur une longue distance (suppression des échos, adaptation, etc.).

Si nous regardons le temps de transit des octets pour la parole sortant d'un combiné téléphonique, nous avons :

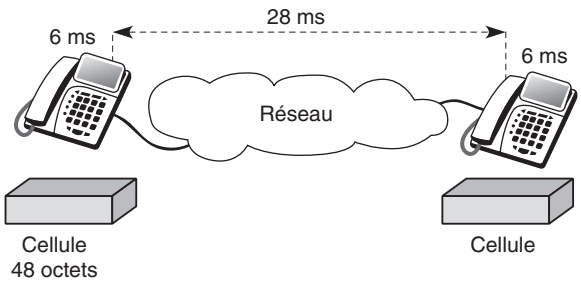
- Un temps de remplissage de la cellule par les octets qui sortent du combiné téléphonique toutes les 125 µs. Il faut donc exactement 6 ms pour remplir la cellule de 48 octets de longueur.
- Le temps de transport de la cellule dans le réseau.
- Encore 6 ms pour vider la cellule à l'extrémité, puisqu'on remet au combiné téléphonique un octet toutes les 125 µs.

Comme le temps total ne doit pas dépasser 28 ms, on voit que, si l'on retranche le temps aux extrémités, il n'y a plus que 16 ms de délai de propagation dans le réseau lui-même. En supposant que le signal soit transmis sur un câble électrique à la vitesse de 200 000 km/s, la distance maximale que peut parcourir le signal sans que l'écho soit détecté est de 3 200 km. Cette distance peut bien évidemment être augmentée si l'on ajoute des équipements adaptés (suppression des échos, adaptation, etc.). Comme le territoire nord-américain est très étendu, il a fallu mettre en place tous ces types de matériels dès les premières générations. C'est pourquoi les Américains préconisaient une meilleure utilisation de la bande passante en allongeant la zone de données des cellules par rapport à la partie supervision.

En Europe, pour éviter d'avoir à adapter le réseau terrestre, on aurait préféré une taille de cellule plus petite, de 32, voire 16 octets, de façon à gagner du temps aux extrémités. Ces contraintes sont illustrées à la figure G.11.

Figure G.11

Contraintes de propagation de la parole téléphonique



La commutation de cellules

L'ATM introduit une technique de commutation utilisant un circuit virtuel pour acheminer les cellules, qui ne sont autres que des trames ATM, d'une extrémité à l'autre du réseau.

La commutation de cellules est une commutation de trames assez particulière, puisque toutes les trames sont de longueur constante, cette longueur étant toute petite. La cellule est formée d'exactement 53 octets, comprenant 5 octets d'en-tête et 48 octets de données.

La cellule ATM est une trame et non un paquet. Pour retrouver le début et la fin de cette trame lors d'une transmission, il suffit de compter jusqu'à 424 bits pour déterminer la fin de la trame, le bit suivant correspondant nécessairement au début de la trame suivante. La difficulté de cette méthode de transmission, que nous préciserons plus loin, concerne la resynchronisation lorsqu'une erreur se produit et que le comptage des éléments binaires est perturbé.

Circuit virtuel et conduit virtuel

Le champ suivant contient la référence composée de l'identificateur de voie virtuelle et de l'identificateur de conduit virtuel, VCI/VPI (Virtual Channel Identifier/ Virtual Path Identifier). Le rôle des conduits virtuels est de fournir des connexions semi-permanentes.

Le circuit virtuel (VC), la connexion de circuit virtuel (VCC), le conduit virtuel (VP) et la connexion de conduit virtuel (VPC) se définissent comme suit :

- Le circuit virtuel, ou VC (Virtual Channel), est un terme générique utilisé pour décrire la capacité de communication pour le transport des cellules ATM. Un identificateur de circuit virtuel, ou VCI, classiquement appelé référence de commutation, est affecté à une liaison de VC qui transporte des cellules ATM entre deux nœuds ATM. Le nœud ATM, dans lequel la valeur VCI est traduite, s'appelle aussi un commutateur ATM.
- La connexion de circuit virtuel, ou VCC (Virtual Channel Connection), définit la connexion de bout en bout entre les deux points d'accès à la couche AAL. Une VCC est composée de la concaténation d'un ou plusieurs VC.
- Le conduit virtuel, ou VP (Virtual Path), est un faisceau de VC. Tous les VC d'un faisceau ont les mêmes nœuds extrémité.
- La connexion de conduit virtuel, ou VPC (Virtual Path Connection), est composée de la concaténation d'un ou plusieurs VP. Le nœud ATM est alors appelé un brasseur.

La figure G.12 illustre la hiérarchie VP/VC et la figure G.13 des exemples de VPC et de VCC. Le parcours d'une connexion VPC est établi par un routage de l'acheminement dans les brasseurs intermédiaires (A, B et C pour VP1 à la figure G.13).

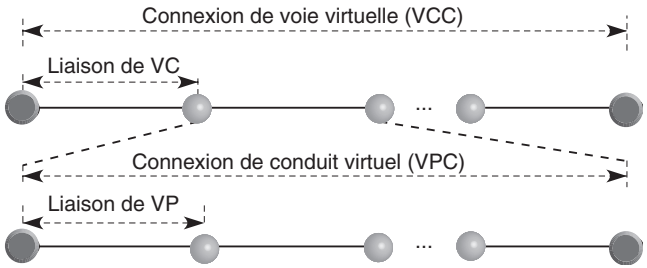


Figure G.12

Hiérarchie de liaison des VC, VCC, VP et VPC

Les nœuds de la partie supérieure de la figure G.13 sont des commutateurs. Les brasseurs ne participent pas à l'administration de la bande passante des conduits virtuels.

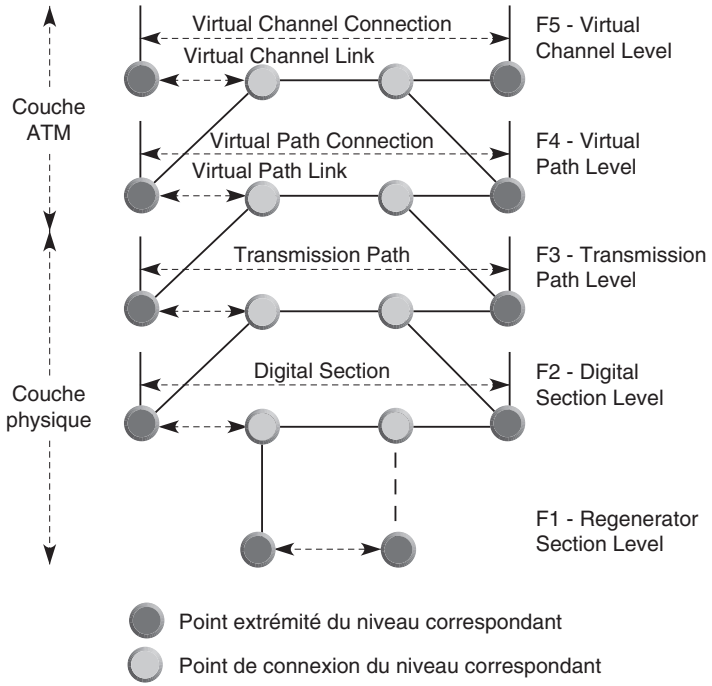


Figure G.13

Brasseurs et commutateurs ATM

L'architecture en couches de l'ATM

Les réseaux à commutation de cellules suivent les principes d'une nouvelle architecture, où les fonctionnalités ne sont pas regroupées aux mêmes niveaux que dans le modèle de référence.

La couche physique de ce nouveau modèle correspond à la couche physique du modèle de référence, mais avec une différence importante : la couche physique regroupe les bits par 424 pour retrouver directement la structure de la trame. La couche physique effectue donc un transport 424 bits par 424 bits et non bit par bit. Cette propriété permet à la couche du dessus d'appartenir au niveau trame puisque le début et la fin du bloc de données ont été déterminés par la couche physique. Nous verrons que la troisième couche du modèle ATM est de niveau message, avec également des différences importantes. L'architecture ATM est illustrée à la figure G.14.

Le rôle de ce nouveau modèle, dit modèle UIT-T, est de prendre en charge les applications multimédias, c'est-à-dire la superposition de la voix, des données et de l'image. Le modèle de référence de l'ISO n'était bâti que pour les applications de données et correspondait donc à l'architecture des réseaux d'ordinateurs.

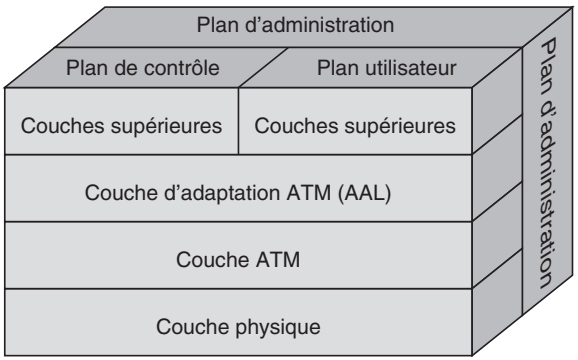


Figure G.14

Architecture ATM (modèle de référence UIT-T)

Le modèle UIT-T ne s'intéresse qu'au transport de bout en bout de l'information, et non à son traitement aux extrémités du réseau. Il est constitué de trois couches : la couche prenant en charge le transport des cellules sur un support physique, la couche se préoccupant de l'acheminement des cellules de bout en bout et la couche chargée de l'interface avec les couches supérieures et regroupant les cellules pour les délivrer à l'utilisateur.

La couche la plus basse concerne les protocoles de niveau physique dépendant du médium, ou PMD (Physical Medium Dependent). Cette couche PMD est elle-même divisée en deux sous-couches :

- La couche TC (Transmission Convergence), chargée du découplage du taux de transmission des cellules, de la génération et de la vérification de la zone de détection

d'erreur de l'en-tête, le HEC, de la délimitation des cellules, de l'adaptation de la vitesse de transmission et de la génération et de la récupération des cellules sur le support physique.

- La couche PM (Physical Medium), chargée de la transmission sur le support physique et des problèmes d'horloge.

Le protocole PMD décrit la façon dont les cellules sont émises sur le support physique. Plusieurs solutions ont été définies pour cela, dont les plus couramment implémentées reposent sur l'utilisation de SONET (Synchronous Optical NETwork) et de SDH (Synchronous Digital Hierarchy), normalisées par l'UIT-T. SONET décrit la structure d'une trame synchrone émise toutes les 125 µs. La longueur de cette trame dépend de la vitesse de l'interface. Les diverses valeurs des connexions SONET sont classées suivant la rapidité du support optique, ou OC (Optical Carrier).

La deuxième couche est celle de l'ATM proprement dite. Cette couche gère le transport de bout en bout de la cellule.

Enfin, la couche AAL (ATM Adaptation Layer), ou couche d'adaptation à l'ATM, se charge de l'interface avec les couches supérieures. Cet étage est lui-même subdivisé en deux niveaux, l'un prenant en compte les problèmes liés directement à l'interfonctionnement avec la couche du dessus, et l'autre ceux concernant la fragmentation et le réassemblage des messages en cellules. Dans cette couche AAL, quatre classes de services (A, B, C et D) ont été définies. Elles sont décrites au tableau G.1. À ces quatre classes de services correspondaient quatre classes de protocoles, numérotées de 1 à 4. Cette subdivision en quatre classes de protocole a été modifiée en 1993 par le regroupement des classes 3 et 4 et par l'ajout d'une nouvelle classe de protocoles, la classe 5, qui définit un transport de données simplifié.

TABLEAU G.1 • Classes de services de la couche AAL

	Classe A	Classe B	Classe C	Classe D
Synchro. source récepteur	Forte		Faible	
Flux	Constant	Variable		
Type de connexion	Orienté connexion			Sans connexion

La première classe de services correspond à une émulation de circuit, la deuxième au transport d'une application synchrone mais dont le débit est variable, la troisième à un transfert de données en mode avec connexion et la dernière à un transfert de données en mode sans connexion.

Performance des réseaux ATM

Les réseaux ATM n'ont que peu d'originalité. On y retrouve de nombreux algorithmes utilisés dans les réseaux classiques à commutation de paquets. Cependant, la hiérarchie des protocoles utilisés est assez différente de celle de la première génération de réseaux.

Dans les réseaux ATM, le temps d'émission d'une cellule demande quelques nanosecondes, ce qui est négligeable par rapport au temps de propagation sur le support, qui s'exprime généralement en microseconde. On peut donc considérer que la ligne physique, surtout si elle est un peu longue, représente une mémoire de plusieurs mégabits par seconde. Dans la structure des réseaux ATM, il faut toutefois tenir compte du temps d'attente dans les files de sortie des nœuds. Si l'on veut des portées de l'ordre de plusieurs milliers de kilomètres, il faut impérativement minimiser ces temps d'attente, de façon qu'ils restent relativement négligeables par rapport au délai de propagation.

Cette problématique est illustrée à la figure G.15. Si l'on suppose une liaison d'une longueur de 2 000 km et un débit de 1 Gbit/s, le temps de propagation est de 1 ms et le temps d'émission d'une cellule de 424 ns. Il y a donc 2 358 cellules en cours de propagation sur la liaison.

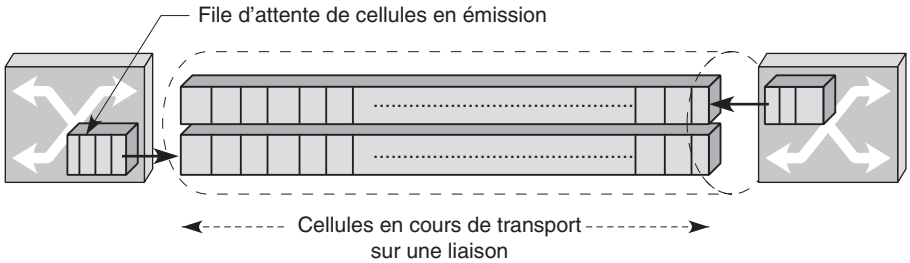


Figure G.15

Capacité de la ligne de transmission

Le réseau ATM est asynchrone, mais cet asynchronisme est faible du fait du rapport entre le temps de transmission et le délai de propagation. Ces contraintes de temps sont illustrées à la figure G.16, qui les compare avec la commutation de paquets. Le paquet, ici fragmenté en cinq cellules, arrive bien avant le paquet transporté en commutation de paquets.

La commutation de cellules a pour objectif de remplacer à la fois la commutation de circuits et la commutation de paquets. Pour ce faire, les principes des deux techniques doivent être respectés. Si l'on considère que l'ATM utilise des vitesses de transmission très élevées, le temps de transmission est très petit et même négligeable par rapport au temps de propagation du signal. Prenons l'exemple de lignes de communication à 1 Gbit/s. Pour émettre les 53 octets de la cellule, il faut un peu moins de 500 ns. Si l'on suppose qu'il faut ajouter quelques microsecondes pour franchir le commutateur, la somme du temps de traversée du commutateur et du temps de transmission est négligeable en comparaison du délai de propagation, qui vaut approximativement 1 ms pour 250 km, soit 10 ms pour 2 500 km.

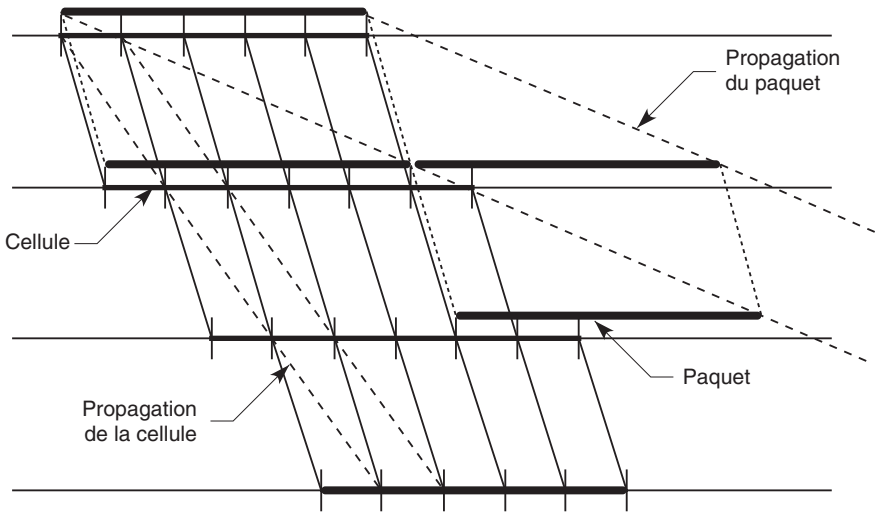


Figure G.16

Comparaison de la commutation de paquets et de cellules

Avantage de la séparation entre administration et établissement

La séparation entre l'administration de la bande passante et l'établissement des connexions de conduits virtuels procure les avantages suivants :

- Diminution des tâches d'administration : les tâches d'administration sont nécessaires uniquement pour les conduits virtuels, et non pour tous les circuits virtuels transitant dans les brasseurs. Une étude sur l'utilisation des conduits virtuels indique que, lorsque le brassage seul est utilisé, le nombre d'instructions diminue de 90 % par rapport à une commutation VP/VC.
- Facilité du contrôle de la bande passante dynamique : les changements de bande passante d'une connexion de conduit virtuel n'étant pas indiqués aux nœuds intermédiaires du conduit, le contrôle de la bande passante peut être réalisé plus facilement.
- Utilisation efficace de la bande passante : le contrôle dynamique permet d'utiliser efficacement la bande passante. Par exemple, la capacité d'un conduit virtuel réservé mais non utilisé peut être mise à zéro ou ramenée à une valeur déterminée à l'avance. De plus, la bande passante disponible peut être allouée aux conduits virtuels saturés.

Le concept de conduit virtuel permet d'avoir des services de ligne louée (*leased line services*). La figure G.17 illustre un réseau privé construit autour de deux réseaux locaux, ou CPN (Customer Premise Network), reliés par un conduit virtuel. Les connexions sont multiplexées sur le conduit virtuel et se partagent la bande passante disponible. L'augmentation ou la diminution de la bande passante d'un circuit virtuel étant simple à réaliser, l'utilisateur peut adapter son débit, étant entendu que la bande passante totale en utilisation ne peut dépasser la bande passante réservée au conduit virtuel.

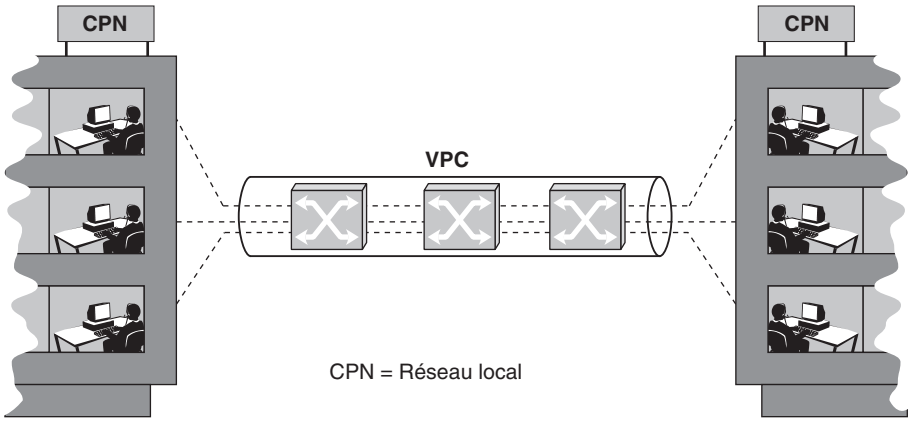


Figure G.17
Réseaux locaux reliés

La réduction des tables de commutation est l'une des raisons les plus importantes de ce découpage en VP et VC. Une fois le circuit virtuel établi, les cellules doivent être commutées d'une ligne d'entrée vers une ligne de sortie. Si la table de commutation compte plus de 4 000 entrées, le temps de commutation devient incompatible avec les temps de traversée des commutateurs souhaités par les opérateurs. Pour réduire cette table de commutation, la subdivision de l'adresse en deux parties permet de ramener le champ à examiner à 12 bits sur la partie intérieure au réseau. Pour les réseaux locaux, dans lesquels le nombre de clients connectés est bien moindre, le problème est différent, et des tables de commutation employant des références VP/VC sont permises.

Le champ PTI (Payload Type Identifier)

Le champ PTI permet d'identifier deux types d'informations de la cellule (*voir tableau G.2*). Les codes PTI, pour les cellules utilisateur, contiennent deux indications additionnelles :

- indication de congestion (référencée par le bit n° 3) ;
- indication d'utilisateur de la couche ATM à un autre utilisateur distant (référencée par le bit n° 2).

Tableau G.2 • Définition des identificateurs de capacité utile

0	Contrôle	0 1	Identificateur d'utilisateur	0 1	Notification de congestion
1	Gestion	0	Flux OAM F5 Gestion de CV	0	Locale
				1	De bout en bout
		1	Gestion de ressources	0	De ressources
				1	Réservé

Pour les cellules de gestion, les codes PTI permettent de distinguer les cellules du flux OAM (Operation And Maintenance) pour la gestion de CV des cellules de gestion de ressources. Les cellules appartenant au flux OAM sont également divisées en deux classes : de bout en bout et locale.

Le bit CLP (Cell Loss Priority)

Le bit CLP indique la priorité de la cellule. Si le bit est marqué (CLP = 1), la cellule est détruite en cas de congestion dans le réseau. S'il ne l'est pas (CLP = 0), la cellule est prioritaire par rapport aux cellules marquées. Le bit CLP permet de différencier deux classes de cellules d'une même connexion et de disposer de deux qualités de service en termes de perte de cellules ou de temps de transfert. Par exemple, dans le cas du service vidéo, les cellules de synchronisation peuvent être prioritaires.

Le bit CLP a une signification assez complexe puisqu'il peut être utilisé par l'opérateur pour marquer les trames en surplus après dépassement du seuil de débit négocié entre l'utilisateur et l'opérateur. De ce fait, un bit CLP marqué à 1 à l'intérieur du réseau peut avoir deux significations : soit l'utilisateur considère la cellule comme peu importante, soit la cellule est importante mais elle fait partie d'un surplus.

De par cette double signification, les équipementiers ont dû introduire des différences de gestion assez importantes dans leur architecture de contrôle au détriment de la compatibilité. C'est la raison pour laquelle on essaye de ne plus utiliser le bit CLP, dont la signification véritable est généralement incompatible entre équipementiers.

Le champ HEC (Header Error Control)

Le champ HEC est utilisé par la couche physique pour la délimitation de la cellule et le contrôle d'erreur dans l'en-tête.

La première fonction du HEC est de déterminer le début des cellules. Tant que la synchronisation n'a pas été trouvée, le coupleur génère le polynôme formé des quatre derniers octets reçus et le divise par le polynôme générateur. Si le reste correspond à ce qui se trouve dans le cinquième octet, ce sont bien les cinq premiers octets d'une cellule qui ont été trouvés, et cela correspond au début d'une cellule. Comme la cellule est elle-même transformée par un code de mixage, il est quasiment impossible de détecter un début de cellule qui n'en soit pas un. Rappelons que la cellule est une trame, et non un paquet, puisqu'il est possible de détecter son début et sa fin.

Les normalisateurs ont considéré que le taux d'erreur en ligne pour l'en-tête de la cellule n'était pas suffisant sur les lignes utilisées par la commutation ATM. Le HEC sert donc également à détecter les erreurs et à les corriger. Plus exactement, deux modes de fonctionnement ont été placés dans la norme. En mode normal, le mode par défaut, le HEC sert à détecter si un seul bit est en erreur et à corriger cette erreur. Si plusieurs erreurs sont détectées, la cellule est détruite, et l'on passe en mode de détection. Toutes les cellules avec une ou plusieurs erreurs sont alors détruites. On repasse en mode normal dès qu'une cellule est reçue sans erreur.

Le champ HEC est calculé à l'aide du polynôme constitué par les bits du champ de contrôle, à l'exception du champ HEC. Ce polynôme est divisé par le polynôme générateur $x_8 + x_2 + x + 1$. Le reste est introduit dans le HEC.

La couche d'adaptation ATM (AAL)

La couche AAL (ATM Adaptation Layer) a pour rôle de gérer l'interface avec les couches de protocole situées chez l'utilisateur. Ses fonctions dépendent des exigences de la couche supérieure. L'AAL doit supporter les besoins des différents utilisateurs du service d'AAL et donc des protocoles multiples.

L'AAL est composée de deux sous-couches : la sous-couche de convergence, CS (Convergence Sublayer), et la sous-couche de segmentation et de réassemblage, SAR (Segmentation And Reassembly). La fonction essentielle de la couche SAR est de segmenter les données des couches supérieures en un ensemble de segments de données correspondant à la taille des cellules. Au niveau du destinataire, la couche SAR rassemble les cellules pour restituer des données aux couches supérieures. La sous-couche CS dépend du service qui doit être rendu à l'utilisateur. Elle fournit le service de l'AAL au SAP (Service Access Point), ou point d'accès au service. Selon le protocole de niveau AAL, les sous-couches peuvent être vides si la couche ATM est suffisante pour les exigences des utilisateurs.

Les classes de services

L'UIT-T répartit les services du réseau ATM en quatre classes, fondées sur la relation de temps entre la source et le destinataire, le débit constant ou variable et le mode de connexion :

- Pour les services de classe A, le débit est constant et le service en mode avec connexion. Le service de type parole téléphonique à 64 Kbit/s en est un exemple typique. La relation de temps existe entre la source et la destination.
- Pour les services de classe B, le débit est variable. Un service typique peut être une parole téléphonique ou une vidéo compressée.
- Les classes C et D correspondent aux applications de transfert de données. Le débit est variable, et la relation de temps n'est pas nécessaire. Les transferts de données des classes C et D sont respectivement en mode avec connexion et sans connexion.

L'UIT-T recommande quatre types de protocoles AAL pour supporter ces classes de services (ces protocoles ayant été modifiés en 1993, nous donnons ici les dernières versions) :

- **AAL-1.** Supporte les services de la classe A et fournit de ce fait un service d'émulation de circuit en permettant d'utiliser toute la souplesse de l'ATM. Cependant, il n'exploite pas toute l'efficacité de l'ATM résultant du multiplexage statistique. Le service rendu par l'AAL-1 s'appelle CBR (Constant Bit Rate).
- **AAL-2.** L'histoire de ce protocole est plus complexe. Il a été défini au départ pour supporter les services de la classe B. Le service vidéo à débit variable en est un exemple.

Il permet d'exploiter non seulement la flexibilité mais aussi l'efficacité de l'ATM. Le service rendu par cette classe s'appelle VBR (Variable Bit Rate). L'AAL-2 a été abandonné au cours des années 95 pour être redéfini dans le cadre d'applications ayant des contraintes temporelles fortes et un débit variable. Pour arriver à paquétiser suffisamment rapidement, on a commencé à multiplexer plusieurs connexions sur le même circuit virtuel. Ce protocole est utilisé, par exemple, sur la partie accès de l'UMTS. C'est la raison pour laquelle ce nouvel AAL-2 est présenté à l'annexe S, consacrée à la téléphonie IP. Son rôle, dans ce cas, est de permettre le multiplexage de plusieurs connexions bas débit sur une connexion ATM de façon à tenir compte aux mieux des contraintes temporelles.

- **AAL-3/4.** Supporte les services de données en mode avec ou sans connexion, à débit variable et sans relation de temps. Le contrôle de flux entre les extrémités et la retransmission des fragments perdus ou altérés sont possibles. Les exemples de services que peut rendre ce type d'AAL sont nombreux : X.25, relais de trames (FMBS, Frame Mode Bearer Services), signalisation, etc. Cette classe n'est plus utilisée depuis 2005.
- **AAL-5.** L'autre nom de ce type d'AAL est SEAL (Simple Efficient Adaptation Layer). Il permet de transporter des trames de données non superposées en mode avec connexion (service de classe C). Le service rendu est de type élastique et utilise le service ABR (Available Bit Rate).

À ces quatre types correspondent quatre structures de trames de la couche SAR, appelées SAR-PDU (Segmentation And Reassembly-Protocol Data Unit).

La couche SAR (Segmentation And Reassembly)

Cette sous-couche définit les structures qui serviront réellement au transport de l'information. Les services CBR (Constant Bit Rate), VBR (Variable Bit Rate), ABR (Available Bit Rate), GFR (Generic Frame Rate) et UBR (Unspecified Bit Rate) sont définis sur les classes 1, 2, 3-4 et 5, qui introduisent une segmentation spécifique à chaque classe de services.

En résumé, le niveau AAL d'adaptation, et plus particulièrement sa sous-couche SAR, doit rendre les services suivants :

- assembler et désassembler les cellules ;
- compenser le délai variable de la méthode ATM ;
- prendre en charge les cellules perdues ;
- récupérer la synchronisation horloge.

L'unité de données du niveau SAR, la SAR-PDU, dépend du service qui doit être rendu, c'est-à-dire de la classe de transport de données.

AAL-1

La classe 1, qui correspond au service CBR, possède une SAR-PDU relativement simple, illustrée à la figure G.18.

Les champs SN (Sequence Number) et SNP (Sequence Number Protection) sont découpés suivant le schéma illustré à la figure G.19.

Figure G.18
SAR-PDU de type 1

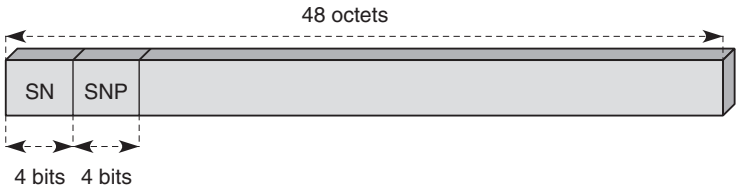
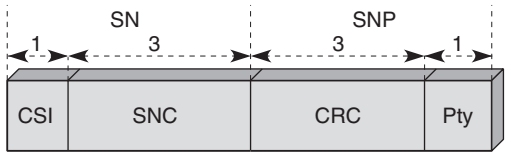


Figure G.19
Champ de supervision de l'AAL-1



CSI (Convergence Sublayer Information)
SNC (Sequence Number Counter)
CRC (Cyclic Redundancy Check)
Pty (Parity bit)

Le champ SNC (Sequence Number Counter) numérote la cellule sur 3 bits, c'est-à-dire de 0 à 7. En règle générale, l'émetteur émet plusieurs centaines de cellules avant que l'acquittement revienne, si bien qu'une numérotation de 0 à 7 apparaît très insuffisante. Les cellules sont numérotées en séquence de 0 à 7, et une cellule perdue est détectée par un trou dans la numérotation. Par exemple, si le récepteur reçoit la séquence 0, 1, 2, 4, 5, il en déduit que la cellule 3 a été perdue. S'il reçoit la séquence 2, 3, 4, 7, 0, 1, le récepteur comprend que les cellules 5 et 6 ont été perdues. Si huit cellules successives sont perdues, il n'y a plus aucun moyen de s'en apercevoir. On compte sur le fait que la probabilité de perdre plus de deux ou trois cellules successives est négligeable.

La zone SNP doit protéger le numéro de séquence afin de ne pas avoir à détecter d'erreur de déséquencement dues à une erreur sur la zone de numérotation elle-même. Ce champ est composé d'une zone de détection d'erreur sur 3 bits et d'un bit de parité paire.

Le bit CSI (Convergence Sublayer Information) permet de transporter une marque de temps RTS (Residual Time Stamp) pour caler l'horloge du récepteur ou délimiter des blocs de données. La marque de temps est sur 4 bits, transportée par le bit CSI d'une cellule sur deux (les cellules impaires d'une suite de huit cellules).

La vitesse d'arrivée des marques autorise le calcul d'un temps moyen entre deux arrivées, ce qui permet de synchroniser la restitution des cellules. Si la vitesse d'arrivée augmente, la restitution des cellules augmente aussi. C'est la technique SRTS (Synchronous Residual Time Stamp).

Pour le transfert isochrone de données à $n \times 64$ Kbit/s, un cadrage est effectué par un pointeur qui occupe le premier octet de la zone de données (il reste 46 octets de données).

Ce pointeur est indiqué par le bit CSI, présent dans les cellules d'ordre pair pour préserver la compatibilité avec la technique SRTS. Lorsque le bit CSI est à 1 dans une cellule paire (numérotée 0, 2, 4, 6), il indique l'existence d'un pointeur qui permet de connaître le degré de remplissage des 46 + 47 octets (93 octets) de la cellule paire, suivie de la cellule impaire. Dans l'octet du pointeur, seuls 7 bits sont utilisés, le huitième étant réservé à des développements futurs.

Une technique d'entrelacement d'octets (*byte interleave*) peut être ajoutée pour éviter la perte successive d'octets, une faute grave dans une transmission isochrone. Par exemple, si 47 octets sont en erreur, au lieu de perdre 47 octets successifs, on perd un octet tous les 47 octets. Dans le transport de la parole, il vaut mieux perdre un échantillon tous les 47 échantillons que 47 échantillons de suite.

La technique d'entrelacement est illustrée à la figure G.20.

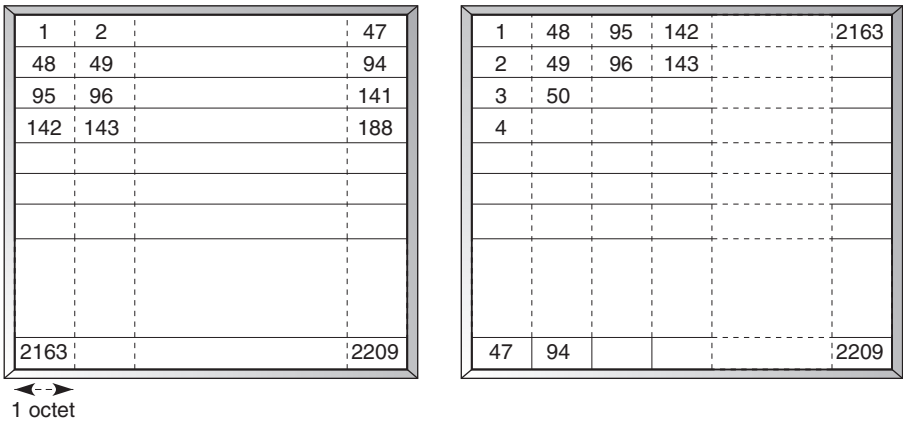


Figure G.20

Entrelacement des octets dans l'AAL-1

AAL-2 de 1990

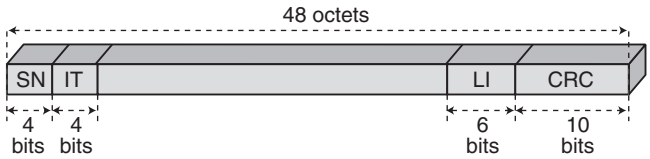
Nous présentons ici la version AAL-2 définie au début des années 1990 pour le service VBR.

Pour les services VBR, le rôle de la couche SAR est assez semblable à celui des services CBR :

- division et récupération des trames d'information ;
- prise en charge des cellules en partie remplies ;
- adaptation du débit ;
- prise en charge des cellules perdues.

La SAR-PDU de la classe 2 est illustrée à la figure G.21.

Figure G.21
SAR-PDU de type 2



Dans la structure de la SAR-PDU, on trouve quatre zones de supervision :

- SN (Sequence Number), sur 4 bits, qui permet de numéroter les trames modulo 16. Cette numérotation permet de détecter les trames perdues.
- IT (Information Type), sur 4 bits, qui indique le début, la continuation ou la fin d'un message.
- LI (Length Indicator), sur 6 bits, qui permet de détecter la zone de données effectivement occupée sur les 45 octets disponibles. Si ce champ porte la valeur 16, cela indique que les 16 premiers octets sont des données de l'utilisateur et que les 29 octets suivants ne sont pas utilisés.
- CRC (Cyclic Redundancy Check), sur 10 bits, qui permet de détecter des erreurs au cours du transfert.

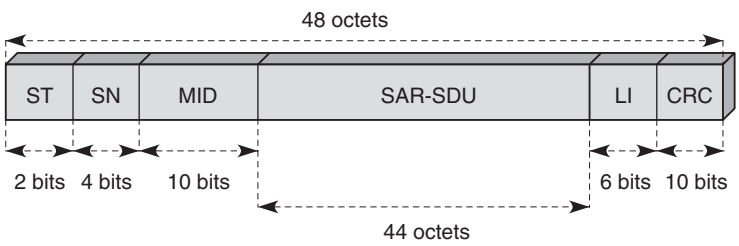
Ce protocole n'a pu être réellement utilisé à cause des évolutions technologiques sur la compression des applications vidéo. En effet, si la compression est extrêmement forte, une détection et une correction d'erreur doivent être ajoutées. En revanche, si la compression n'est pas trop poussée, le protocole n'a pas à se soucier d'une correction d'erreur. Devant ces incertitudes, les choix de l'AAL-2 n'ont pas résisté, et une nouvelle version tournée vers le transport de la parole et de la visioconférence dans l'UMTS est apparue en 2000.

AAL-3/4

Les types 3 et 4 ont été rassemblés dans une classe unique pour le transport sécurisé des données. Dans chaque cellule, une partie du message est transmise, et chaque partie est sécurisée par un CRC, permettant de détecter les erreurs qui peuvent survenir pendant le transport. Il y a donc, dans chaque cellule, tout un ensemble de zones de supervision, ce qui rend la procédure peu efficace.

La figure G.22 illustre la classe 3/4 de la couche AAL.

Figure G.22
SAR-PDU de type 3/4



Le champ ST (Segment Type) permet de structurer la communication. Quatre possibilités sont recensées :

- BOM (Beginning Of Message) – Début 10
- COM (Continuation Of Message) – Continuation 00
- EOM (End Of Message) – Fin de segment 01
- SSM (Single Segment Message) – Segment simple 01

Le champ SN (Sequence Number) permet la numérotation des cellules modulo 16. Le champ MID (Multiplexing IDentifier) est utilisé pour identifier les SAR-PDU appartenant à différentes SAR-SDU. S'il n'y a pas de multiplexage, ce champ est mis à 0. Le champ LI (Length Indicator) indique la longueur de la zone de données utilisée. Le reste du champ de données (*payload field*) est mis à 0.

Le polynôme permettant la détection des erreurs et générant le champ CRC est :

$1 + x + x_4 + x_5 + x_9 + x_{10}$

Assez complexe, la classe 3/4 comporte de nombreux champs de contrôle. Une nouvelle classe a été introduite en 1993, la classe 5, pour compléter le transport de données dans un cadre simple. Son rôle était au départ de permettre l'interconnexion de réseaux locaux. Sa conception a pris en compte la facilité de découpage de l'information provenant de la couche supérieure.

AAL-5

Le rôle de la classe 5 est de prendre l'entité de niveau supérieur et de la découper en tronçons de 48 octets pour l'introduire dans la zone de données de la cellule ATM. Ce schéma de découpage provient d'études préalables de la part de l'UIT-T sur le protocole SEAL (Simple Efficient Adaptation Layer).

La structure de la cellule SAR-5 et le découpage de l'entité de niveau supérieur sont illustrés à la figure G.23. Il y a un minimum de perte, puisque la CPCS-PDU (unité de données du protocole commun de la couche CS) est directement découpée en fragments de 48 octets.

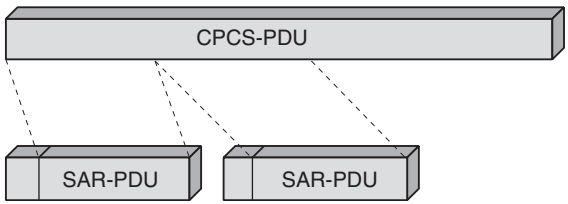


Figure G.23
Découpage de l'information dans la classe 5

La couche CS (Convergence Sublayer)

La couche CS se trouve au-dessus de la couche SAR. Elle définit le bloc d'information qui doit être transporté de bout en bout par la couche ATM après fragmentation

dans la couche SAR. Pour les classes 1 et 2, la couche CS délimite un bloc qui sera découpé suivant les principes exposés à la section précédente. Pour les classes 3/4 et 5, des fonctionnalités supplémentaires peuvent être introduites. Pour ces deux classes, la recommandation I.363 propose un découpage de la couche CS en deux sous-couches, la couche supérieure, SSCS (Service Specific Convergence Sublayer), et la couche inférieure, CPCS (Common Part Convergence Sublayer). La couche SSCS peut être vide.

La couche CPCS prend en charge les fonctions suivantes :

- délimitation ;
- séquencement ;
- réservation de mémoire aux extrémités ;
- détection d'erreur (en classe 5).

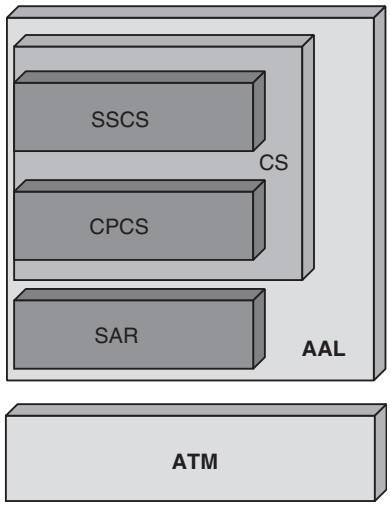
Les fonctionnalités de SSCS sont les suivantes :

- segmentation-réassemblage ;
- blocage-déblocage ;
- correction d'erreur ;
- contrôle de flux ;
- remise optionnelle des segments de ce niveau au niveau supérieur ;
- mode assuré, restreint aux communications point-à-point.

La taille maximale de la CS-PDU est de 65 535 octets.

L'architecture globale de la couche AAL est illustrée à la figure G.24.

Figure G.24
Architecture de la couche AAL

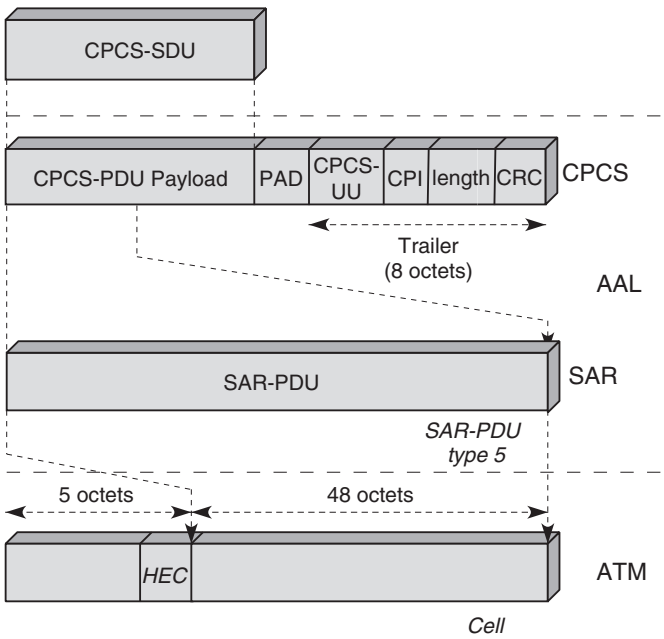


La couche CS-5

La figure G.25 illustre l'empilement des protocoles pour la classe 5.

Le champ PAD permet d'obtenir un champ de données d'une longueur multiple de 48 octets. Le découpage doit fournir des fragments d'une longueur de 48 octets. Il y a donc entre 0 et 47 octets mis à 0. Le champ CPCS-UU (CPCS User-to-User indication) permet d'indiquer le début, la continuation et la fin de la CPCS-PDU.

Figure G.25
Empilement des protocoles dans la couche CS-5



On retrouve dans le champ de supervision de fin de trame la zone Length, qui indique la longueur de la CPCS-SDU, et la zone CPI. La zone CRC, sur 4 octets, permet de détecter les erreurs sur la CPCS-PDU.

Les classes de services ATM

La technique de transfert ATM s'est stabilisée vers la fin des années 1990, après plus de dix années de normalisation intensive. La technologie a tellement évolué entre 1988 et aujourd'hui qu'il a fallu adapter les possibilités de l'ATM. La qualité de service constitue un point particulièrement sensible, puisque c'est l'élément qui permet de distinguer l'ATM des autres types de protocoles. Pour arriver à donner une qualité de service, il faut allouer des ressources, lesquelles sont parfois fortement sous-utilisées. Les recherches ont été nombreuses, et la solution a fini par être trouvée, sous la forme de classes de services.

La vision du contrôle des informations dans le réseau a beaucoup varié. Au départ, elle était fortement liée aux classes de services de la couche AAL définies dans les recommandations de l'UIT-T. L'ATM Forum a ensuite proposé cinq classes de services, définies dans un contexte un peu différent. Du coup, l'idée étant bonne, les opérateurs de télécommunications l'ont reprise en essayant de l'améliorer.

Les cinq classes de services de l'ATM Forum sont les suivantes (*voir aussi le tableau G.3*) :

- CBR (Constant Bit Rate), qui correspond à une émulation d'un circuit virtuel avec une bande passante fixe. Les services de cette classe incluent la voix et la vidéo temps réel sans compression.
- VBR (Variable Bit Rate), qui correspond à un circuit virtuel pour des trafics d'intensité variable dans le temps et plus spécifiquement les services par à-coups *(bursty).* Les services de cette classe incluent les transports d'applications vocales ou vidéo mais compressées ainsi que les services d'interconnexion de réseaux locaux ou le transactionnel. Il existe une classe VBR RT (Real-Time), qui doit prendre en compte les problèmes de temps réel.
- ABR (Available Bit Rate), qui permet d'utiliser la bande passante restante pour des applications aux débits variables et sensibles aux pertes. Un débit minimal doit être garanti pour que les applications puissent passer en un temps acceptable. Le temps de réponse n'est pas garanti dans ce service.
- GFR (Guaranteed Frame Rate), qui correspond à une amélioration du service ABR en ce qui concerne la complexité d'implantation de ce dernier sur un réseau. Le service GFR se fonde sur l'utilisation d'un trafic minimal. Si un client respecte son service minimal, le taux de perte de ses cellules doit être très faible. Le trafic dépassant le trafic minimal est marqué, et, si le réseau est en état de congestion, ce sont ces cellules qui sont perdues en premier. Le contrôle des paquets s'effectue sur la trame : si une cellule de la trame est perdue, le mécanisme de contrôle essaie d'éliminer toutes les cellules appartenant à la même trame.

Tableau G.3 • Comparaison des classes de services de l'ATM Forum

	Garantie de bande passante	Garantie de variance du délai	Garantie de débit	Retour d'indication de congestion
CBR	Oui	Oui	Oui	Non
VBR	Oui	Oui	Oui	Non
UBR	Non	Non	Non	Oui
ABR et GFR	Non*	Non	Oui	Oui

* Un minimum peut être garanti.

- UBR (Unspecified Bit Rate), qui correspond au service best-effort. Il n'y a aucune garantie ni sur les pertes ni sur le temps de transport. Le service UBR, qui n'a pas de garantie de qualité de service, n'est d'ailleurs pas accepté par les opérateurs télécoms,

qui ne peuvent se permettre de proposer un service sans qualité de service. Le service UBR correspond au service offert sur Internet. Cependant, la solution est totalement différente ici, puisque la priorité de plus basse qualité de service qu'offre l'UBR est appliquée non à l'ensemble des utilisateurs mais uniquement aux clients qui se partagent le résidu des ressources délaissées par les autres classes.

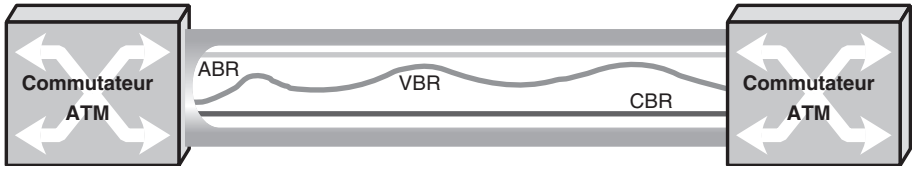


Figure G.26

Allocation des classes de services entre deux nœuds

La figure G.26 illustre l'allocation des classes de services. Dans un premier temps, les classes CBR et VBR sont allouées avec des ressources permettant une garantie totale de la qualité de service des données qui transitent dans les circuits virtuels concernés. Pour cela, on peut allouer les ressources sans restriction, puisque tout ce qui n'est pas utilisé peut être récupéré dans le service ABR. La partie basse de la figure indique la bande passante occupée par les clients CBR et celle du dessus la partie de la bande prise par les clients VBR. La partie supérieure est celle qui est laissée libre, et donc prise par les clients ABR. Si, dans les bandes CBR et VBR, une partie des bandes n'est pas utilisée, cette partie est affectée aux clients ABR.

Les classes de services de l'UIT-T

L'UIT-T a repris la proposition de l'ATM Forum en modifiant parfois légèrement les classes et en proposant une classe supplémentaire, ABT. Elle a supprimé l'UBR car les opérateurs ne souhaitaient pas offrir de service sans garantie.

Les quatre classes de l'UIT-T sont les suivantes :

- DBR (Deterministic Bit Rate). La bande passante est allouée sur la base du débit crête, ou PCR (Peak Cell Rate). C'est l'équivalent du service CBR de l'ATM Forum.
- SBR (Statistical Bit Rate). La bande passante est allouée sur la base du débit crête, du débit moyen, ou SCR (Sustainable Cell Rate), et de la longueur de la crête déterminée par l'IBT (Intrinsic Burst Tolerance). Le SCR fournit la moyenne en dehors des pointes. L'IBT donne une idée de la durée pendant laquelle le débit est au niveau crête.
- SBR + SBR RT (Statistical Bit Rate Real-Time). C'est le même type de service que le précédent, mais avec une contrainte de temps primordiale.
- ABR (Available Bit Rate). C'est le même service que dans l'ATM Forum.
- ABT (ATM Block Transfer). C'est un nouveau service normalisé par l'UIT-T. Il apporte une certaine souplesse tout en conservant une garantie complète aussi bien sur le taux d'erreur que sur le temps de réponse. Le service s'effectue sur des blocs de cellules

pour lesquels on doit indiquer le débit moyen. Le service ABT est similaire au service DBR mais pour un temps limité au bloc. Deux cas se produisent : soit le bloc est long, et l'opérateur peut effectuer une réservation de ressources pour garantir la qualité de service, soit le bloc est très court, et le temps de réservation devient long par rapport au temps d'émission des cellules du bloc. Dans ce dernier cas, la solution proposée par l'UIT-T consiste à envoyer le bloc sans réservation, en comptant sur la capacité statistique du réseau à supporter ce léger à-coup. Les deux services suivants sont appelés :

– ABT/DT (ABT with Delayed Transmission) ;

– ABT/IT (ABT with Immediate Transmission).

Le tableau G.4 récapitule les garanties fournies par les différents services de niveau ATM.

Tableau G.4 • Garanties des services de niveau ATM

	Service du niveau ATM					
Attribut	**DBR**	**SBR Real-Time**	**SBR Non-Real-Time**	**ABR**	**UBR**	**ABT**
Taux de perte de cellules	Spécifié (sauf pour CLP = 1)			Spécifié	Non spécifié	Spécifié
Délai de transfert de cellules Gigue	Spécifié	Spécifié	Spécifié Non spécifié	Non spécifié	Non spécifié	Spécifié
Débit crête	Spécifié	Spécifié	Spécifié	Spécifié	Spécifié	Spécifié
SCT/IBT	Non applicable	Spécifié	Spécifié	Non applicable	Non applicable	Spécifié
Contrôle temps réel par cellule RM	Non	Non	Non	Oui	Non	Oui

Comme nous le verrons, il faut ajouter un contrôle de flux, associé au service ABR, pour s'assurer que le taux de perte des cellules est négligeable. Le contrôle de flux choisi est de type rate-based.

La qualité de service ATM

Si l'ATM a été choisi comme mode de transfert pour le RNIS large bande plutôt que son concurrent, le mode de transfert temporel synchrone, ou STM (Synchronous Transfer Mode), c'est parce qu'il apporte un gain économique grâce au multiplexage statistique. Cependant, le multiplexage statistique de trafic en rafale peut provoquer des problèmes de congestion. Les travaux de l'UIT-T et de l'ATM Forum ont visé à minimiser cette congestion et à maximiser le taux d'utilisation du réseau, tout en garantissant la qualité de service spécifiée par l'utilisateur. Ces efforts ont abouti à la définition d'un contrat de trafic dépendant de la qualité de service requise et à la normalisation de fonctions de gestion de trafic.

Avant de regarder plus avant ces fonctions, nous allons définir précisément la qualité de service.

Une classe de qualité de service doit préciser des paramètres de performance (QoS spécifiée). Il est possible de ne spécifier aucun paramètre (QoS non spécifiée). Dans ce dernier cas, comme la QoS n'est pas précisée, on parle de la technique du meilleur effort possible de la part du réseau, ou service best-effort, pour satisfaire la demande de l'utilisateur. Comme expliqué au chapitre 7, le réseau Internet n'a jusqu'à présent proposé que ce service du fait des limitations de la première génération du protocole IP, IPv4. Si un utilisateur entre dans le réseau, on lui attribue une partie des moyens du réseau en les prélevant sur les ressources de tous les autres utilisateurs. Il y a donc partage des ressources. Il en ira autrement avec IPv6, qui permet une certaine qualité de service. Dans le cas de l'ATM, pour garantir une qualité de service, on préfère ne pas admettre de nouveaux clients, qui pourraient dégrader la qualité de service des autres utilisateurs.

Si la QoS est spécifiée par des paramètres de performance, on adopte, entre autres, les paramètres suivants :

- taux d'erreur par cellule (cell error ratio) ;
- taux de perte de cellules (cell loss ratio) ;
- délai de transfert par cellule (cell transfer delay) ;
- variation du délai de transfert par cellule, ou gigue (cell delay variation) ;
- taux de cellules mal insérées (cell misinsertion rate) ;
- délai moyen de transfert par cellule (mean cell transfer delay).

Un contrat de trafic est négocié entre l'utilisateur et l'opérateur du réseau ATM via l'interface UNI. Ce contrat de trafic doit contenir :

- une classe de QoS ;
- un descripteur de trafic sur la connexion demandée ;
- une définition de la conformité (on utilise également le mot anglais *conformance*).

La conformité (conformance) se réfère aux paramètres permettant d'être conforme à la demande de service d'un utilisateur. La classe de services peut être spécifiée ou non. Si elle ne l'est pas, cela correspond au service best-effort.

Le descripteur de trafic est un sous-ensemble des paramètres de trafic qui servent à décrire les caractéristiques du trafic des cellules sur la connexion. Ce descripteur contient les variables suivantes, qui diffèrent suivant les recommandations de l'UIT-T ou les propositions de l'ATM Forum :

- Descripteur du trafic source, qui peut lui-même contenir :
  - le débit crête, ou PCR (Peak Cell Rate) ;
  - le débit projeté, ou SCR (Sustainable Cell Rate) ;
  - la durée des rafales tolérée, ou BT (Burst Tolerance) ;
  - la tolérance de gigue, ou CDV tolerance (Cell Delay Variation tolerance).
- Algorithme déterminant le taux de génération des cellules, ou GCRA (Generic Cell Rate Algorithm), qui définit la conformité du trafic. Deux paramètres sont utilisés : le temps minimal entre deux émissions de cellule et la capacité maximale de

mémorisation. Lorsqu'une cellule se présente et que la capacité maximale est atteinte (cellule non conforme), cette cellule doit soit être détruite, soit être émise en surplus, soit prendre la place d'une autre cellule, qui, elle-même, peut être détruite ou envoyée en surplus. C'est là que le bit CLP devient opérationnel : si la cellule est envoyée en surplus, elle est marquée par le bit CLP = 1, qui permet à un nœud interne du réseau de la détruire en cas de congestion. Il y a donc deux classes de priorité : CLP = 0, qui correspond aux cellules les plus prioritaires, et CLP = 1, pour les cellules pouvant être détruites dans le réseau.

- Paramètres expérimentaux, qui permettent de faire passer dans la demande des caractéristiques spécifiques, correspondant le plus souvent à des propriétés particulières à des constructeurs.

Le contrôle de flux

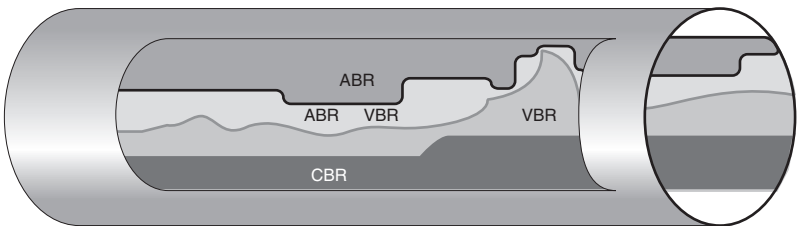
La conception des mécanismes de contrôle de flux efficaces pour ATM, permettant d'utiliser au mieux les ressources du réseau et de satisfaire la qualité de service requise, a été un véritable défi.

Toute la difficulté est située dans le temps de réaction des extrémités. Pour arriver à un contrôle relativement simple des flux ATM, l'ATM Forum, suivi par l'UIT-T, a décidé de regrouper les flux en différentes classes, comme expliqué précédemment. L'idée sous-jacente est la suivante : certains peuvent demander des tuyaux correspondant à des modes circuit, dans lesquels la garantie est complète, aussi bien en temps de réponse qu'en taux de perte, et d'autres se contenter de prendre l'espace laissé libre dans les tuyaux, un espace minimal étant toutefois réservé, même en cas de tuyaux complètement saturés.

La figure G.27 illustre cette idée de base. On y voit, en fonction du temps, le débit demandé par les clients CBR (la ligne interne la plus basse) et VBR (la ligne interne la plus haute), ainsi que la somme CBR plus VBR réellement utilisée (la ligne située entre les deux). Le trafic ABR peut atteindre cette ligne intermédiaire (débit CBR plus VBR réellement utilisé).

Figure G.27

Répartition des débits en fonction des classes de services



La répartition des informations par classe s'effectue de la façon suivante :

1. On affecte tout d'abord la bande passante au trafic CBR, et l'opérateur ne fait qu'additionner les bandes passantes demandées par les clients. On suppose que la bande passante ainsi réservée est bien utilisée.

2. Si ce n'est pas le cas, la place restant libre est réaffectée au trafic ABR.
3. Une fois cette affectation réalisée, l'opérateur retient une bande passante pour y faire transiter le trafic VBR. Cette réservation correspond, sur la figure G.27, à la somme des zones notées VBR et ABR VBR.

Cette réservation est à la charge de l'opérateur, qui peut l'effectuer de différentes façons, par exemple en réservant la somme des débits crêtes ou, après calcul, en faisant une surallocation, sachant qu'il y a peu de chance que tous les clients aient besoin du débit crête en même temps. Cela est du ressort de l'opérateur. Le client, quant à lui, doit pouvoir considérer qu'il dispose quasiment du débit crête pour que les garanties de ce service puissent être réalisées à coup sûr.

Dans la réalité, l'utilisation de cette bande passante réservée est largement inférieure à la réservation faite par l'opérateur. La zone utilisée est, sur la figure, la zone non hachurée notée VBR. La partie hachurée est la partie réservée mais non utilisée par le trafic VBR et qui est donc réaffectée au trafic ABR.

On comprend pourquoi le contrôle de flux est indispensable au trafic ABR. En effet, le rôle de ce trafic est de remplir, le plus près possible des 100 %, le tuyau global. Comme, à chaque instant, le volume de trafic avec garantie varie, il faut transmettre plus ou moins de trafic ABR de façon à être capable de dire à l'émetteur à tout instant quelle quantité de trafic ABR il faut laisser entrer pour optimiser l'utilisation des tuyaux de communication dans le réseau. Comme le trafic ABR n'a pas de garantie sur le temps de réponse, on peut se dire que si le contrôle de flux est parfait, on est capable de remplir complètement les voies de communication du réseau.

En d'autres termes, l'opérateur affecte l'équivalent de circuits aux utilisateurs qui veulent une garantie de temps de réponse et de taux de perte. Ces équivalents circuits correspondent à des cellules qui seront prioritaires dans les nœuds du réseau et pour lesquelles il n'y aura pas d'attente, si ce n'est l'arrivée simultanée de plusieurs cellules allant dans la même direction. Les cellules étant très courtes, cela entraîne un retard extrêmement faible, de quelques microsecondes. Il n'y aura donc pas de problème lors de la resynchronisation extrémité. Ensuite, toute la bande passante qui n'est pas utilisée par ces équivalents circuits est affectée au trafic ABR. On voit bien de la sorte que la technique de contrôle dans les réseaux ATM est devenue simple grâce à l'apparition de la structure en classes.

La quatrième classe, UBR, non illustrée à la figure G.27, peut fournir les données à transporter, sans aucune garantie de service, et remplir définitivement les tuyaux si, par hasard, le contrôle de flux ABR ne permettait pas d'arriver au niveau de 100 %.

Le contrôle de flux ABR

La méthode de contrôle de flux ABR (Available Bit Rate) a été introduite par l'ATM Forum. C'est une méthode réactive, qui essaye d'adapter nœud par nœud le débit provenant de la source pour contrôler le niveau du débit sur chaque circuit virtuel. Il faut définir un débit maximal, le PCR (Peak Cell Rate), un débit minimal, le MCR (Minimum Cell Rate), un débit initial, ICR (Initial Cell Rate), un accroissement de débit,

AIR (Additive Increase), un facteur de décroissance, RDF (Rate Decrease Factor), et un nombre de cellules Nrm entre deux cellules de gestion de ressource RM (Resource Management).

La source envoie une cellule de gestion de ressource RM toutes les Nrm cellules et, au pire, toutes les 100 ms. Cette source ne peut émettre à un débit supérieur à PCR et doit émettre au débit d'au moins MCR. Lors de l'initialisation de la source, un débit d'au moins ICR doit être émis. Une cellule RM est envoyée avant le début de la transmission. Suivant le débit entre deux cellules RM, la station source augmente son débit par AIR jusqu'au maximum PCR ou le diminue par RDF jusqu'à son minimum MCR.

La difficulté avec cette politique consiste à optimiser les paramètres d'augmentation et de diminution du débit sur chaque circuit virtuel et à faire remonter les informations de contrôle jusqu'à la source sans toutefois perdre trop de bande passante. L'obstacle majeur réside dans l'éloignement des nœuds puisque la méthode est réactive.

Considérons une liaison de 2 000 km, impliquant un délai de propagation de 10 ms, et un circuit virtuel au débit de 34 Mbit/s. Supposons que le dernier nœud du circuit virtuel décide de passer d'un débit ABR de valeur 34 Mbit/s à la valeur 0. Pour avertir l'émetteur de cette nouvelle valeur de débit acceptable dans le circuit virtuel, un temps de 10 ms est nécessaire. Cependant, il faut attendre 10 ms supplémentaires pour que le débit devienne nul à l'entrée du dernier nœud. Un temps aller-retour est en effet nécessaire pour que le débit ABR devienne effectivement nul, ce qui représente dans notre exemple 20 ms. Pendant ce temps, la quantité d'information arrivée au nœud congestionné correspond à 680 Kbit. Il suffit que ce nœud possède une mémoire de 85 Ko pour qu'aucun débordement n'ait lieu, ce qui représente une quantité relativement minime pour un canal à 34 Mbit/s.

On peut reprendre cet exemple de la façon suivante : si un nœud de commutation ATM possède un débit total de 34 Gbit/s, correspondant, par exemple, à 1 000 canaux de 34 Mbit/s, et si les nœuds extrémité, qui contrôlent les débits, sont situés en moyenne à 2 000 km, il faut une mémoire de 85 Mo pour garantir qu'aucune cellule ne sera perdue. Cette quantité est à la fois importante, à cause du coût des mémoires rapides (la mémoire doit absorber le débit de 34 Mbit/s), et faible par rapport à ce que l'on sait faire.

Cet exemple nous permet de comprendre les implémentations réalisées : placer dans les nœuds de grosses mémoires, capables de stocker les cellules lors d'une baisse du trafic ABR due au trafic prioritaire. Cette solution n'est toutefois pas compatible avec la conception des premiers commutateurs.

Un second problème est la reconnaissance du type de flux qui doit passer dans le commutateur. Si le flux est de type prioritaire, il faut traiter ses cellules immédiatement, en mettant en attente les cellules des flots ABR. La difficulté réside dans la possibilité de discerner instantanément les différents types de flux. Une première solution a consisté à noter le type de flux dans la table de commutation VPI/VCI au moment de l'ouverture du circuit virtuel. La qualité de service est alors inscrite dans la table de commutation par

la cellule de signalisation. Malheureusement, cette solution extrêmement lourde ne peut mener à de très hauts débits dans les commutateurs.

Une solution à ce problème consisterait à ce que la cellule porte en elle un indice permettant de détecter directement la qualité de service. C'est ce que font les paquets IPv6 dans les quatre premiers octets. Dans l'en-tête de la cellule ATM, les bits disponibles sont rares, voire inexistants. On pourrait penser que la zone Payload Type pourrait jouer ce rôle, mais il n'en est rien, cette zone se chargeant de transporter des notifications ou des flux de gestion F5 (niveau circuit virtuel). De plus, le bit CLP n'a plus vraiment d'intérêt avec le contrôle ABR et des mémoires tampons en nombre suffisant.

Le contrôle de flux du service ABR est très complexe à mettre en œuvre dès que le nombre de circuits virtuels passant par un nœud est important. En effet, pour déterminer les valeurs à faire remonter vers les sources, on utilise des algorithmes complexes, dits du max-min, qui demandent une forte puissance de calcul et qui n'optimisent pas les valeurs qui remontent. Pour les réseaux locaux, l'ABR est plus facile à mettre en œuvre. Devant cette difficulté, l'ATM Forum réfléchit à de nouvelles solutions plus aisées à mettre en œuvre.

Parmi ces solutions, la plus souvent citée est l'UBR+, qui offre une qualité de service supérieure à celle de l'UBR mais inférieure à celle de l'ABR. L'idée de base de cette solution consiste à contrôler le flux essentiellement à l'entrée du réseau. Dans l'UBR+, on définit deux seuils. Lorsque le premier seuil est franchi, une première limitation du flux entrant est effectuée. Au-dessus du second seuil, le débit d'entrée est plus fortement limité, et les paquets les moins importants sont détruits.

Gestion des réseaux ATM

Comme expliqué précédemment, dans l'ATM, le plan utilisateur doit être complété par deux autres plans : le plan de gestion et le plan de contrôle. Pour la partie gestion de réseau, la principale contribution de l'UIT-T est la recommandation I.610. Cette recommandation concerne à la base la maintenance de l'interface UNI et les accès au réseau. Son rôle est de décrire les fonctions permettant de maintenir le niveau physique et l'accès au niveau de l'interface ATM.

La recommandation I.610 se préoccupe des opérations de contrôle et de maintenance, ou OAM (Operation And Maintenance). Cinq environnements sont privilégiés : la gestion de performance, la détection de pannes, la protection du système, l'information sur les pannes et les performances et enfin la localisation des fautes.

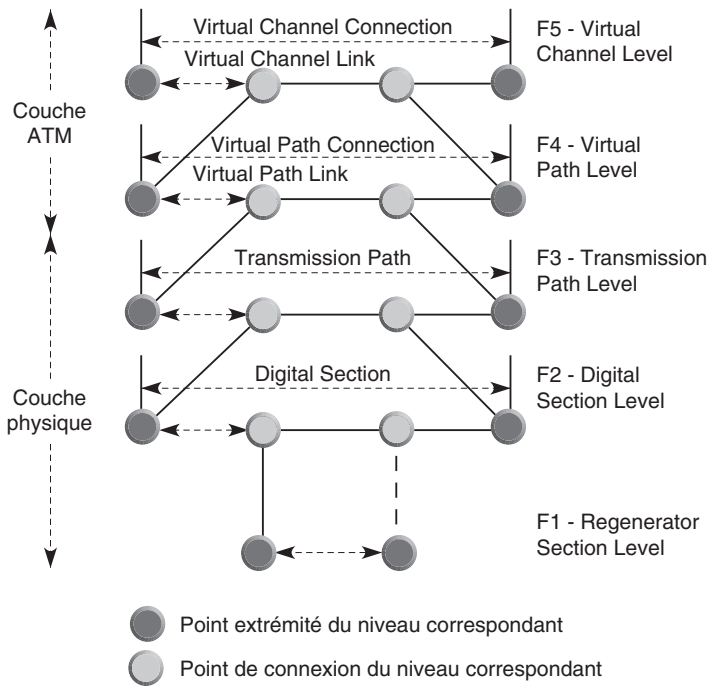
Les fonctions OAM sont réalisées dans le réseau par l'intermédiaire de cinq niveaux hiérarchiques OAM, associés aux deux niveaux ATM et PMD du modèle de référence UIT-T. Ces fonctions de contrôle et de gestion sont effectuées par des flots de données bidirectionnels : les flots F1, F2, F3, F4 et F5, dont voici la description :

- F1 : niveau section de régénération des signaux ;
- F2 : niveau section numérique ;
- F3 : niveau de transmission sur le chemin ;

- F4 : niveau du conduit virtuel ;
- F5 : niveau de la voie virtuelle.

Seuls les deux niveaux les plus élevés concernent la partie ATM. Toutes les autres fonctions s'appliquent au niveau physique. Nous avons représenté ces cinq niveaux de contrôle à la figure G.28.

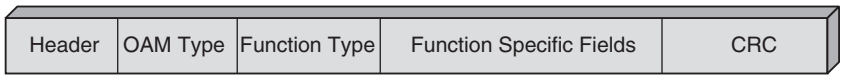
Figure G.28
Niveaux de contrôle et de gestion



Le flot F5 concerne le niveau de la voie virtuelle. Les cellules OAM du flot F5 sont identifiées par le champ PT (Payload Type), qui se trouve dans la zone de supervision. Ce champ indique une valeur PTI (Payload Type Identifier). La cellule OAM, pour chaque direction du flot F5, doit suivre une même route physique, de telle sorte que chaque nœud soit au courant de toutes les informations transportées dans un sens ou dans l'autre.

Les cellules OAM peuvent être insérées ou extraites aux différents points de connexion des VCC (Virtual Channel Connection).

Le flot F4 se préoccupe du niveau des conduits virtuels et a en charge le contrôle des VPC (Virtual Path Connection). Le flot F4 est bidirectionnel, comme le flot F5. Il est identifié par une valeur du VPI préassignée, généralement la valeur VCI = 3 pour le flux F4 sur un segment et VCI = 4 de bout en bout. Ses propriétés sont identiques à celles du flot F5. Cependant, le flot F5 est identifié par le format de la cellule OAM. Ce format est illustré à la figure G.29. En travaillant sur la gestion des performances, il est possible d'engendrer des messages qui transmettent les informations vers le récepteur ou vers l'émetteur.



OAM Type		Function type	
0001	Fault Management	0000	AIS (Alarm Indication Signal)
		0001	RDI (Remote Defect Indication)
		0010	Loopback
		0100	Continuity Check
0010	Performance Management	0000	Forward Monitoring
		0001	Backward Reporting
		0010	Monitoring and Reporting

Figure G.29

Format des cellules OAM

L'ATM Forum a défini une interface de gestion, nommée ILMI (Interim Local Management Interface). Cette interface permet à l'utilisateur d'obtenir des informations concernant les VP et les VC de l'interface UNI. Le protocole ILMI se fonde sur le standard de fait SNMP. Le mot intérim indique que ce standard n'est considéré que comme transitoire en attendant les recommandations de l'UIT-T. Cependant, il risque de devenir définitif puisque l'UIT-T est partie dans une direction différente en reprenant les standards CMIS/CMIP et TMN.

Le protocole ILMI est défini dans la RFC 1695.

Les principales fonctions du protocole ILMI sont les suivantes :

- indiquer le statut, la configuration et les informations de contrôle des niveaux liaison et physique de l'interface UNI ;
- gérer les adresses au travers de l'UNI.

La base de données de gestion de l'interface UNI fournit différents types d'informations, en particulier :

- des statistiques sur le niveau physique ;
- des informations sur le niveau ATM ;
- des statistiques sur les connexions VP et VC ;
- des informations sur les adresses enregistrées.

Le protocole ILMI supporte toutes les interfaces physiques définies par l'ATM Forum. Les deux extrémités de l'interface UNI gèrent un ensemble d'attributs, appelés UME (UNI Management Entities).

Les informations contenues dans les bases de données VPC ILMI MIB (VCC ILMI MIB) renseignent sur la connaissance de l'UME en fournissant des informations de configuration et les paramètres de QoS. Les enregistrements d'adresse permettent l'échange d'informations d'adresse et d'identificateur.

H

Annexe du chapitre 10 (Les réseaux IP)

Cette annexe décrit l'évolution d'Internet, depuis ses débuts et sa normalisation jusqu'à la solution actuelle, puis détaille certaines techniques de NAT.

Les débuts du réseau Internet

L'adoption quasi universelle de l'environnement IP en fait son principal intérêt. La DARPA (Defense Advanced Research Projects Agency) a développé un concept de réseaux interconnectés, Internet, au milieu des années 1970, avec une architecture et des protocoles qui ont acquis leur forme actuelle vers 1977-1979.

À cette époque, la DARPA est connue comme le premier centre de recherche sur les réseaux à transfert de paquets avec la création d'ARPAnet, à la fin des années 1960. Il est à noter qu'un projet assez semblable est développé en même temps en France sous le nom de Cyclades. Malheureusement, ce projet est arrêté pour laisser place au protocole X.25.

La disponibilité des fonds de recherche de la DARPA attire l'attention et éveille l'imagination de plusieurs groupes de chercheurs, notamment ceux qui ont déjà l'expérience du transfert de paquets dans ARPAnet. La DARPA organise des rencontres informelles avec les chercheurs pour mettre en commun des idées et discuter des expérimentations effectuées. À partir de 1979, il y a tant de chercheurs impliqués dans TCP/IP que la DARPA fonde un comité de coordination, appelé ICCB (Internet Control and Configuration Board). Le groupe se réunit régulièrement jusqu'en 1983, année où il est réorganisé.

Le réseau Internet démarre en 1980, quand la DARPA commence à convertir les protocoles du réseau de la recherche à TCP/IP. La migration vers Internet est complète en 1983, quand le bureau du secrétariat de la Défense rend obligatoires les protocoles pour

tous les hôtes connectés aux réseaux grande distance. Au même moment, ARPAnet est scindé en deux réseaux séparés, un pour la recherche, qui garde le nom d'ARPAnet, et un plus grand, réservé aux militaires, appelé Milnet.

Pour encourager les chercheurs à adopter les nouveaux protocoles, la DARPA propose des implémentations à bas prix. La plupart des ordinateurs des universités utilisent une version UNIX de l'Université de Californie, de Berkeley Software Distribution, appelée UNIX Berkeley. En fondant la société Bolt Beranek et Newman pour implémenter les protocoles et en finançant Berkeley pour intégrer TCP/IP dans ses produits, la DARPA réussit à couvrir 90 % des ordinateurs des universités scientifiques. Ce succès avec les ordinateurs scientifiques produira un effet d'entraînement sur les autres communautés.

En 1985, la NSF (National Science Foundation) commence à développer un programme destiné à mettre en place un réseau autour de ses six centres de supercalculateurs. En 1986, elle crée un réseau longue distance fédérateur, le NSFNET, pour relier tous ses centres de calcul et se connecter à ARPAnet. L'ensemble de ces réseaux interconnectés forme Internet, auquel viennent se greffer peu à peu de nouveaux réseaux.

Internet se développe alors rapidement pour interconnecter des milliers de réseaux aux États-Unis et en Europe et connaît un taux de croissance d'environ 15 % par an en 1987 avant d'atteindre le rythme de 60 % par an.

L'adoption des protocoles d'Internet s'élargit ensuite aux entreprises privées, qui commencent à se relier à Internet, avant de s'étendre aux réseaux privés d'entreprise, même s'ils ne sont pas connectés à Internet. Ces réseaux privés prennent le nom d'intranet.

La normalisation des réseaux IP

De nos jours, des centaines de sociétés importantes commercialisent des produits TCP/IP. Ce sont elles qui décident de la mise sur le marché de nouvelles technologies, et non plus les chercheurs, comme à l'origine. La gouvernance de l'Internet a été totalement repensée à la fin des années 2000. L'autorité sur les fonctions de coordination centrales d'Internet est exercée par l'IANA (Internet Assigned Numbers Authority). En fait, c'est Jon Postel qui exerçait cette charge jusqu'à son décès en 1998. Aujourd'hui c'est l'ICANN qui exerce cette fonction.

L'ICANN (Internet Corporation for Assigned Names and Numbers) est une organisation à but non lucratif domiciliée en Californie. Ses principales missions sont l'attribution des plages d'adresses de l'environnement IP, la sélection des paramètres des protocoles utilisés, la gestion du DNS (Domain Name System) et la gestion du nœud racine américain. Il est à noter qu'il existe un deuxième réseau Internet, indépendant de celui géré par l'ICANN, et qui est l'Internet chinois, doté de son propre nœud racine. Les Européens songent fortement à mettre en place également leur propre réseau Internet avec un nœud racine en Europe.

L'ICANN est géré par un conseil d'administration composé de 20 membres. À l'ICANN sont associées trois organisations, nommées SO (Supporting Organization), et des

comités consultatifs. Les trois organisations SO sont responsables de missions pour le compte de l'ICANN :

- DNSO (Domain Name SO) s'occupe des questions liées aux noms de domaines ;
- ASO (Address SO) prend en charge la gestion des adresses IP ;
- PSO (Protocol SO) traite des protocoles Internet.

Les comités consultatifs sont les suivants :

- Government Advisory Committee
- Root Server System Advisory Committee
- Budget Advisory Group
- Membership Implementation Task Force
- At-Large Member Study Committee

Nous ne détaillons ici que le PSO, qui s'occupe de la partie technique d'Internet. Le PSO (Protocol Supporting Organization) a pour mission de soumettre au conseil d'administration de l'ICANN des avis et recommandations pour toutes les questions touchant aux protocoles utilisés sur Internet, aux standards techniques permettant aux équipements d'extrémité d'échanger des informations et de gérer les communications sur Internet. Les signataires du décret de mise en place du PSO sont l'IETF, le W3C (World-Wide Web Consortium), l'UIT, l'ETSI et l'ICANN.

Quatre organismes sont regroupés dans le PSO :

- IETF
- IAB (Internet Activities Board)
- ISOC (Internet Society)
- IESG (Internet Engineering Steering Group)

L'IETF est un groupe d'individus qui se réunit trois fois par an pour contribuer au développement et à l'évolution d'Internet. Ses missions consistent à proposer des solutions aux problèmes techniques, formaliser les solutions retenues, les porter auprès de l'IESG en vue de la standardisation des protocoles et de leur utilisation sur Internet et être un forum de discussions. L'IETF n'est pas une organisation de standardisation au sens classique du terme, puisque tout le monde peut y participer et qu'il n'y a pas de représentation des organismes officiels de normalisation. Cependant, ses spécifications deviennent des standards.

La première réunion de l'IETF a lieu en janvier 1986 à San Diego. Seules 15 personnes y participent. Le quatrième meeting de l'IETF, en Californie également, en octobre 1986, est le premier à accueillir des participants étrangers. Le concept des groupes de travail est introduit lors du cinquième meeting, tenu toujours en Californie en février 1987. La barre des 100 participants est atteinte dès le septième meeting, tenu en Virginie en juillet 1987. En juillet 1989, lors du quatorzième meeting, tenu à Stanford, la structure de l'IETF est profondément remaniée, avec la séparation des activités de l'IAB en deux pôles distincts : l'IETF et l'IRTF (Internet Research Task Force), qui se préoccupe des projets de

recherche à long terme. Après la formation de l'ISOC en janvier 1992, l'IAB passe sous son autorité.

L'IAB a pour objectif d'arbitrer et de conseiller les autres organismes en ayant une vue d'ensemble de l'architecture Internet. Il peut aussi, dans le cadre de la procédure de définition des standards d'Internet, juger en appel de décisions prises par l'IESG. L'IAB est responsable de la sélection des membres de l'IESG parmi les nominés proposés par le comité de nomination de l'IETF.

L'ISOC est une association de professionnels qui s'intéresse à la croissance et à l'évolution d'Internet dans le monde en termes sociaux, politiques et techniques. Les responsables de l'ISOC doivent sélectionner les membres de l'IAB parmi les nominés proposés par le comité de nomination de l'IETF.

L'IESG supervise les activités techniques de l'IETF et le processus de définition des standards. Dépendant de l'ISOC, il applique les règles définies par cet organisme. L'IESG est directement responsable de la définition des standards, depuis le choix des propositions jusqu'à leur validation finale.

Les documents de travail, propositions et normes Internet sont édités dans une série de rapports techniques, appelés RFC (Request For Comments). Ces dernières peuvent couvrir des sujets précis ou vastes et faire figure de normes ou seulement de propositions. Les normes et la documentation relatives aux protocoles peuvent être obtenues auprès du site de l'IETF.

Chaque protocole Internet a un état et un statut. L'état du protocole spécifie l'avancement des travaux de normalisation :

- Initial (*initial*) : le protocole est soumis pour être examiné.
- Norme proposée (*proposed standard*) : le protocole est proposé comme norme et subit la procédure initiale.
- Norme de travail (*draft standard*) : le protocole a passé l'examen initial et peut être considéré comme étant dans sa forme semi-finale. Au moins deux implémentations indépendantes sont produites. Le document les décrivant est étudié par le groupe de travail *ad hoc*. Des modifications sont souvent introduites avant la norme finale.
- Norme (*standard*) : le protocole examiné est accepté comme une norme complète. Il fait officiellement partie de TCP/IP.
- Expérimental (*experimental*) : le protocole n'est pas soumis à normalisation mais reste utilisé dans des expérimentations.
- Historique (*historic*) : le protocole est périmé et n'est plus utilisé.

Normalement, les protocoles soumis doivent être passés en revue par le groupe de travail correspondant de l'IETF puis par les organismes cités plus haut avec une formalisation par l'IAB d'un statut. Le statut du protocole indique sous quelles conditions le protocole doit être utilisé :

- Exigé (*required*) : toutes les machines et les passerelles doivent implémenter le protocole.

- Recommandé (*recommended*) : toutes les machines et les passerelles sont encouragées à implémenter le protocole.
- Facultatif (*elective*) : on peut choisir d'implémenter ou non le protocole.
- Utilisation limitée (*limited use*) : le protocole n'est pas spécifié pour une utilisation générale, comme dans le cas d'un protocole expérimental.
- Non recommandé (*non recommended*) : l'utilisation du protocole n'est pas recommandée, par exemple pour un protocole périmé.

Le tableau H.1 récapitule les normes principales du monde Internet.

Tableau H.1 • Normes Internet

Nom	Description	Statut/RFC
ARP	Address Resolution Protocol	Elect. 826
RARP	Reverse ARP	Elect. 903
IP	Internet Protocol	Req. 791
ICMP	Internet Control Message Protocol	Req. 792
IGMP	Internet Group Multicast Protocol	Rec. 1112
UDP	User Datagram Protocol	Rec. 768
TCP	Transmission Control Protocol	Rec. 793

Les trois catégories de NAT

Le mécanisme de NAT que nous avons pris comme exemple précédemment, consistant à jouer sur les ports pour masquer plusieurs terminaux avec une adresse IP unique, est un cas particulier. Il repose sur une translation de port appelée NPT (Network Port Translation). Lorsqu'elle se combine avec le NAT, on parle de NAPT (Network Address and Port Translation).

Bien que les concepts soient différents, le processus de NAT inclut fréquemment par abus de langage le processus de NPT. En réalité, il faut distinguer trois formes de NAT, le NAT statique, le NAT dynamique et NATP. Ces formes peuvent se combiner selon les besoins de chaque utilisateur et les politiques d'administration établies dans un réseau. D'autres formes de classification du NAT sont possibles. La RFC 3489 en recense quatre types, par exemple. Nous nous contenterons de détailler dans les sections suivantes les formes les plus courantes.

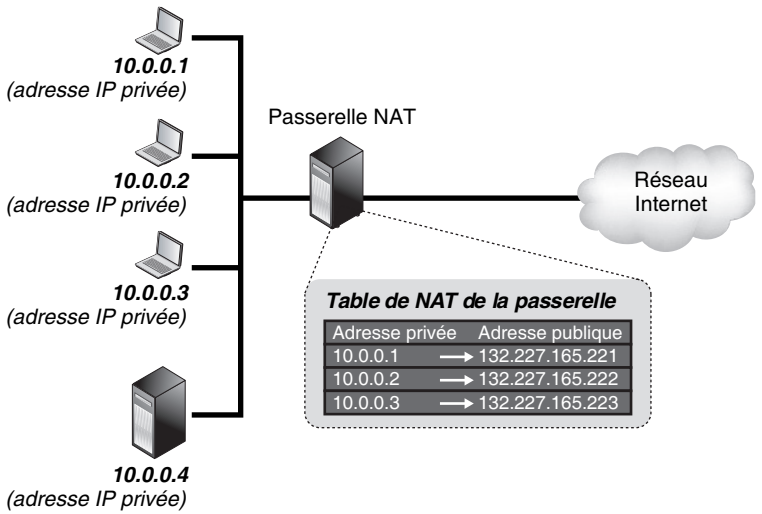
Le NAT statique

Dans le NAT statique, à toute adresse IP privée qui communique avec l'extérieur, une adresse IP publique fixe lui est affectée. Avec ce type de NAT, les utilisateurs du réseau local sont joignables de l'extérieur, car la passerelle réalise la correspondance d'une adresse IP locale en une adresse IP publique dans les deux sens. C'est un avantage

indéniable, en particulier pour la téléphonie, car un utilisateur à l'extérieur du réseau privé peut appeler un abonné à l'intérieur du réseau privé puisqu'il connaît son adresse IP fixe.

Ce cas de figure est illustré à la figure H.1. Le terminal ayant l'adresse IP privée 10.0.0.4 n'a pas de correspondance d'adresse IP publique, car c'est un serveur interne. Les administrateurs font l'économie d'une adresse IP pour ce serveur et s'assurent en outre que ce dernier n'est pas joignable directement de l'extérieur. Un changement de FAI ne remet pas en cause le plan d'adressage en local.

Figure H.1
Le NAT statique



Le NAT dynamique

Avec le NAT dynamique, une plage d'adresses IP publiques est disponible et partagée par tous les utilisateurs du réseau local. Chaque fois qu'une demande d'un utilisateur local (avec une adresse privée) parvient à la passerelle NAT, celle-ci lui concède dynamiquement une adresse IP publique. Elle maintient cette correspondance pour une période fixe, mais renouvelable selon l'activité de l'utilisateur, qui assure le suivi des communications.

Avec ce type de NAT, les utilisateurs locaux ne sont joignables de l'extérieur que s'ils ont une entrée dans la table de la passerelle NAT, autrement dit que s'ils entretiennent une activité avec le réseau Internet. En effet, les correspondants externes ne peuvent s'adresser qu'à la passerelle NAT pour envoyer leur flux. Or tant que le correspondant interne n'a pas d'activité réseau, aucune entrée ne lui est attribuée dans la table de NAT. De plus, l'adresse IP qui leur est affectée est temporaire et peut être différente à la prochaine connexion, ce qui restreint les possibilités d'être joignable de l'extérieur.

Il existe même une forme de NAT particulière, appelée NAT symétrique ou « full cone » dans la RFC 3489, qui consiste à établir une correspondance entre l'adresse IP privée et publique selon la destination d'une communication. Autrement dit, un utilisateur du

réseau local aura une certaine adresse IP publique lorsqu'il communique avec un correspondant extérieur et une autre adresse IP publique lorsqu'il communique avec une autre destination.

Le modèle dynamique offre une plus grande souplesse d'utilisation que le modèle statique puisque les associations d'adresses IP privées et publiques n'ont pas besoin d'être mentionnées statiquement par l'administrateur, mais sont attribuées automatiquement. En outre, il présente l'avantage d'optimiser au maximum les ressources. Si un utilisateur n'exploite pas sa connexion Internet et se contente de sa connexion locale, la passerelle NAT n'a pas besoin de lui attribuer une adresse IP. Le NAT dynamique est cependant plus complexe puisqu'il impose à la passerelle NAT de maintenir les états des connexions pour déterminer si les utilisateurs exploitent leur adresse IP publique ou s'il est possible, passé un certain délai, de les réutiliser.

Ce modèle ressemble à celui déployé avec la téléphonie RTC. Le nombre de lignes sortantes d'un commutateur téléphonique d'entreprise et même d'immeubles de particuliers est généralement inférieur au nombre de lignes entrantes. Autrement dit, tous les abonnés disposent d'un téléphone, mais tous ne peuvent appeler en même temps. Dans la pratique, il est assez exceptionnel que tous les abonnés appellent en même temps, si bien que ces derniers ne perçoivent pas cette restriction, qui permet aux opérateurs de limiter le nombre de lignes. Avec le NAT dynamique, les notions sont différentes, mais le principe est le même : l'attribution des adresses IP se fait à la demande, avec les limitations du nombre d'adresses IP publiques disponibles que cela suppose.

Le NAPT

Variante du NAT dynamique, le NAPT (Network Address Port Translation) est en fait celui que nous avons présenté précédemment sans le nommer. Il consiste à attribuer une même adresse IP à plusieurs utilisateurs d'un même réseau local.

Comme nous l'avons expliqué, pour associer une même adresse IP publique à deux terminaux ayant une adresse privée distincte, la passerelle NAT joue sur les ports des applications : une requête envoyée à partir du port A d'une source est retransmise avec le port B de la passerelle, tandis qu'une requête émise à partir du port C d'une autre source est retransmise avec le port D de la passerelle. De cette manière, la passerelle peut contrôler et distinguer chacune des demandes qui lui parviennent.

L'inconvénient de cette méthode est que seuls les utilisateurs du réseau local peuvent amorcer une communication vers l'extérieur. Autrement dit, ils ne peuvent répondre à une communication qu'ils n'ont pas préalablement initiée. Les correspondants externes à la passerelle NAT ne possèdent en effet des entrées que pour une adresse IP et un port source privés. Or si le port source est mentionné, c'est qu'une application a déjà été ouverte par le terminal du réseau local. Le correspondant externe n'a aucun moyen d'établir une telle association en lieu et place du terminal dont il ignore la véritable adresse IP.

Le NAPT est sans conteste la méthode la plus économe puisqu'elle permet de masquer tout un réseau local avec une seule adresse IP. Elle est la plus couramment employée chez les particuliers et les petites et moyennes entreprises.

Les problèmes engendrés par le NAT

Pour être pratiques et courantes, les fonctionnalités du NAT n'en posent pas moins des problèmes de différente nature, comme les protocoles dits « sensibles » au NAT, la difficulté de recevoir une connexion derrière un NAPT ou la sécurité.

Les sections suivantes détaillent chacun de ces problèmes.

Les protocoles sensibles au NAT

Le problème le plus important à considérer concerne les protocoles dits « sensibles » au NAT. C'est le cas des principaux protocoles de signalisation utilisés pour les échanges multimédias, dont H.323, SIP et MGCP, mais également de bien d'autres protocoles, comme Kerberos, SNMP, DNS, ICMP ou encore les protocoles de partage de fichiers tels que FTP et les protocoles de mobilité tels que Mobile IP.

Ces protocoles ne se contentent pas de mentionner leur adresse IP dans l'en-tête des paquets qu'ils envoient, mais ils l'indiquent également dans le corps de leurs messages. Par exemple, avec le protocole SIP, un message d'invitation INVITE comporte dans le paquet des informations sur l'adresse IP de la source. Ces informations permettent d'établir entre les correspondants la connexion dans laquelle les données véritables (la voix ou la vidéo notamment) sont transmises. Dans cette situation, même si le boîtier NAT modifie l'adresse IP source du paquet, le récepteur ne peut répondre correctement à la requête puisque cette dernière comporte une adresse IP source initiale, qui est une adresse privée. Le récepteur envoie donc sa réponse vers l'adresse IP source spécifiée qui ne lui est pas accessible, et le paquet de réponse n'arrive jamais à son destinataire.

Cette contrainte ne se pose pas pour toutes les applications. Par exemple, les flux d'application Web utilisent le protocole HTTP, dont les paquets ne contiennent pas l'adresse IP de la source à l'origine de la requête. En conséquence, le récepteur peut répondre sans connaître de problème de routage. Ce cas est en fait celui de la majorité des protocoles.

Recevoir une connexion derrière un NAPT

Ce problème est spécifique au NAPT, qui translate les utilisateurs à la fois selon une adresse IP et selon un port. La question qui se pose est de savoir comment solliciter une entité masquée derrière un boîtier NAPT.

Nous avons vu le cas où un terminal en adressage local effectuait une demande de connexion. La table de NAPT est alors mise à jour conformément à la demande du terminal local, et la connexion avec l'extérieur peut se poursuivre. Mais comment faire si ce n'est pas le terminal local au boîtier NAPT qui initie la connexion, mais un terminal distant ? Dans ce cas, le terminal distant ne sait pas vers où envoyer sa demande de connexion, puisque la seule adresse publique est celle du boîtier NAPT et que la table de NAPT ne contient à ce stade aucune entrée permettant de déterminer à qui est destinée cette communication.

Une solution élémentaire à ce problème pourrait consister à connaître le port d'écoute d'une application et à configurer sur le boîtier NAPT une règle de redirection des paquets externes à destination de ce port d'écoute vers une machine locale en particulier. Par

exemple, tous les paquets reçus d'Internet à destination du port 34567 sont systématiquement redirigés vers le terminal dont l'adresse IP est 10.0.0.2. Si ce dernier a configuré son application pour utiliser le port 34567 comme port d'écoute, la connexion devient possible.

Malheureusement, cette solution n'est guère satisfaisante. Deux applications qui tournent sur deux terminaux distincts ne sont pas adressables simultanément. En outre, la procédure n'est pas automatique, et il est nécessaire de configurer statiquement les règles de redirection, ce qui rend le mécanisme contraignant pour l'administrateur du réseau, en plus de ne pas être toujours une fonctionnalité disponible sur les boîtiers NAPT. Sur la majorité des équipements, les règles de redirection sont configurées au moyen d'une interface Web propriétaire et non compatible selon les différents constructeurs.

La sécurité avec le NAT

Comme les codes de contrôle (checksums) inclus dans les en-têtes TCP d'un paquet sont calculés en fonction de l'adresse et du port du terminal source, ils deviennent invalides lorsque la passerelle NAT a modifié l'un ou l'autre de ces deux éléments. Si le destinataire reçoit le paquet avec le code de contrôle initial, il considère le paquet comme corrompu et demande sa réémission. En conséquence, la passerelle NAT doit recalculer les codes de contrôle et remplacer les originaux afin que les paquets restent valides et ne soient pas considérés par le destinataire comme corrompus.

Pour cette raison, le mécanisme de NAT est davantage une parade à la pénurie d'adresses IP qu'une véritable solution. Il ne se met en place qu'au prix de traitements sensibles et pas toujours réalisables. Par exemple, si l'émetteur crypte ses flux avec une couche IPsec, il devient impossible pour la passerelle NAT d'accéder aux en-têtes TCP des paquets relayés et donc de les modifier, si bien qu'ils sont transmis de manière erronée aux destinataires, qui les refusent.

On peut considérer le NAT comme une forme de « hack », en ce qu'il impose une rupture entre un émetteur et son récepteur et ne respecte pas les en-têtes d'origine des paquets, puisqu'il doit retravailler certains champs pour que les paquets demeurent conformes aux spécifications des protocoles.

En résumé

Conçue essentiellement pour faciliter l'administration d'un réseau et offrir une solution alternative aux restrictions d'adressage du protocole IP dans sa version 4, la translation d'adresses est aujourd'hui largement déployée, à la fois chez les particuliers et dans les entreprises, sous différentes formes, plus ou moins restrictives. Elle fait néanmoins intervenir, de manière obligatoire, une entité tierce intermédiaire entre l'émetteur et le récepteur. Cette technique impose donc des traitements supplémentaires sur les flux. Or ces traitements ne sont pas toujours compatibles avec d'autres protocoles. En particulier, le NAPT bloque la réception d'appel. Et surtout, les protocoles de signalisation les plus courants ne prennent pas en compte la translation d'adresse qui sera appliquée aux flux et insèrent dans leur message des adresses privées, invalides pour un récepteur distant.

Le passage des pare-feu

Les pare-feu constituent des remparts indispensables pour se protéger des attaques extérieures. Ils sont aujourd'hui couramment employés, à la fois par les particuliers et par les entreprises. Par le biais de règles de filtrage, ils inspectent tous les paquets qui transitent et vérifient s'ils sont conformes à la politique de sécurité implémentée. Si c'est le cas, les paquets sont autorisés à traverser le pare-feu et à poursuivre leur cheminement vers leur destinataire. Si ce n'est pas le cas, ils sont détruits.

Les pare-feu les plus classiques distinguent cinq éléments qui caractérisent les flux : l'adresse IP de la source, le port utilisé par la source, l'adresse IP du destinataire, le port utilisé par le destinataire et enfin le protocole de transport spécifié dans un paquet. Une règle de filtrage mentionne donc la valeur de chacun de ces cinq éléments et ordonne une action à entreprendre lorsque toutes ses valeurs sont validées.

L'action entreprise revient soit à autoriser, soit à interdire le paquet, c'est-à-dire respectivement à laisser passer le paquet ou à le détruire. Typiquement, un pare-feu adopte pour politique de bloquer tous les paquets pour lesquels aucune règle d'acceptation ne convient. La politique inverse, consistant à autoriser tous les paquets pour lesquels aucune règle d'interdiction ne convient, est trop permissive.

L'état d'une connexion peut être un sixième élément à prendre en compte par un pare-feu. Lorsqu'une communication est établie avec les cinq éléments précédemment mentionnés, on considère que la connexion est à l'état actif ou établi. Autrement, l'état est considéré comme inactif.

On distingue ainsi deux catégories de pare-feu :

- Les pare-feu sans état (*stateless*), qui ne maintiennent aucun état des connexions et se contentent des cinq éléments caractéristiques d'un flux, précédemment cités pour autoriser ou interdire les flux qui transitent dans le réseau.
- Les pare-feu avec état (*statefull*), qui maintiennent l'état des connexions et sont capables de distinguer si une communication s'effectue sur un port déjà ouvert ou sur un port que le paquet demande d'ouvrir.

La notion d'état est utile pour les protocoles à ports dynamiques. Avec des applications exploitant ces protocoles, une communication s'établit sur un port fixe vers un destinataire (canal de contrôle). Lorsque ce dernier est contacté, il convient avec l'émetteur de poursuivre la communication sur un autre port dynamiquement et arbitrairement sélectionné (canal de données). De cette façon, il reste disponible pour servir un autre correspondant qui tenterait de le joindre ultérieurement sur le port fixe. Face à une telle situation, seul un pare-feu avec état est capable d'autoriser l'usage du port dynamique. Pour cela, il lui faut analyser les paquets et déterminer s'ils sont liés ou non à une connexion préalablement établie.

Imaginons à titre d'exemple un protocole dans lequel un destinataire demande à la source de remplacer le port statique initial par un port dynamique qu'il lui impose. Les trois étapes suivantes sont nécessaires :

- La source émet un premier paquet vers un port fixé du destinataire.

- Le destinataire lui répond en précisant le port sur lequel il souhaite poursuivre la communication.
- La source reprend la communication en utilisant le port mentionné.

Pour le pare-feu sans état, seules les deux premières étapes sont possibles puisqu'elles peuvent correspondre à une règle statique simplement fondée sur le « 5-uplets » initial. L'ouverture d'un port dynamique lui est impossible, car aucune règle n'en permet la définition, sauf à être totalement permissive et d'ouvrir tous les ports possibles, ce qui constituerait une piètre politique de sécurité.

Pour le pare-feu avec état, la troisième étape est possible. En effet, ce type de pare-feu est capable d'analyser les flux et de déterminer que le port dynamique sur lequel la source tente de communiquer correspond à la demande qui a été faite précédemment par la destination. La gestion des états offre une performance accrue dans le traitement des paquets, mais cela a un coût en ce qu'elle introduit une latence supplémentaire pour le pare-feu, qui doit en outre savoir analyser les protocoles correctement et, pour cela, connaître leur syntaxe.

L'état est facilement discernable avec le protocole TCP, puisque ce dernier positionne des bits indiquant si la connexion est nouvelle, se poursuit ou se termine. Au contraire, le protocole UDP ne fournit pas ces indications. Pourtant, le pare-feu ne peut attribuer éternellement le statut d'actif à une connexion UDP. Il alloue généralement le statut actif à une connexion UDP pendant un certain délai. Passé ce délai, la connexion est considérée comme perdue et devient par conséquent inactive.

Cette manière de procéder est cependant très approximative et ne convient pas aux applications de voix sur IP, qui utilisent très majoritairement le protocole UDP pour transporter leurs données. Si, lors d'une communication, les intervenants cessent de parler, le silence correspondant n'est pas transmis, et aucun paquet n'est transmis durant cet intervalle de temps. Le pare-feu risque de considérer ce silence comme une terminaison de la communication, ce qui est erroné.

Un pare-feu est utile pour centraliser la politique de sécurité au sein d'un équipement unique. De cette manière, la gestion du contrôle des applications autorisées n'est pas laissée au libre choix des utilisateurs, mais est à la charge du réseau, ce qui réduit les possibilités de contournement des règles édictées au sein de l'entreprise.

Les fonctionnalités de NAT sont souvent implémentées en parallèle avec les fonctionnalités de pare-feu. En effet, l'opération réalisée par le NAT comme par le pare-feu doit s'appliquer au niveau d'une passerelle, point de jonction entre le réseau local privé et le réseau public. En outre, dans ces deux fonctions, une notion de filtrage est requise. Lorsque les flux traversent le réseau, le boîtier NAT détecte l'adresse IP source privée et la translate avec une adresse IP publique, tandis que le pare-feu inspecte l'adresse IP source pour savoir si l'utilisateur est autorisé à émettre des flux. Dans le même temps, le pare-feu détecte les ports et protocoles utilisés par l'application pour opérer un filtrage avec une granularité plus forte. Autrement dit, l'analyse des paquets est un mécanisme partagé par les fonctions de NAT et de pare-feu, ce qui justifie leur couplage.

I

Annexe du chapitre 11 (MPLS et GMPLS)

Cette annexe introduit l'environnement IP sur ATM, qui a longtemps été considéré comme la solution de base des opérateurs de télécommunications, et décrit les diverses technologies qui se sont succédé depuis une vingtaine d'années pour parvenir à la technologie MPLS.

IP sur ATM

L'environnement IP est devenu le standard de raccordement à un réseau pour tous les systèmes distribués provenant de l'informatique. De son côté, la technique de transfert ATM a incarné la solution préférée des opérateurs pour relier deux routeurs entre eux avec une qualité de service. Il était donc plus que tentant d'empiler les deux environnements pour permettre l'utilisation à la fois de l'interface standard IP et de la puissance de l'ATM. Cette opération a donné naissance aux architectures dites IP sur ATM.

La difficulté de cette solution se situe au niveau de l'interface entre IP et ATM, avec le découpage des paquets IP en cellules, et lors de l'indication dans la cellule d'une référence correspondant à l'adresse IP du destinataire. En effet, le client que l'on souhaite atteindre est connu par son adresse IP, alors que les données doivent transiter par un réseau ATM. Pour ouvrir le chemin, ou circuit virtuel, il faut nécessairement connaître l'adresse ATM du client récepteur. La problématique vient de la correspondance d'adresses : en connaissant l'adresse IP du destinataire, comment trouver son adresse ATM ?

On peut regrouper les solutions à ce problème en trois grandes classes :

- Les techniques d'émulation, lorsque la correspondance d'adresses utilise un intermédiaire, l'adresse MAC.
- Le protocole CIOA (Classical IP over ATM), lorsqu'il n'y a qu'un seul sous-réseau ATM.
- Les techniques de serveur de routes MPOA (MultiProtocol Over ATM), PNNI (Private Network Node Interface) et NHRP (Next Hop Resolution Protocol), lorsqu'il y a plusieurs sous-réseaux ATM potentiels à traverser.

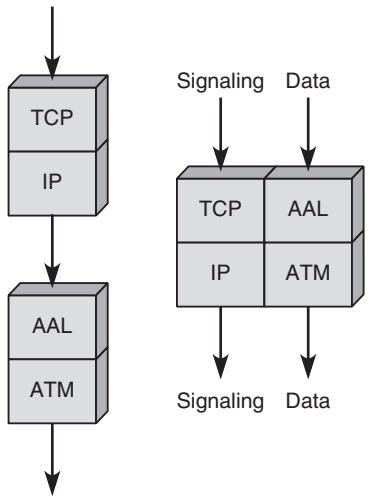
Ces trois techniques sont de plus en plus remplacées par un protocole beaucoup plus homogène, normalisé par l'IETF sous le nom de MPLS (MultiProtocol Label-Switching). Comme Ethernet et ATM, MPLS utilise des techniques de commutation de références, ou label-switching, mais avec d'autres types de trames, comme LAP-F ou PPP. MPLS fait appel à un chemin LSP (Label Switched Path), qui n'est autre qu'un circuit virtuel. Les paquets qui suivent ce chemin sont commutés dans les nœuds.

Pour le monde des opérateurs de télécommunications et, de façon plus fragmentaire, pour les très grandes sociétés internationales dotées de leur propre réseau, MPLS est devenu la technique de base depuis le début de la décennie.

Des extensions à MPLS ont été apportées avec GMPLS (Generalized MPLS), qui introduit de nouveaux paradigmes de commutation. Cette annexe commence par décrire les techniques IP sur ATM avant de détailler MPLS puis GMPLS.

La figure I.1 illustre deux architectures potentielles pour IP sur ATM. L'architecture de gauche (IP over ATM) est celle qui a été retenue par la quasi-totalité des constructeurs et des opérateurs. L'architecture de droite est une solution non implémentée, qui consiste à mettre en parallèle une infrastructure ATM et une pile TCP/IP. L'idée est de faire passer la signalisation par le plan TCP/IP et les données par le plan ATM. L'intérêt de cette solution est d'utiliser l'universalité de l'adressage IP et la puissance de transfert de l'ATM.

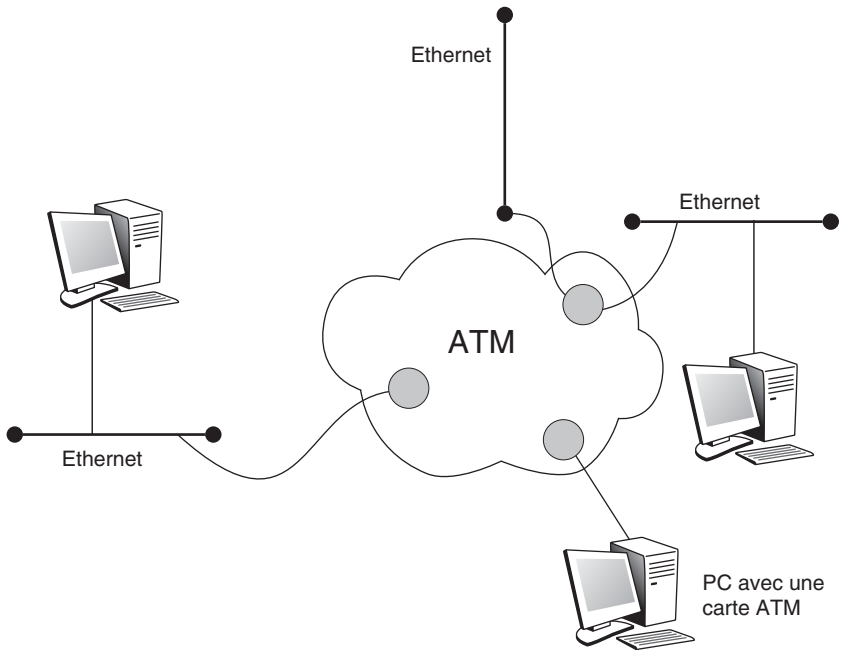
Figure I.1
Deux architectures IP sur ATM



Son inconvénient est de devoir mettre sur pied un double réseau et de ne pas avoir d'interface native ATM. C'est cette architecture qui va servir de base à MPLS.

Une troisième solution, de moins en moins utilisée, est ce que l'on appelle l'émulation de réseau, ou LANE (LAN Emulation). Elle est illustrée à la figure I.2. Dans cette solution, on se sert d'une adresse Ethernet comme intermédiaire entre l'adresse IP et l'adresse ATM. Cela permet d'ajouter une infrastructure ATM sans que les équipements terminaux aient à s'en soucier. C'est une façon d'introduire de l'ATM dans l'entreprise de manière transparente pour l'utilisateur. Nous en donnons ci-après quelques caractéristiques.

Figure I.2
Architecture LANE



LANE (LAN Emulation)

Le protocole LANE poursuit trois objectifs :

- remplacer un sous-réseau par un réseau ATM ;
- conserver les interfaces utilisateur ;
- faire communiquer des équipements terminaux ATM avec des équipements terminaux LAN.

L'un des inconvénients majeurs de cette solution est qu'elle nécessite une double correspondance IP-MAC et MAC-ATM.

Il existe de nombreuses façons de définir une émulation, dont l'une des meilleures est proposée par l'ATM Forum sous le sigle L-UNI (LAN emulation User-to-Network

Interface). Comme elle est de niveau MAC, cette émulation supporte toutes les applications existantes.

L'émulation L-UNI comporte quatre parties :

- L'émulation client, ou LEC (LAN Emulation Client), qui travaille comme un délégué pour le terminal ATM.
- L'émulation serveur, ou LES (LAN Emulation Server), qui résout la correspondance des adresses MAC et ATM.
- L'émulation serveur pour les applications multipoint, ou BUS (Broadcast and Unknown Server), qui résout la correspondance des adresses multipoint.
- L'émulation serveur de configuration, ou LECS (LAN Emulation Configuration Server), qui permet de mettre à jour une station qui se connecte.

Le logiciel LEC, que doit posséder toute station ou tout routeur qui veut être émulé, détient une adresse ATM d'accès. Le LES mémorise toutes les adresses MAC des stations des réseaux locaux qui sont logiquement attachés et leur adresse ATM associée. Le BUS est un serveur du même type que le LES mais pour les adresses de diffusion et multipoint. Enfin, le LECS possède les informations de configuration, comme l'adresse du LES du réseau émulé auquel appartient une station qui s'active.

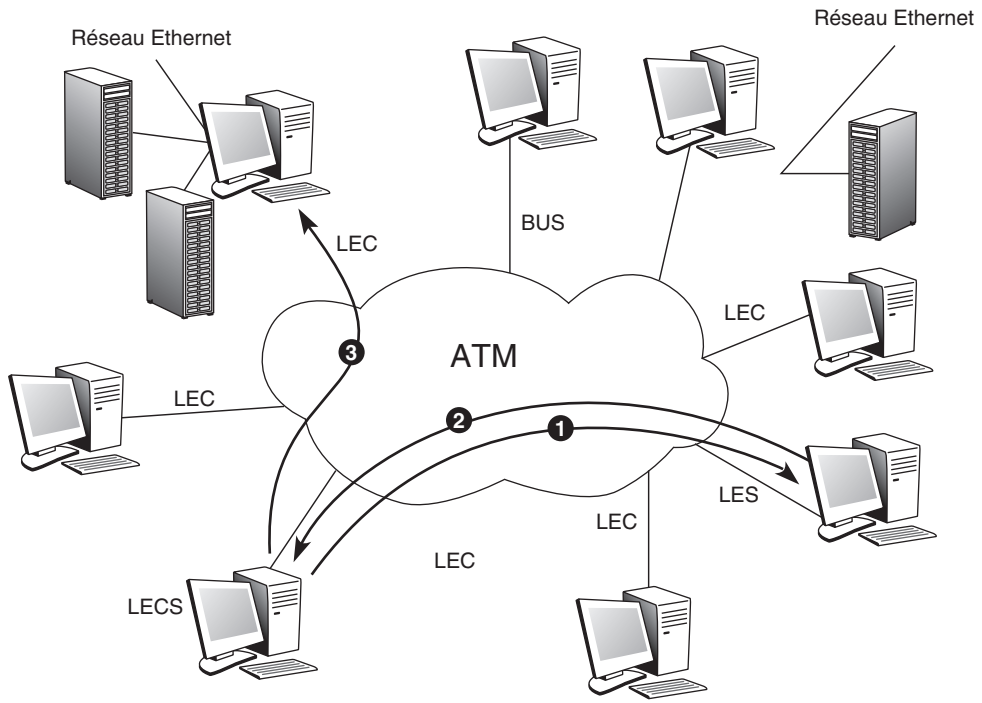
Quand un client désire envoyer une trame vers une autre station, il fait parvenir au serveur LES une requête sur l'adresse ATM correspondant à l'adresse MAC de la station destinataire. Le serveur répond avec l'adresse ATM du LEC auquel la station destination est connectée. Ensuite, le LEC ouvre un circuit virtuel avec son correspondant, déterminé par l'adresse ATM que lui a procurée le LES, et convertit la trame MAC en plusieurs trames ATM et envoie les cellules. Au LEC d'arrivée, les cellules sont converties en trames MAC, qui sont alors envoyées vers le terminal approprié.

Le cheminement des flots s'effectue de la façon illustrée à la figure I.3. Le parcours 1 correspond à l'envoi par le client d'une requête, portant une demande de conversion d'une adresse IP en une adresse ATM, envoyée au serveur LES. Le parcours 2 illustre la réponse à cette requête. Le client connaissant maintenant l'adresse ATM de son correspondant, il peut lui envoyer un flot de paquets IP encapsulés dans des trames ATM et circulant sur le circuit virtuel ouvert vers l'adresse ATM du destinataire. Le parcours 3 correspond à l'ouverture du circuit virtuel avec la machine distante dont l'adresse ATM a été obtenue grâce à la conversion effectuée.

Si le serveur LES n'est pas capable d'effectuer la traduction d'adresse, il faut envoyer une demande de traduction au BUS. Celui-ci émet en diffusion cette demande vers l'ensemble des récepteurs du réseau ATM. La station de réception qui se reconnaît comme étant le correspondant, grâce à l'adresse IP incluse dans la demande, renvoie son adresse ATM à l'émetteur, qui peut enfin ouvrir un circuit virtuel, où transitera le flot des paquets IP.

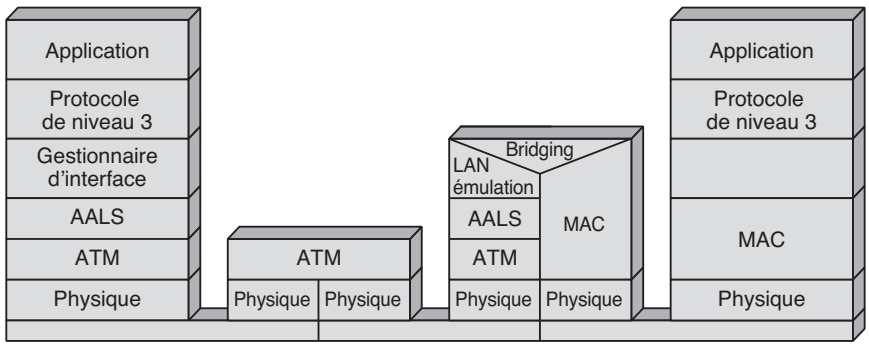
Le serveur BUS est également utilisé lorsque l'adresse IP du récepteur est multicast. Le serveur BUS possède pour cela des circuits virtuels ouverts avec l'ensemble des machines participant au réseau ATM.

Figure I.3
Émulation L-UNI



La figure I.4 illustre l'architecture du LANE. La pile protocolaire de droite représente une machine terminale connectée à un réseau local. Celui-ci mène à un équipement de connexion au réseau ATM. La pile protocolaire de gauche représente une station ATM attachée directement au réseau ATM mais travaillant en émulation LAN. Les piles protocolaires du milieu représentent, à droite, un commutateur ATM et, à gauche, la passerelle de passage entre le réseau local et le réseau ATM.

Figure I.4
Architecture de l'émulation de réseaux locaux LANE



LANE 2.0 introduit une évolution notable par rapport à cette première génération en ajoutant le respect de la qualité de service et le support d'applications multipoint. Cette

génération n'a cependant pas eu le temps de s'étendre, du fait de l'arrivée de MPLS, que nous détaillons dans la suite de cette annexe.

CIOA (Classical IP over ATM)

La solution CIOA permet de transporter les paquets IP par l'intermédiaire d'un réseau ATM sans émulation de réseau local. Pour ce faire, l'adresse IP est traduite directement dans une adresse ATM. Pour réaliser le transport de l'information, il suffit d'encapsuler les paquets IP dans des cellules ATM. À la différence de la solution précédente, on ne passe pas par une première encapsulation dans une trame Ethernet, elle-même encapsulée dans des cellules ATM.

Issue du groupe de travail ION (Internetworking Over NBMA), chargé par l'IETF en 1996 de redéfinir les environnements IP sur ATM, CIOA est la solution la plus répandue aujourd'hui. Le sigle NBMA (Non Broadcast Multiple Access) a été attribué à tous les réseaux qui n'offrent pas une diffusion au niveau physique, comme celle obtenue dans un réseau Ethernet partagé. Un réseau ATM est un NBMA au même titre qu'un réseau relais de trames.

Pour réaliser la correspondance d'adresses, comme dans le couple IP-Ethernet, il faut un protocole de type ARP (Address Resolution Protocol), ici ATMARP (ATM's Address Resolution Protocol). Ce protocole est défini dans la RFC 1577, qui précise la notion de sous-réseau IP, ou LIS (Logical IP Subnetwork). Tous les utilisateurs connectés sur un LIS ont un préfixe d'adresse en commun. Un LIS regroupe l'ensemble des machines et des routeurs IP appartenant au même sous-réseau au sens IP. Un LIS comporte un serveur ATMARP, connu de toutes les machines connectées sur le LIS et contenant les correspondances d'adresses IP et ATM des stations du LIS.

Une station qui veut communiquer avec une autre station sur le LIS envoie une requête au serveur (phase 1), lequel, dans le cas standard, lui communique l'adresse ATM correspondante (phase 2), permettant à la station source d'ouvrir un circuit virtuel avec la station destination (phase 3). Ces trois phases sont illustrées à la figure I.5

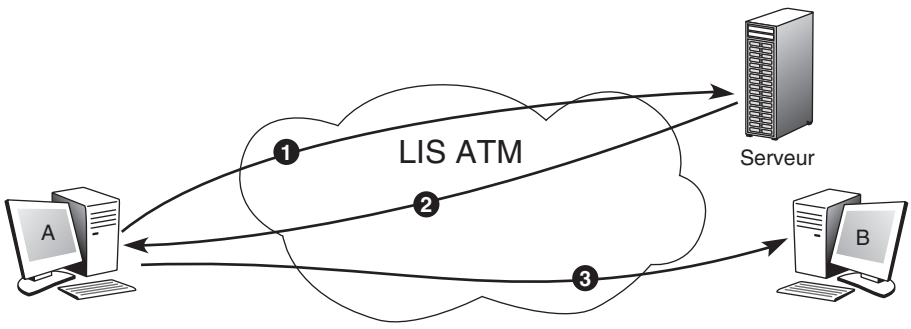
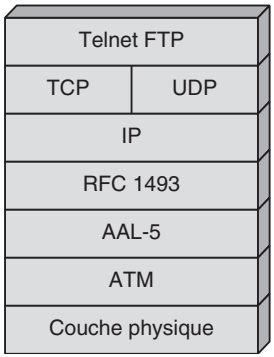


Figure I.5
Connexion CIOA

Les paquets IP sont encapsulés dans des cellules ATM au moyen d'une fragmentation effectuée par l'AAL-5. Les spécifications de la fragmentation et du réassemblage sont indiquées dans les RFC 1577 et 1483. L'architecture protocolaire de l'encapsulation CIAO est illustrée à la figure I.6.

Figure I.6

Architecture protocolaire de l'encapsulation CIAO



CIOA se place au niveau 3 de l'architecture OSI et utilise une résolution d'adresse IP directement en ATM. La résolution d'adresse de l'émulation LAN opère pour sa part au niveau MAC. Ce sont bien sûr deux solutions incompatibles. CIOA est beaucoup plus simple que l'émulation LAN, mais elle ne permet pas de gérer la diffusion.

De nombreuses autres possibilités d'encapsulation ont été proposées, dont les plus connues sont les suivantes :

- TULIP (TCP and UDP Lightweight IP), RFC 1932 ;
- TUNIC (TCP and UDP over a Non-existing IP Connection), également décrite dans la RFC 1932.

Le rôle de ces deux encapsulations concernant deux stations appartenant au même LIS est de simplifier les traitements dans le niveau IP en supprimant en grande partie l'en-tête.

Comme nous venons de le voir, la corrélation d'adresses dans CIOA se fait au niveau IP-ATM, ce qui simplifie la recherche de la correspondance d'adresses mais limite son utilisation aux réseaux IP. Avec la deuxième génération du protocole CIOA, la résolution d'adresse s'effectue par un mécanisme InATMARP (Inverse ATM's ARP), qui est une extension du mécanisme RARP (Reverse ARP) d'Internet. Dans CIOA 2, le protocole NHRP, que nous détaillons à la section suivante, peut être utilisé.

Le groupe ION de l'IETF a mis au point le système MARS (Multicast Address Resolution Server) pour émuler le multicast au-dessus d'ATM. Ce service est étendu à tous les protocoles de la couche réseau au-dessus des réseaux NBMA. Le système MARS comporte un serveur et des clients. Dans le cadre d'IPv4, MARS ne travaille que sur un LIS. Il est possible d'ajouter des serveurs spécialisés MCS (Multicast Cluster Server) pour remplacer le serveur MARS dans la distribution des paquets et de la gestion des applications multicast. Il n'est toutefois pas évident de trouver l'architecture optimale entre une

centralisation dans un serveur MARS unique et une distribution totale dans un réseau de serveurs MCS.

Avec l'arrivée d'IPv6, le protocole ATMARP ne peut plus être exploité. IPv6 au-dessus d'ATM remplace le processus ATMARP par ND (Neighbor Discovery), ce qui empêche le fonctionnement du protocole CIOA tel que nous l'avons décrit. De ce fait, l'IETF a normalisé dans les RFC 2491 et 2492 deux nouveaux protocoles pour le remplacer. Ces protocoles spécifient la mise en place d'IPv6 au-dessus de réseaux NBMA. Le protocole MARS est repris mais étendu pour transporter du trafic IPv6 unicast. Dans ce nouvel environnement, les LIS sont remplacés par des LL (Logical Link). Le serveur MARS réalise les fonctions auparavant réalisées par le serveur ATMARP.

NHRP et MPOA

Les deux solutions décrites précédemment, LANE et CIOA, s'appliquent facilement à un LIS (Logical IP Subnetwork) unique. Les protocoles utilisés par le BUS ou la procédure ATMARP requièrent une diffusion. Si les requêtes peuvent traverser des passerelles, la diffusion devient difficile à maîtriser. Il faut donc un protocole pour rechercher l'adresse du destinataire sans diffusion afin que l'environnement IP puisse se mettre au-dessus d'un ensemble de sous-réseaux ATM.

Considérons un ensemble de LIS ATM formant un NBMA. Chacun des réseaux ATM interconnectés a donc des utilisateurs possédant un préfixe d'adresse en commun et formant un LIS. Connaissant l'adresse IP du destinataire, il est possible de déterminer l'adresse ATM correspondante. La figure I.7 illustre le processus consistant à trouver l'adresse ATM du destinataire en connaissant son adresse IP alors qu'il ne se trouve pas sur le même réseau.

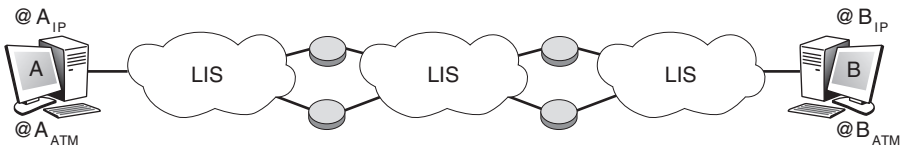


Figure I.7

IP sur plusieurs LIS interconnectés

NHRP (Next Hop Resolution Protocol)

Le protocole NHRP provient du monde Internet et est décrit dans la RFC 1932. Il permet de rechercher l'adresse ATM correspondant à une adresse IP dans un réseau NBMA composé de plusieurs LIS. Plus précisément, NHRP permet la résolution d'une adresse IP d'une station de travail se trouvant sur un LIS distant en une adresse du réseau NBMA (adresse ATM, relais de trames, etc.).

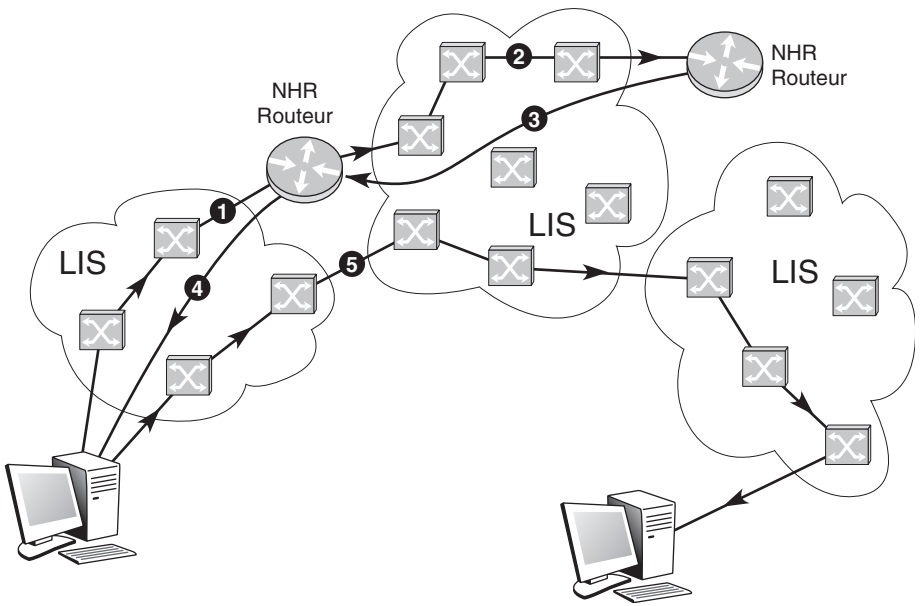
Chaque LIS possède un serveur de route, appelé NHS (Next Hop Server), souvent situé dans un routeur. Lorsqu'un client demande une connexion, il s'adresse au NHS du LIS

auquel il appartient pour obtenir les informations de routage sur son paquet. Si le NHS local ne peut résoudre le problème de la localisation, il adresse une requête vers les NHS connexes, et ainsi de suite jusqu'à arriver au LIS auquel le destinataire appartient.

Cette solution permet de trouver une route beaucoup plus directe que le passage par les différents NHS, comme l'illustre la figure I.8. La phase 1 correspond à la demande de conversion d'adresse au NHR Routeur du premier LIS, lequel s'adresse avec la phase 2 au NHR Routeur du LIS dont dépend l'utilisateur distant. Les phases 3 puis 4 correspondent au retour de la conversion d'adresse. Avec l'adresse ATM le client ouvre un circuit virtuel avec le distant : c'est la phase 5. On peut ainsi obtenir une connexion directe en mode ATM de deux stations appartenant à des LIS distants, sans qu'il soit nécessaire de remonter au niveau IP du routeur.

Figure I.8

Mise en place d'une route par NHRP



MPOA (MultiProtocol Over ATM)

MPOA est un protocole mis au point par l'ATM Forum. Plus complexe que NHRP, il se sert des techniques décrites aux sections précédentes en les unissant et en les complétant pour réaliser le transport de paquets IP ou de paquets d'autres protocoles, comme IPX, sur une interconnexion de réseaux ATM. La route peut être déterminée soit par une solution centralisée de type serveur de route, soit par une solution distribuée utilisant les protocoles PNNI ou NHRP.

Le rôle de MPOA est toujours de trouver l'adresse ATM du correspondant pour ouvrir une connexion directe, ou shortcut, entre deux stations ATM qui ne se connaissent au départ que par leur adresse IP.

Les deux composantes de MPOA sont les suivantes :

- MPC (MPOA Client), qui, à la demande d'un client, recherche la meilleure route pour ouvrir un circuit virtuel avec un client dont il connaît l'adresse IP.
- MPS (MPOA Server), situé dans un routeur, qui, à l'aide d'un routage classique, tel que RIP (Routing Information Protocol), OSPF (Open Shortest Path First), etc., achemine les requêtes NHRP de demandes de correspondance.

La figure I.9 illustre le fonctionnement de MPOA. La phase 1 correspond à la demande de conversion d'adresse qui remonte jusqu'au serveur MPS connaissant la réponse. La phase 2 transporte la réponse à la demande de conversion qui permet l'ouverture du circuit virtuel vers le distant.

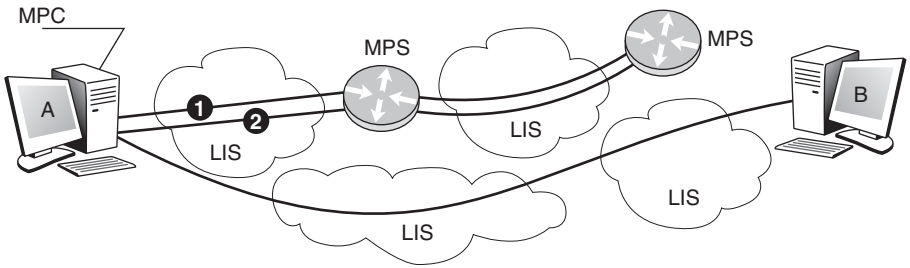


Figure I.9
Fonctionnement de MPOA

PAR et I-PNNI

Issu de l'ATM Forum, le protocole PNNI a pour fonction de mettre en place une connexion entre deux utilisateurs en subdivisant le réseau en sous-réseaux, chaque sous-réseau possédant un nœud leader capable de connaître l'état des autres sous-réseaux et de renvoyer ces informations à ses propres nœuds dans son sous-réseau.

Lorsque des routeurs IP sont interconnectés par un ensemble de réseaux ATM, il est difficile de déterminer le chemin à suivre. Une solution pour trouver un chemin consiste à utiliser le protocole PNNI. Les mécanismes PAR et I-PNNI ont pour objet d'établir cette jonction entre les routeurs et le protocole PNNI.

- PAR (PNNI Augmented Routing) permet d'élire un serveur de route sur une machine de chaque sous-réseau ATM. Ce routeur est appelé DR (Designated Router). C'est lui qui est capable de faire la résolution d'adresse entre la partie IP et le réseau ATM et qui déclenche le protocole PNNI pour mettre en place une route sur l'interconnexion de réseaux ATM.
- I-PNNI (Integrated PNNI) étend le protocole PNNI de sorte qu'il puisse être utilisé sur les sous-réseaux IP. Dans chaque sous-réseau LIS, on indique en ce cas un leader.

Les solutions pré-MPLS

Introduite par la société Ipsilon, IP-switching a été la première version du label-switching. Dans cette architecture, la route est déterminée par le flot IP.

Les autres solutions, principalement le tag-switching de Cisco Systems et ARIS (Aggregate Route-based IP Switching) d'IBM, utilisent des routes déterminées par la topologie et non plus par le flot. La norme MPLS a également choisi cette solution du choix de la route déterminée par la topologie pour des raisons de passage à l'échelle. Le tag-switching a été proposé quelques mois après l'annonce de l'IP-switching. Cisco a essayé de promouvoir sa solution *via* l'IETF, et de nombreuses RFC sont disponibles sur le type de sous-réseaux — ATM, PPP, Ethernet — à utiliser, ainsi que sur la possibilité de faire du multicast et d'utiliser le protocole RSVP.

La proposition ARIS d'IBM a été soumise à l'IETF sous forme de RFC. Comme dans le tag-switching, la mise en place des routes s'effectue par un algorithme dépendant de la topologie du réseau et non par une signalisation utilisant le premier paquet du flot de données. Les routes sont donc déterminées à l'avance.

Ces solutions reposent sur le principe de la détermination d'une route entre l'émetteur et le récepteur, cette route étant établie par des serveurs de route. Les fragments de paquets IP sont étiquetés à l'entrée du réseau pour suivre la route déterminée. La route peut traverser des réseaux divers, aussi bien ATM que relais de trames ou Ethernet. La référence se trouve dans la zone VPI/VCI de la cellule ATM, dans la zone DLCI de la trame LAP-F d'un réseau relais de trames ou dans une zone supplémentaire de la trame Ethernet. On retrouve là la solution de mise en place d'une route à l'intérieur du réseau et de commutation de trames le long de cette route.

Les différences d'implémentation proviennent des antécédents des constructeurs. Si le constructeur propose des routeurs à son catalogue, il doit ajouter la partie ATM pour commuter les cellules ATM. Si le constructeur provient de l'environnement ATM, c'est un serveur de route IP qui est ajouté.

J

Annexe du chapitre 15 (Les réseaux d'accès terrestres)

Cette annexe détaille les accès *x*DSL, ainsi que leurs protocoles et leur utilisation. Elle se penche en outre plus en détail sur les accès par modem câble, qui sont assez peu utilisés en France, mais beaucoup aux États-Unis, et sur le passage de la vidéo sur la boucle locale.

Le protocole L2TP

Pour réaliser les communications entre les BAS et les serveurs, un protocole de tunneling doit être mis en place puisque ce chemin peut être considéré comme devant être emprunté par tous les paquets ou trames provenant des différents DSLAM et allant vers le même serveur. Le tunneling est une technique courante, qui ressemble à un circuit virtuel. Les trois protocoles utilisés pour cela sont PPTP (Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding) et L2TP (Layer 2 Tunneling Protocol). Ces protocoles permettent l'authentification de l'utilisateur, l'affectation dynamique d'adresse, le chiffrement des données et éventuellement leur compression.

Le protocole le plus récent, L2TP, supporte difficilement le passage à l'échelle, ou scalabilité, et n'arrive pas à traiter correctement et suffisamment vite un nombre de flots dépassant les valeurs moyennes. Dans ce cas, on ajoute des concentrateurs d'accès L2TP, ou LAC (L2TP Access Concentrator), qui récupèrent tous les clients provenant d'un même DSLAM et allant vers un même BAS et les multiplexent sur un même circuit virtuel.

La figure J.1 illustre l'architecture protocolaire d'une communication d'un PC vers un serveur situé dans un réseau de FAI différent de celui de l'opérateur d'entrée. Le PC travaille sous TCP/IP et est connecté à un modem ADSL par le biais d'un réseau Ethernet.

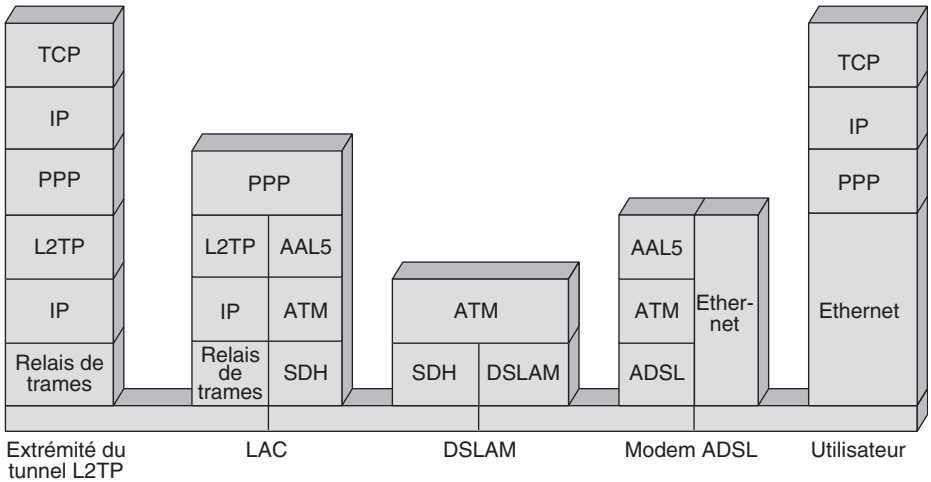


Figure J.1

Architecture protocolaire d'une communication ADSL

La parole et la vidéo sur *x*DSL

Nous avons vu qu'en *x*DSL la parole téléphonique était transportée parallèlement aux données sur la partie basse du spectre. Cette technologie convient très bien aux opérateurs historiques, aussi appelés ILEC (Incumbent Local Exchange Carrier). Les nouveaux venus, ou CLEC (Competitive Local Exchange Carrier), peuvent aujourd'hui espérer concurrencer les opérateurs historiques grâce à la déréglementation de la boucle locale.

Pour prendre en charge des clients sur la boucle locale de l'opérateur historique, ces opérateurs entrants peuvent faire passer la parole téléphonique sur la partie DSL. On appelle cette solution ToDSL (Telephony over DSL). Le passage de la parole sur la partie donnée s'apparente aux technologies de voix sur IP.

Les paquets de parole devant arriver au récepteur avant 150 ms, il faut qu'une priorité leur soit appliquée. Dans ce cas, la dizaine de kilobits par seconde de la parole compressée passe assez facilement. Il faut toutefois que la priorité puisse s'exercer non seulement sur la partie modem mais aussi sur les parties réseau précédant et suivant les deux modems. Cela suppose, pour la partie réseau d'entreprise, l'application d'une technique de priorité et, pour le réseau du FAI, la possibilité de négocier un SLA (Service Level Agreement) compatible avec le temps maximal de traversée de bout en bout.

Une autre solution, moins intégrée mais plus simple à mettre en œuvre, est commercialisée par de nombreux FAI pour offrir le service téléphonique ToDSL. Elle consiste à utiliser une bande spécifique du modem, de 4,3 MHz, donnant un débit de 32 Kbit/s. L'inconvénient de cette solution est que si la parole téléphonique n'est pas utilisée, la

bande passante correspondante est perdue. Cependant, comme la bande passante utilisée est très faible, cela ne pose pas vraiment problème.

La ligne DSL doit aussi convoyer la signalisation téléphonique, ce qui constitue la deuxième difficulté après la contrainte temporelle. Sur le modem, plutôt que d'utiliser une priorité sur les données, il est possible d'utiliser l'AAL-1, qui offre des fonctionnalités de synchronisation et de priorité. Cette solution, appelée VoATM (Voice over ATM), est complémentaire de la technologie ToDSL.

La télévision est une deuxième application qui est offerte aux utilisateurs de modems ADSL. Avec la première génération de modems ADSL, une bande passante spécifique est dévolue au canal de télévision, en général de 3 Mbit/s. Lorsque la télévision est en marche, le canal ne fait que transporter des signaux numériques de l'image de télévision. Lorsque la télévision est éteinte, les 3 Mbit/s sont alloués à la bande passante utilisée pour le transport des données. Dans la seconde génération, l'image de télévision est intégrée avec les autres flots, et les paquets transportant le flux d'images sont facilement repérables par une adresse spécifique correspondant à la prise sur le boîtier sur laquelle est branchée la télévision. Enfin, dans la troisième génération, le flot de paquets provenant de la télévision est un flot IP totalement intégré aux autres paquets, un marquage spécifique permettant de reconnaître les paquets pour leur donner une priorité acceptable pour la qualité de service nécessaire.

La vidéo est un autre service qui peut être offert par les modems DSL. S'il est encore difficilement imaginable de voir ce système supplanter la vidéo diffusée à grande échelle, la vidéo sur DSL, ou VoDSL (Video over DSL), commence à être déployée par de nombreux FAI pour des diffusions limitées et des services de VoD (Video on Demand).

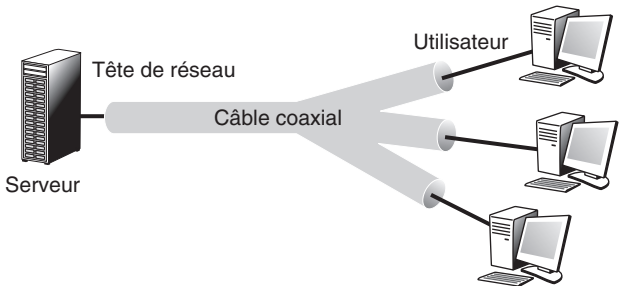
Les deux solutions que nous avons examinées pour la téléphonie sont possibles pour la vidéo : soit on intègre les paquets vidéo dans le flot en leur donnant si possible une priorité forte, soit on leur affecte un canal spécifique. Dans ce dernier cas, la largeur de la bande passante affectée à la vidéo diffère suivant les opérateurs pour aller de 800 Kbit/s à quelques mégabits par seconde. Pour une télévision à 800 Kbit/s, il suffit de récupérer 25 des 256 sous-bandes, chacune transportant 32 Kbit/s.

Dans le cas du multipoint, c'est-à-dire de la diffusion limitée à un petit nombre d'utilisateurs, la vidéo est compressée en MPEG-4 ou éventuellement en MPEG-2 et émise en utilisant un protocole multipoint. Le plus performant de ces protocoles est IP Multicast, puisque les paquets sont à l'origine IP. Cependant, comme il faut compresser au maximum les données vidéo, le choix du codec vidéo est capital pour que le flot arrive dans les temps.

Les modems câble

Les câblo-opérateurs disposent d'un environnement leur permettant de relier l'utilisateur à un ou plusieurs opérateurs. Ce câblage est réalisé à partir du câble coaxial CATV reliant la tête de réseau aux utilisateurs, comme l'illustre la figure J.2. Les canaux de télévision dans le sens descendant sont diffusés sur toutes les branches du câblage. Dans le sens montant, les canaux doivent se superposer sur le tronc de l'arbre.

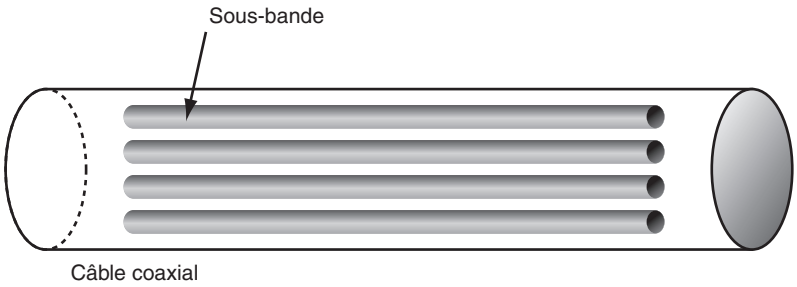
Figure J.2
Distribution de programmes TV par un câblo-opérateur



Le câblage part d'une tête de réseau pour atteindre l'utilisateur après une diffusion sur l'ensemble des branches. Dans le cadre de la diffusion de la télévision, les différents programmes sont poussés vers les utilisateurs. Chaque abonné reçoit l'ensemble des chaînes et en sélectionne une à visualiser. Cette technique est à l'opposé de l'ADSL, où seule la chaîne sélectionnée par l'utilisateur est acheminée.

Dans le CATV, un multiplexage en fréquence est utilisé pour le transport des différents canaux de télévision (*voir figure J.3*). La division en fréquence donne naissance à des sous-bandes, chaque sous-bande portant un canal de télévision.

Figure J.3
Multiplexage en fréquence dans le CATV



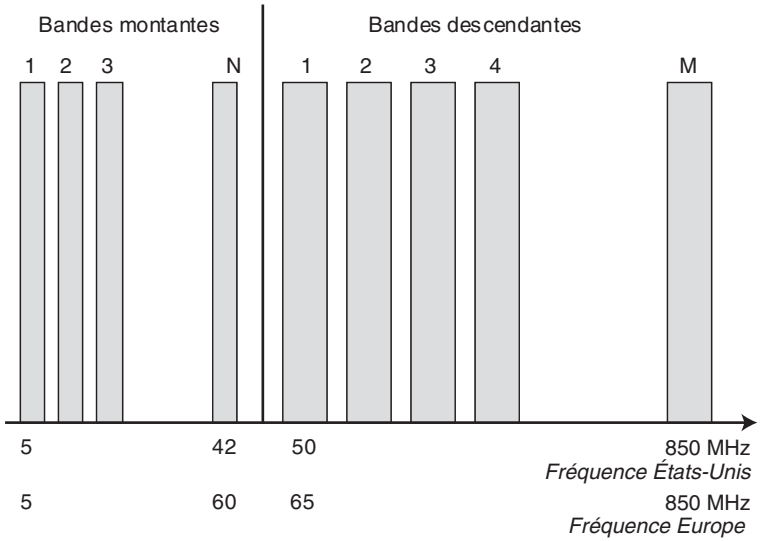
On peut affecter une bande étroite, de 32 ou 64 Kbit/s par utilisateur, pour transporter de la parole téléphonique entre le combiné de l'utilisateur et la tête de réseau qui est reliée à un opérateur télécoms.

Il est possible de réserver une sous-bande pour la connexion à un opérateur de type FAI. Cette sous-bande doit toutefois être suffisante pour supporter la somme des débits crêtes des utilisateurs. Par exemple, 1 000 utilisateurs connectés à 1 Mbit/s exigent un débit total potentiel de 1 Gbit/s. La solution à ce problème consiste à choisir sur le CATV une bande très large et à utiliser une technique de multiplexage pour faire passer un maximum d'utilisateurs simultanément.

La figure J.4 illustre un partage de la bande passante d'un CATV en Amérique du Nord et en Europe. Les bandes montantes en Europe se situent entre 5 et 42 MHz et ont une largeur de 200 kHz à 3,2 MHz. Les bandes descendantes se situent entre 50 et 850 MHz. La largeur des bandes de télévision est de 8 MHz. Le nombre de bandes montantes et

descendantes est laissé libre aux opérateurs. Les valeurs pour l'Amérique du Nord sont indiquées sur la figure. Les bandes de télévision sont de 6 MHz.

Figure J.4
Plage de fréquences dans un CATV



Pour réaliser le multiplexage des utilisateurs sur la bande commune, trois normes ont été proposées :

- IEEE 802.14, qui utilise une technologie ATM.
- MCNS-DOCSIS, qui est surtout utilisée en Amérique du Nord mais que les câblo-opérateurs européens ont adoptée par la suite.
- DVB-DAVIC, que nous détaillons un peu plus loin.

IEEE 802.14 et MLAP

La transmission numérique sur un CATV s'effectue d'une manière unidirectionnelle, de la station terminale vers la tête de réseau ou l'inverse. La bande passante du CATV est subdivisée en une bande montante vers la tête de ligne et une bande descendante vers les équipements terminaux.

Cette partie du câblage peut desservir entre 500 et 12 000 utilisateurs depuis la tête de réseau. Si chaque utilisateur veut effectuer une application de vidéo à la demande, ou VoD, la bande passante n'est pas suffisante, ou, du moins, chaque client doit se limiter à une partie de cette bande passante. Pour permettre une meilleure adéquation de la bande passante, surtout aux applications interactives, le groupe de travail IEEE 802.14 a développé le protocole MLAP (MAC Level Access Protocol), qui permet de distribuer le support entre les machines connectées.

La difficulté principale de ce système réside dans la technique d'accès. Comme les canaux sont unidirectionnels, l'équipement le plus en aval ne peut écouter les émissions des autres stations qu'après un certain laps de temps, qui correspond à la propagation du signal jusqu'à la tête de réseau et à celle en retour jusqu'à la station. La portée du CATV pouvant atteindre plusieurs dizaines de kilomètres, il faut trouver une solution intermédiaire entre les techniques satellite et les méthodes utilisées dans les réseaux locaux.

Le protocole MLAP repose sur une succession d'états correspondant à des actions découpées en cinq phases :

1. La station que l'on examine est inactive.
2. Elle devient active, c'est-à-dire qu'elle veut émettre des trames.
3. Elle avertit la tête de réseau par des primitives UP.FRAME et UP.REQ et par un mécanisme d'accès aléatoire.
4. La tête de réseau notifie à toutes les stations, par le biais du canal aval, les intervalles de temps pendant lesquels les stations peuvent émettre. Les canaux sont utilisés dans un mode avec contention. Cela signifie que l'allocation d'un canal ne se fait pas de façon unique du premier coup et que des collisions peuvent se produire. Associé à la tête de réseau, un contrôleur peut modifier l'allocation des canaux en tenant compte de la demande de qualité de service des stations. L'algorithme est alors réinitialisé, et les informations sont mises à jour. Une nouvelle allocation est ensuite déterminée. Les stations reçoivent une notification de la tête de réseau indiquant les nouveaux intervalles de temps qui leur sont alloués. Ce processus se poursuit jusqu'à ce que les stations aient leur canal réservé.
5. Si une station modifie sa demande de bande passante ou de qualité de service, la nouvelle demande s'effectue par les canaux partagés.

L'algorithme d'allocation de bande passante du contrôleur ne fait pas partie de la norme.

DVB-DAVIC

Le groupe DAVIC (Digital Audio VIsual Council) a été formé en 1994 pour normaliser les interfaces et les architectures des réseaux transportant de la vidéo. Le choix s'est dirigé en grande partie vers la norme DVB, qui permet le transport de tout type d'information, en particulier la vidéo.

Une version spécifique du DVB a été développée pour le câble. Elle utilise des bandes de 6 Mbit/s de débit et une technologie de modulation de phase et d'amplitude. Le DVB utilise la compression MPEG-2 pour la télévision numérique. MPEG-2 permet le multiplexage de plusieurs canaux numériques dans des trames spécifiques. Pour le transport des paquets MPEG, voire directement du paquet IP, puisque c'est permis par l'interface DAVIC, c'est la trame ATM qui est utilisée. Nous retrouvons là des techniques semblables à celles utilisées dans IEEE 802.14 et DOCSIS.

Le contrôle des paquets IP

Les normes IEEE 802.14 et DOCSIS assurent une bonne utilisation de la partie du câble affectée au transport des données. Nous avons vu que la norme associée au modem était l'ATM. En réalité, ces paquets ATM ne sont là que pour transporter des paquets IP, le paquet de base restant le paquet IP. Les paquets IP doivent être contrôlés, de telle sorte que chaque utilisateur n'en émette pas trop et que le réseau demeure fluide.

Le contrôle des flots IP s'effectue grâce à un algorithme, dit slow-start and congestion avoidance, qui limite la valeur de la fenêtre afin que chaque utilisateur puisse continuer à jouir de son débit, même lorsque le réseau est surchargé. Les paquets IP, dont le nombre est limité par la fenêtre, sont découpés pour cela en morceaux de 48 octets pour être introduits dans la zone de données de la trame ATM. Le nombre des cellules ATM dépend de la fenêtre IP.

Une difficulté de cette méthode provient de la couche d'accès au support physique, qui n'est pas corrélée au débit des trames ATM. Si la connexion n'a pas de débit, du fait que la demande d'accès n'a pas obtenu de réservation, les acquittements des paquets IP arrivent trop tard, et il en résulte un redémarrage du slow-start à la valeur 1 pour la fenêtre de contrôle. Même si la connexion reçoit une réservation réussie grâce à la technique d'accès, cette réservation est de nouveau perdue après l'émission des trames ATM en attente, qui ne sont qu'en petit nombre. En revanche, lorsque la technique d'accès a réussi à réserver un slot et que la valeur de la fenêtre de contrôle augmente, la connexion n'a plus de raison de perdre la main, et elle se met à très bien fonctionner.

K

Annexe du chapitre 16 (Les réseaux d'accès hertziens)

Cette annexe commence par détailler les bandes de fréquences utilisées dans les réseaux d'accès hertziens, avant d'examiner les réseaux WiMAX de première génération, qui n'ont guère rencontré le succès. C'est la raison pour laquelle WiMAX phase 2 a été développé, qui fait partie intégrante de la génération 4G. Nous examinons enfin des réseaux hertziens particuliers, comme WiBro, qui a été défini en Corée, et WRAN, qui est poussé par le groupe de travail IEEE 802.22 comme futur réseau régional.

WiMAX

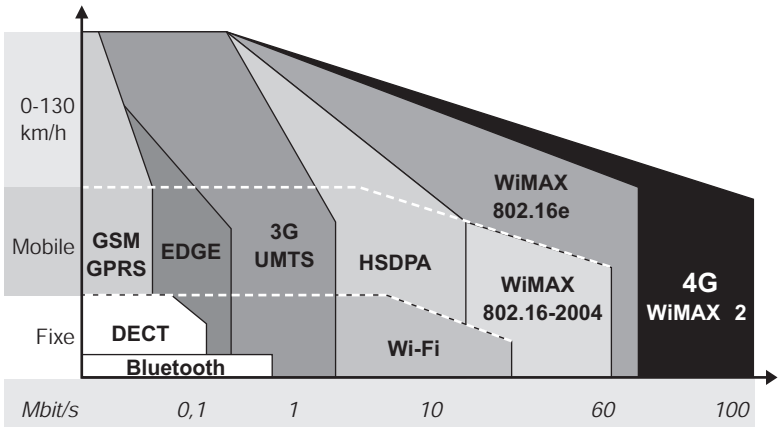
WiMAX (Worldwide Interoperability for Microwave Access) est issu d'une initiative lancée en 2001 par l'Alliance WiMAX. Son objectif était de promouvoir le standard 802.16 de l'IEEE en se proposant de vérifier la conformité et l'interopérabilité des équipements. Malheureusement, ce réseau n'a pas rencontré le succès escompté.

WiMAX se présente en deux versions, une version fixe, qui a été finalisée sous le nom de WiMAX IEEE 802.16-2004 et la version mobile IEEE 802.16e-2005.

L'utilisation de WiMAX est très semblable à celle d'un modem ADSL, si ce n'est qu'au lieu d'un câble téléphonique on utilise la voie hertzienne. C'est pourquoi l'on parle de WDSL (Wireless DSL) pour décrire la solution WiMAX fixe. En ce qui concerne la version mobile, son utilisation est identique celle d'un ADSL mobile. L'avantage évident de WiMAX mobile est qu'on l'a toujours sur soi. Avec un équipement muni d'une connexion WiMAX, il est possible de se connecter de partout, tout le temps, y compris en situation de mobilité.

La figure K.1 illustre la position de WiMAX dans le contexte de réseaux sans fil.

Figure K.1
Place de WiMAX dans les technologies hertziennes



Au sein du groupe 802.16, deux sous-groupes s'occupent des communications dans des fréquences situées, pour le premier, entre 1 et 11 GHz et, pour le second, entre 10 et 66 GHz. En Europe, la normalisation du même domaine s'effectue à l'ETSI (European Telecommunications Standards Institute), où le groupe de travail BRAN (Broadband Radio Access Networks) propose la norme HiperAccess (High-Performance Radio Access), ou HiperLAN 3, comme solution pour les réseaux d'accès à très haut débit. Cette proposition permet de réaliser des réseaux IP ou ATM offrant des débits de l'ordre de 25 Mbit/s.

Le groupe de travail 802.16 a mis en place des sous-groupes, qui se sont attaqués à des problèmes distincts. Le groupe de travail de base a normalisé un accès métropolitain dans la bande des 10-66 GHz avec une vue directe entre les antennes et un protocole point-à-point. Finalisée en 2001, la norme IEEE 802.16 a été complétée par la norme 802.16c de 2002, qui introduit des profils système WiMAX, et par une partie de la norme 802.16d de 2004, qui apporte des correctifs et des fonctionnalités supplémentaires autorisant la compatibilité avec la norme 802.16e.

Sortie en 2003, la norme 802.16a concerne la bande des 2 à 11 GHz, avec la possibilité d'utiliser des protocoles multipoint en plus de l'environnement point-à-point de base. La norme 802.16e a pour objectif d'étendre WiMAX à des machines terminales mobiles, impliquant la possibilité de réaliser des connexions *x*DSL vers des mobiles. Les fréquences utilisées se situent entre 2 et 6 GHz.

Les portées annoncées sont de 50 km à un débit de 70 Mbit/s, mais ces valeurs ne sont que théoriques, puisqu'elles nécessitent une très forte puissance avec une grande directivité et une vue directe. Dans les faits, la distance maximale est d'une dizaine de kilomètres et, suivant la puissance, la directivité et la vue directe, les débits se situent entre 40 et 50 Mbit/s. Plus classiquement, en partageant la ligne et en étant dans des conditions classiques avec des antennes de 90°, le débit maximal est plutôt de l'ordre de 30 Mbit/s.

On peut en déduire que le nombre de clients ADSL pouvant bénéficier d'un débit de l'ordre du mégabit par seconde peut atteindre la centaine en « surallouant » la ligne.

Pour augmenter les débits, il faut diminuer la portée en réduisant, par exemple, la puissance. Des débits d'une cinquantaine de mégabits par seconde sont dans ce cas possibles. Pour utiliser WiMAX en ville et bénéficier d'un grand nombre de clients, le diamètre des cellules ne doit pas dépasser 1 km environ.

Bandes de fréquences

Les bandes de fréquences attribuées pour les liaisons WLL varient suivant les pays et les continents. Une première bande fortement utilisée en France et en Europe concerne le DECT. Cette bande a été déterminée pour la téléphonie résidentielle et d'entreprise. Elle correspond à la partie du spectre située entre 1 880 et 1 900 MHz. Bien que particulièrement étroite, avec ses 20 MHz disponibles, cette bande peut être utilisée pour la BLR.

Le DECT se présente comme une solution potentielle pour la téléphonie mobile, mais au prix d'une limitation de la mobilité du terminal, qui doit rester dans une même cellule. Cette norme ETSI (European Telecommunications Standards Institute) de 1992 utilise une technique de division temporelle TDMA.

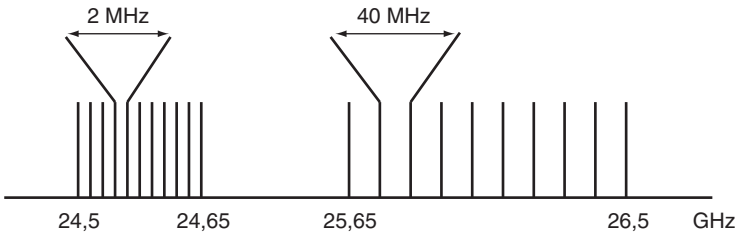
Une seconde bande, dédiée à la technologie MMDS, a été affectée aux techniques WLL. Cette bande était au départ dévolue à des canaux de télévision analogique en mode unidirectionnel, puisque la télévision est diffusée. Un canal de retour, permettant d'envoyer des commandes vers l'émetteur, était permis par l'utilisation du réseau téléphonique commuté. Cette bande sert maintenant à la BLR, mais de nouveau avec une bande passante assez faible. Les antennes réceptrices, d'un diamètre de 20 cm environ, doivent être quasiment en vue directe de l'antenne du fournisseur, sans obstacle entre les deux. Dans la bande des 3,5 GHz, les ondes réussissent à traverser les bosquets d'arbres et à être à peu près insensibles à la pluie. Les distances moyennes acceptables pour cette bande vont de 3 km dans les zones fortement urbanisées à quelque 10 km en zone rurale. La bande des 10,5 GHz est également disponible, mais une fois encore avec une très faible bande passante. Pour de réelles capacités, il faut utiliser des bandes au-dessus de 20 GHz, dont un grand nombre est disponible.

Les distances entre la station de base et l'antenne du client varient en fonction de la fréquence, du relief, de la météo, des obstacles, etc. Une vue directe entre les deux antennes qui communiquent est toujours nécessaire, cette directivité étant plus ou moins prononcée suivant la fréquence utilisée. La pluie peut devenir une contrainte forte compte tenu de la nature des ondes utilisées, dont la longueur est de l'ordre du millimètre, ce qui correspond à une fréquence d'environ 30 GHz. Toutes ces difficultés limitent la distance maximale entre l'émetteur et le récepteur à environ 3 km.

En France, deux licences nationales permettent l'utilisation des fréquences MMDS. Les licences régionales utilisent des fréquences dans la bande 24,5-26,5 GHz. Dans les DOM. Les licences concernent la bande des 3,5 GHz. Aux États-Unis, une bande de 1,3 GHz a été attribuée à cette technologie dans la gamme de fréquences 27,5-31,3 GHz. Sur une telle bande, une capacité de transmission au-dessus de 2 Gbit/s est envisageable. Une

partie de la bande 24,5-26,5 GHz sert à l'accès montant et une autre à l'accès descendant. Ces bandes sont illustrées à la figure K.2. D'une largeur de 150 MHz, la bande montante, c'est-à-dire de l'utilisateur vers la station de base, est divisée en sous-bandes de 2 MHz. La bande descendante, beaucoup plus large, avec 850 MHz, est découpée en sous-bandes de 40 MHz. Les canaux montants et descendants sont multiplexés en fréquence. Chaque sous-bande peut accueillir plusieurs utilisateurs multiplexés temporellement, c'est-à-dire se répartissant les tranches de temps entre eux. Nous détaillons le multiplexage temporel un peu plus loin.

Figure K.2
Canaux WLL de la bande 24,5-26,5 GHz



Couche physique et technique d'accès

La couche physique de WiMAX utilise la technologie OFDM (Orthogonal Frequency Division Multiplexing), qui découpe les fréquences en sous-fréquences orthogonales afin que deux fréquences voisines puissent être utilisées sans interférence.

Pour augmenter le débit des versions les plus évoluées, le MIMO (Multiple Input Multiple Output) est autorisé. Dans ce cas, comme expliqué au chapitre 20 pour IEEE 802.11n, plusieurs antennes peuvent émettre en parallèle sur la même fréquence en jouant sur les multiples chemins suivis par les signaux pour récupérer ces signaux à des instants légèrement différents.

WiMAX demande une technique d'accès puisque l'antenne joue le rôle d'équipement commun à tous les clients. La solution retenue est de type OFDMA (Orthogonal Frequency Division Multiple Access).

La technique d'accès de WiMAX est illustrée à la figure K.3.

Dans cette figure, les tranches de temps sont données aux différents clients suivant des ordres de priorité. WiMAX possède quatre classes de priorités :

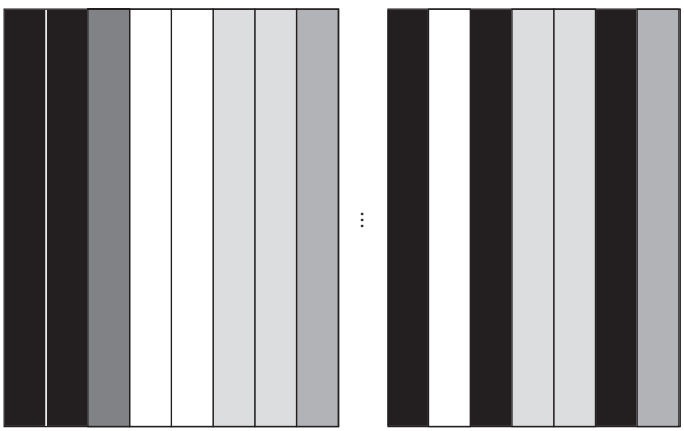
- UGS (Unsolicited Grant Service), la priorité la plus haute, a pour objectif de faire transiter des applications qui ont un débit constant en générant des paquets de longueur constante à des intervalles réguliers. Cette classe reçoit une allocation de tranches à intervalles réguliers de telle sorte que chaque paquet puisse être émis sans attente. Cette classe correspond aux applications de téléphonie classique qui produisent un débit constant. C'est une classe provenant de l'ATM mais un peu plus sophistiquée : le CBR (Constant Bit Rate). Les paramètres de qualité de service sont le Maximum Sustained Traffic Rate, c'est-à-dire le trafic moyen en période d'émission, le Minimum

Reserved Traffic Rate, c'est-à-dire le taux minimal à réserver pour que les paquets puissent passer et le Request/Transmission Policy, qui indique la politique de retransmission. Dans cette classe, si une tranche de temps est réservée, elle ne peut être préemptée par une autre classe. Il y a donc possibilité de perte de la tranche si le client ne l'utilise pas. Comme nous le verrons avec le WiMAX mobile, une autre classe a été ajoutée pour la téléphonie compressée.

- rtPS (real-time Packet Service) correspond à la transmission d'applications de type vidéo. Cette classe prend en charge les applications qui produisent des trames de longueur variable à intervalles réguliers. Les tranches de temps qui ne seraient pas utilisées peuvent être réutilisées. Les paramètres de qualité de service sont les suivants : Maximum Sustained Traffic Rate, Minimum Reserved Traffic Rate, Request/Transmission Policy comme dans l'UGS et Maximum Latency Traffic Priority, qui indique le temps maximal entre deux trames prioritaires.
- nrtPS (non real-time Packet Service) correspond à des applications élastiques qui acceptent une variabilité du délai et dont les paquets ont des tailles variables, mais qui demandent un débit minimal. Cette classe de trafic est bien adaptée au transfert de fichiers et aux applications sans contraintes temporelles mais qui demandent malgré tout un débit minimal pour s'assurer d'être transmis après un temps correspondant à ce débit minimal. Les tranches de temps peuvent être volées par des classes de priorité supérieures si c'est nécessaire à la qualité de service de ces applications. Les paramètres définissant la qualité de service de sont Maximum Sustained Traffic Rate et Request/Transmission Policy ainsi que Minimum Reserved Traffic Rate, correspondant au trafic minimal souhaité par l'utilisateur, et Priority Traffic, correspondant au trafic des trames indispensables à l'application.
- BE (Best Effort) ne demande aucune qualité de service particulière et aucun débit minimal. Les paramètres de cette classe de service sont Maximum Sustained Traffic Rate, Traffic Priority, Request/Transmission Policy. Les services associés sont bien entendu ceux qui ne demandent aucune garantie sur le trafic, comme le trafic des applications Web.

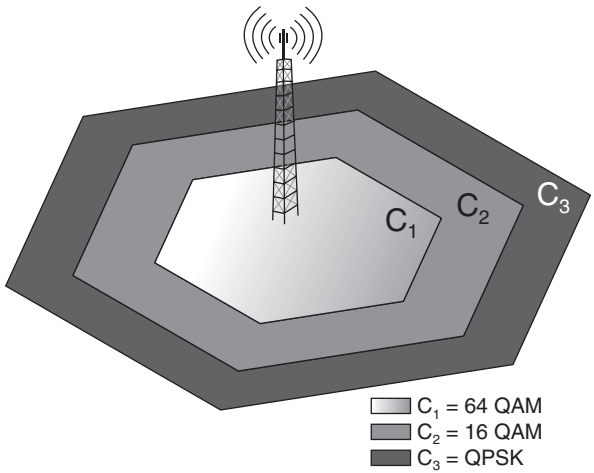
Figure K.3

Technique d'accès de WiMAX



WiMAX utilise également une technique d'adaptation du codage à la qualité de la communication. Cette adaptation est illustrée à la figure K.4.

Figure K.4
Adaptation du codage à la qualité de la communication



Dans cette figure, le codage utilisé lorsque le client est assez près de l'antenne est le 64QAM, qui permet de faire passer 8 bits à chaque intervalle élémentaire. Si le client s'éloigne et que la qualité du signal se dégrade, ce qui est observé par le nombre de retransmissions, le codage passe au 16QAM et le transport à 4 bits par baud. Si le client est assez éloigné de l'antenne, une nouvelle dégradation implique le passage en QPSK et à l'émission de seulement 2 bits simultanément.

Ce comportement est assez sophistiqué puisqu'il implique une adaptation du terminal à la qualité du signal. Comme dans la plupart des réseaux de la gamme Wi-*xx,* cela crée des difficultés de gestion de la qualité de service des applications puisqu'il n'est pas possible de déterminer à l'avance le débit brut de l'antenne de l'opérateur. Ce débit dépend en fait des terminaux raccordés et non de l'antenne elle-même. Chaque terminal peut en effet transmettre à sa vitesse, allant du simple au quadruple. C'est une des raisons pour lesquelles les tests effectués autour de WiMAX affichent un débit beaucoup plus bas qu'attendu dès que la plupart des terminaux sont situés à des distances de plus de 5 km. C'est aussi pour cela qu'il est recommandé, si l'on veut obtenir un débit approchant 50 Mbit/s, de restreindre la taille des cellules WiMAX à des rayons de quelques kilomètres, idéalement deux ou trois.

La réception de WiMAX nécessite des antennes fixes qui relient la maison ou l'entreprise à l'antenne de l'opérateur. L'irrigation dans la maison ou l'entreprise peut se faire par le biais d'une autre technologie, comme Wi-Fi. Les ordinateurs personnels peuvent toutefois être dotés d'une carte spécifique incluant l'antenne. Des processeurs spécifiques intégrant les composants WiMAX sont également disponibles, mais ils ne sont encore que peu utilisés.

Pour voir se déployer des architectures WiMAX de bout en bout, il faudra attendre l'arrivée de processeurs multitechnologie permettant de se connecter à plusieurs antennes différentes simultanément.

Couche MAC

La couche MAC de WiMAX possède trois sous-couches :

- La sous-couche de convergence, qui permet d'utiliser la technologie IP que ce soit sur le relais de trames, Ethernet ou l'ATM.
- La sous-couche « Common part », qui permet l'accès au système et l'allocation de bande passante.
- La sous-couche sécurité, qui reprend un certain nombre d'éléments de chiffrement des techniques à l'œuvre dans les réseaux Wi-Fi.

La trame échangée entre l'équipement mobile et la station de base est illustrée à la figure K.5. Il s'agit d'une trame MAC générique, qui contient les requêtes de bande passante.

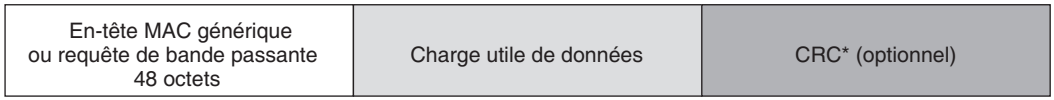


Figure K.5

La trame MAC WiMAX

Cette trame est composée de trois parties : l'en-tête, qui est soit un en-tête MAC générique, soit une requête de bande passante. La longueur de l'en-tête est de 48 octets. Viennent ensuite les données à transporter et une zone de détection d'erreurs optionnelle.

L'en-tête est illustré à la figure K.6.

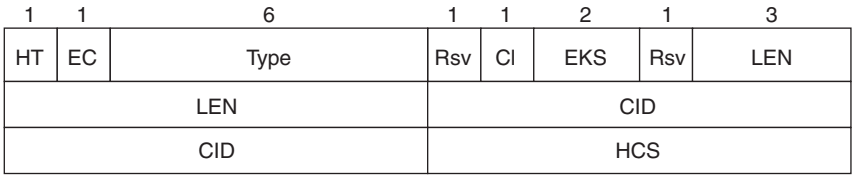


Figure K.6

En-tête de la trame MAC de WiMAX

Les valeurs possibles des différents champs sont les suivantes :

- Le bit HT est égal à 0 si l'en-tête est générique et à 1 si c'est une demande de bande passante.

- Le bit EC indique si la trame est chiffrée : si EC=0 les informations transportées ne sont pas chiffrées. Si EC=1, l'information est chiffrée. Il est à noter que EC doit être égal à 0 si HT=1.
- Le type, sur 6 bits, indique ce que contient le champ d'information. Si le premier bit est égal à 1, le réseau est un réseau mesh. Si le deuxième est égal à 1 c'est qu'un algorithme de ARQ Feedback Payload est appliqué. Si le troisième est égal à 1, une fragmentation du champ d'information ou bien une compression est acceptée. Les deux bits suivants indiquent si la fragmentation ou la compression est effectivement utilisée. Le sixième bit indique si un algorithme de Fast Feedback est utilisé.
- Les bits Rsv (reserved) sont positionnés à 0.
- Le bit CI est un indicateur d'existence d'un CRC. Si CI=0, il n'y a pas de CRC ; si CI=1, la zone de détection d'erreur CRC est présente dans la trame.
- La zone EKS (Encryption Key Sequence) n'a une valeur à prendre en compte que si EC=1. Dans ce cas, elle indique si une clé de chiffrement du trafic est utilisée, la clé TEK (Traffic Encryption Key), et s'il y a un vecteur d'initialisation.
- La zone LEN (Length) tient sur 11 bits, trois dans le deuxième octet et les huit bits du troisième octet. Cette zone indique la longueur en octets de la trame en y incluant l'en-tête et le CRC s'il y en a un.
- Le champ de deux octets CID (Connection Identifier) indique l'identificateur de la connexion.
- Le champ HCS (Header Check Sequence) sert de détection d'erreur pour l'en-tête. Le polynôme générateur est x^8+x^2+x+1.

En cas de demande de bande passante, l'en-tête se présente sous la forme illustrée à la figure K.7.

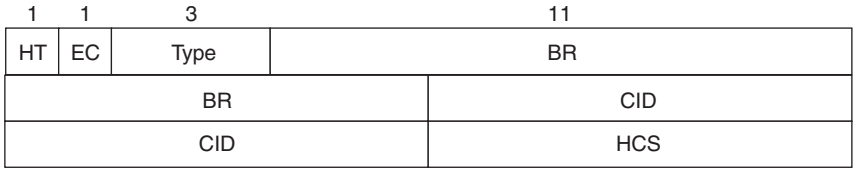


Figure K.7

Format de l'en-tête pour une demande de bande passante

Le champ HT est égal à 1 et le champ EC à 0 puisqu'il ne doit pas y avoir de chiffrement. Le champ Type indique le type de bande passante demandée par la trame. Pour le moment, seules sont admises les valeurs 000, pour indiquer une valeur incrémentale, et 001, pour une valeur agrégée. Le champ BR (Bandwidth Request) indique la demande d'une bande passante pour la voie montante en nombre d'octets. Cette demande n'inclut pas les overheads qui proviendraient de la couche physique.

La couche MAC comporte de nombreuses trames de gestion : quarante-neuf sont indiquées dans la norme IEEE 802.16-2004. La trame possède dans ce cas deux champs, le premier pour indiquer le type de message de gestion et le second pour préciser le contenu de l'information de gestion transportée.

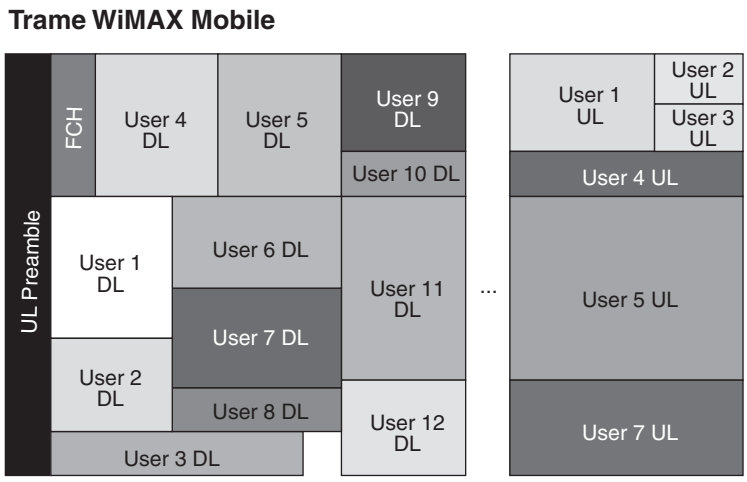
WiMAX mobile

WiMAX mobile correspond à la version mobile de WiMAX fixe. Il existe cependant d'importantes différences entre les deux technologies.

Dans WiMAX mobile, la couche physique OFDM donne naissance à un partage du support de type SOFDMA (Scalable OFDMA), dans lequel les clients prennent un ensemble de fréquences de l'OFDM pendant un certain nombre de tranches. Cette solution permet d'améliorer fortement l'utilisation du canal en récupérant des fréquences ou des tranches inutilisées.

La figure K.8 illustre cette technique d'accès de WiMAX mobile.

Figure K.8
Technique d'accès de WiMAX mobile



À un instant donné, plusieurs utilisateurs se partagent les fréquences du canal de communication. Ce partage s'effectue en fonction des besoins et des classes de clients. L'ordonnancement optimal n'est pas toujours simple à trouver, d'autant que certaines fréquences peuvent avoir un meilleur rendement grâce à une qualité supérieure de leur canal.

La couverture peut être améliorée par des antennes directives. WiMAX mobile utilise la diversité d'antenne ainsi qu'une méthode de retransmission automatique (H-ARQ). Cette technique de retransmission permet de garder en mémoire les paquets erronés de telle sorte que la confrontation de plusieurs paquets erronés puisse être suffisante pour rétablir le paquet correctement. Cette technique est fondamentalement différente de celles qui

retransmettent les paquets jusqu'à ce que le paquet arrive correctement en entier. Ces techniques sont également utilisées dans les réseaux de mobiles HSDPA et HSUPA.

La couverture et les débits, c'est-à-dire la diversité qui permet soit d'augmenter le débit, soit la qualité de la communication, sont également améliorés par l'utilisation du MIMO. De plus, différentes technologies de codage de nouvelle génération sont utilisées, comme les turbocodes et les LDCP (Low Density Parity Check). Ces solutions permettent d'adapter les communications d'un terminal vers l'antenne de l'opérateur en tenant compte de leurs caractéristiques propres et de la qualité de la transmission, lesquelles sont surtout dépendantes de l'éloignement de l'antenne et des atténuations dues au champ électromagnétique.

Dans WiMAX mobile, une classe de trafic supplémentaire a été introduite pour prendre en charge la parole téléphonique compressée de débit variable. Il s'agit de l'ertPS (enhanced real-time Packet Service). Cette classe correspond à de la téléphonie dans laquelle une compression rend le débit variable ou dans laquelle les silences sont supprimés de telle sorte que le débit devienne également variable. Les paramètres de qualité de service sont Maximum Sustained Traffic Rate, Minimum Reserved Traffic Rate, Maximum Latency Tolerated Jitter et Request/Transmission Policy. Ces paramètres sont les mêmes que dans l'UGS.

Une autre amélioration importante de WiMAX mobile provient de la compression des trames et plus généralement de l'utilisation intensive de la classe ertPS. Ces améliorations sont illustrées à la figure K.9.

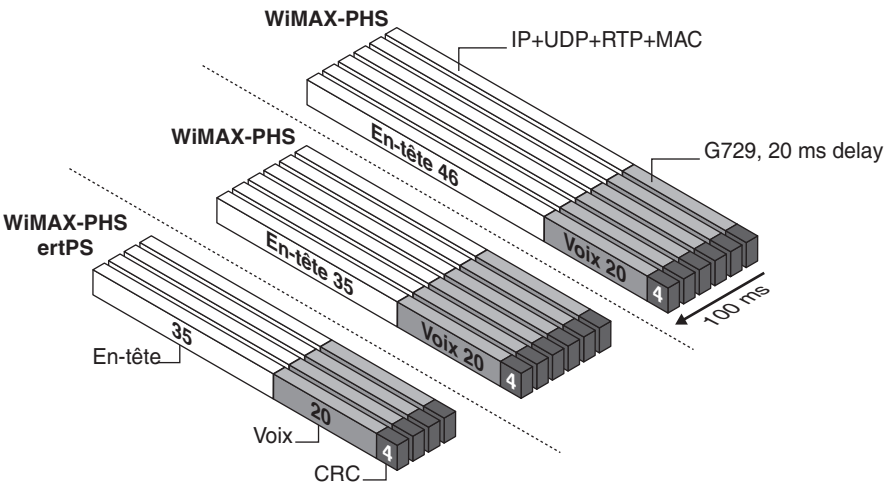


Figure K.9

Améliorations de WiMAX mobile

La première partie de la figure (en haut) illustre la transmission dans WiMAX (fixe) : les en-têtes font 46 octets de long, la zone de détection d'erreur (CRC 4), fait 4 octets et

le paquet (Voix) 20 octets de téléphonie. Dans la version WiMAX améliorée, WiMAX-PHS, l'en-tête est compressé, ce qui permet de faire descendre sa longueur de 46 à 35 octets. La partie basse de la figure illustre l'utilisation de la classe ertPS, qui permet de ne rien transmettre pendant les silences.

Comparaison avec les autres technologies

La figure K.10 situe la technologie WiMAX mobile par rapport aux versions UMTS et cdma2000, qui sont ses concurrentes directes. La différence fondamentale entre elles provient de la partie RAN (Radio Access Network). Dans les versions actuelles de l'UMTS ou du cdma2000, la technologie ATM est fortement utilisée pour l'optimisation de l'utilisation des supports physiques. L'AAL2 permet grâce à ses microtrames de bien remplir les trames ATM. Ce n'est pas le cas des paquets IP, qui ne permettent pas d'utiliser au mieux les capacités de transmission des supports fixes des réseaux WiMAX. Les paquets IP dans les techniques 3G (UMTS et cdma2000) sont transportés en tant qu'éléments binaires. Dans la solution WiMAX mobile, l'architecture est nativement Ethernet et IP.

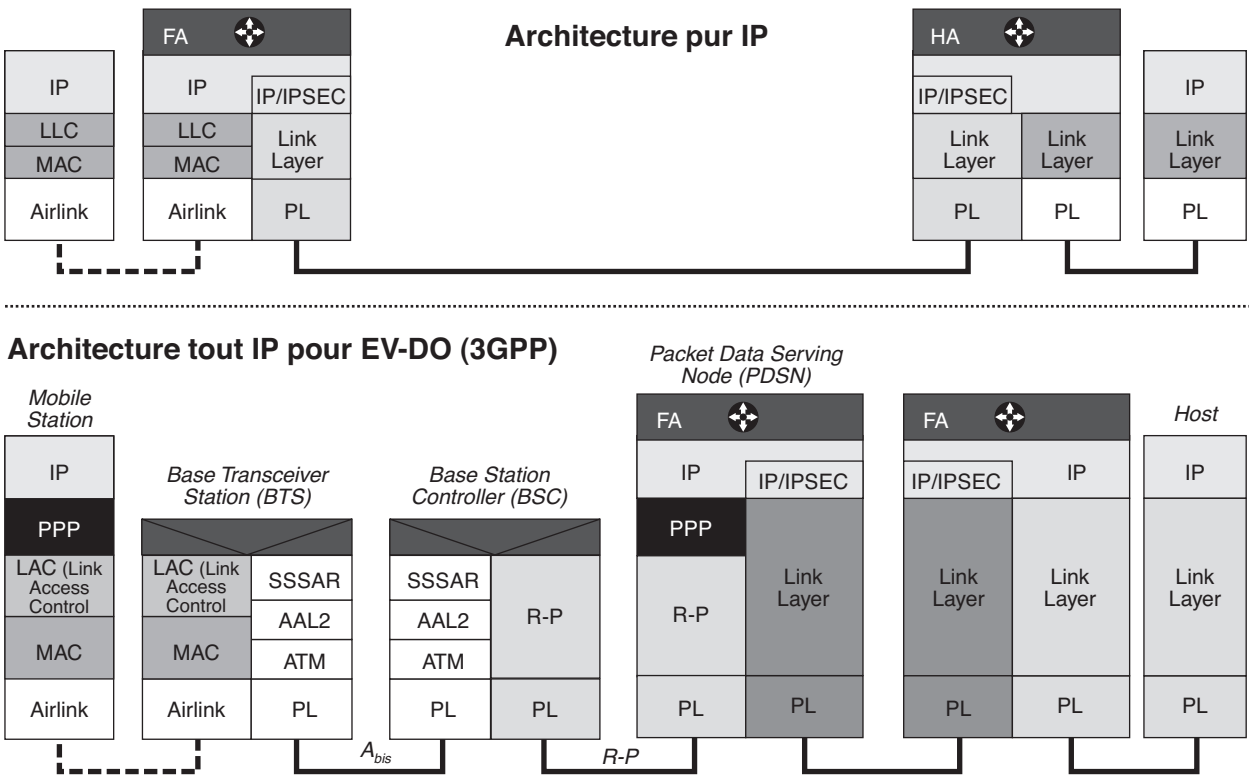


Figure K.10

Comparaison des technologies UMTS/cdma2000 et WiMAX mobile

La comparaison de ces deux architectures illustre la simplicité de WiMAX mobile mais aussi la difficulté à garantir la qualité de service si les canaux ne sont pas de bonne qualité, puisque c'est l'environnement Ethernet/IP qui doit prendre en charge la communication.

Globalement, la compétition entre les deux technologies risque d'être très forte puisque l'objectif est le même : réaliser du multimédia en mobilité avec des débits de quelques mégabits par seconde.

La différence fondamentale entre WiMAX fixe et WiMAX mobile réside dans la gestion des handovers. Trois mécanismes ont été définis dans la norme avec une latence inférieure à 50 ms :

- Hard handoff : le passage d'une cellule à une autre est instantané, et à aucun moment le terminal n'est en communication avec les deux cellules simultanément.
- FBSS (Fast Base Station Switching) : la connexion reste maintenue avec le réseau cœur (core network).
- MDHO (Macro Diversity Handover) : possibilité de réaliser un handover sans couture (*seamless handoff*) qui n'est pas visible du terminal.

Le tableau K.1 compare les caractéristiques de WiMAX mobile à celles des technologies cellulaires de même génération, c'est-à-dire HSDPA/HSUPA et 1x EV-DO Rev A.

Tableau K.1 • Comparaison des techniques cellulaires de nouvelle génération

Attribut	1X EV-DO REVA	HSDPA/HSUPA	WIMAX MOBILE
Standard de base	cdma2000/IS 95	WCDMA	IEEE 802.16e-2005
Méthode de duplexage	FDD	FDD	TDD
Canal descendant	TDM	CDM-TDM	OFDMA
Canal montant	CDMA	CDMA	OFDMA
Largeur de bande du canal	1,25 MHz	5 MHz	5, 7, 8,75, 10 MHz
Taille de la trame descendante	1,67 ms	2 ms	5 ms
Taille de la trame montante	6,67 ms	2,1 ms	5 ms
Modulation sur le canal descendant	QPSK, 8PSK, 16QAM	QPSK, 16QAM	QPSK, 16QAM, 64QAM
Modulation sur le canal montant	BPSK, QPSK, 8PSK	BPSK, QPSK	QPSK, 16QAM
Codage	Turbo	CC, Turbo	CC, Turbo
Vitesse maximale du canal descendant	3,1 Mbit/s	14 Mbit/s	32, 46 Mbit/s
Vitesse maxilae du canal montant	1,8 Mbit/s	5,8 Mbit/s	7, 4 Mbit/s
H-ARQ	Fast 4-channel Synchronous IR	Fast 6-channel Asynchronous CC	Multi-channel Asynchronous CC
Ordonnancement	Fast scheduling sur le canal descendant	Fast scheduling sur le canal descendant	Fast scheduling sur le canal descendant et montant
Handover	Virtual Soft Handover	Network Initiated hard handover	Network optimized hard hanover
MIMO	Simple Open Loop Diversity	Simple Open&Closed Loop Diversity	STBC, SM
Beamforming	Non	Non	Oui

Comme on peut le voir sur ce tableau, de nombreuses propriétés sont communes aux différentes technologies de nouvelle génération correspondant à des réseaux commercialisés

en 2007-2008. Parmi ces technologies, AMC (Adaptive Modulation and Coding), H-ARQ (Hybrid ARQ), FS (Fast Scheduling) et BEH (Bandwidth Efficient Handover).

La première caractéristique commune concerne le codage et la modulation adapatative en fonction de la qualité du canal. La technologie proposée par WiMAX est plus puissante, grâce à la possibilité d'utiliser la technologie AMC sur des paquets de taille variable, aussi bien dans le sens montant que descendant.

La technique de correction des erreurs par une méthode H-ARQ permet, en conservant les paquets erronés, de déterminer le paquet exact sans que l'ensemble des éléments binaires doivent arriver correctement au destinataire. Les techniques de H-ARQ CC (Chase Combining) et H-ARQ IR (Incremental Redundancy) sont les plus utilisées. Dans la première, les paquets retransmis sont les mêmes que ceux transmis la première fois. Dans la seconde, le paquet erroné peut être retransmis à la suite de nouveaux paquets du même flot. Cette solution est beaucoup plus complexe, mais elle permet de continuer à transmettre sans attendre la réussite d'une retransmission.

L'algorithme Fast Scheduling permet de distribuer l'allocation de la bande passante aux clients en tenant compte de la qualité du canal. Il est beaucoup plus efficace de servir les clients qui disposent d'un bon canal que de s'attarder sur ceux dont le canal est de mauvaise qualité.

Les solutions pour effectuer du « Bandwidth Efficient Handover » sont diverses. La technique du soft handover pourrait paraître la plus séduisante. Elle n'est toutefois pas toujours la meilleure, car elle oblige l'équipement terminal à être connecté simultanément sur deux stations de base. Cela exige une gestion de la bande passante plus complexe. Le hard handover est généralement plus efficace et demande moins de ressources.

WiMAX phase 2

La phase 1 de WiMAX n'a eu que peu de succès pour différentes raisons non techniques. Pour rebondir, le groupe IEEE responsable de sa normalisation a demandé au 3GPP de devenir membre de la famille 4G. Cette demande a été accordée puisque WiMAX est complètement compatible avec le monde IP et offre une qualité de service et un système de gestion correspondant aux demandes des opérateurs de télécommunications. Cependant, comme nous l'avons vu, de nombreuses contraintes liées à la 4G devaient encore être prises en compte. C'est ce nouvel environnement qui a pris le nom de WiMAX phase 2.

Pour cela, le comité IEEE 802.16 a introduit les nouveaux groupes de travail suivants :

- IEEE 802.16g : Network Management Task Group (Management Plane Procedures & Services) ;
- IEEE 802.16h : License-Exempt Coexistence Task Group ;
- IEEE 802.16j : Mobile Multihop Relay Task Group ;
- IEEE 802.16m : Advanced Air Interface Task Group.

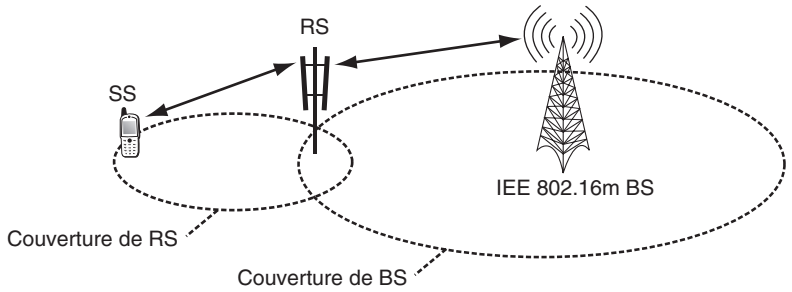
Le groupe le plus important est le dernier. Il a défini une interface radio améliorée permettant de doubler au minimum les débits pour obtenir 46 Mbit/s dans le sens descendant

et toujours 4 Mbit/s dans le sens montant. WiMAX phase 2 augmente encore ces débits pour être du même ordre de grandeur que ceux de LTE Advanced. Cette phase sera suivie de WiMAX phase 3, avec l'objectif de démultiplier de nouveau les vitesses pour atteindre plusieurs centaines de mégabits par seconde, voire le gigabit par seconde.

WiMAX phase 2 atteint déjà 100 Mbit/s en mobilité et jusqu'à 1 Gbit/s lorsque le terminal est immobile. Ces valeurs sont des débits crête et dépendent évidemment du nombre de clients connectés et actifs au moment de la mesure.

Pour ne pas reprendre des éléments communs au LTE Advanced, nous allons essentiellement décrire la proposition de *relais* qui est faite dans le standard IEEE 802.16m. Un tel relais est illustré à la figure K.11. Les relais sont des antennes intermédiaires situées entre l'antenne principale et le terminal de l'utilisateur. Les antennes principales sont raccordées par une fibre optique au réseau cœur de l'opérateur. Lorsque l'on démultiplie les antennes, il faut réaliser du génie civil pour poser de nouveaux câbles terrestres. L'objectif des relais est d'éviter ce problème et de baisser les coûts de connexion. Le terminal est branché sur le relais, qui est lui-même connecté sur l'antenne principale par un faisceau hertzien. Ce dernier peut être situé dans les fréquences hautes, et être donc très directif, avec une large bande passante permettant de faire transiter des gigabits par seconde. Comme le faisceau est directif, il ne pollue pas l'environnement hertzien.

Cette solution permet de diminuer le coût de connexion tout en augmentant le débit global grâce à de petites antennes relais que l'on peut densifier à volonté.



Extension de couverture par déploiement d'équipements relais, ou RS (Relay Station)

BS (Base Station) : Station de base
RS (Relay Station) : Équipement relais
SS (Subscriber Station) : Équipement utilisateur

Figure K.11

Un relais dans WiMAX phase 2

WiBro et IEEE 802.20

WiBro est une solution très semblable à WiMAX développée par la Corée du Sud au tout début des années 2000. En 2004, Intel et LG Electronics se sont mis d'accord pour réaliser une interopérabilité entre les deux techniques. La solution est fortement orientée

WiMAX mobile puisque WiBro a choisi de modifier son interface radio pour prendre le SOFDMA.

Le groupe de travail IEEE 802.20 a un objectif semblable. Formé pour réaliser un réseau MBWA (Mobile Broadband Wireless Access), il devait venir en complément de WiMAX, conçu au départ pour être uniquement fixe. Lorsque le groupe 802.16e s'est mis en place, le groupe 802.20 a été suspendu afin de ne pas dupliquer les efforts. Finalement, il a été remis en marche pour aboutir à une proposition de standard pour la très grande mobilité, jusqu'à 500 km/h, et le très haut débit.

Une proposition de Kiocera a été normalisée dans le cadre d'un groupe très restreint d'industriels. En réponse, les industriels de WiMAX ont lancé le groupe IEEE 802.16m et WiMAX phase 2 avec un objectif similaire à celui du groupe 802.20. Comme l'environnement WiMAX est le sixième système inclus dans l'IMT 2000, la technologie IEEE 802.20 n'a quasiment aucune chance de se développer.

WRAN

Le groupe de travail IEEE 802.22 a démarré ses activités en 2004 dans l'objectif de réaliser un réseau hertzien régional. Les bandes de fréquences utilisées viennent en premier lieu du dividende numérique, c'est-à-dire des bandes de fréquences qui seront libérées lorsque la télévision passera totalement et définitivement en numérique. En France, c'est prévu pour 2010. Dans le reste du monde, cela devrait s'étaler entre aujourd'hui et 2015.

Les études portent sur les « canaux blancs » de la télévision, c'est-à-dire les fréquences ou les bandes de télévision qui ne sont pas utilisées ou qui le sont très mal. L'idée est d'introduire une transmission opportuniste qui utilise les bandes inutilisées à certains instants par la télévision en prenant soin de ne pas brouiller les canaux de télévision.

Les fréquences utilisées se situent en dessous de 1 GHz. Elles possèdent les propriétés des bandes de télévision : pénétration par les murs, très bonne portée et haut débit.

Les clients seront munis de systèmes GPS ou Galileo pour localiser l'émetteur. Après interrogation d'une base de données centrale, ils recevront la fréquence sur laquelle ils peuvent émettre avec la puissance et la directivité voulues.

Ces principes de radio « cognitive » sont étudiés depuis quelques années afin d'utiliser beaucoup mieux le spectre. L'état du réseau et le comportement de l'utilisateur pourront impliquer une modification de la fréquence, de la puissance, etc.

En résumé, la radio cognitive définit la possibilité d'utiliser une bande avec licence sans que l'opérateur qui l'utilise soit gêné. Comme de nombreuses bandes sont peu utilisées, il est possible de récupérer une bande passante considérable.

On peut définir deux types de radio cognitive :

- Full Cognitive Radio, où tous les paramètres utilisables le sont.
- Spectrum Sensing Cognitive Radio, où seulement la fréquence radio utilisée est prise en compte.

Deux sous-ensembles sont également discernables :

- utilisation de la radio cognitive dans un environnement sous licence, comme celle proposé par l'IEEE 802.15.2 ;
- utilisation des fréquences d'une bande sans licence, comme celle proposée par l'IEEE 802.19.

La radio cognitive a été surtout développée dans le cadre de la radio logicielle (Software-Defined Radio) et s'est surtout intéressée à la solution Spectrum Sensing Cognitive Radio dans les bandes de télévision. La difficulté essentielle est évidemment de détecter l'utilisation de la bande par son détenteur légal, puis d'arrêter les émissions secondaires et détecter que la bande est de nouveau non utilisée. La détection de l'énergie n'est pas vraiment suffisante pour être sûr que l'on ne va pas perturber les signaux licenciés. L'utilisation s'effectue par une technologie OFDM, dans laquelle seules les sous-bandes correspondant aux bandes libres sont utilisées.

IEEE 802.22 travaillant en mode point-à-multipoint, un signal peut être diffusé sur une large surface et s'adresser simultanément à un ensemble de points. Le système est formé de stations de base, ou BS (Base Station), et d'équipements terminaux. La station de base reçoit de la part des équipements terminaux des rapports réguliers de l'écoute des porteuses. À partir de ces informations, la station de base peut décider de changer ou non de fréquence et définir la puissance d'émission des équipements terminaux.

Le support physique travaille en OFDM et détermine les sous-bandes à utiliser, et le codage de la modulation. Les essais montrent que l'émission sur un canal de télévision de la station de base permet d'acheminer une vingtaine de mégabits par seconde sur 30 km.

L

Annexe du chapitre 17 (Les small cells et les réseaux multisaut)

Cette annexe s'intéresse à l'environnement satellite dans les réseaux hertziens avec relais. Elle commence par introduire les fréquences radio qui sont utilisées dans ces réseaux puis détaille les politiques d'accès au canal satellite et donne quelques exemples de constellations.

Les fréquences radio

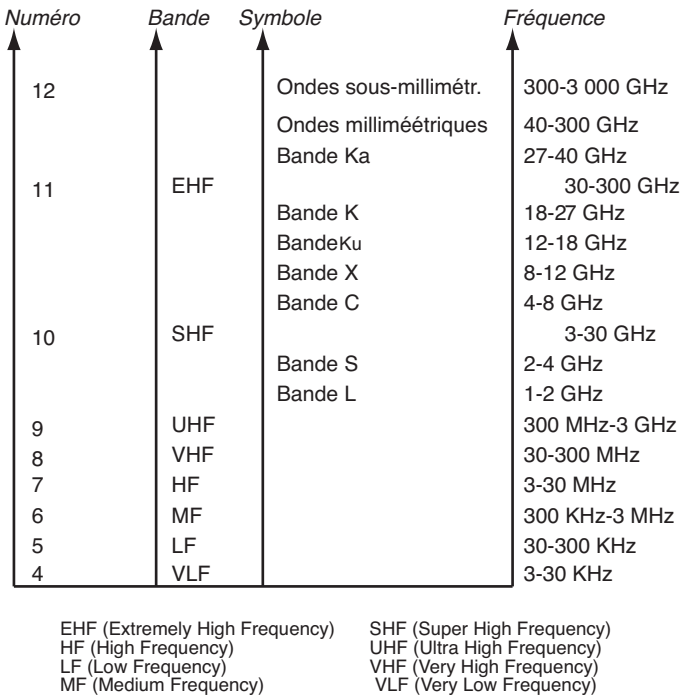
Les fréquences radio sont divisées en bandes, déterminées par un groupe de travail IEEE, le SRD (Standard Radar Definitions). Les numéros de bandes et les noms sont donnés par l'organisme international de régulation des bandes de fréquences. La figure L.1 illustre les bandes de fréquences allouées aux systèmes satellitaires.

La bande C est la première à avoir été utilisée pour les applications commerciales. La bande Ku accepte des antennes beaucoup plus petites, dites VSAT (Very Small Aperture Terminal), de 45 cm de diamètre seulement. La bande Ka autorise des antennes encore plus petites, et c'est pourquoi la plupart des constellations de satellites l'utilisent. De ce fait, les terminaux peuvent devenir mobiles, grâce à une antenne presque aussi petite que celle des terminaux de type GSM. On qualifie ces terminaux de USAT (Ultra Small Aperture Terminal). En revanche, l'utilisation de la bande S permet d'entrer dans le cadre de l'UMTS et des réseaux de mobiles terrestres.

Les fréquences classiquement utilisées pour la transmission par satellite concernent les bandes 4-6 GHz, 11-14 GHz et 20-30 GHz. Les bandes passantes vont jusqu'à 500 MHz

et parfois 3 500 MHz. Elles permettent des débits très élevés, jusqu'à plusieurs dizaines de mégabits par seconde. Un satellite comprend des répéteurs, de 5 à 50 actuellement. Chaque répéteur est accordé sur une fréquence différente. Par exemple, pour la bande des 4-6 GHz, il reçoit des signaux modulés dans la bande des 6 GHz, les amplifie et les transpose dans la bande des 4 GHz. S'il existe n stations terrestres à raccorder par le canal satellite, le nombre de liaisons bipoint est égal à $n \times (n - 1)$. Ce nombre est toujours supérieur à celui des répéteurs. Il faut donc, là aussi, avoir des politiques d'allocation des bandes de fréquences et des répéteurs.

Figure L.1
Fréquences radio des systèmes satellite



Les très grands projets qui ont été finalisés juste avant les années 2000 ne visent que la téléphonie, par suite d'un manque flagrant de bande passante des systèmes satellitaires non militaires. Cette limitation est cependant partiellement compensée par le grand nombre de satellites défilant à basse altitude, qui permet une bonne réutilisation des fréquences. Plusieurs grands projets techniquement aboutis se sont effondrés ces dernières années pour des raisons financières, et l'environnement satellite doit se trouver des niches de marché correspondant aux zones non couvertes par les réseaux cellulaires terrestres ou la diffusion massive.

Les techniques d'accès au satellite

Les canaux satellite, comme tous les systèmes à canaux partagés, demandent une technique d'accès. La différence essentielle avec les interfaces radio des réseaux de mobiles provient du long délai de propagation entre l'émetteur et le récepteur. Dans les réseaux cellulaires ou les réseaux locaux, le délai de propagation très court permet de gérer simplement les instants de transmission. Dans le cas de satellites géostationnaires, les stations terrestres ne découvrent qu'il y a eu chevauchement des signaux que 0,27 s après leur émission — elles peuvent s'écouter grâce à la propriété de diffusion —, ce qui représente une perte importante sur un canal d'une capacité de plusieurs mégabits par seconde.

Les techniques d'accès pour les réseaux satellite sont généralement classées en quatre catégories :

- les méthodes de réservation fixe, ou FAMA (Fixed-Assignment Multiple Access) ;
- les méthodes d'accès aléatoires, ou RA (Random Access) ;
- les méthodes de réservation par paquet, ou PR (Packet Reservation) ;
- les méthodes de réservation dynamique, ou DAMA (Demand Assignment Multiple Access).

Les protocoles de réservation fixe réalisent des accès non dynamiques aux ressources et ne dépendent donc pas de l'activité des stations. Les procédures FDMA, TDMA et CDMA forment les principales techniques de cette catégorie. Ces solutions offrent une qualité de service garantie puisque les ressources sont affectées une fois pour toutes. En revanche, l'utilisation des ressources est mauvaise, comme dans le cas d'un circuit affecté au transport de paquets. Lorsque le flux est variable, les ressources doivent permettre le passage du débit crête.

Les techniques d'accès aléatoires donnent aux utilisateurs la possibilité de transmettre leurs données dans un ordre sans corrélation. En revanche, ces techniques ne se prêtent à aucune qualité de service. Leur point fort réside dans une implémentation simple et un coût de mise en œuvre assez bas.

Les méthodes de réservation par paquet évitent les collisions par l'utilisation d'un schéma de réservation de niveau paquet. Comme les utilisateurs sont distribués dans l'espace, il doit exister un sous-canal de signalisation à même de mettre les utilisateurs en communication pour gérer la réservation. Les méthodes de réservation dynamique ont pour fonction d'optimiser l'utilisation du canal. Ces techniques essaient de multiplexer un maximum d'utilisateurs sur le même canal en demandant aux utilisateurs d'effectuer une réservation pour un temps relativement court. Une fois la réservation acceptée, l'utilisateur vide ses mémoires tampons jusqu'à la fin de la réservation puis relâche le canal.

Les communications par l'intermédiaire d'un satellite montrent des propriétés légèrement différentes de celles d'un réseau terrestre. Les erreurs, en particulier, se produisent de façon fortement groupée, en raison de phénomènes physiques survenant sur les antennes d'émission ou de réception. Au contraire des réseaux locaux, aucun protocole de niveau liaison n'est normalisé pour les réseaux satellite. Plusieurs procédures ont été proposées, mais aucune ne fait l'unanimité. Le délai d'accès au satellite constitue le problème

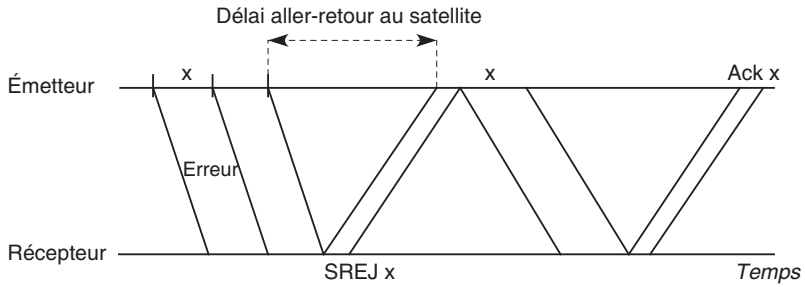
principal, puisque, pour recevoir un acquittement, un temps égal à deux fois l'aller-retour est nécessaire. À ce délai aller-retour, il faut encore ajouter le passage dans les éléments extrémité, qui est loin d'être négligeable. Ce délai dépend bien sûr de la position de l'orbite sur laquelle se trouve le satellite. Lorsque les capacités des liaisons sont importantes, les techniques utilisant des reprises explicites à partir de la trame en erreur ne sont pas efficaces, la quantité d'information à retransmettre devenant très grande. Les techniques sélectives posent également des questions de dimensionnement des mémoires permettant d'attendre l'information qui n'est pas parvenue au récepteur.

Contrairement aux réseaux locaux, les réseaux satellite n'ont pas donné lieu à une normalisation spécifique. Plusieurs protocoles ont été proposés, mais aucun ne s'est vraiment imposé.

Un réseau utilisant un satellite géostationnaire ou un satellite situé sur une orbite moyenne se caractérise par un très long temps de propagation, comparativement au temps d'émission d'une trame. Pour cette raison, il existe des extensions aux procédures classiques, qui permettent l'émission d'un grand nombre de trames sans interruption. Si le débit est très élevé et qu'une procédure HDLC (High-level Data Link Control) avec une méthode SREJ (Selective REJect) soit adoptée, l'anticipation doit être très importante ou bien la longueur des trames très grande. Par exemple, si le débit de la liaison satellite est de 10 Mbit/s, sachant qu'il faut au moins prévoir d'émettre sans interruption pendant un temps égal à deux allers-retours (*voir figure L.2*), la valeur minimale de la trame est de 20 Ko. Cette quantité est très importante, et la qualité de la ligne doit être excellente pour qu'un tel bloc de données (160 000 bits) arrive avec un taux d'erreur bit inférieur à 10^{-10}.

Figure L.2

Reprise sur une liaison satellite



Les politiques de réservation fixe

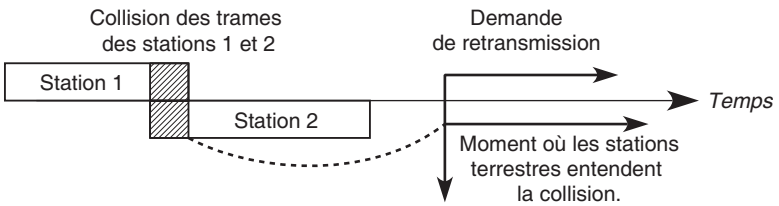
Les politiques de réservation fixe, ou FAMA (Fixed-Assignment Multiple Access), utilisées dans les systèmes satellite sont les mêmes que celles utilisées dans les réseaux de mobiles : FDMA, TDMA et CDMA. Pour le moment la technique CDMA n'est pas employée dans les réseaux satellite, mais elle devrait venir en complément des techniques terrestres de troisième génération, telles que l'UMTS, le cdma2000, etc.

Les politiques d'accès aléatoire

Les techniques d'accès aléatoire ont été introduites dans les réseaux locaux. Dans un réseau satellite, où le délai de propagation est très important par rapport aux réseaux locaux, les stations terrestres qui émettent des signaux ne sont informées d'une éventuelle collision de leur paquet que 270 ms après l'émission. L'accès aléatoire consiste donc, pour les stations terrestres, à émettre dès qu'elles ont un paquet de données en leur possession. S'il y a collision, les stations terrestres concernées s'en aperçoivent puisqu'elles écoutent les signaux émis sur le canal. Les paquets perdus sont retransmis ultérieurement, après un temps aléatoire, de façon à réduire au maximum le risque de nouvelles collisions.

La figure L.3 illustre la collision entre deux paquets sur un canal satellite.

Figure L.3
Collision entre deux paquets sur un canal satellite



Les deux techniques d'accès aléatoire

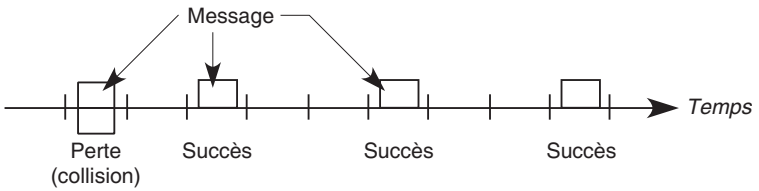
Les deux grandes catégories de politiques d'accès aléatoires sont l'aloha et l'aloha discrétisé.

La technique aloha tire son nom d'un mot hawaïen, car elle a pour origine des expériences réalisées à l'Université de Hawaï pour relier les centres informatiques dispersés sur de nombreuses îles. Dans le système aloha, la propriété de diffusion et les codes détecteurs d'erreur permettent aux stations terrestres de savoir si leurs émissions de paquets se sont effectuées correctement. Si ce n'est pas le cas, les paquets sont retransmis après un délai aléatoire. Ce délai est un paramètre essentiel, qui détermine les performances du système.

Des méthodes d'évaluation de performance montrent que, si le nombre de stations terrestres est très grand et tend mathématiquement vers l'infini et qu'aucune politique précise ne soit suivie pour la retransmission des messages perdus dans les collisions, l'utilisation du canal tend vers 0, et le débit devient nul. Les deux grandes politiques de contrôle consistent à allonger les temps avant retransmission en fonction du nombre de paquets en attente de réémission ou bien à stopper les nouvelles émissions dès que le nombre de paquets en attente de retransmission dépasse une valeur fixée à l'avance. Malgré tout, le débit maximal correspond à une utilisation du canal satellite égale à $\frac{1}{2e} = 0{,}184$.

Le concept d'aloha discrétisé repose sur la division du temps en tranches de longueur égale correspondant au temps de transmission d'un paquet, qui, de ce fait, doit avoir une longueur constante. Les collisions se produisent dans ce cas sur l'ensemble de la tranche, et non plus, comme avant, sur des parties de paquets seulement (*voir figure L.4*). Les émissions doivent être synchronisées en début de tranche de temps.

Figure L.4
Aloha en tranches



Calculons le taux d'utilisation maximal du canal satellite dans ce dernier cas, en supposant que les demandes d'émission de messages arrivent suivant un processus de Poisson, et que le nombre de stations terrestres est grand. Si S est le débit du canal et G le trafic total en comptabilisant aussi bien les réussites que les échecs, la proportion de réussite S/G est égale à la probabilité de réussite sur une tranche de temps, c'est-à-dire e^{-G}, ce qui correspond à la probabilité qu'un seul paquet à la fois soit émis sur une tranche. Nous obtenons :

$$S = G\, e^{-G}$$

où le débit S est optimisé pour G = 1. Cela permet d'obtenir le taux d'utilisation maximal : 1/e = 0,368. On voit que, en découpant le temps en tranches, on peut doubler le débit du canal. Cependant, ce débit reste faible, et des techniques de réservation peuvent parfois être utilisées pour améliorer les performances du système.

Les protocoles avec réservation par paquet

Les politiques de réservation par paquet sont très nombreuses. Les sections qui suivent en décrivent trois avec plusieurs variantes. Le dénominateur commun de ces méthodes réside dans la faculté de réserver à l'avance des tranches de temps pour les stations qui ont des paquets à émettre.

R-aloha

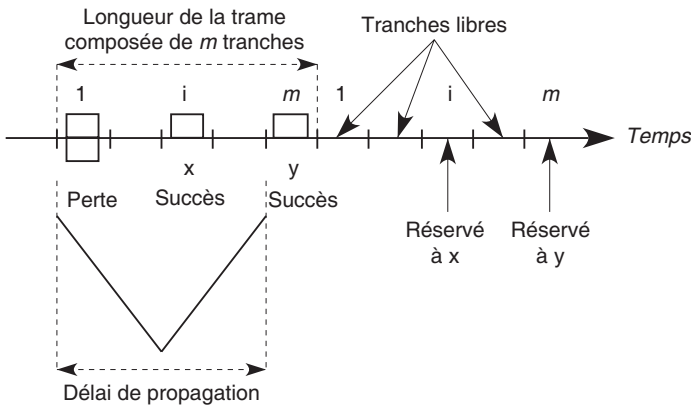
Les protocoles de réservation par paquets utilisent généralement une partition du temps en tranches fixes. Ces tranches sont regroupées pour former des trames. Une station ne peut émettre dans une tranche que si elle a effectué une réservation. La réservation peut être explicite ou implicite. Par exemple, dans la technique R-aloha, une transmission réussie signifie automatiquement une réservation dans la même tranche de la trame suivante. En effet, en informatique, les messages sont très souvent subdivisés en plusieurs paquets, ce qui signifie qu'une station terrestre qui vient d'émettre un paquet a toutes les chances d'en émettre un autre immédiatement derrière, d'où l'idée de lui réserver des tranches de temps.

La technique aloha avec réservation utilise le principe précédent : les tranches de temps sont réunies en trames d'une longueur supérieure au temps aller-retour, de telle sorte que toutes les stations au début d'une tranche sont au courant de ce qui s'est passé dans la même tranche de la trame précédente. Si une tranche est libre ou reflète une superposition de plusieurs paquets, la tranche correspondante dans la trame suivante est libre d'accès.

Au contraire, si une station *x* réussit une transmission, la tranche correspondante dans la trame suivante lui est réservée, comme l'illustre la figure L.5. Dès qu'une tranche

réservée est inoccupée, elle redevient libre d'accès. Le débit permis par cette technique dépend du nombre de paquets par message. Des débits correspondant à des taux d'utilisation du canal de l'ordre de 1 peuvent être obtenus pour de très longs messages.

Figure L.5
Aloha avec réservation



PODA (Priority-Oriented Demand Assignment)

La procédure PODA utilise également une réservation par paquets. Dans ce cas, la trame est divisée en une première partie, qui permet de réaliser des réservations, et une seconde pour le transport des paquets des émetteurs ayant réussi leur réservation. Toutes les stations écoutent la partie réservation et utilisent le même algorithme pour classer les réservations. La frontière entre les deux parties dépend du nombre de stations et de la charge globale.

Dans le cas le plus classique, le temps est découpé en tranches, supposées de longueur égale, correspondant à la durée de transmission d'un paquet. Les tranches sont regroupées en trames, dont la durée est supérieure au temps de propagation aller-retour. Chaque trame débute par une première partie contenant des minitranches de réservation, suivie d'une deuxième partie contenant les tranches d'émission effective des paquets (*voir figure L.6*).

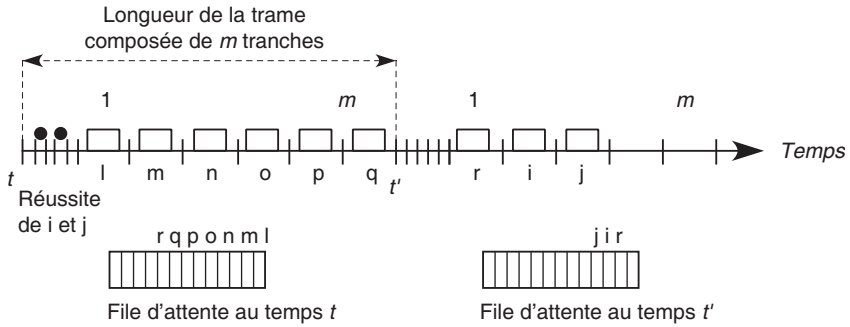


Figure L.6
Fonctionnement de PODA

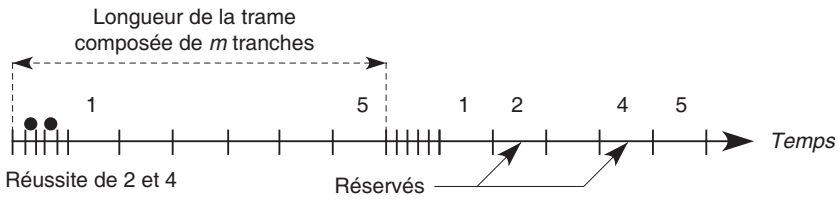
La méthode aloha permet d'accéder aux minitranches de réservation. Les réussites déterminent une file d'attente fictive dans l'ordre premier arrivé, premier servi. Cette file se vide en servant les clients un par un dans les tranches de temps.

La principale lacune de cette méthode provient du manque d'information qu'elle génère, qui ne permet pas de connaître à l'avance le nombre optimal de tranches ni de minitranches dans une trame. Un manque de réussite sur les minitranches peut engendrer un relatif effondrement du débit du système. En revanche, une trop grande réussite peut allonger la file jusqu'à provoquer des débordements.

Réservation ordonnée

Dans la réservation ordonnée, la structure de la trame est la même que dans le cas précédent, mais il y a autant de minitranches dans l'en-tête que de tranches dans la trame et que de stations terrestres. Chaque minitranche est dédiée à une station terrestre. Cela permet à une station terrestre d'avertir les autres émetteurs qu'elle va occuper la tranche qui lui appartient. Dans le cas contraire, la tranche correspondante devient libre, et tous les utilisateurs peuvent y accéder dans un mode d'accès aléatoire. La technique de réservation ordonnée est illustrée à la figure L.7.

Figure L.7
Réservation ordonnée



Réservation à tour de rôle

Dans la politique de réservation dite à tour de rôle, le temps est toujours découpé en tranches. Une trame est formée de *m* tranches, *m* étant supérieur à *n,* qui est le nombre de stations terrestres. Les *n* premières tranches sont réservées aux stations correspondantes. Elles permettent de transporter la valeur d'un compteur indiquant la longueur de la file d'attente de ces stations. Plus précisément, cette valeur indique le nombre de paquets en attente de transmission.

Une file d'attente commune est construite à partir des valeurs transportées dans les *n* premières minitranches indiquant le nombre de paquets en attente pour chaque station. Les $m - n$ dernières tranches de la trame sont occupées à tour de rôle par les stations d'émission en attente, suivant la file d'attente commune, comme illustré à la figure L.8.

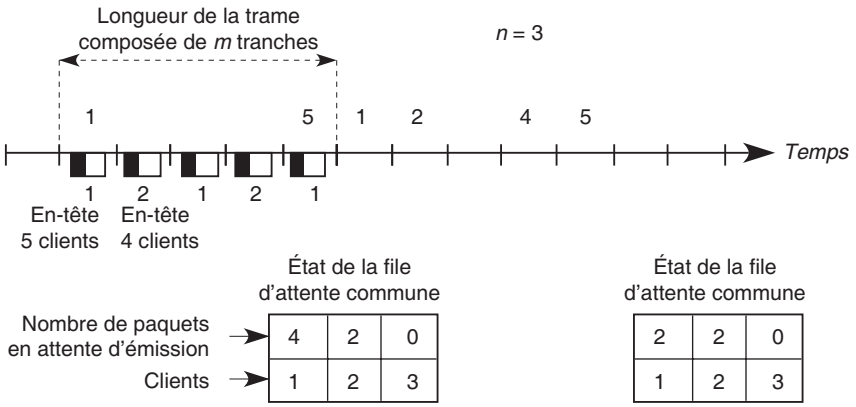


Figure L.8

Réservation à tour de rôle

Les protocoles de réservation dynamique et les méthodes hybrides

Les protocoles de réservation dynamique allouent les ressources en fonction de la demande des utilisateurs. Des priorités peuvent être attribuées aux différents utilisateurs. Le séquenceur, qui peut se trouver dans le satellite, organise les réservations suivant les niveaux de priorité. Les garanties de service dépendent de l'allocation des ressources. Par exemple, CF-DAMA (Combined Free DAMA) garantit une qualité de service pour les priorités hautes et une distribution équitable des ressources restantes pour les basses priorités.

Techniques hybrides

Un grand nombre de techniques hybrides ont été proposées, parmi lesquelles les trois suivantes :

- L'association d'un protocole FAMA, qui assure une qualité de service pour quelques classes de clients à haute priorité, et d'une politique DAMA, pour partager le reste de la bande passante. Un exemple d'une telle solution est offert par la politique FBA/DAMA, qui fournit une garantie minimale de bande passante sur une partie, le reste de la bande passante étant répartie par une technique DAMA.
- Le schéma RRR (Round-Robin Reservation), qui requiert un nombre de stations inférieur au nombre de tranches nécessaires à la discipline TDMA. Chaque station possède une tranche dédiée. Les tranches restantes sont accédées par les stations suivantes selon un accès aléatoire de type aloha.
- La technique IFFO (Interleaved Frame Flush-Out), dans laquelle la trame est divisée en trois parties, une pour le contrôle, une pour les tranches réservées et une en accès

aléatoire. La partie contrôle, qui est subdivisée en minitranches, une pour chaque station, permet d'effectuer des réservations. Tous les émetteurs qui deviennent actifs après le passage de la partie réservation de la trame peuvent accéder aux tranches en libre-service. Si une collision se produit, les stations concernées utilisent leur tranche réservée. Les tranches appartenant à la partie réservée mais qui n'ont pas fait l'objet d'une réservation peuvent être utilisées pour l'accès aléatoire.

Dans les techniques de réservation par paquet, on peut accéder aux minitranches soit nominalement, soit par accès aléatoire. On essaie également d'utiliser au maximum les tranches qui n'ont pas été réservées, et ce par une file d'attente commune, avec une discipline de service déterminée à l'avance ou par un accès aléatoire.

Le temps de réponse en fonction du débit lorsque 50 stations terrestres émettent des messages relativement courts peut fournir un critère de performance des techniques d'accès. Les temps de réponse les meilleurs sont obtenus par l'aloha pour de faibles débits, par la méthode de réservation par paquet pour des débits moyens et par la méthode TDMA pour les taux d'utilisation du canal de l'ordre de 1.

Les satellites de deuxième génération peuvent embarquer du matériel de commutation et de mémorisation. De ce fait, les signaux sont démodulés à bord, et les erreurs en ligne peuvent être détectées, donnant naissance à une nouvelle génération de protocoles.

De nouvelles possibilités d'accès au canal sont également permises pour ces satellites de deuxième génération. L'intelligence introduite dans le satellite permet de ne retransmettre vers la Terre que les paquets corrects. Par exemple, si une politique d'accès aléatoire est utilisée dans le sens montant, les paquets ayant réussi leur transmission sans collision sont placés dans une file d'attente et retransmis vers la Terre dans l'ordre premier arrivé, premier servi. La largeur de bande dans le sens descendant peut de la sorte être beaucoup plus petite que dans le sens montant.

Les systèmes satellite bande étroite

Les satellites bande étroite correspondent à la première génération. Ils ont été construits essentiellement pour les services de téléphonie et la diffusion de canaux de télévision. Du fait de la baisse des coûts de mise en orbite d'un satellite et de l'augmentation des performances des stations terrestres, de nombreux services nouveaux se sont ouverts sur les satellites bande étroite, surtout dans le domaine de la transmission de données.

Ces services peuvent être monodirectionnels, ou monovoies, une station terrestre émettant vers une ou plusieurs stations simultanément, sans voie de retour. Si une voie de retour est nécessaire, elle peut être terrestre. Ce type de communication correspond à la diffusion d'informations sans acquittement. Il est également possible de prévoir des voies de retour spécifiques par le satellite. Malheureusement, ces voies de retour ne sont utilisées que par les acquittements et les informations de contrôle et de gestion, procurant ainsi une très mauvaise utilisation de la liaison de retour.

La transmission de données dans les systèmes bande étroite s'effectue dans les spectres 12-14 GHz en TDMA, avec un ajout de canaux de télévision.

Les services mobiles correspondent à des stations terrestres pouvant se déplacer, c'est-à-dire munies d'antennes mobiles, mais à des vitesses très faibles comparées à celles des satellites défilants. Le développement de ces services mobiles est relativement lent du fait de la difficulté d'obtenir des antennes mobiles suffisamment puissantes à des coûts acceptables pour l'utilisateur. Le début des services mobiles s'est effectué dans le cadre des liaisons entre bateaux. Ces développements ont mené à la constitution d'Inmarsat (International Marine Satellite Organization), qui est aujourd'hui, et de très loin, l'organisation la plus importante dans les services mobiles par satellite. Elle compte 66 membres et s'occupe depuis 1989 des services de communications mobiles pour l'aéronautique. Cette association dépend des opérateurs, comme expliqué précédemment, qui revendent les services d'Inmarsat aux utilisateurs.

Les satellites bande étroite

Les fréquences suivantes, concernant l'utilisation de satellites bande étroite, ont été définies en 1987 par la WARC (World Administrative Radio Conference) :

- 1,530-1,544 GHz pour les communications du satellite vers les mobiles terrestres et les bateaux ;
- 1,544-1,545 GHz pour les communications du satellite vers les mobiles en détresse ;
- 1,545-1,599 GHz pour les communications du satellite vers les mobiles aéronautiques ;
- 1,626-1,645 GHz pour les communications des mobiles terrestres et des bateaux vers le satellite ;
- 1,645-1,646 GHz pour les communications des mobiles en détresse vers le satellite ;
- 1,646-1,660 GHz pour les communications des mobiles aéronautiques vers le satellite.

Les antennes dépendent du type de service recherché. Trois grandes possibilités ont été développées :

- antennes Inmarsat A, d'un mètre de diamètre ;
- antennes Inmarsat C, d'un diamètre largement inférieur à 1 m, mais fixes, c'est-à-dire non repliables, pour des communications de données pouvant atteindre 600 Kbit/s ;
- antennes Inmarsat M, d'un diamètre inférieur à 1 m, permettant la téléphonie avec une compression à 6,4 Kbit/s et des données jusqu'à 2,4 Kbit/s.

Les communications d'affaires entre les différents points d'une même société ont commencé à se développer au début des années 1980. Il fallait pour cela des antennes de petit diamètre à des coûts acceptables pour les utilisateurs. Le vrai démarrage a eu lieu avec l'utilisation des VSAT (Very Small Aperture Terminal), dont le début des années 1990 a connu l'essor, aussi bien en Europe qu'aux États-Unis.

Intelsat et Eutelsat

Deux organisations internationales se consacrent aux services entre stations fixes : Intelsat et Eutelsat. Intelsat a été lancée en 1964 et regroupe aujourd'hui plus de cent vingt

pays membres. Son objectif est d'organiser, de coordonner et d'offrir une très grande bande passante à ses membres, dans le but de réaliser des communications téléphoniques, des diffusions de canaux de télévision et des services intégrés pour les grandes entreprises. Intelsat a été fondée par les opérateurs de télécommunications et a installé à leur intention tout un réseau de satellites. Pendant de nombreuses années, Intelsat a eu la complète maîtrise de toutes les communications par satellite. Il a commencé à perdre ce monopole dans les années 1980, lorsque les Européens ont lancé Eutelsat pour coordonner les communications par satellite en Europe et que d'autres organisations nationales ou internationales, telles que Panamsat, ont commencé à offrir des services similaires avec des techniques légèrement différentes.

Intelsat a défini plusieurs standards de stations terrestres. Le premier, le standard A, définit une antenne de 15 à 18 m de diamètre, dans la fréquence des 4-6 GHz. Les derniers standards, D, E, F, définissent des antennes entre 3,5 et 10 m de diamètre, dans des fréquences élargies à 4-6 ou aux bandes 11-12/14 GHz.

Bien que constituée en 1977, Eutelsat n'est une organisation à part entière que depuis 1985, du fait de l'opposition d'Intelsat, craignant pour son monopole. Plus d'une trentaine de membres sont aujourd'hui dénombrés. Le rôle d'Eutelsat est semblable à celui d'Intelsat mais centré sur l'Europe. Eutelsat a élargi son champ de compétences en proposant aux petites entreprises des services de diffusion et de communication intégrés. Une société possédant un grand nombre de succursales peut, d'une seule émission, toucher toutes les succursales et en même temps émettre un message particulier à l'une des succursales. Par exemple, les numéros de cartes Visa volées peuvent être envoyés simultanément à toutes les billetteries et, en même temps, un message particulier peut être adressé à telle ou telle billetterie.

M

Annexe du chapitre 18 (Les réseaux de mobiles 1G à 6G)

Cette annexe décrit la première génération de réseaux de mobiles puis la deuxième, avec le GSM, GPRS et Edge, et introduit les versions américaines, avec l'IS.

Les systèmes cellulaires de première génération

Les systèmes cellulaires de première génération sont caractérisés par des terminaux analogiques dotés d'une mobilité restreinte et de services limités. Deux standards ont été développés, le CT0 (Cordless Telephone), principalement utilisé aux États-Unis et au Royaume-Uni, et le CT1, utilisé en Europe, notamment en Allemagne et en Italie.

Les réseaux cellulaires de première génération ont été les premiers à permettre à un utilisateur mobile d'utiliser un téléphone de façon continue, n'importe où dans la zone de service d'un opérateur.

Les systèmes téléphoniques sans fil

Les premiers terminaux sans fil sont introduits avec la technologie CT0 aux États-Unis et en Europe au cours des années 1970 pour remplacer les téléphones filaires. Ces terminaux offrent des performances modestes, le canal radio étant fortement parasité et de nombreuses interférences avec les installations électriques environnantes perturbant la qualité des émissions.

Les téléphones sans fil, très chers dans les années 1970, souffrent alors d'un manque de sécurité, d'une faible autonomie et d'une qualité de restitution de la parole en dessous

de la moyenne. Cependant, la flexibilité et la portabilité qu'ils proposent les rendent rapidement populaires.

Une nouvelle génération de technologie sans fil, le CT1, est développée au début des années 1980 et est utilisée dans une douzaine de pays européens. Malheureusement, chaque pays en commercialise une version spécifique, ce qui oblige les constructeurs à concevoir autant de versions que de pays. De plus, le CT1 ne permet pas aux terminaux sans fil de communiquer avec des stations de base provenant d'autres constructeurs et souffre de limitations importantes concernant l'itinérance et le handover. Ces téléphones sans fil analogiques fonctionnent autour de 900 MHz. Leur marché n'a jamais été à la hauteur des ambitions des constructeurs, essentiellement à cause de leur prix élevé et de la non-compatibilité entre constructeurs et entre versions de la norme.

Des recherches sur les systèmes sans fil fondés sur la technologie numérique sont menées à partir des années 85 afin de fournir plus de capacité et une meilleure qualité de service. La deuxième génération voit ainsi apparaître une téléphonie à faible mobilité, le Télépoint, reposant sur le standard CT2 (Cordless Telephone of 2nd Generation).

Les systèmes cellulaires

Le concept cellulaire est introduit dans les années 1970 par les Bell Labs. Les systèmes cellulaires sont conçus pour augmenter la mobilité des terminaux. Une cellule est une zone géographique couverte par une antenne de transmission. Un utilisateur est en mesure de passer d'une cellule à une autre sans coupure de la communication. Ce passage, appelé handover ou handoff, permet au terminal de changer de cellule sans interruption. À cette fin, le terminal doit embarquer tous les composants nécessaires à la gestion de la communication.

Le premier système cellulaire opérationnel, l'AMPS (Advanced Mobile Phone System), se met en place aux États-Unis à la fin des années 1970. En Europe du Nord, des opérateurs de télécommunications et des constructeurs lancent une génération assez similaire, le NMT (Nordic Mobile Telecommunication system). Le NMT est développé en Suède, en Norvège, au Danemark et en Finlande au début des années 1980.

D'autres réseaux, fondés sur les concepts de l'AMPS et du NMT, sont également commercialisés, comme le TACS (Total Access Communication System) au Royaume-Uni ou des versions du NMT en France. France Télécom introduit Radiocom 2000 en 1985 et SFR met en place son service en 1989. Tous ces systèmes cellulaires reposent sur une transmission de la voix analogique avec une modulation de fréquence dans les bandes des 450 et 900 MHz.

Les réseaux téléphoniques sans fil

En raison de la faible qualité du CT1, plusieurs constructeurs européens ont développé, en 1984, le système CT2 de téléphonie sans fil de deuxième génération. Dans le but d'autoriser un service de Télépoint, c'est-à-dire un service de téléphonie public fondé sur le CT2 dans lequel le client est quasiment immobile, une interface commune, connue sous

le nom de CAI (Common Air Interface) est spécifiée en 1988. Son objectif est de fournir une norme uniforme pour le Télépoint public, qui permette aux utilisateurs de changer de réseau et d'opérateur tout en gardant le même terminal.

Le Télépoint

Cette norme concerne l'accès au réseau téléphonique commuté par une interface air en faible mobilité, le terminal ne pouvant effectuer de handover entre deux cellules. Les systèmes de type Télépoint ne fournissent pas de couverture nationale mais peuvent être installés en des endroits où le trafic d'appel est important, comme les gares, aéroports, centres commerciaux et restaurants. Le Télépoint est le premier exemple d'un service de téléphonie personnelle peu onéreux, utilisable en résidentiel, au bureau ou dans des lieux publics, car il se sert du réseau téléphonique existant. En outre, le coût de l'implémentation d'un réseau de stations de base Télépoint est très bas.

Le Télépoint donne donc la possibilité d'établir un réseau public à faible coût, comparativement aux systèmes cellulaires, qui nécessitent une intelligence sophistiquée incluant la gestion de la mobilité. Plusieurs réseaux de Télépoint ont été créés en Europe, tels Rabbit au Royaume-Uni, Bi-Bop en France, Greenpoint aux Pays-Bas et CITEL en Belgique. Le principal inconvénient du Télépoint réside dans l'incapacité quasi permanente des terminaux à recevoir des appels. Il est également impossible avec de tels systèmes d'avoir une conversation continue en déplacement. Tous ces éléments ont empêché le lancement commercial du CT2 dans de bonnes conditions, et la plupart des services de Télépoint européens ont été des échecs.

Le DECT

Le DECT est un standard de télécommunications sans fil conçu par l'ETSI. La plupart des concepts ayant présidé à son lancement s'inspirent d'un système suédois, connu sous le nom de DCT (Digital Cordless Telephone) ainsi que du CT2. Les Suédois ont conçu le DCT parce qu'il leur fallait une nouvelle norme, mieux appropriée que le CT1 aux environnements à grande capacité, comme les PABX sans fil. Le DECT bénéficie en Europe d'une bande de fréquences de 1 880 à 1 900 MHz et offre des services qui vont au-delà de ceux fournis par les systèmes précédents. En particulier, l'environnement radio DECT est conçu pour des applications résidentielles et professionnelles ainsi que pour un accès public. De plus, l'interfonctionnement des systèmes DECT dans les zones publiques et privées est fiable.

Développé au Japon à partir de 1989 sur des bases légèrement différentes des systèmes européens, le PHS est un système sans fil offrant un accès public, aussi bien pour un usage domestique que professionnel, à la fois à l'intérieur et à l'extérieur, avec un terminal de poche à très faible coût. Le système PHS est introduit commercialement au Japon en 1995 comme un système d'accès public. Des fonctionnalités supplémentaires sont rapidement ajoutées, comme la mise en place de boucles locales sans fil, la transmission de données à des débits que l'on peut qualifier d'importants (32 ou 64 Kbit/s) et l'itinérance, ou roaming.

Aux États-Unis, plusieurs standards sont également définis au milieu des années 1990 :

- PCI (Personal Communications Interface), qui s'appuie sur le CT2.
- PWT (Personal Wireless Telecommunications), qui repose sur le DECT.
- PACS-UA (Personal Access Communications System), élaboré à partir du PHS.

Les objectifs de tous ces systèmes sont de fournir une couverture extérieure totale dans les zones urbaines ainsi qu'une continuité de service entre les zones publiques et privées et de permettre aux utilisateurs d'émettre et de recevoir des appels. Pour ce type d'application, la technologie sans fil est une solution de rechange aux technologies cellulaires numériques.

Fonctionnement du DECT

Le DECT définit une technique d'interface radio pour des télécommunications sans fil à courte portée. La mobilité offerte par un système DECT est donc réduite. Le DECT couvre seulement l'interface air entre le terminal, ou PP (Portable Part), et la partie fixe, ou FP (Fixed Part), équivalente à une station de base du GSM. L'élément principal de la normalisation du DECT consiste en l'IC (Interface Control), qui définit le fonctionnement de l'interface air et prévoit un ensemble complet de protocoles.

Le DECT ne fournit aucun service. Il procure la connexion radio à un environnement capable de proposer des services, comme le réseau téléphonique, un PABX, le RNIS, un réseau de données d'opérateur, Internet ou tout autre réseau. L'objectif est de permettre la connexion de terminaux sans fil à un PABX ou à un site central dans un environnement cellulaire.

Les cellules sont de taille variable, leur rayon variant de 10 m à 5 km, selon les obstacles susceptibles de freiner la propagation des ondes. Le DECT fournit des services de voix d'une qualité équivalente à celle rencontrée dans les réseaux fixes ainsi qu'un large ensemble de services de données, incluant la connexion au RNIS ou à Internet. Il peut être implémenté comme un simple téléphone sans fil résidentiel ou comme un système complet, capable de prendre en charge tous les services classiques de téléphonie.

Le DECT prévoit tous les outils nécessaires à la mobilité. Les procédures liées à l'identification, aux droits d'accès, à l'allocation de clés, à la récupération de données, à l'authentification, au chiffrement, au transfert intercellulaire, à la recherche de l'abonné et à la localisation du terminal sont décrites dans la norme. Ses recommandations portent essentiellement sur l'interface radio. En tant que technique permettant l'accès à de nombreux réseaux, et donc aux services correspondants, l'interface DECT doit être indépendante des caractéristiques techniques de ces réseaux tout en étant capable de laisser passer les commandes adaptées aux réseaux à atteindre. C'est ce qu'on désigne sous le terme de profil.

Chacun des profils DECT décrit la façon dont l'interface commune est utilisée pour une application particulière. Un profil est un ensemble de commandes et de procédures fournissant une description non ambiguë de l'interface air pour accéder à des services et à des applications spécifiques. Dans la réalité, la plupart de ces profils ont pour objet

l'interfonctionnement et l'interopérabilité. L'interfonctionnement désigne la capacité d'utiliser plusieurs systèmes ensemble, tandis que l'interopérabilité se réfère à la possibilité d'utiliser ensemble des équipements de différents fabricants fonctionnant sous des systèmes différents. Le GAP (Generic Access Profile) et le profil d'interfonctionnement entre le DECT et le GSM constituent deux exemples importants de profils.

Le GAP permet l'interopérabilité entre les équipements terminaux et les stations de base. Un terminal d'un premier constructeur peut être compatible avec une station de base d'un second constructeur, à condition que ces deux équipements respectent le profil GAP. Le profil GAP est le profil DECT de base. Il contient les fonctionnalités nécessaires pour supporter des applications telles que la voix, pour des téléphones sans fil domestiques, les PABX sans fil professionnels et les applications à partir d'un accès public. Il inclut la gestion de la mobilité et le contrôle des appels. Les protocoles gérant le contrôle des appels sont fortement liés à la fourniture des services de voix. Les protocoles traitant la gestion de la mobilité couvrent notamment le traçage de la localisation, les identités et les aspects de sécurité.

Les normes DECT spécifient des protocoles autorisant la mobilité mais ne définissent pas comment les éléments de réseau gardent trace de la localisation d'un terminal DECT ni comment délivrer un appel entrant à un terminal. Ces aspects sont en dehors de la norme DECT, qui n'est qu'une technologie d'accès. L'interface DECT permet d'accéder à de nombreux réseaux, même à des systèmes cellulaires comme le GSM. Pour les réseaux GSM, la mobilité étant une fonctionnalité bien définie, il est possible d'utiliser cette fonctionnalité pour fournir la mobilité à travers une interface air DECT. Les composants spécifiques de l'interface commune nécessaires à l'interfonctionnement entre un terminal DECT et un réseau GSM, en particulier l'interface A, sont définis dans le profil d'interfonctionnement DECT/GSM.

L'ETSI a défini les besoins du protocole de l'interface air et la façon dont les protocoles DECT s'interconnectent avec les protocoles GSM au niveau de l'interface A. Ce profil permet à un équipement DECT d'être compatible GSM, c'est-à-dire de bénéficier des services du réseau GSM, tels que grande mobilité, sécurité ou services de messages courts SMS (Short Message Service). La normalisation de ce profil implique des modifications dans la norme DECT afin qu'elle supporte les services GSM.

D'autres profils ont été définis par l'ETSI, comme l'interfonctionnement entre le DECT et le RNIS. Ce dernier profil permet d'accéder à des services du RNIS, avec des transferts de données d'un débit maximal de 64 Kbit/s.

Vers la 2G

Avec les terminaux DECT et PHS, il est possible d'appeler et d'être appelé, donc de transmettre et recevoir des données. Cependant, ces terminaux n'offrent pas une mobilité globale. Les systèmes sans fil s'appuyant sur les réseaux fixes, la mobilité du terminal n'est pas totale. L'utilisateur d'un terminal DECT peut certes se déplacer, mais cette mobilité n'est pas comparable à celle qui caractérise les terminaux GSM.

L'interfonctionnement entre les systèmes sans fil et cellulaires n'a pas fait l'objet d'études approfondies. Par exemple, si un utilisateur veut bénéficier du même service à partir de son terminal DECT et de son terminal GSM, il doit interrompre sa communication pour changer de terminal. Aujourd'hui, des terminaux multimodes GSM/DECT sont disponibles chez certains fabricants de terminaux, mais, la plupart du temps, ces terminaux correspondent à un terminal GSM et à un terminal DECT réunis.

La technologie DECT semble dotée du potentiel nécessaire à une mobilité locale extérieure, mais elle est inadaptée à une mobilité large. Le DECT permet à un utilisateur d'accéder à des services avancés, implémentés dans les réseaux fixes, à l'aide du réseau intelligent (*voir le chapitre 4*) dans le cadre du concept CTI (Computer Telephony Integration). Le GSM offre une mobilité large mais nécessite l'aide des réseaux intelligents CAMEL (Customized Applications for Mobile Network Enhanced Logic) pour implémenter de nouveaux services, plus spécifiques des opérateurs. Au finale, les solutions GSM et DECT sont davantage complémentaires que concurrentes.

La figure M.1 illustre l'évolution des systèmes mobiles de première, deuxième et troisième générations.

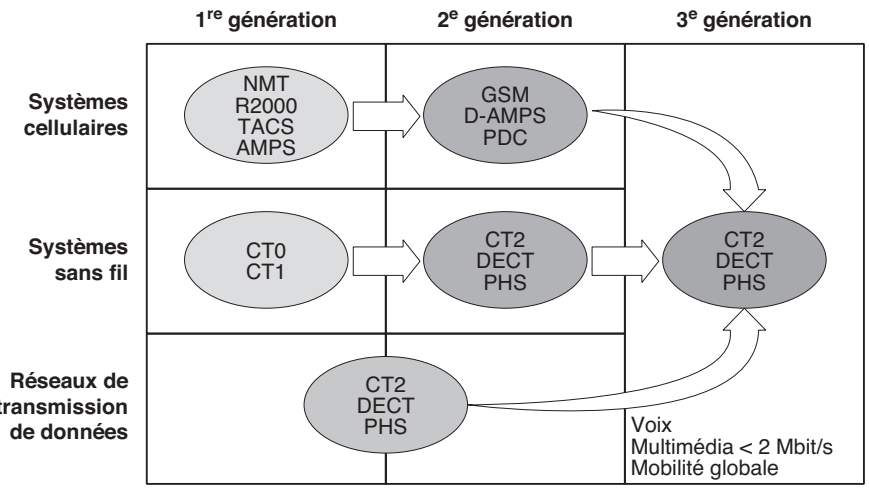


Figure M.1

Évolution des systèmes de communication mobile

Même si les systèmes cellulaires et sans fil ont évolué dans le but de répondre aux besoins des utilisateurs, les systèmes actuels ne proposent pas tous les services attendus par ces derniers. Le manque de compatibilité entre systèmes est également à souligner. Par exemple, il est difficile de connecter un terminal DECT au réseau GSM, bien qu'un profil DECT/GSM soit défini.

En conclusion, de nouveaux systèmes étaient nécessaires pour une meilleure prise en compte des besoins de l'utilisateur. Ces réseaux devaient être plus universels, en intégrant

le cellulaire et le sans-fil. Cela nécessitait de nouveaux standards, dits de deuxième génération et demie et de troisième génération, qui font l'objet des sections suivantes.

Les protocoles des réseaux de mobiles

Les protocoles utilisés dans les réseaux de mobiles s'appliquent à quatre types d'interfaces, que nous allons décrire. Nous ne détaillons dans la suite que les protocoles de l'interface air, qui constituent la spécificité des réseaux de mobiles.

L'architecture de l'IMT 2000 peut être décrite par ses interfaces (*voir figure M.2*). Les quatre interfaces suivantes sont définies :

- **UIM-MT** (User Identity Module-Mobile Terminal). Située entre la carte à puce, qui détermine l'identité de l'utilisateur, et le terminal mobile, cette interface authentifie l'utilisateur et permet de facturer correctement le client qui effectue une communication.
- **MT-RAN** (Mobile Terminal-Radio Access Network). Située entre le terminal mobile et l'antenne, cette interface est aussi appelée interface radio ou interface air. Lorsqu'on parle de réseaux de mobiles, on pense immédiatement à cette interface, car c'est là que réside la spécificité de ces réseaux.
- **RAN-CN** (Radio Access Network-Core Network). Située entre l'antenne et le réseau cœur du réseau de mobiles, cette interface permet, une fois l'antenne atteinte, de transporter les signaux vers l'utilisateur distant par l'intermédiaire d'un réseau terrestre, que l'on appelle le réseau cœur.
- **CN-CN** (Core Network-Core Network). Située entre deux nœuds de transfert du réseau cœur, cette interface est aussi appelée interface NNI (Network Node Interface).

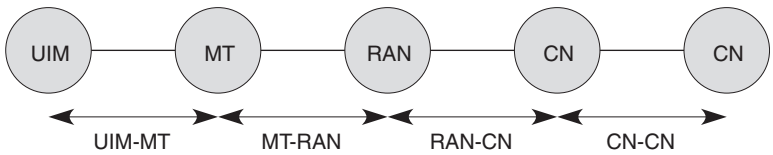


Figure M.2

Interfaces de l'architecture IMT 2000

Un réseau de mobiles d'opérateur doit posséder toutes ces interfaces. Un réseau privé de mobiles peut ne pas disposer d'interfaces UIT-MT et CN-CN.

L'interface UIM-MT, ou SIM-MT, se situe entre la carte à puce et le terminal mobile. Son rôle principal est de sécuriser la communication qui s'établit à partir du mobile. Une carte à puce est insérée dans le terminal à cet effet. Il existe des cartes à puce sans contact, que l'on porte sur soi et qui communiquent directement avec le terminal, les contrôles d'accès et les vérifications s'effectuant par le biais de cette interface. À mesure que les performances des puces s'accroissent, d'autres services peuvent être mis en place et sécurisés, tel le VHE.

L'interface MT-RAN relie le terminal mobile, de type GSM, UMTS ou autre, à l'antenne ou éventuellement à un autre terminal. Dans le cas des systèmes satellitaires, cette interface permet la connexion directe du terminal au satellite. Elle concerne la traversée de la partie air du réseau et définit comment un terminal accède à l'antenne et réciproquement. L'interface air, ou interface radio, est celle que l'on met en avant dans les réseaux de mobiles et sans fil.

Des algorithmes permettent de déterminer quel terminal est en train de transmettre ou comment le signal est transmis, dans le cas où plusieurs terminaux émettent en même temps tout en restant compréhensibles par l'antenne. Dans le GSM, les stations mobiles parlent à tour de rôle, tandis que dans l'UMTS les mobiles peuvent parler en parallèle. Les interfaces air présentent des différences, qui servent souvent à caractériser une technologie, bien que ce ne soit qu'une des quatre interfaces nécessaires pour obtenir un système complet.

L'interface radio constitue souvent le point le plus sensible du réseau, car les ressources y sont faibles et doivent être optimisées. De nombreux défauts peuvent entacher par ailleurs la qualité de service délivrée par cette interface. Les puissantes rivalités politiques et économiques suscitées par la mise en place de l'interface radio n'ont pas permis aux différents continents de se mettre d'accord sur les grandes directions à emprunter. C'est la raison pour laquelle, par exemple, le GSM n'est pas compatible avec les systèmes américains.

L'interface RAN-CN concerne la transmission de l'antenne au premier commutateur du réseau cœur. Cette interface regroupe plusieurs antennes pour permettre de gérer ces dernières collectivement. Dans le cas de l'antenne satellite, l'interface est interne au satellite puisque l'antenne et le commutateur sont tous deux situés dans le satellite.

Cette interface assure la gestion des appels, en acheminant correctement chaque appel arrivant sur le commutateur du réseau cœur de liaison vers l'antenne adéquate, laquelle diffuse l'information de façon qu'elle soit captée par le client destinataire. Cette interface doit également gérer la mobilité, puisque le client se déplace et peut se trouver connecté à une autre antenne, soit à l'intérieur du même sous-système, soit au sein d'un sous-système indépendant.

L'interface CN-CN décrit les protocoles utilisés entre deux nœuds de la partie fixe d'un réseau de mobiles ou d'un réseau satellite, dans le cas d'une constellation de satellites. Les nœuds du réseau sont constitués par les commutateurs du réseau cœur. Cette interface définit, entre autres choses, la technologie réseau utilisée pour acheminer les informations. La technologie réseau du GSM est la commutation de circuits, tandis que celle du GPRS superpose commutation de circuits et commutation de paquets. L'UMTS met en œuvre la commutation de paquets, d'abord ATM, pour la première génération attendue, puis IP. Dans les environnements satellitaires l'interface est de type ATM.

L'interface CN-CN est également importante dans les constellations de satellites, dans lesquelles les interconnexions des satellites forment par elles-mêmes le réseau fixe. La limitation de cette interface provient de l'impossibilité d'offrir une qualité de service garantie.

L'interface radio

L'antenne d'émission-réception, généralement unique pour chaque cellule, est un élément critique des réseaux de mobiles. Si deux mobiles émettent en même temps, l'antenne ne peut généralement capter qu'un des deux messages. Comme dans les réseaux locaux, il faut une technique d'accès pour sérialiser les arrivées des messages sur l'antenne. Les techniques d'accès sont semblables à celles que l'on trouve dans les réseaux locaux.

Les réseaux satellite présentent la même problématique, avec pour différence essentielle une distance très grande entre les stations.

Les méthodes le plus souvent utilisées dans les réseaux de mobiles sont le FDMA, le TDMA et le CDMA. Ces trois méthodes étant décrites au chapitre 16, nous ne ferons ici que rappeler brièvement leurs différences. Dans la technique CDMA, tous les utilisateurs parlent en même temps, l'antenne étant capable de récupérer correctement tous les signaux qui lui arrivent grâce au code de puissance. Chaque terminal émet sur une fréquence donnée avec une puissance déterminée par le code. Il faut respecter la puissance arrivant au récepteur pour que le déchiffrage soit possible.

L'avantage évident de cette technique est de permettre de garder son code, et donc sa bande passante, sur des cellules connexes. En revanche, une première difficulté consiste à fournir des codes suffisamment différents à chaque utilisateur connecté pour qu'il n'y ait pas d'interférences et que l'antenne soit capable de récupérer les émissions qui s'effectuent en parallèle. Une seconde difficulté consiste à contrôler précisément la puissance d'émission, de façon que le récepteur qui se trouve plus ou moins loin reçoive le signal avec la bonne puissance. La figure M.3 présente une comparaison des trois grandes techniques d'accès. Dans le CDMA, la bande passante est partagée par les cinq terminaux suivant un code, c'est-à-dire un niveau de puissance de réception.

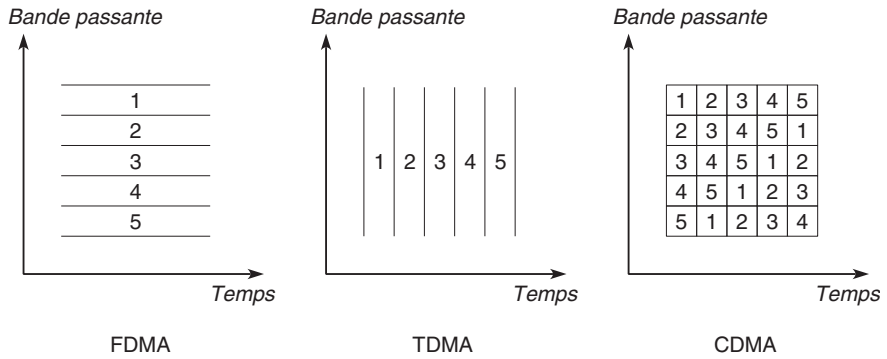


Figure M.3

Comparaison des techniques d'accès

Les techniques que nous venons de décrire peuvent se superposer. Par exemple, un découpage en fréquences (FDMA) peut être suivi d'un TDMA sur chaque fréquence, comme dans le GSM. Dans l'UMTS, un découpage en fréquence est associé sur chaque

fréquence à un TDMA puis sur chaque slot à un CDMA. Le cdma2000 divise la bande passante en grandes sous-bandes auxquelles est appliqué un CDMA. Enfin, le WCDMA (Wideband-CDMA) utilise toute la bande passante en CDMA.

La deuxième génération (2G)

Les réseaux cellulaires de deuxième génération, tels IS-95 et le GSM pour les réseaux de mobiles et le DECT pour les réseaux sans fil, sont caractérisés par l'introduction de la technologie numérique.

Le DECT (Digital Enhanced Cordless Telecommunications) et le PHS (Personal Handyphone System) offrent une couverture radio permettant une utilisation en résidentiel (station de base domestique), au bureau (PABX sans fil) et dans la rue (station de base publique). La complexité technique pour accéder au service est assez faible. Le système ne sachant pas effectuer de handover, l'utilisateur doit se trouver impérativement dans une cellule et y rester.

Plusieurs technologies numériques cellulaires font leur apparition au début des années 1990 :

- GSM (Global System for Mobile communications), en Europe, fonctionnant à 900 MHz ;
- DCS 1800 (Digital Cellular System 1800), système équivalent au GSM, mais fonctionnant à des fréquences plus élevées (1 800 MHz) ;
- PCS (Personal Communication System) 1900 et D-AMPS, version numérique de l'AMPS, aux États-Unis ;
- PDC (Pacific Digital Cellular) au Japon.

Les systèmes cellulaires numériques de deuxième génération favorisent la mise au point d'un terminal portable doté d'une autonomie acceptable.

Le GSM

Le GSM a été déployé au départ en Europe et partout dans le monde, à l'exception de l'Amérique, avant d'être adopté par plusieurs opérateurs américains.

La CEPT (Conférence européenne des Postes et Télécommunications) entreprend en 1970 d'établir une norme unique en matière de communication avec les mobiles. Dans le même temps, elle affecte une bande de 25 MHz dans la bande des 900 MHz pour réaliser un réseau cellulaire. Un groupe de travail, le groupe spécial mobile (GSM), est constitué pour réaliser ces études. En 1987, treize pays européens se mettent d'accord pour développer un réseau GSM. En 1990, une adaptation de la bande des 1 800 MHz est mise en place sous le nom de DCS 1800 (Digital Communication System 1 800 MHz). À cette époque, l'ETSI remplace la CETP pour finaliser la normalisation du GSM900 et du DCS 1800. De leur côté, les Américains reprennent une version du GSM dans la

bande des 1 900 MHz, sous le nom de DCS1900. Les principes généraux du GSM sont les mêmes pour les trois adaptations.

Le GSM est un environnement complet, rassemblant l'interface air, mais aussi les interfaces entre le système radio et le système de commutation et l'interface utilisateur. Les appels sont contrôlés par la norme Q.931, déjà rencontrée dans le RNIS et le relais de trames.

La station mobile est constituée de deux éléments, le terminal portatif et la carte SIM. Cette carte à puce contient les caractéristiques de l'utilisateur et les éléments de son abonnement.

L'interface radio travaille dans les bandes 890-915 MHz dans le sens montant et 935-960 MHz dans le sens descendant. Une version GSM étendue, le E-GSM, travaille dans les bandes 880-915 MHz dans le sens montant et 925-960 MHz dans le sens descendant. Le réseau DCS 1800 utilise un sens montant entre 1 710 et 1 785 MHz et un sens descendant de 1 805 à 1 880 MHz. Enfin, le PCS1900 se place entre 1 850 et 1 910 MHz dans le sens montant et 1 930 à 1 990 MHz dans le sens descendant. Chaque porteuse radio exige 200 kHz, de telle sorte que 124 porteuses sont disponibles en GSM900, 174 en E-GSM, 374 en DCS 1800 et 298 en DCS1900.

De nombreux canaux sont disponibles sur l'interface radio GSM pour la transmission des données et des différents contrôles :

- Le canal plein débit TCH/FS (Traffic CHannel/Full Speed), au débit net de 13 Kbit/s, pour la transmission de la parole ou des données. Ce canal peut être remplacé par :
  - Le canal demi-débit TCH/HS (Traffic CHannel/Half Speed) à 5,6 Kbit/s.
  - Le canal plein débit pour les données à 9,6 Kbit/s, pour la transmission de données à un débit net de 12 Kbit/s.
  - Le canal demi-débit pour les données à 4,8 Kbit/s, pour la transmission de données à un débit net de 6 Kbit/s.
- Le canal SDCCH (Standalone Dedicated Control CHannel), au débit brut de 0,8 Kbit/s, qui sert à la signalisation (établissement d'appel, mise à jour de localisation, transfert de messages courts, services supplémentaires). Ce canal est associé à un canal de trafic utilisateur.
- Le canal SACCH (Standalone Access Control CHannel), au débit brut de 0,4 Kbit/s, qui est un canal de signalisation lent associé aux canaux de trafic. Son rôle est de transporter les messages de contrôle du handover.
- Le canal FACCH (Fast Access Control CHannel), qui est obtenu par un vol de trames (c'est-à-dire qui utilise la place de certaines trames d'un autre canal) sur le canal trafic d'un utilisateur, dont il est chargé d'exécuter le handover. Il est associé à un canal de trafic et peut servir à des services supplémentaires, comme l'appel en instance.
- Le canal CCCH (Common Control CHannel), qui est un canal de contrôle commun aux canaux de trafic pour faire transiter des demandes d'établissement de communication ou des contrôles de ressources.

- Le canal BCCH (Broadcast Control CHannel), au débit de 0,8 Kbit/s, qui gère le point-à-multipoint.
- Le canal AGCH (Access Grant CHannel), ou canal d'allocation des accès, qui s'occupe de la signalisation des appels entrants.
- Le canal RACH (Random Access CHannel), qui s'occupe de la métasignalisation, correspondant à l'allocation d'un premier canal de signalisation.
- Le canal FCCH (Frequency Control CHannel), qui prend en charge les informations de correction de fréquence de la station mobile.
- Le canal SCH (Synchronous CHannel), qui est dédié aux informations de synchronisation des trames pour la station mobile et pour l'identification de la station de base.

Le protocole de niveau trame chargé de la gestion de la transmission sur l'interface radio provient du standard HDLC, avec quelques modifications pour s'adapter à l'interface air. Plus précisément, ce protocole est appelé LAP-Dm (Link Access Protocol on the Dm channels). Il transporte des trames avec une fenêtre de 1, la reprise éventuelle s'effectuant sur un temporisateur.

Le protocole de niveau paquet est lui-même divisé en trois sous-niveaux :

- La couche RR (Radio Resource), qui se préoccupe de l'acheminement de la supervision.
- La couche MM (Mobility Management), qui prend en charge la localisation continue des stations mobiles.
- La couche CM (Connection Management), qui gère les services supplémentaires, le transport des messages courts SMS et le contrôle d'appel. Ce dernier contrôle reprend en grande partie la recommandation Q.931 du réseau numérique à intégration de services.

Le GSM définit les relations entre les différents équipements qui constituent le réseau de mobiles :

- sous-système radio BSS ;
- sous-système réseau NSS (Network SubSystem), avec ses bases de données pour la localisation des utilisateurs HLR et VLR ;
- relations entre les couches de protocoles et les entités du réseau ;
- interfaces entre sous-système radio (BSS) et sous-système réseau (NSS) ;
- itinérance (roaming).

L'IS-95

L'IS-95 est la principale version normalisée pour la deuxième génération américaine. L'interface air utilise la technologie CDMA. La version IS-95A est celle qui est déployée en Amérique du Nord. La version 1999, IS-95B, augmente les débits numériques. C'est elle que nous prenons comme référence dans cette section.

Le canal de contrôle descendant regroupe le canal pilote, le canal de paging et le canal de synchronisation. Le canal réservé au trafic des utilisateurs est multiplexé avec les canaux

de contrôle par des trames de 20 ms. La trame est ensuite codée pour être transportée sur l'interface air. Le canal de synchronisation travaille à la vitesse de 1,2 Kbit/s. Chaque utilisateur possède un canal en division par code (CDMA) et jusqu'à 7 canaux de trafic supplémentaires. Deux taux de trafic ont été définis, l'ensemble 1 propose des débits de 9,6, 4,8, 2,4 et 1,2 Kbit/s, et l'ensemble 2 des débits de 14,4, 7,2, 3,6 et 1,8 Kbit/s. Les trames de 20 ms sont divisées en seize groupes de contrôle de puissance d'une durée de 1,25 ms.

La structure du canal montant est différente. Ce canal est subdivisé en deux canaux, le canal de trafic et le canal de gestion de l'accès. Les trames font également 20 ms et prennent en charge l'ensemble du trafic.

L'IS-95 a trois mécanismes différents pour le contrôle de puissance. Sur le lien montant, un contrôle en boucle ouverte et un contrôle en boucle fermée sont disponibles. Sur le lien descendant, un contrôle en boucle plus lent est implémenté.

Deux technologies de codage de la parole sont utilisées, l'une à 8 Kbit/s et l'autre à 13 Kbit/s. Ce dernier codage utilise le taux de 14,4 Kbit/s du canal de transmission. Le premier codage utilise un codec EVRC (Enhanced Variable Rate Codec) à 8 Kbit/s, s'adaptant aux canaux à 1,2, 2,4, 4,8, et 9,6 Kbit/s pour des décompositions éventuelles du canal dans les débits de 1, 2, 4 et 8 Kbit/s.

L'IS-136

L'IS-136 est une norme américaine pour les téléphones mobiles de deuxième génération utilisant le TDMA. Moins développée que l'IS-95, cette norme offre cependant une base intéressante pour la troisième génération.

Une première amélioration intermédiaire, ressemblant au GPRS, examiné à la section suivante, concerne l'augmentation du flux de données jusqu'à une valeur de 384 Kbit/s. La version suivante introduira des microcellules et des picocellules sur lesquelles l'utilisateur pourra récupérer un grand nombre de tranches dans le TDMA pour atteindre des débits de 2 Mbit/s.

Le GPRS

L'activité majeure de développement de la phase 2+, ou 2,5G, du GSM concerne le GPRS. Ce dernier incarne une nouvelle génération du standard GSM, rendant possible la prise en charge des applications de données à moyen débit dans le cadre de la mobilité. Il constitue en outre une transition vers la troisième génération, caractérisée par le passage d'un débit de 14,4 Kbit/s (9,6 Kbit/s utilisable) à un débit beaucoup plus important, pouvant être multiplié par 8 au maximum.

Le GPRS utilise la même infrastructure que le GSM mais avec un double réseau cœur, celui du GSM, c'est-à-dire d'un réseau à commutation de circuits, et celui d'un réseau à transfert de données. Si l'utilisateur téléphone, l'information transite par le réseau cœur de type circuit téléphonique. Si l'utilisateur émet des paquets, ces derniers sont

acheminés par le réseau cœur de type paquet. Le réseau cœur utilise une technique de relais de trames. Nous ne considérons dans la suite que la partie paquet ajoutée au GSM.

Le terminal intègre les composants nécessaires au traitement de la parole téléphonique pour la numériser de façon plus ou moins compressée et se complète d'un modem, qui émet les paquets de l'utilisateur vers le réseau cœur paquet. La traversée de l'interface radio utilise les slots du TDMA qui ne sont pas utilisés par la parole téléphonique.

L'architecture du GPRS est illustrée à la figure M.4. Cette architecture est composée de divers types de nœuds :

- Les SGSN (Serving GPRS Support Node), qui sont des routeurs connectés à un ou plusieurs BSS.
- Les GGSN (Gateway GPRS Support Node), qui sont des routeurs acheminant le trafic vers des réseaux de données GPRS ou externes.

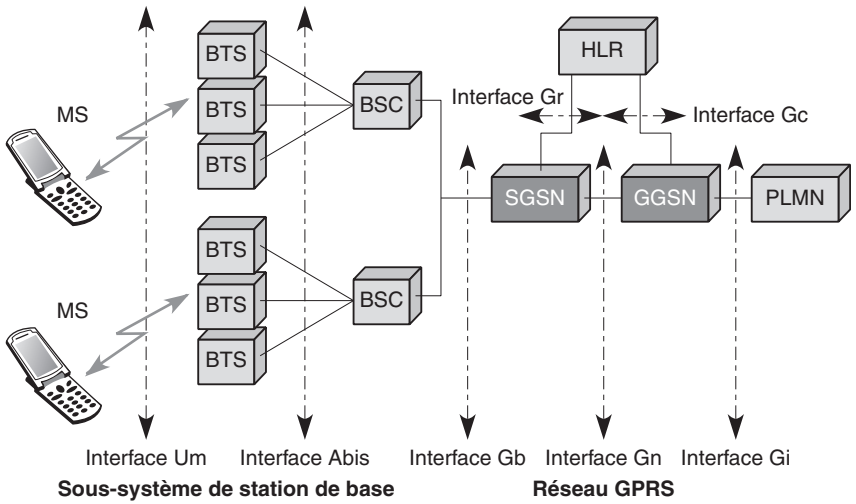


Figure M.4

Architecture du GPRS

Le réseau GPRS possède deux plans, le plan utilisateur et le plan de signalisation. Les couches de protocoles du plan utilisateur sont illustrées à la figure M.5.

Par rapport au GSM, le GPRS requiert de nouveaux éléments pour créer un mode de transfert de paquets de bout en bout. De plus, le HLR est amélioré pour les clients qui demandent à transporter des données. Deux services sont permis :

- le point-à-point PTP (Point-To-Point) ;
- le point-à-multipoint PTM (Point-To-Multipoint).

Les transferts de paquets et le routage s'effectuent, comme nous venons de l'indiquer, par les nœuds logiques SGSN. Ils utilisent les passerelles GGSN avec les réseaux de transfert

de paquets externes. Dans le réseau GPRS, les unités de données sont encapsulées par le SGSN de départ et décapsulées dans le SGSN d'arrivée. Entre les SGSN, le protocole IP est utilisé. L'ensemble de ce processus est défini comme le tunneling du GPRS.

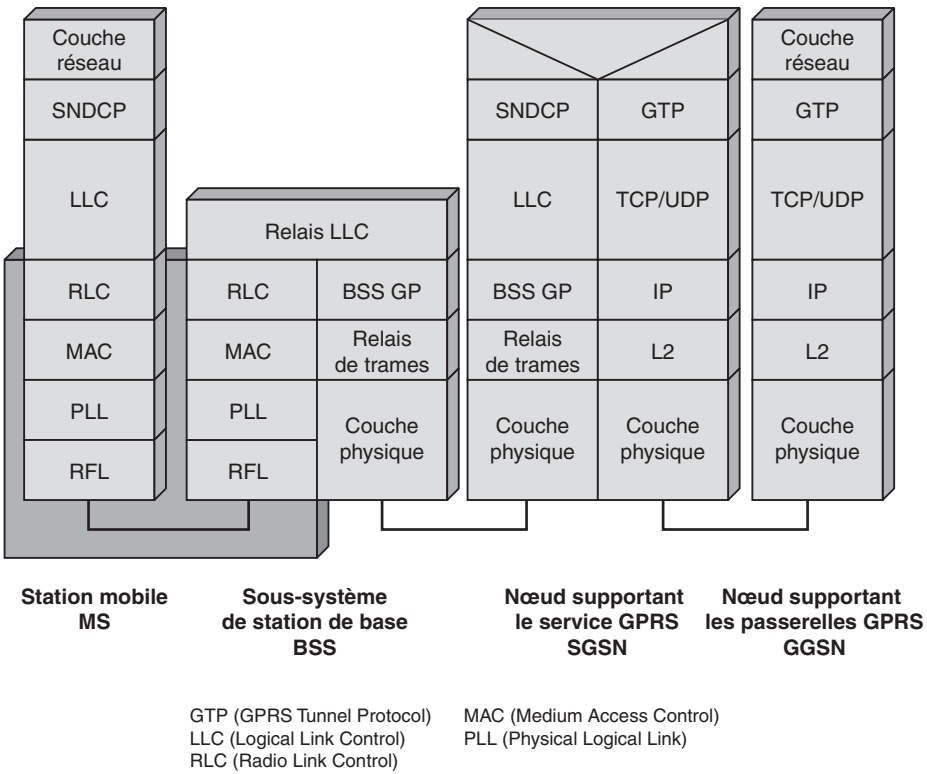


Figure M.5

Couches de protocoles du réseau GPRS

Le GGSN maintient les informations de routage pour réaliser les tunnels et les maintenir. Ces informations sont stockées dans le HLR. Le protocole en charge de ce travail, le GTP (GPRS Tunnel Protocol) utilise TCP et UDP pour effectuer le transport effectif. Entre le SGSN et les MS, le protocole SNDCP (SubNetwork Dependent Convergence Protocol) effectue le multiplexage de niveau paquet, le chiffrement, la segmentation et la compression. Entre les MS (Mobile Station) et les BSS, le niveau trame est subdivisé en deux sous-couches, la couche LLC (Logical Link Control) et la couche RLC/MAC (Radio Link Control/Medium Access Control).

La couche LLC se sert du protocole LAP-Dm, déjà utilisé pour la signalisation dans l'environnement GSM. Le RLC/MAC s'occupe du transfert physique de l'information sur l'interface radio. Ce protocole prend en charge les retransmissions éventuelles sur erreur par une technique BEC (Backward Error Correction), consistant en une retransmission

sélective des blocs en erreur. La technique d'accès s'effectue par le protocole slotted aloha, ou aloha en tranches. Le protocole RLC/MAC s'appuie sur un protocole de niveau physique effectuant la transmission des éléments binaires sur le support physique et prenant en charge le codage, la récupération de certaines erreurs physiques et même un contrôle de flux.

EDGE (Enhanced Data for GSM Evolution)

En utilisant plusieurs slots dans le GPRS, un utilisateur peut augmenter son débit. Le GPRS offre de surcroît différents taux de codage, permettant d'augmenter le débit lorsque les conditions de propagation sont correctes. Néanmoins, le débit brut sur un slot reste celui du GSM, c'est-à-dire environ 270 Kbit/s. EDGE (Enhanced Data for GSM Evolution) permet de s'affranchir de cette limite, moyennant l'introduction d'une nouvelle modulation, de nouveaux schémas de codage et la généralisation du principe de l'adaptation de lien (*link adaptation*).

L'association de EDGE et de GPRS est aussi connue sous le nom de E-GPRS (Enhanced-General Packet Radio Service). L'E-GPRS est souvent considéré comme un système de troisième génération. De leur côté, les principes d'EDGE ont été repris et adaptés pour l'évolution de l'IS-136, le standard TDMA américain. Cette évolution est connue sous le nom d'UWC136 ou d'EDGE Compact.

EDGE est issu de la constatation que, dans un système cellulaire, tous les mobiles ne disposent pas de la même qualité de transmission. Le contrôle de puissance tente de pallier ces inégalités en imposant aux mobiles favorisés une transmission moins puissante. Cela permet plutôt d'économiser les batteries des terminaux que d'augmenter les capacités de transmission. Nous verrons qu'avec l'UMTS, qui utilise un accès par répartition en code tel que CDMA, ce contrôle de puissance a un rôle autrement plus important.

EDGE permet à ses utilisateurs de bénéficier de transmissions plus efficaces, augmentant par conséquent le trafic moyen offert dans la cellule. En réalité, EDGE fait correspondre à chaque condition radio rencontrée le schéma de modulation et de codage, ou MCS (Modulation and Codage Scheme), le plus approprié en regard de la qualité de service requise sur la liaison. Pour cela, EDGE a évidemment introduit de nouveaux MCS, en comparaison de ceux existant dans le GSM ou le GPRS.

Le cdma2000

Le cdma2000 adopté par les Américains ressemble au WCDMA, à quelques notables différences près. En particulier, au lieu de faire du CDMA sur l'ensemble de la bande, la bande passante allouée à la troisième génération est découpée en plusieurs sous-bandes, et le CDMA est appliqué à chacune de ces sous-bandes.

La transition entre la deuxième génération IS-95, que l'on appelle encore IS-95A, et le cdma2000 s'effectue par l'intermédiaire de la norme IS-95B. Cette dernière reste compatible avec l'IS-95A mais augmente fortement les débits des données par l'intégration de plusieurs codes simultanés, huit au maximum, pour un même utilisateur. Un terminal haut

débit a la possibilité de gagner jusqu'à sept codes supplémentaires pendant la période de débit crête. Le canal peut être asymétrique, avec des canaux montant et descendant différents. Le contrôle de puissance pour les canaux supplémentaires n'est pas indépendant du canal de base. Le débit total offert dans la version IS-95B est de 76,8 ou 115,2 Kbit/s, suivant que l'on compte le débit total ou le débit utile du canal de base.

L'interface radio du cdma2000 reprend les attributs de l'IS-95 mais avec une largeur de bande de 5 MHz. Elle peut regrouper un nombre de codes supérieur à 8. Un pilote de gestion du canal a été ajouté, permettant des gains significatifs de performances, notamment par une réduction du temps nécessaire au contrôle de puissance. Des turbocodes peuvent être utilisés à la place des codes de convolution.

Des débits pouvant atteindre jusqu'à 2 Mbit/s sont accessibles sur des picocellules à l'intérieur des bâtiments, jusqu'à 384 Kbit/s pour les piétons restant dans une même cellule et jusqu'à 144 Mbit/s pour les véhicules qui effectuent des changements de cellules.

La technique d'accès au support hertzien est fortement modifiée entre l'IS-95 et le cdma2000. Alors qu'il n'y avait que deux états possibles de l'interface IS-95, il y en a quatre avec le cdma2000.

La troisième génération (3G)

Les systèmes de télécommunications mobiles de troisième génération fournissent toute une gamme de services de télécommunications aux utilisateurs fixes et mobiles, situés dans une variété d'environnements autour de la bande de fréquences des 2 GHz. En 1985, l'UIT a commencé ses études des réseaux FPLMTS (Future Public Land Mobile Telephone System), renommés IMT 2000 (International Mobile Telecommunications system for the year 2000) en 1993. L'ETSI a entamé les siennes pour l'Europe en 1990 avec l'UMTS. L'UMTS n'est qu'une des cinq normes de la famille IMT 2000, qui inclut également WCDMA, cdma2000, EDGE et DECT de troisième génération.

Ces systèmes mobiles de troisième génération se présentent comme des concurrents des infrastructures de deuxième génération déjà déployées. Il a toutefois fallu penser à la transition entre les deux générations, qui ne pouvait être instantanée, et à la possibilité de créer un maximum de services communs. La troisième génération améliore la précédente par une qualité du service rendu au moins comparable à celle fournie par les réseaux fixes. De plus, les réseaux IMT 2000, comme l'UMTS, cherchent à fournir de nouvelles avancées significatives incluant l'itinérance mondiale, une large gamme de services, à haut débit ou non, des services audiovisuels et l'utilisation d'un seul terminal dans différents environnements radio. La gamme des services de télécommunications doit pouvoir s'adapter de façon flexible aux besoins des utilisateurs et leur permettre de communiquer indépendamment de leur localisation et de leur méthode d'accès.

Un autre objectif des réseaux de troisième génération est de rendre les services fixes et mobiles compatibles pour former un service transparent de bout en bout pour les utilisateurs.

La liste suivante, extraite de la norme UMTS, présente quelques-unes des conditions requises pour ces réseaux :

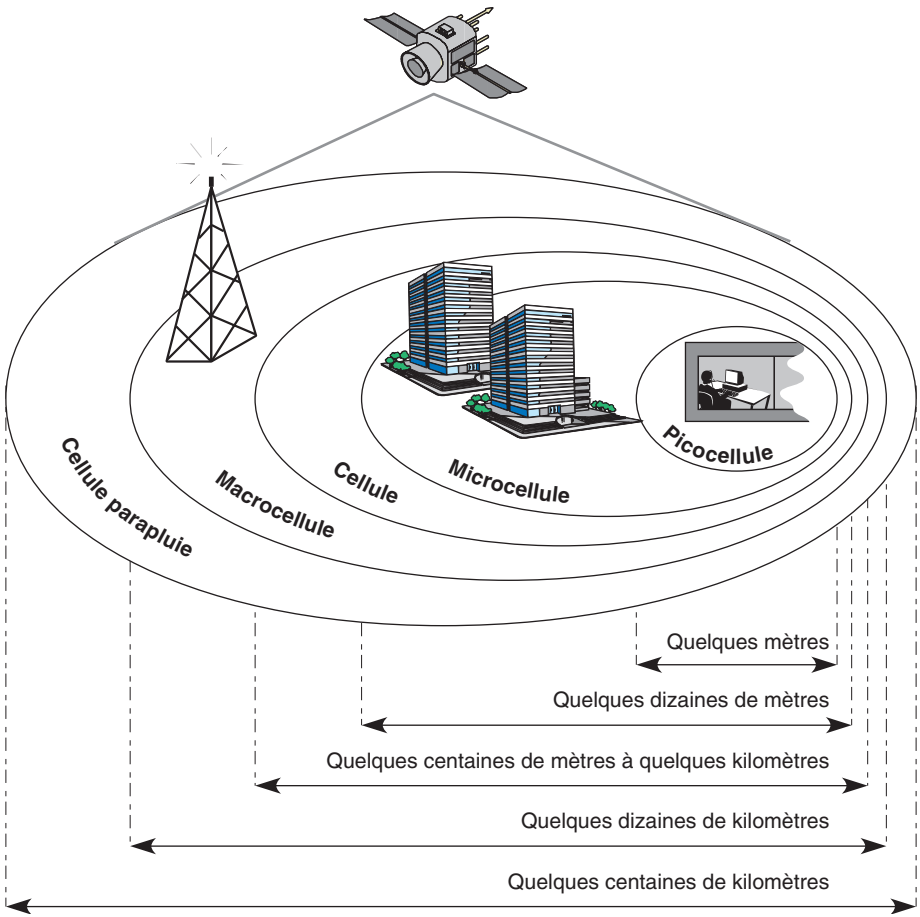
- Fournir un seul système intégré, dans lequel l'utilisateur peut facilement accéder aux services UMTS d'une façon uniforme dans tous les environnements, qu'ils soient résidentiels, de bureau ou cellulaires, avec un même équipement, à condition que le terminal soit adapté.
- Fournir des services accessibles à des terminaux portatifs, qu'ils soient portables, montés dans des véhicules, transportables ou fixes, incluant ceux qui sont normalement connectés aux réseaux fixes, dans les environnements aussi bien résidentiels, que publics ou radio.
- Fournir une large gamme de services de télécommunications, incluant ceux fournis par les réseaux fixes, caractérisés par des débits utilisateur pouvant atteindre 2 Mbit/s, ainsi que les services propres aux communications mobiles. Ces services doivent être supportés par les environnements résidentiels, publics et de bureau, dans des zones de densité de population diverses. La qualité, particulièrement en ce qui concerne la voix, doit être comparable à celle fournie par les réseaux fixes comme le RNIS.
- Supporter des services audio, vidéo, texte et graphique, c'est-à-dire les éléments essentiels d'un appel multimédia, et de données.
- Offrir des débits de 64 à 144 Kbit/s en forte mobilité, 384 Kbit/s en mobilité moyenne et 2 à 10 Mbit/s en faible mobilité.
- Supporter la mobilité globale, à savoir la mobilité du terminal, comme dans le GSM, la mobilité personnelle universelle et la mobilité des services, le service étant assuré quels que soient l'accès et le lieu.
- Supporter les utilisateurs itinérants en leur permettant d'accéder aux services de leurs fournisseurs de façon toujours identique, même s'ils se déplacent.
- Permettre la différenciation entre les offres de services des différents réseaux et fournisseurs de services.
- Séparer les concepts de fournisseur de services et d'opérateur.
- Offrir un numéro unique, indépendant du réseau et du fournisseur de services.
- Permettre à un utilisateur piéton d'accéder à tous les services normalement accessibles par les réseaux fixes.
- Permettre à un utilisateur piéton d'accéder à tous les services normalement accessibles par PABX et réseaux locaux.
- Favoriser de petits terminaux, faciles à utiliser, dotés d'une grande autonomie et peu coûteux.
- Introduire facilement des services peu onéreux.
- Optimiser l'utilisation des ressources, en particulier du spectre radio.
- Partager les ressources spectrales entre les multiples opérateurs de réseaux publics et privés.
- Garantir une couverture radio transparente et globale.

- Garantir un accès satellite direct.
- Utiliser la bande de fréquences définie par la Conférence administrative mondiale des radiocommunications en 1992 (1 885-2 025 et 2 110-2 200 MHz).
- Adopter un système ouvert pour accélérer la création et la personnalisation de nouveaux services.
- Supporter une large gamme de services pouvant s'adapter aux souhaits de l'utilisateur.
- Introduire des recommandations dans l'IMT 2000 pour aboutir à une compatibilité entre les différentes normes (UMTS, WCDMA, cdma2000, etc.).

Plusieurs de ces conditions requièrent un seul système intégrant plusieurs environnements fonctionnant de façon concertée. Les services seront disponibles dans toutes les situations dans lesquelles pourra se trouver l'utilisateur, à l'intérieur ou à l'extérieur des zones urbaines denses, même dans les bureaux, dans le cas d'une utilisation intensive, dans les zones reculées, suburbaines et rurales. La figure M.6 illustre les différents environnements définis pour les réseaux IMT 2000.

Figure M.6

Environnement des réseaux IMT 2000



Chacune des quatre zones représentées sur la figure caractérise un environnement spécifique. La première zone, de quelques mètres, correspond à un environnement de grande densité, comme le centre d'une ville, avec des picocellules dans lesquelles le trafic est très important. Dans ce type d'environnement, le débit maximal peut atteindre 2 à 10 Mbit/s, rejoignant, voire dépassant celui des offres ADSL. Dans les deux zones suivantes, de quelques dizaines à quelques centaines de mètres, la mobilité augmente tandis que le débit diminue. Dans la dernière zone, de quelques dizaines à quelques centaines de kilomètres, caractérisée par le composant satellite, la mobilité est globale, avec un débit pouvant atteindre 2 Mbit/s. Les situations terrestre, maritime et aéronautique sont incluses dans les objectifs de ces cellules parapluie. De ce fait, l'utilisateur se trouvant dans un véhicule, sur un bateau ou dans un avion bénéficie d'une disponibilité continue des services.

Les réseaux IMT 2000 utilisent simultanément les techniques cellulaires et sans fil ainsi que le composant satellite, complément des réseaux fixes et mobiles, qui fournit une couverture globale, à l'intérieur et à l'extérieur des bâtiments, ce que ne permet pas un déploiement terrestre conventionnel.

Les services de l'IMT 2000

En principe, les services de l'IMT 2000 doivent être compatibles avec ceux des réseaux de télécommunications fixes en matière de fonctionnalités, d'interface utilisateur, de coût et de qualité. Les réseaux IMT 2000 étendent les services multimédias multipartites, comme ceux fournis par les réseaux fixes, au domaine mobile. Ce point est important, car un utilisateur équipé d'un téléphone mobile peut de la sorte bénéficier avec plus de liberté des services auxquels il a souscrit, sans souffrir d'une perte de qualité de service.

Les services fournis vont de l'audio à la vidéo, en passant par les données et le multimédia. L'utilisateur d'un même terminal doit pouvoir établir et maintenir plusieurs connexions simultanément. Il doit de plus se voir offrir des applications réclamant des paramètres différents de qualité de service. Les services proposés dépendent des propriétés, ou capacités, du terminal ainsi que de l'offre de l'opérateur concerné. Les services demandant de hauts débits de transmission sont concentrés dans les zones de grande densité, comme les centres d'affaires, plutôt que dans les zones suburbaines. Les utilisateurs d'IMT 2000 ne se rendront pas compte qu'un lien radio connecte leur terminal aux réseaux mondiaux de télécommunications.

La stratégie déployée pour intégrer de nouveaux services dans les réseaux IMT 2000 ressemble à ce qui a été conçu dans le cadre des réseaux intelligents. Elle consiste à définir des capacités de service et non les services eux-mêmes. Les capacités de service concernent les techniques de transport nécessitées par les paramètres de qualité de service ainsi que les mécanismes nécessaires à leur réalisation. Ces mécanismes incluent les fonctionnalités fournies par les différents éléments de réseau, la communication entre eux et le stockage des données associées. Ces capacités normalisées fournissent une plate-forme supportant la voix, la vidéo, le multimédia, les messages, les données et autres téléservices, des applications utilisateur et des services supplémentaires. Elles permettent la

création d'un marché pour des services déterminés par les utilisateurs et les fournisseurs de service.

La mobilité globale est impossible à réaliser aujourd'hui du fait de la multiplicité des systèmes et des réseaux. Il est quasiment impossible pour un utilisateur de bénéficier des mêmes services dans les mêmes conditions dans son réseau d'abonnement et dans les réseaux visités. Lorsqu'elle deviendra une réalité, la mobilité des services permettra aux utilisateurs de disposer des mêmes services dans les mêmes conditions, quelle que soit leur localisation. L'itinérance, ou mobilité du terminal, permettra de construire un réseau universel. Les futurs réseaux supporteront de surcroît le concept de VHE (Virtual Home Environment), qui vise à offrir à l'utilisateur un ensemble complet de services ayant une même apparence, que ce dernier se trouve dans son réseau d'abonnement ou dans un autre réseau.

L'offre de mobilité personnelle n'est possible que si l'utilisateur IMT 2000 possède un identificateur indépendant du réseau et du fournisseur de services. Les opérateurs de réseau et les fournisseurs de service pouvant être deux entités distinctes, le fait de posséder un numéro spécifique avec chacune de ces entités rend plus compliquée la fourniture des services, en particulier le routage des appels. C'est pourquoi l'identificateur de l'utilisateur doit être unique. Grâce à ce numéro personnel unique, le seul connu par les appelants, l'utilisateur peut être joint n'importe où dans le monde.

Les réseaux IMT 2000 supportent la portabilité des numéros aux niveaux à la fois du fournisseur de services, de la localisation et des services. La portabilité des numéros au niveau du fournisseur de services implique qu'un identificateur, appelé IMUN (International Mobile User Number), est alloué à chaque nouvel abonné IMT 2000. Un abonné peut changer de fournisseur de services tout en gardant son IMUN, à condition que le nouveau fournisseur de services offre le service concerné dans la même zone géographique. De même, un fournisseur de services peut changer d'opérateur réseau tout en conservant son IMUN. La portabilité de la localisation signifie que chaque abonné peut être appelé indépendamment de sa localisation, et donc de sa mobilité. La portabilité du numéro signifie que le numéro à composer pour joindre un utilisateur est indépendant du service requis.

Le spectre radio doit être utilisé de façon efficace et éventuellement partagé entre différents opérateurs dans le but d'offrir une couverture radio globale, transparente pour l'usager, avec la portion satellite. Il doit être possible pour un terminal IMT 2000 de s'adapter à l'interface radio fournie dans une région spécifique et de déterminer les capacités de services disponibles dans celle-ci. De plus, comme plus d'une interface radio est disponible dans une région donnée, la norme doit prévoir un mécanisme qui permette à un terminal IMT 2000 de sélectionner les interfaces radio capables de fournir les capacités de services appropriées.

Les clients individuels possèdent un profil de services particulier, avec une définition des types de services souscrits, incluant, par exemple, le moment de la journée où ces services sont utilisés. Le fournisseur de services a la charge du contrôle de tous les aspects de service de l'abonné et de l'utilisateur. Quand l'abonné et l'utilisateur sont des entités distinctes, l'abonné contrôle le profil de services de l'utilisateur dans les limites

de l'abonnement. L'abonné peut facilement modifier ce profil et décider si l'utilisateur détient le contrôle de l'activation-désactivation des services définis dans le profil de services de l'utilisateur. Tout changement du profil de services doit être effectué de façon sécurisée. Les informations concernant l'utilisateur, nécessaires pour l'identifier sans ambiguïté et permettre son enregistrement pour un service sont enregistrées sur sa carte, de type circuit intégré et comportant l'USIM.

Le concept de profil multiple est introduit dans les réseaux IMT 2000. Un profil multiple permet à un utilisateur d'obtenir certains services de la part d'un fournisseur de services et d'autres services de la part d'un autre fournisseur, et ce à l'aide d'une même carte. Dans le cas où des abonnements multiples sont possibles sur la même carte, si ceux-ci concernent plusieurs fournisseurs de services, un numéro différent est alloué pour chacun d'eux. Pour les appels sortants, l'utilisateur doit être capable de sélectionner le fournisseur de services qu'il préfère pour chaque appel ou en fonction de son abonnement. Plusieurs abonnements multiples peuvent être actifs simultanément. Le standard permet en outre de supporter l'enregistrement multiple sur un même terminal par l'insertion de cartes à puce multiples.

La sécurité des futurs réseaux de mobiles sera un critère essentiel de leur réussite. Les réseaux IMT 20000 prévoient une sécurité mutuelle : le réseau peut authentifier l'utilisateur afin de vérifier qu'il est bien celui qui est autorisé à utiliser les services, et l'utilisateur peut demander à authentifier le réseau au moment de son enregistrement et avant d'initier un service. De même, les réseaux peuvent s'authentifier entre eux. D'autres relations d'authentification seront définies dans les réseaux et seront détaillées par la suite. Ces nouveaux services seront flexibles afin d'être les plus proches possibles des souhaits de l'utilisateur.

Les normes IMT 2000 devront être cohérentes pour garantir la compatibilité entre réseaux. Les futurs réseaux de mobiles seront compatibles avec les systèmes mobiles de deuxième génération, qui continueront à fonctionner (GSM, DCS 1800, DECT, etc.) à pleine capacité, afin d'autoriser le déplacement des utilisateurs à travers le monde. Les réseaux IMT 2000 intégreront les réseaux de mobiles cellulaires et satellite et les réseaux fixes dans un seul système afin de fournir une couverture globale, à l'intérieur et à l'extérieur, de façon uniforme, permettant aux utilisateurs d'accéder aux services, quels que soient le terminal et le réseau qu'ils utilisent et leur emplacement géographique.

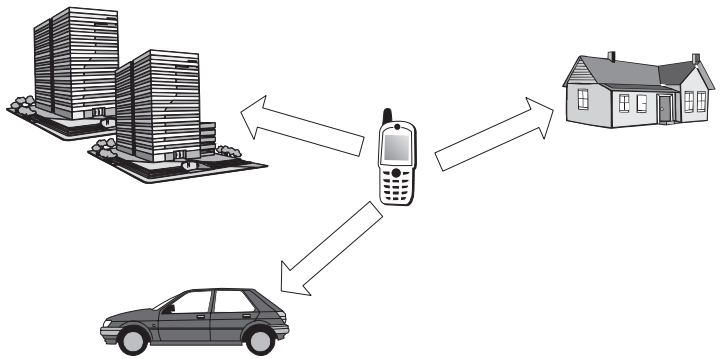
En résumé, l'utilisateur d'une technologie de troisième génération bénéficiera d'une offre complète de services grâce à l'intégration des réseaux fixes et mobiles. L'intégration et la compatibilité entre les différents réseaux correspondant à des normes différentes (UMTS, WCDMA, cdma2000, GSM, etc.) autoriseront l'itinérance et l'interfonctionnement. L'utilisateur pourra se déplacer entre réseaux de troisième génération de façon transparente, tout en gardant la continuité des services, même si, dans certains cas, la qualité pourra en pâtir du fait des caractéristiques d'un nouvel environnement radio. Si des accords d'itinérance n'existent pas entre le fournisseur de services de l'utilisateur et le réseau visité par ce dernier, il sera possible d'établir de tels accords. Lorsque plus d'un réseau visité sera disponible, l'utilisateur aura la possibilité de sélectionner manuellement ou automatiquement un réseau particulier, en fonction de son profil de services.

La mobilité dans les réseaux de troisième génération

Le fait d'offrir une mobilité globale, rassemblant mobilité du terminal, mobilité personnelle et mobilité des services, représente l'atout décisif des réseaux de troisième génération.

La mobilité du terminal correspond à la capacité du terminal à accéder aux services de télécommunications, quels que soient l'endroit où il se trouve et sa vitesse de déplacement. Cette mobilité, illustrée à la figure M.7, implique que le réseau est capable d'identifier, de localiser et de suivre les utilisateurs, indépendamment de leurs mouvements, puis de router les appels vers eux. Un enregistrement précis de la localisation de l'utilisateur et de son terminal associé doit être maintenu. L'itinérance est liée à la mobilité du terminal, puisqu'elle permet à un utilisateur de se déplacer d'un réseau à un autre.

Figure M.7
Mobilité du terminal

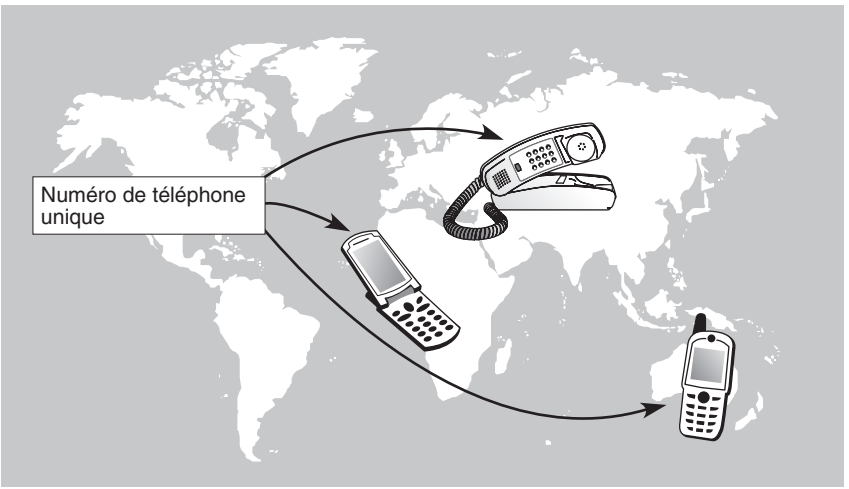


La mobilité personnelle correspond à la capacité d'un utilisateur à accéder aux services de télécommunications entrants et sortants sur tout terminal, à n'importe quel endroit. Sur la base d'un numéro personnel unique, l'utilisateur peut initier et recevoir des appels à partir de n'importe quel terminal. La mobilité personnelle implique la capacité du réseau à identifier les utilisateurs lorsqu'ils se déplacent afin de leur fournir des services en fonction de leur profil de services et de localiser le terminal associé à l'utilisateur pour adresser, acheminer et facturer les appels de l'utilisateur. Cette mobilité personnelle est symbolisée à la figure M.8.

Figure M.8
Mobilité personnelle

La mobilité des services, aussi appelée portabilité des services, se réfère à la capacité du réseau à fournir les services souscrits à l'endroit où se trouvent le terminal et ses utilisateurs. Cette mobilité est décrite à la figure M.9. Les services exacts que l'utilisateur peut demander sur son terminal dépendent de la capacité du terminal à cette localisation et du réseau qui dessert ce terminal. La portabilité des services est assurée par des mises à jour régulières du profil de services de l'utilisateur et l'interrogation de ce profil si nécessaire. La mobilité des services associe les services à un utilisateur et non à un accès particulier du réseau. Les services doivent suivre les utilisateurs lorsque ceux-ci se déplacent.

Figure M.9
Mobilité des services



Lié à la mobilité des services, le VHE (Virtual Home Environment) prend en charge les utilisateurs itinérants en leur permettant d'accéder aux services fournis par leurs fournisseurs de services toujours de la même façon, même s'ils se déplacent. Grâce au VHE, l'utilisateur peut utiliser ses services dans n'importe quel réseau qu'il visite, de la même manière et avec les mêmes caractéristiques que lorsqu'il se trouve dans son propre réseau d'abonnement. Il dispose ainsi d'un environnement personnalisé de services, qui le suit partout où il se déplace. Le VHE sera fourni à condition que les différents réseaux visités par l'utilisateur soient capables de proposer les mêmes fonctionnalités que le réseau d'abonnement.

On regroupe parfois dans le concept de mobilité de l'utilisateur la mobilité du terminal et la mobilité personnelle.

N

Annexe du chapitre 19 (Les réseaux personnels)

Cette annexe décrit l'environnement de la norme UWB supportée par la WiMedia Alliance. Cette norme ne s'est pas développée comme prévu du fait de la consommation électrique des terminaux mobiles dotés de batteries standards, qui n'a pu être ramenée à une valeur acceptable. Cette annexe décrit également les réseaux de domicile qui forment un cas particulier des réseaux personnels par leur portée réduite à une dizaine de mètres.

UWB (Ultra Wide Band)

UWB est une technologie radio sans fil pour la transmission point-à-point entre équipements électroniques grand public, les périphériques PC et les dispositifs mobiles, sur de courte distance et à très grande vitesse, tout en consommant peu de puissance. Elle est bien adaptée au transfert de données multimédias, tel que la transmission sans fil de vidéos à partir d'un magnétoscope numérique vers une télévision haute définition dans le salon ou d'un PC mobile vers un vidéo-projecteur dans une salle de conférence pour réaliser une présentation sur grand écran.

Une grande valeur est attachée à la mise en place de dispositifs permettant aux équipements de se découvrir automatiquement et de communiquer, d'imprimer ou de demander un service sans intervention des utilisateurs. En règle générale, cette découverte automatique est impossible au travers d'un environnement câblé utilisant des interfaces incapables de communiquer entre elles.

L'adoption rapide des communications UWB dépendra de leur facilité d'utilisation et de leur coût. Les utilisateurs sont en outre en droit d'attendre un système fiable et fortement testé.

L'interopérabilité est une question clé pour permettre des opérations transparentes pour l'utilisateur, indépendamment des fabricants choisis. Par conséquent, il est crucial que la

standardisation des protocoles soit effectuée et que l'ensemble des protocoles soit incorporé dans une plate-forme unifiée, notamment les suivants :

- USB (Universal Serial Bus). Conçue au départ pour raccorder par câble des périphériques à un PC, cette interface est surtout utilisée pour le transfert de données.
- IEEE 1394, également connu sous le nom de FireWire. Spécifiquement conçu pour transmettre des flots multiples de types divers, comme l'audio et la vidéo, cette norme a été adoptée dans beaucoup de foyers pour remplacer les systèmes hétérogènes de diffusion audio, vidéo et de jeu.
- Bluetooth. L'objectif de cette technologie était de remplacer les câbles mais à des débits relativement faibles, tels qu'on en trouve dans les téléphones portables, ordinateurs personnels, PDA, écouteurs, etc.

Si chacun de ces protocoles correspond à des segments de marché différents, les consommateurs en souhaitent l'interopérabilité sans couture. À cet effet, des consortiums d'industriels, comme DLNA (Digital Living Network Alliance), essayent de définir des solutions d'interopérabilité complète à l'intérieur de la maison.

Parmi les applications ciblées, citons notamment les suivantes :

- Téléchargement depuis un caméscope vers un PC pour traitement, puis vers la télévision.
- Synchronisation des données d'un PDA vers un PC.
- Chargement de jeux audio/vidéo vers un PDA.
- Liaison d'un ordinateur portable vers une console de jeu.
- Passerelle résidentielle vers un serveur de jeux.
- Transfert de fichiers audio vers un lecteur MP3 à partir d'une base de données située sur un serveur de la maison.
- Télévision haute définition (HDTV) depuis ou vers le téléviseur pour stocker ou jouer des films. Cette application demande un débit de l'ordre de 20 Mbit/s.
- Communication d'un téléphone portable vers une oreillette.
- Transferts de photos d'un appareil numérique ou d'un téléphone portable.
- Téléchargement de jeux ou de films d'un point d'accès sans fil à un portable dans un lieu public tel qu'une gare.
- Téléchargement d'une présentation vers un vidéo-projecteur.

La partie du spectre choisie par l'UWB est également utilisée pour des applications telles que les radars de contrôle de collision et de découverte d'obstacles, les systèmes de positionnement de personnes, les systèmes d'inventaire automatique et les systèmes de transport intelligent. Plusieurs sociétés développent des technologies pour satisfaire des besoins spécifiques de communication sans fil robuste et sécurisée dans divers secteurs, tels que la santé, les opérations d'urgence ou les environnements militaires.

Dans le domaine de la santé, la localisation des équipements de diagnostic ou le transfert des données des patients dans les milieux hospitaliers peuvent être réalisés par le biais

de plates-formes logicielles/matérielles en indiquant le cheminement des objets grâce à un contact radio permanent par le biais d'un réseau de capteurs placés dans le bâtiment.

Dans les opérations de secours, ces systèmes peuvent permettre le positionnement de personnes physiques prises dans un feu ou un accident de produits toxiques ou lors d'un acte de terrorisme. Dans ce dernier cas, signalons que le NASC (Naval Air Systems Command) américain a commandé des systèmes d'intercommunication entre avions par UWB nommés AWICS (Aircraft Wireless Intercommunication Systems).

Les réseaux de domicile

Les réseaux de domicile forment une nouvelle catégorie de réseaux encore peu développée. Le domicile est vu par les opérateurs comme une étoile autour de la Home Gateway, qui est la « box » construite autour du modem ADSL. La nouvelle génération de réseaux de domicile devient un petit réseau d'entreprise, avec une centaine de connexions de matériels extrêmement divers provenant de trois mondes distincts : les télécommunications, l'électronique et l'informatique.

Parmi ces équipements, on trouve les téléphones avec et sans fil, offrant des fonctionnalités de vidéophonie, de téléphonie sur IP et de télévision. La haute définition et la parole de meilleure qualité que celle du GSM sont également disponibles.

Les industriels des équipements grand public de la maison proposent des télévisions, des consoles de jeu, des appareils photo et caméras ainsi que des machines à laver, réfrigérateurs, aspirateurs et futurs robots ménagers dotés d'adresses IP.

La difficulté majeure avec ces réseaux est de faire communiquer l'ensemble des équipements entre eux et avec l'extérieur. Nous détaillons dans cette section les couches basses de leur architecture sous-jacente, ainsi que celles permettant à tous les équipements du domicile de s'échanger des informations.

La télésurveillance, les alarmes, les capteurs de présence forment une autre catégorie d'équipements qui doivent pouvoir être ajoutés aux réseaux de domicile pour pouvoir être jointes à distance. S'y ajoutent également les ampoules électriques et plus généralement tout ce qui est connecté au réseau électrique, comme les chaudières et pompes à chaleur.

Le but du réseau de domicile est de connecter tous les équipements du domicile pour leur permettre de communiquer avec l'extérieur et entre eux. Les problèmes à résoudre se divisent en deux grandes catégories : la connexion des équipements entre eux par le biais d'un réseau proposant un protocole acceptable par l'ensemble des machines et la gestion des applications communes, qui, beaucoup plus qu'une connexion réseau, demandent un interfonctionnement.

Les couches basses de l'architecture

Les couches basses de l'architecture des réseaux de domicile, concernant les éléments physiques, les trames et les paquets, sont fondées essentiellement sur Ethernet, que ce soit sous forme hertzienne, courant porteur ou câblée. Ces trois supports se partagent en fait les connexions des équipements du domicile.

Les courants porteurs en ligne forment une catégorie importante des réseaux de domicile.

Le CPL

L'utilisation des courants porteurs en ligne, ou CPL, dans le domaine du domicile est aujourd'hui une réalité qui ne cesse d'attirer des clients. Les distances sont généralement assez faibles, de l'ordre de quelques mètres entre les différentes prises.

L'objectif est de réaliser sur l'ensemble des câbles électriques d'une même habitation un réseau partagé, de telle sorte qu'un message émis par un client par l'intermédiaire de sa prise électrique puisse être capté par l'ensemble des prises électriques de l'habitation. Le tableau électrique n'offrant qu'une faible protection contre la diffusion vers l'extérieur de l'habitation, il faut sécuriser les communications, comme dans les réseaux hertziens, où l'écoute est simple à réaliser.

Puisque le câble est partagé, une technique d'accès de type MAC est requise. La solution la plus souvent proposée est d'utiliser la norme Ethernet, qui permet le partage d'un câble commun. Cependant, contrairement à l'Ethernet classique, qui utilise la technique CSMA/CD comme méthode de partage, Ethernet sur courant porteur utilise la même technique que Wi-Fi c'est-à-dire le CSMA/CA. Il est en effet difficile avec la composante électrique d'écouter en même temps qu'on émet.

Le comportement de ces réseaux est similaire à celui de Wi-Fi : les performances se dégradent dès qu'une des stations subit un fort taux d'erreur en ligne l'obligeant à réduire sa vitesse d'émission. D'une vitesse brute annoncée de 200 Mbit/s dans le standard CPL HomePlug, le débit peut chuter jusqu'à 0,9 Mbit/s.

Les principaux produits pour l'environnement du domicile proviennent de la technologie HomePlug, avec les versions 1.0 turbo, Turbo, AV (Audio Video), AV2, GreenPHY et Access BPL (Broadband Power Line). Ces versions ont des débits bruts annoncés de 14, 80 et 200 Mbit/s. Comme nous l'avons indiqué, ces débits sont très fluctuants en fonction de l'environnement et peuvent chuter fortement, jusqu'à 1 Mbit/s.

Le second grand standard de fait provient de HD-PLC (High Definition PLC) qui définit une couche physique à partir de wavelets.

La normalisation s'est effectuée dans le groupe IEEE P1901 et prend pour base le HomePlug AV et le HD-PLC, ce qui donne le choix entre deux couches physiques différentes. Le nom de la norme est plus exactement BPL (Braodband over Power Line) ou encore IEEE 1902-2010 pour indiquer la date de finalisation. Les débits montent jusqu'à 500 Mbit/s.

Dans le domicile, il est possible de mettre en place une passerelle entre le réseau CPL et les autres réseaux Ethernet. La difficulté principale de cette interconnexion réside dans l'adéquation des classes de priorités entre les différents réseaux, qui ne sont pas toujours exactement positionnées de la même façon.

La sécurité de l'information qui transite sur ce réseau constitue également un problème. Le courant faible peut traverser le compteur électrique, même en présence de filtres spécialisés. Il faut donc chiffrer l'information avec une clé, par exemple la clé NEK (Network Encryption Key) de HomePlug, et implémenter cette clé sur l'ensemble des équipements

au moyen d'un logiciel de configuration spécifique. Des équipements de type routeur, passerelle, gestion des NAT sont également indispensables. Ils sont très similaires à ceux des réseaux Wi-Fi.

Caractéristiques

La technologie CPL consiste à émettre des signaux sur le support physique qui transporte l'électricité. De nombreuses implémentations ont été effectuées depuis les années 1950, comme le relevé de compteur à distance et les applications de domotique à bas débit. Les communications CPL à haut débit sont beaucoup plus récentes.

Deux catégories de réseaux CPL doivent être distinguées : le CPL pour réaliser une communication sur la boucle locale et permettre à un utilisateur d'accéder à Internet à haut débit, d'une part, et la transmission de données sur un réseau électrique privé correspondant à un domicile, une entreprise ou au cabinet d'une profession libérale, d'autre part. La première catégorie n'a eu que peu de succès jusqu'à présent pour les hauts débits, compte tenu de la difficulté de traverser un ensemble d'équipements électriques ou de les contourner. Dans cette annexe, nous ne nous intéressons qu'au CPL dans l'environnement privé. La partie boucle locale a été examinée au chapitre 15, en particulier avec le standard G3-PLC.

Dans l'environnement du réseau de domicile, le câble électrique correspond à un support à accès multiple et en diffusion, c'est-à-dire qu'un émetteur connecté au câble voit son signal diffusé sur l'ensemble du câble. Le câble électrique se comporte comme un réseau Ethernet, et plus précisément comme un réseau Wi-Fi. On retrouve donc exactement les caractéristiques d'un réseau Wi-Fi, avec sa technique d'accès et les difficultés d'y apporter de la qualité de service, une forte sécurité et des performances.

La technique d'accès CSMA/CA est en tout point identique à celle de Wi-Fi. La qualité de service est apportée par un ensemble de quatre classes de clients qui permettent, comme dans IEEE 802.11e, de privilégier certains flots par rapport à d'autres. La priorité s'exerce par le biais de temporisateurs de reprise plus ou moins longs en fonction de la classe de priorité. Cette solution n'est pas complètement efficace lorsque le réseau est saturé puisque les temporisateurs de reprise sont nombreux.

En fonction des interférences électriques, le débit brut peut décroître sans que l'utilisateur puisse le savoir, si ce n'est par le temps plus long nécessaire à la récupération d'un fichier. Le débit brut moyen est très difficile à estimer puisqu'il dépend du bipoint en communication. À chaque trame émise correspond une vitesse brute, de telle sorte qu'il faut faire une moyenne des débits bruts en tenant compte du temps de transmission de chaque trame. Pour un réseau qui posséderait deux bipoints, c'est-à-dire quatre stations communiquant deux à deux, l'une à 100 Mbit/s et l'autre à 1 Mbit/s, il faut cent fois plus de temps pour émettre une trame entre le bipoint lent par rapport au bipoint rapide. En moyenne, le débit n'est donc que très légèrement supérieur à 1 Mbit/s. On peut estimer qu'un réseau CPL a un débit brut moyen à peu près égal à celui du bipoint le plus lent.

Pour éviter cet effondrement des performances, les dernières normalisations intègrent des technologies de partage, comme le TDMA, qui limitent fortement la chute de débit engendrée par les bipoints de mauvaise qualité.

Comme dans les réseaux Wi-Fi, le débit réel est très inférieur au débit brut. On peut estimer de façon très simplifiée que le débit réel est le tiers du débit brut. Si l'on prend l'exemple de la technologie HomePlug, qui possède six générations, 1.0, turbo, AV (Audio Vidéo), AV2, Green PHY et BPL, les débits bruts maximaux et les débits réels sont récapitulés au tableau N.1.

TABLEAU N.1 • Débits réels et bruts des réseaux HomePlug

Standard	Débit brut	Débit réel
HomePlug 1.0	14 Mbit/s	4,5 Mbit/s
HomePlug Turbo	85 Mbit/s	12 Mbit/s
HomePlug AV	180 Mbit/s	55 Mbit/s
HomePlug AV2	1 000 Mbit/s	200 Mbit/s
HomePlug Green PHY	10 Mbit/s	5 Mbit/s
HomePlug Access BPL	500 Mbit/s	100 Mbit/s

Comme nous l'avons souligné, il faut ajouter une dégradation de la vitesse brute dès que le taux d'erreur sur les communications augmente. Dans le cas de HP 1.0, les vitesses brutes se dégradent de 14 à 12,83 Mbit/s, 10,16 Mbit/s, 8,36 Mbit/s, 6,35 Mbit/s, 4,04 Mbit/s, 2,67 Mbit/s, 0,9 Mbit/s. Comme le débit réel est très inférieur au débit brut, on s'aperçoit qu'il est possible d'avoir un réseau CPL débitant moins de 500 Kbit/s si l'une des stations travaille à la vitesse dégradée de 0,9 Mbit/s.

Le CPL met en œuvre une méthode très similaire à celle de Wi-Fi pour la transmission de données dans le domaine privé (*voir le chapitre 20*). D'ailleurs les contrôleurs Wi-Fi qui connectent les points d'accès Wi-Fi peuvent également prendre en charge les réseaux CPL. Lorsqu'une des deux solutions baisse en régime, l'autre prend le relais.

La sécurité est une fonctionnalité essentielle pour mettre en œuvre un réseau CPL. Comme indiqué précédemment, les signaux peuvent traverser le compteur électrique, même en présence de filtres spécifiques. Pour éviter cet inconvénient, il suffit de chiffrer l'information de la même manière que dans Wi-Fi. De plus, le contrôleur peut contenir un serveur RADIUS pour identifier les demandes de connexion.

Fonctionnement

Dans le domicile, le signal numérique est émis vers les équipements d'extrémité entre 3 et 148 kHz pour les réseaux bas débit et entre 1 et 30 MHz pour les réseaux haut débit. Chaque équipement dispose de sa propre adresse et peut-être commandé par l'élément émetteur.

Du fait de son rayonnement électromagnétique, le câblage électrique fonctionne comme une antenne, de telle sorte que les interférences avec les ondes radio externes peuvent devenir importantes. Dans la zone des 1 à 30 MHz, qui nous intéresse ici, les interférences avec les radioamateurs et les DRM peuvent poser problème.

Les modems CPL utilisant l'OFDM permettent de gérer approximativement les interférences en n'utilisant pas les sous-bandes correspondant à des fréquences déjà utilisées par d'autres équipements. Une technique de *notching* a été mise au point pour éteindre et allumer les sous-bandes qui interfèrent avec d'autres émissions. En temps réel, un mécanisme d'analyse du niveau du rapport signal sur bruit permet de réaliser cet algorithme d'ajout et de retrait de certaines sous-bandes de l'OFDM.

Les bandes utilisées par les principaux produits sont indiquées au tableau N.2.

TABLEAU N.2 • Bandes de fréquences et porteuses des réseaux CPL

Réseaux CPL	Bande de fréquences	Nbre de porteuses OFDM
HomePlug 1.0	4,49-20,7 MHz	76
HomePlug AV	2-28 MHz	917
DS2 45 Mbit/s	1,6-30 MHz	100
DS2 200 Mbit/s	2,46-11,725 et 13,8-22,8 MHz	2560
Spidcom	2-30 MHz	900

Des expériences à des fréquences beaucoup plus élevées que 30 MHz, dans les bandes Wi-Fi à 2,4 et 5,15 GHz ont permis d'obtenir des débits de l'ordre du gigabit par seconde.

Plusieurs modes d'utilisation des réseaux CPL peuvent être envisagées : maître-esclave, pair-à-pair et centralisé. Le mode maître-esclave permet à un système central, situé sur le compteur électrique, de jouer le rôle de maître par rapport aux différentes branches de l'arbre composé des câbles électriques partant de ce centre. Le système central joue le rôle de pont entre les différents brins électriques. Le mode pair-à-pair correspond à une technologie Ethernet classique dans laquelle chaque émetteur peut aller directement à chaque récepteur. Le mode centralisé est une combinaison des deux précédents, dans lequel une station maître s'occupe de la gestion et du contrôle et met en place des communications dans le mode pair-à-pair.

La version AV de HomePlug utilise la solution centralisée. La station centralisée décide des tranches de temps accordées aux différentes stations communicant en pair-à-pair. Cette solution permet d'affecter les vitesses de communication pour chaque couple d'émetteur-récepteur.

Une autre propriété importante des technologies CPL concerne l'adaptation des vitesses de transmission pour chaque station. Comme la vitesse de transmission entre un émetteur et un récepteur dépend de la qualité du support et de l'affaiblissement du signal, cette vitesse est tributaire de l'emplacement des deux stations en train de communiquer : si elles sont très éloignées et si du bruit électromagnétique perturbe le support, le débit peut être très bas, moins de 1 Mbit/s comme nous l'avons vu.

Chaque couple de stations transmet à sa propre vitesse, comme une station Wi-Fi et son point d'accès. Pour déterminer la vitesse de transmission, chaque station possède une table « Tone Map » qui indique la meilleure vitesse de transmission par rapport aux

autres stations du réseau. Cette table est mise à jour en un temps variant généralement de 10 ms à une seconde.

La figure N.1 illustre, pour HomePlug 1.0, ce champ Tone Map, qui est transmis dans les en-têtes des trames de telle sorte que chaque station qui écoute le support puisse déterminer sa vitesse de transmission.

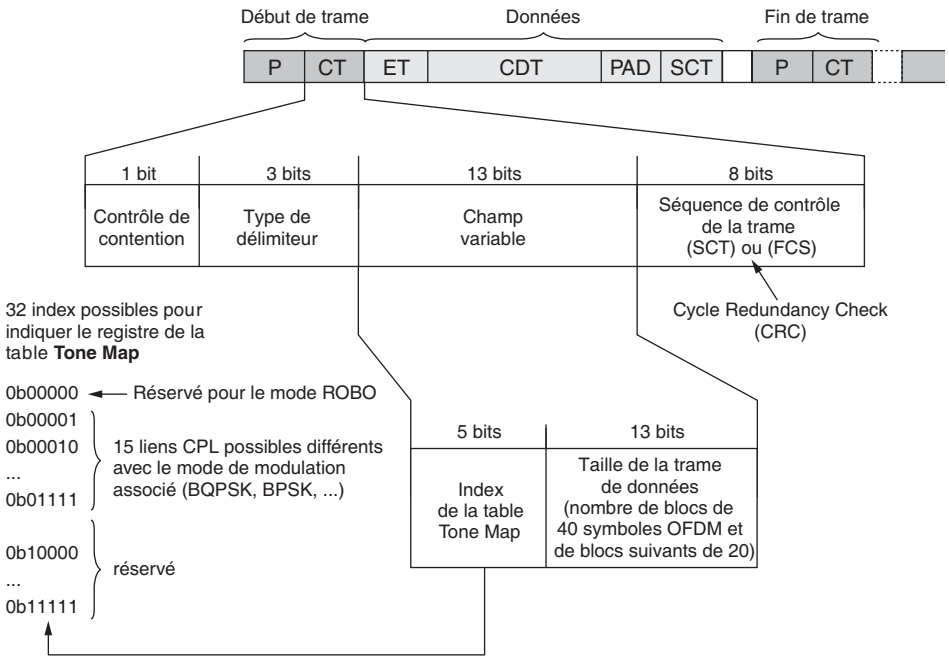


Figure N.1

Le champ Tone Map dans HomePlug 1.0

Le champ d'indication de la vitesse sur 13 bits indique les valeurs des 15 débits possibles, ainsi que la modulation associée (DQPSK, DBPSK, etc.). Pour HomePlug AV, le nombre de liaisons est de 255 stations, et le champ tient sur 16 bits.

Le tableau N.3 indique les différents débits de HomePlug 1.0 en fonction de la technique de modulation utilisée.

TABLEAU N.3 • Débits du réseau HomePlug 1.0

Technique de modulation	Paramètre de l'encodeur	FEC (taux de codage du code convolutionel)	Débit PHY (Mbit/s)
DQPSK	23/39 à 238/254	3/4	14,1
DQPSK	23/39 à 238/254	1/2	9,1
DQPSK	23/39 à 238/254	3/4	4,5
ROBO (DBPSK)	31/39 à 43/51	1/2	0,9

L'inconvénient de cette solution est qu'elle ne permet pas de déterminer avec précision la capacité du réseau CPL. On peut estimer que le débit moyen du réseau est un peu supérieur au débit de la liaison la plus lente si les débits de chaque liaison sont à peu près équivalents.

Les versions à très haut débit, comme HomePlug AV, proposent des variantes du CSMA/CA permettant d'optimiser les débits. Les affectations du support se font en TDMA pour permettre en particulier le passage d'applications de streaming et des applications temps réel comme la parole téléphonique. Certains slots TDMA sont affectés à ces applications prioritaires et d'autres sont utilisés en CSMA/CA.

Les réseaux CPL introduisent des améliorations de la qualité de service par un système identique à celui d'IEEE 802.11e consistant à déterminer la taille de la fenêtre de contention. Plus la fenêtre est petite, plus la priorité est forte. Le choix de cette fenêtre est effectué au moment de l'exécution de l'algorithme de back-off, c'est-à-dire du tirage du temporisateur de reprise.

Comme le support physique n'est pas de bonne qualité, de nombreuses erreurs se produisent. Une reprise sur erreur étant nécessaire, les acquittements sont envoyés dès la réception d'un paquet. Les protocoles ARQ (Automatic Repeat reQuest) permettent d'effectuer la retransmission. Ils emploient pour cela des paquets d'acquittement positif et négatif ainsi que des paquets « fail », qui indiquent la non-réception du paquet pour cause de mémoire saturée ou de très mauvaise qualité du signal.

Globalement, les performances des réseaux CPL sont extrêmement variables. Malgré l'augmentation des débits bruts, le passage d'un canal de télévision haute définition n'est pas garanti sur la durée. C'est la raison pour laquelle dans le réseau de domicile on utilise un réseau maillé contenant à la fois le CPL et le Wi-Fi.

Sécurité

Comme indiqué précédemment, on retrouve en matière de sécurité les mêmes problématiques que celles rencontrées dans le monde Wi-Fi, atténuées toutefois par le fait qu'il faut pouvoir se connecter physiquement sur le médium électrique pour l'écouter, ce qui est beaucoup plus complexe à réaliser que l'écoute d'un signal radio. Cependant, les signaux véhiculés sur le câble peuvent traverser le compteur électrique et être captés par les voisins. Il faut donc se protéger des écoutes potentielles et des stations pirates à l'intérieur comme à l'extérieur du réseau.

Les attaques peuvent être du même genre que dans Wi-Fi : écoute, modification de l'information, utilisation non autorisée du support, etc.

Le chiffrement est une solution pour contrer les écoutes. Pour cela, il suffit que chaque station chiffre les trames émises avec une clé commune à l'ensemble des utilisateurs du réseau. Le réseau possède une clé de chiffrement, appelée NEK (Network Encryption Key), qui est transmise à l'ensemble des stations pour le chiffrement et le déchiffrement. Elle peut être transportée par deux moyens : une interface de configuration qui introduit la clé dans chaque station ou l'interface électrique, chaque équipement possédant une clé DEK (Default Encryption Key).

L'authentification des équipements entre eux s'effectue à l'aide de la clé NEK. En l'absence de cette clé, la communication n'est pas possible entre équipements non identifiés. Certains réseaux CPL peuvent avoir des fonctions plus évoluées en utilisant également l'adresse MAC pour l'authentification.

L'intégrité des échanges peut être assurée par une signature électronique, qui empêche un attaquant de modifier les informations transportées.

D'autres solutions, comme les contrôleurs ou l'utilisation de cartes à puce et de VPN, peuvent s'ajouter aux fonctions de sécurité proposées par les équipementiers.

Un contrôleur est un équipement par lequel transitent toutes les communications et qui contient un serveur d'authentification ainsi que des fonctions de sécurisation des communications. Un filtre applicatif peut contrôler les applications échangées et détruire certaines trames non reconnues. Le contrôleur peut accélérer certains flots et en ralentir d'autres, jusqu'à éliminer les trames non désirées. Le filtre applicatif peut également jouer un rôle pour la qualité de service en ralentissant les communications entre certains bipoints relativement lents.

L'inconvénient de ce système est qu'il implique une double transmission entre un point et un autre point, de l'émetteur vers le contrôleur et du contrôleur vers le destinataire. Cet intermédiaire peut ralentir le débit, mais il peut également, de façon assez inattendue, l'accélérer. En effet, si le bipoint émetteur-récepteur est éloigné, la vitesse peut être très faible du fait d'un fort affaiblissement. Si un contrôleur intermédiaire permet de retransmettre à une vitesse beaucoup plus grande, il y a un gain évident.

Les cartes à puce peuvent intégrer les mots de passe et les certificats nécessaires pour une authentification de plus haut niveau. Enfin, l'utilisation de VPN (Virtual Private Network) est recommandée lorsque la communication sort du réseau pour aller vers un site distant.

Les VLAN (Virtual LAN) permettent de définir des réseaux locaux virtuels et donc de séparer les trafics. En règle générale, cette séparation est réalisée par l'utilisation de plusieurs clés NEK. Les sous-réseaux virtuels peuvent être interconnectés entre eux par un pare-feu ou un contrôleur. Cette fonctionnalité permet, par exemple, d'intégrer un réseau CPL dans un réseau d'entreprise.

La normalisation

La normalisation des réseaux CPL est menée aujourd'hui principalement par l'IEEE. Plusieurs groupes ont été formés, dont le plus important est P1901.

L'IEEE a créé des groupes de travail pour normaliser les réseaux courant faible sur courant fort. Ces groupes sont les suivants :

- IEEE P1575 (Standard for Broadband over Power Line Hardware), qui s'occupe de la normalisation des installations et de la sécurité du réseau.
- IEEE P1775 (Powerline Communication Equipment-Electromagnetic Compatibility Requirements-Testing and Measurement Methods), qui s'est focalisé sur les rayonnements électromagnétiques et la compatibilité avec les autres équipements radio. Ce groupe a également édicté les mécanismes à utiliser pour effectuer des mesures et des tests sur ces réseaux électriques.

- IEEE P1901 (Standard for Broadband over Power Line Networks Medium Access Control and Physical Layer Specifications), qui avait pour objectif de réaliser une normalisation effective d'un réseau CPL. Tous les principaux groupes qui ont travaillé dans le domaine sont présents, comme l'Alliance HomePlug, OPERA, UPA et CEPCA. Ce standard s'intéresse uniquement aux hauts débits, de 200 Mbit/s, 500 Mbit/s et 1 Gbit/s.

Un standard préliminaire a été approuvé à la fin de 2009 et publié au début de 2010. L'acceptation finale date de fin 2010. Deux niveaux physiques ont été définis, un utilisant une modulation OFDM, provenant de la technique HomePlug, et un second utilisant une modulation fondée sur les wavelets. Ces supports physiques sont optionnels. L'implémentation d'un seul support est acceptable, mais comme les deux solutions sont incompatibles, les utilisateurs doivent faire un choix.

Les principaux produits CPL

Les débits des principaux produits sont illustrés à la figure N.2.

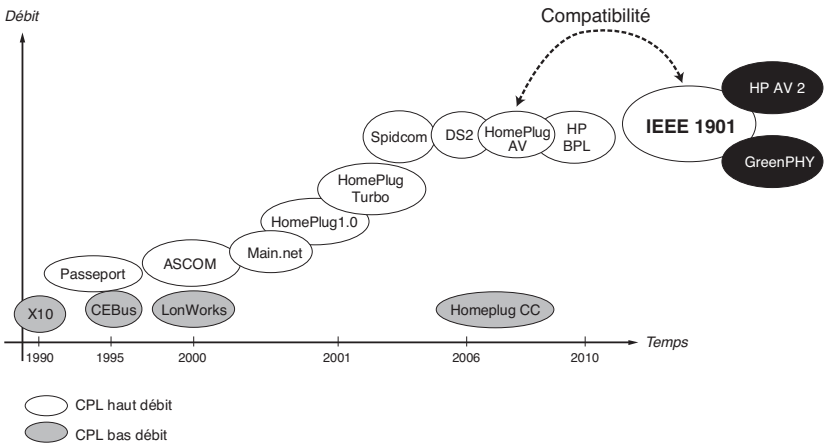


Figure N.2

Débits des principaux produits CPL

HomePlug

Un réseau HomePlug est constitué de cartes coupleurs reliées aux prises de courant électrique. Une trame de type Ethernet est utilisée, mais avec plusieurs modifications afin de tenir compte des contraintes des réseaux électriques.

Nous retrouvons dans ce réseau des caractéristiques similaires à celles des réseaux hertziens, en particulier IEEE 802.11. Les cartes coupleurs s'adaptent à l'environnement électrique en adoptant quatre vitesses différentes. Si le bruit électromagnétique est trop important et perturbe la qualité de la communication, le système dégrade sa vitesse pour continuer à transmettre avec un taux d'erreur acceptable par l'utilisateur. La vitesse de base du réseau, de 14 Mbit/s, se dégrade par palier jusqu'à moins de 1 Mbit/s. Les cartes coupleurs se calent sur la vitesse correspondant au bipoint.

La structure de la trame HomePlug est illustrée à la figure N.3. Des classes de clients travaillent suivant une priorité indiquée dans l'en-tête de la trame.

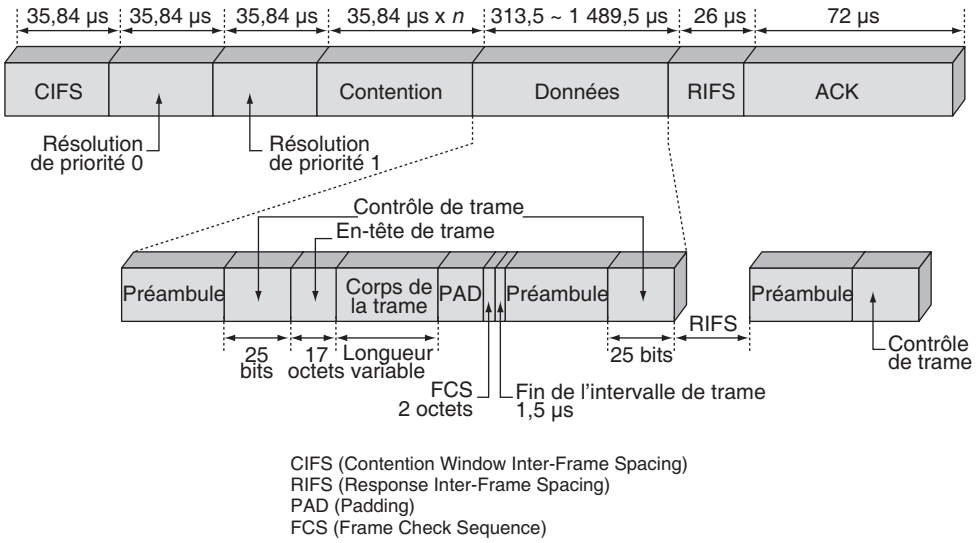


Figure N.3

Structure de la trame HomePlug

Cette structure de trame est suffisamment complexe pour prendre en charge toutes les caractéristiques de ce réseau.

À partir de la version HomePlug AV le réseau intègre de nouvelles améliorations sur le contrôle et la technique d'accès. En particulier, ce standard intègre un gestionnaire de connexion (Connection Manager) et un coordinateur central, qui rendent la gestion maître-esclave compatible avec les versions HomePlug précédentes. Ils optimisent en outre l'utilisation des bipoints ainsi que les tranches de temps provenant du TDMA introduites dans cette version. Les versions les plus élaborées AV2, BPL et Green PHY permettent d'améliorer les débits à 200 et 500 Mbit/s et de réduire fortement la consommation électrique, mais en réduisant en ce cas drastiquement les débits à 10 Mbit/s.

Les réseaux hertziens

L'utilisation des méthodes hertziennes s'est propagée avec Wi-Fi, mais de nombreux autres réseaux hertziens ont vu le jour, notamment UWB (Ultra Wide Band) et WiGig, le Wi-Fi personnel.

Ces réseaux étant présentés en détail aux chapitres 19 et 20, nous ne donnerons ici que des informations complémentaires utiles aux réseaux de domicile.

Wi-Fi

Wi-Fi est une excellente solution dans le domicile, mais il ne va pas sans un certain nombre de défauts, notamment en raison de son succès.

Dans une grande ville d'un pays développé, il est classique de détecter, en un point donné, une dizaine de réseaux Wi-Fi, voire beaucoup plus. Comme indiqué au chapitre 20, il n'est possible de choisir que trois fréquences réellement utilisables simultanément. Il existe donc de fortes interférences entre les réseaux Wi-Fi. De ce fait, il n'est pas rare, même avec un débit brut de plus de 100 Mbit/s, qu'un utilisateur ne dispose que d'un débit très bas, en dessous de 1 Mbit/s, du fait d'interférences électromagnétiques.

De plus, certains utilisateurs sont équipés de plusieurs points d'accès, ce qui complique encore l'ingénierie à mettre en œuvre. Il faut dans ce cas modifier non seulement le plan de fréquences, mais la puissance d'émission, comme cela se fait dans les entreprises.

Une solution, qui pourrait devenir un standard dans les réseaux de domicile consiste à implanter Wi-Fi dans chaque prise de courant électrique ou au moins dans une prise de courant de chaque pièce. Cela permet de réduire la taille des cellules et de limiter leur puissance, mais ce n'est pas toujours possible avec les points d'accès bon marché.

Une autre solution pour obtenir un débit et une couverture convenables consiste à adopter l'IEEE 802.11n ou l'IEEE 802.11ac, qui offrent des débits raisonnables, même en cas de forte demande, ou les réseaux mesh.

Du fait des interférences, il faut que les utilisateurs abaissent la puissance d'émission de leur point d'accès, ce qui présente l'inconvénient de réduire la portée. La solution à ce problème consiste à placer des bornes relais (ou bridges), qui communiquent entre elles en Wi-Fi ou par le biais du réseau électrique ou d'un réseau Ethernet spécifique. Les bornes relais servent à la fois de point d'accès et de relais, permettant aux clients de se connecter et de jouer le rôle d'un réseau mesh (*voir le chapitre 17*). En d'autres termes, dans le futur, les domiciles seront couverts par un ensemble de points d'accès reliés entre eux par des liaisons radio.

Autres solutions

De nombreuses autres solutions pourraient être adaptées à l'univers de la maison, à commencer par un réseau Ethernet standard avec un câblage spécifique. Cette solution est utilisée par de nombreux particuliers en raison de son efficacité. Les domiciles neufs pourraient disposer directement d'un câblage Ethernet dans les murs, mais c'est rarement le cas.

Le réseau Ethernet peut aussi utiliser le câblage téléphonique du domicile. Cette solution n'est toutefois pas toujours satisfaisante, car ces câbles sont de très mauvaise qualité et sont perturbés par les courants de sonnerie.

Une technique potentiellement intéressante, appelée FSO (Free Space Optics), utilise l'infrarouge et est limitée à une pièce. Le réseau se sert de l'électricité et des ampoules pour la diffusion de l'infrarouge.

Un câblage en fibre optique peut être réalisé dans un domicile en continuité de celui d'un opérateur. Cette solution est examinée avec soin actuellement, mais son coût est

important, et elle demande la mise en place d'étoiles optiques supplémentaires, ce qui pose des problèmes d'atténuation du signal optique.

Plusieurs solutions pour raccorder des capteurs sont également envisagées, comme l'utilisation de ZigBee ou l'une des propositions du groupe 6LowPAN de l'IETF. L'implémentation de nombreux capteurs devrait permettre de suivre les personnes dans la maison afin d'éteindre ou allumer automatiquement les lumières, de déceler des effractions et de gérer des éléments de sécurité (capteur d'incendie) ou de confort (capteur de température).

Dernière solution en date, le WiGig, qui, porté par une alliance de nombreux grands constructeurs, la Gigabit Wireless Alliance, pourrait avoir son mot à dire, surtout par sa compatibilité Wi-Fi et son très haut débit de 6 Gbit/s.

En résumé, on peut voir le réseau de domicile comme un double réseau Wi-Fi- CPL, comme illustré à la figure N.4. Ce réseau possède des bridges pour passer d'un réseau à l'autre et introduire le maillage. Si l'un des réseaux, ou une partie de réseau, pose problème on utilise l'autre.

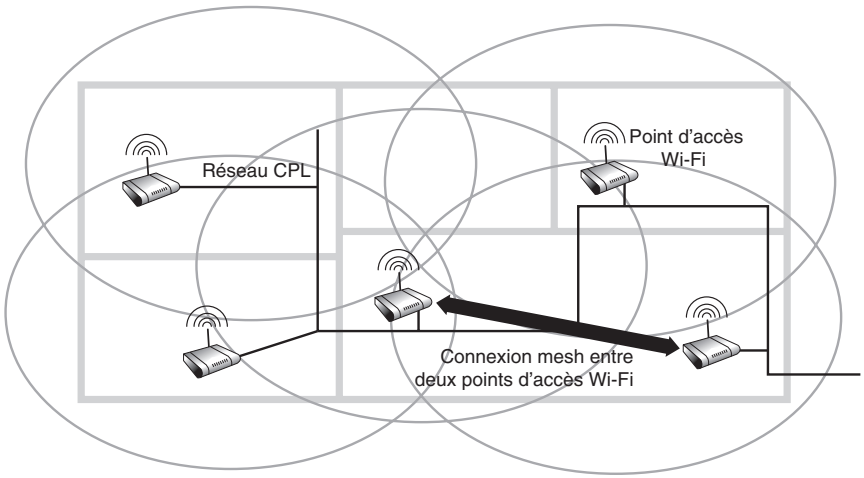


Figure N.4

Réseau de domicile de nouvelle génération

Les accès

Les débits des accès au domicile ne cessent d'augmenter, depuis les modems ADSL ou VDSL et les InternetBox jusqu'aux accès en fibre optique, de type FTTH (Fiber to the Home). Ces accès utilisent la fibre optique et apportent le gigabit par seconde par utilisateur.

Pour des raisons de coût, l'arrivée de la fibre peut s'arrêter au trottoir avec FTTC (Fiber to the Curb) ou entrer dans le bâtiment avec FTTB (Fiber to the Building). Dans ces deux derniers cas, la continuité s'effectue par le biais de câbles métalliques jusqu'à la porte de l'utilisateur.

Cette révolution de l'accès donne au réseau de domicile la puissance d'un réseau de très grande entreprise d'il y a cinq ans. Elle devrait permettre l'arrivée de nouveaux services à très haut débit, comme les murs de présence, le téléchargement de vidéos ou la diffusion de plusieurs canaux de télévision haute définition.

Même si la fibre optique n'arrive pas jusqu'au domicile, d'autres solutions, comme l'ADSL ou le VDSL, devraient être largement suffisantes pour irriguer le domicile. Ces technologies offrent des débits maximaux de 25 et 100 Mbit/s, tout à fait acceptables pour prendre en charge les applications moyen et haut débit. Les Home Gateways jouent ici un rôle capital. Si elles sont aujourd'hui optimisées pour le Triple ou le Quadruple-Play, elles devraient être dimensionnées pour les applications du domicile dans un avenir proche.

Les couches supérieures de l'architecture

Les couches supérieures ont pour objectif de réaliser la communication entre les équipements du réseau de domicile entre eux. Les exemples les plus classiques concernent la télévision provenant de la Home Gateway à destination de l'un des écrans de la maison ou bien l'enregistrement d'un programme de télévision vers un DVD pouvant se trouver à l'autre bout du domicile.

Les applications de téléphonie présentent moins de difficulté du fait de leur faible débit. En revanche, elles demandent une gestion particulière de la mobilité en environnement de domicile.

En réalité, c'est la superposition de toutes ces applications, certaines à haut débit et avec des contraintes temps réel, d'autres avec des problèmes de consommation électrique, d'autres encore avec du multipoint et des débits importants, qui rend le réseau de domicile complexe à contrôler.

L'objectif des couches supérieures est de déterminer les profils qui doivent permettre de mettre deux machines en communication, en parlant le même langage et en proposant une qualité de service.

La figure N.5 illustre certains des objets que l'on peut faire communiquer dans la maison.

Ces objets à connecter viennent de trois univers différents :

- Télécommunications : équipements téléphoniques et terminaux multimédias mobiles (PDA, les smartphones, etc.). Ces objets ont une certaine intelligence, et leur système d'exploitation est capable de supporter des algorithmes de contrôle peu sophistiqués. Leur puissance est très variable, selon l'utilisation autre que téléphonique qui peut être faite de ces terminaux.
- Informatique : ordinateurs portables ou de bureau et plus généralement les équipements qui possèdent un système d'exploitation puissant, de la mémoire et une unité centrale pas trop limitée.
- Électronique grand public : appareils ménagers et électroniques, tels que télévisions, aspirateur, réfrigérateur, etc. Ces équipements disposent d'entrées-sorties analogiques, mais ils sont en train de devenir numériques, permettant leur connexion au réseau de domicile pour y envoyer et en recevoir des paquets IP.

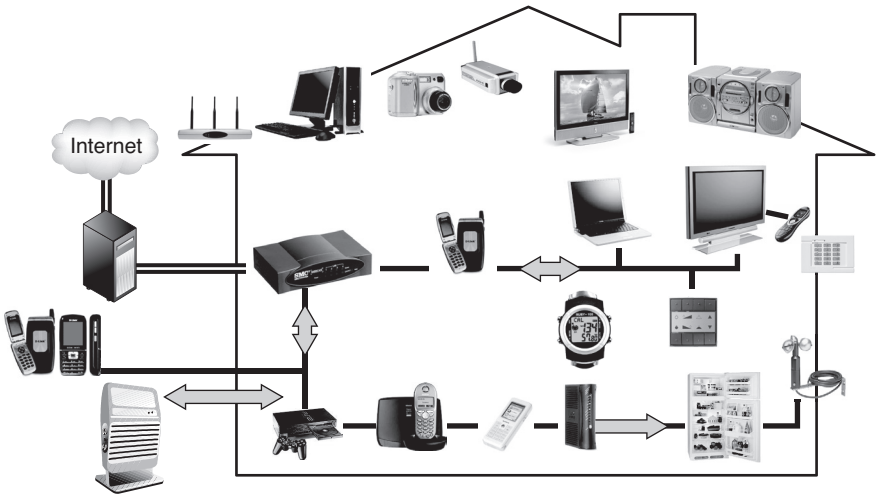


Figure N.5

L'univers des objets que l'on peut faire communiquer dans un réseau de domicile

La révolution dans le domaine des réseaux de domicile a pour objectif de faire communiquer toutes ces machines très différentes venant d'horizons distincts. Pour cela, toutes les machines devront devenir IP. Ainsi les télévisions deviennent-elles des IPTV, les téléphones des téléphones VoIP, et les machines diverses des machines IP. Cette révolution est en cours, même si elle se fait encore peu sentir du fait principalement des coûts de ces équipements IP.

Les industriels du monde de l'informatique ont essayé de développer une technologie de découverte de service aux fonctionnalités minimales, notamment avec le standard UPnP (Universal Plug & Play). Cependant, la découverte de service, si elle est indispensable, n'est pas suffisante pour réaliser la communication. Il est nécessaire de mettre en place une véritable architecture de communication avec le média à utiliser, prenant en compte la vitesse et la qualité de service. Une telle architecture, dite DLNA (Digital Living Network Alliance), effectue un compromis entre l'ensemble des partenaires. Nous l'examinons en détail un peu plus loin dans ce chapitre.

L'architecture DLNA est cependant incomplète, car elle ne prend pas en compte la partie réseau à l'intérieur du domicile. Elle permet essentiellement de mettre d'accord des équipements en vu de communiquer. Pour gérer la qualité de service, la sécurité, la gestion de la mobilité ainsi que la maintenance du réseau de domicile, il faut aller plus loin sur la partie réseau proprement dite. Plusieurs consortiums se proposent d'aller dans ce sens, mais souvent avec des vues partielles. Citons notamment le DSL Forum et surtout HGI (Home Gateway Initiative), que nous détaillons plus loin.

UPnP

UPnP (Universal Plug and Play) est une technologie qui permet la communication des données entre n'importe quelle machine sous le contrôle d'un équipement du réseau domestique. Des DCP (Device Control Protocol) décrivent des méthodes normalisées pour l'interaction entre machines. Ces protocoles utilisent des techniques standards, comme UDP, TCP, HTTP, SSDP (Simple Service Discovery Protocol) ou SOAP. Les descriptions sont effectuées en XML de façon à être totalement compatibles avec le monde Internet.

L'architecture UPnP spécifie six phases d'interaction, comme illustré à la figure N.6 :

- L'adressage (Addressing), par laquelle les équipements obtiennent leur adresse IP.
- La découverte (Discovery), par laquelle les points de contrôle découvrent l'existence des équipements.
- La description (Description), par laquelle les points de contrôle apprennent à connaître les équipements et leurs services.
- Le contrôle (Control), par laquelle les points de contrôle invoquent les actions à réaliser.
- La notification (Eventing), par laquelle les équipements peuvent notifier des contrôles.
- La présentation (Presentation), par laquelle les équipements peuvent présenter des pages Web aux points de contrôle pour obtenir les états et lancer des interactions.

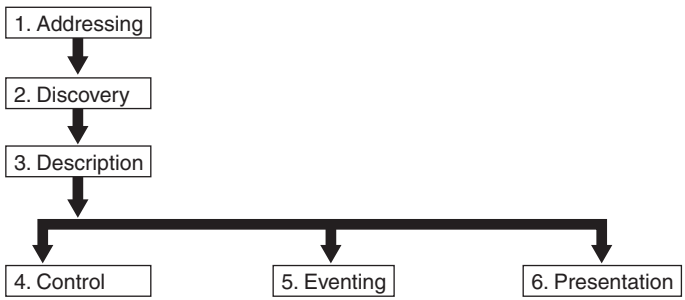


Figure N.6

Les six phases d'interaction d'UPnP

UPnP est un bon début pour l'intercommunication entre des équipements différents, mais il reste insuffisant et peu sécurisé. En particulier, il ne définit pas le média à utiliser pour communiquer, ni le débit, ni la qualité de service nécessaire. C'est la raison de la mise en place de l'initiative DLNA, que nous allons examiner.

DLNA

L'architecture DLNA provient d'un consortium réunissant tous les grands acteurs des télécommunications, de l'électronique grand public et de l'informatique.

Le consortium comprend environ trois cents membres, dont vingt et un promoteurs (*promoter members*). L'objectif de ce consortium est de fournir les formats de base pour

fournir l'interopérabilité des médias. Une de leur tâche importante est de développer des liaisons avec l'ensemble des organismes s'occupant de la normalisation des médias pour uniformiser les présentations et aboutir à un environnement commun, mais sans inventer de nouveaux standards.

DLNA doit également se préoccuper des tests de compatibilité entre les différentes piles protocolaires proposées par les industriels.

L'architecture de DLNA comporte six couches, comme l'illustre la figure N.7.

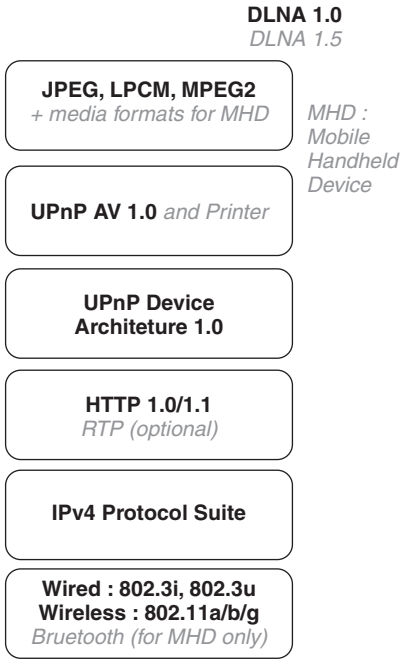


Figure N.7

Les six couches de l'architecture DLNA

La couche la plus haute détermine les médias qui peuvent être utilisés entre deux équipements. Dans la version DLNA 1.5, les médias acceptables sont JPEG, LPCM et MPEG-2, ainsi que des médias destinés aux équipements d'extrémité mobiles, les MHD (Mobile Handheld Device).

De façon plus précise, les médias et leurs options sont indiqués au tableau N.4.

TABLEAU N.4 • Les médias de DLNA

Classe	Format de base	Formats optionnels
Image	JPEG	PNG, GIF, TIFF
Audio	LPCM	AAC, AC-3, ATRAC 3plus, MP3, WMA9
AV	MPEG-2	MPEG-1, MPEG-4, AVC, WMV9

Les couches 5 et 4 reprennent essentiellement UPnP comme technique de découverte des équipements. La couche 3 détermine les protocoles qui peuvent être utilisés entre les équipements d'extrémité. Le principale est HTTP, avec en option RTP.

La couche 2 décrit le protocole de niveau paquet. IPv4 a été choisi comme protocole de base. Le protocole IPv6 pourrait être utilisé en temps voulu.

La couche la plus basse se préoccupe des supports physique et hertzien pour permettre la communication. Les choix tournent autour d'Ethernet avec les Ethernet filaires et la technologie Wi-Fi dans la partie hertzienne. En complément, DLNA supporte MOCA (Multimedia over Coax Alliance) pour les équipements mobiles, la norme Bluetooth a été ajoutée.

L'architecture DLNA est donc beaucoup plus complète que la simple découverte d'équipements. Elle est toutefois encore insuffisante dans les réseaux de domicile pour garantir une communication entre deux équipements avec qualité de service et sécurité.

Après la mise au point de la version 1.5, DLNA s'est donné pour objectif d'étendre cette première génération en y ajoutant les équipements d'impression et les mobiles. Les directives précédentes concernaient deux classes d'équipements, appelées DMS (Digital Media Server) et DMP (Digital Media Player). Avec la nouvelle génération, elles concernent douze classes.

Ces nouvelles possibilités sont les suivantes :

- Introduction de la possibilité d'imprimer sur le réseau vers un DMPr (Digital Media Printer), en particulier pour l'impression de photos.
- Possibilité de pousser (*push*) des images, de la vidéo ou du contenu audio d'un serveur vers un équipement de type Player. DLNA n'offre actuellement que la possibilité de tirer (*pull*) le média d'un serveur vers le Player. Cette solution permet de télécharger les images d'un appareil photo numérique vers un PC ou une télévision pour les visionner.
- Possibilité de contrôler la transmission vers un équipement mobile. Par exemple, donner la possibilité à un téléphone portable de transférer une chanson vers un équipement stéréo pour la diffuser.
- Prendre en charge la norme de codage AVC (MPEG-4). C'est le média d'interopérabilité par excellence pour la vidéo. Ce standard est effectivement conçu pour le stockage et le transfert optimisé de contenus vidéo.
- Prise en charge de la technologie Bluetooth.
- Prise en charge du protocole RTP, qui permet d'introduire une meilleure qualité de service applicative (*voir le chapitre 10*).
- Introduction de la qualité de service pour améliorer le transport des applications de type streaming.
- Prise en charge des téléchargements entre équipements mobiles et équipements audio/vidéo.

Modèle de compatibilité

Le consortium DLNA a développé un modèle de compatibilité entre équipements DLNA. Ce modèle est illustré à la figure N.8. Il définit la compatibilité par le biais de tests de conformité et d'interopérabilité. Des outils de test automatiques ont été développés afin de permettre, entre autres, une certification de la partie UPnP.

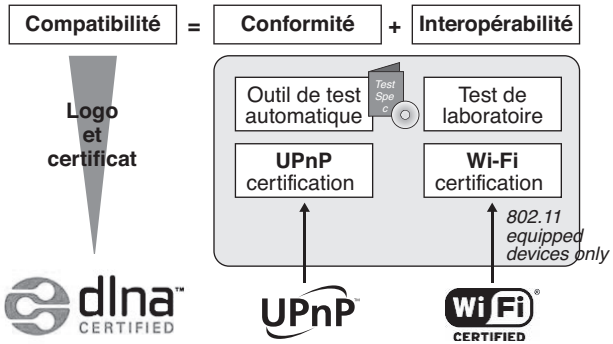


Figure N.8
Modèle de compatibilité DLNA

Pour pouvoir entrer dans le réseau de domicile facilement, les équipements doivent posséder le sigle DLNA indiqué sur la figure. Malheureusement, les équipements DLNA sont assez nettement plus chers que les autres puisqu'ils incorporent un processeur, de la mémoire, des entrées-sorties, des codeurs, etc.

Comme indiqué précédemment, l'architecture DLNA n'est pas suffisante par elle-même pour garantir la traversée du réseau de domicile. Il faut y ajouter des fonctionnalités internes au réseau de communication lui-même. Les architectures de la section suivante visent à apporter ce complément.

Les autres architectures

Le DSL Forum, devenu le Broadband Forum en 2008 compte plusieurs centaines de membres, incluant des FAI, des opérateurs, des équipementiers et des industriels du logiciel. Son objectif est de définir une architecture de bout en bout permettant de garantir les communications entre le serveur se trouvant dans un réseau d'opérateur et la machine terminale de l'utilisateur. C'est donc beaucoup plus que le réseau de domicile qui est concerné.

Le Broadband Forum se préoccupe en premier lieu de l'architecture et de la gestion des équipements d'extrémité.

L'architecture définie dans le document TR-069 vise l'autoconfiguration, le provisionnement de service dynamique, la gestion du logiciel et du firmware, le contrôle du statut des équipements et des liaisons ainsi que le monitoring de performance, la gestion des logs, le diagnostic, etc.

Pour cela, le Forum a défini un modèle de données commun pour la gestion des équipements et déterminé des modèles d'objets pour des applications comme la VoIP.

Un autre standard important pour le futur provient du document TR-196, qui concerne le modèle de données pour les points d'accès Femto, ou FAP (Femto Access Point). Les femtocells que nous avons examinés en détail au chapitre 17 forment également une composante importante des réseaux de domicile.

Un autre forum très important pour les réseaux de domicile provient du rassemblement d'un certain nombre d'opérateurs de télécommunications au sein du HGI (Home Gateway Initiative), parmi lesquels Orange, BT, DT, Belgacom, Telefonica, Telecom Italia, KPN, TeliaSonera et NTT. Cette initiative essentiellement européenne cherche à définir et normaliser par des spécifications industrielles des passerelles du réseau de domicile.

L'objectif du forum HGI est de spécifier un environnement résidentiel multiservice fondé sur une passerelle située entre la Home Gateway et les équipements résidentiels. La spécification HGI est fondée sur des standards existants. Son objectif est de les compléter afin que la normalisation du réseau de domicile soit complète. En particulier, la spécification est fondée sur les standards du Broadband Forum, DLNA, OSGi, DVB, UPnP, ETSI et UMA.

La passerelle HGI devrait ainsi être au cœur du domicile et jouer le rôle de chef d'orchestre de ce réseau.

Conclusion

Le réseau de domicile est devenu un vrai réseau, au même titre que celui d'une petite entreprise d'aujourd'hui. Il faut à la fois gérer le réseau du point de vue des couches basses et des applications afin qu'elles puissent être atteintes de toutes les machines du domicile.

Nous n'avons pas détaillé dans cette annexe les connexions qui devraient provenir des étiquettes électroniques et des réseaux de capteurs ; nous les avons introduites au chapitre 21. Ces connexions devraient se développer énormément dans le domicile pour introduire de nouveaux paramètres, comme la température extérieure sur la porte de sortie ou la possibilité de retrouver ses livres à l'intérieur de la maison. Dans ce dernier exemple, il suffirait de saisir le nom du livre recherché pour qu'une géolocalisation soit possible au travers d'une étiquette électronique associée et une triangularisation pour obtenir l'emplacement géographique.

D'autres développements sont en cours pour étendre le réseau de domicile. La première extension concerne les « extensions » du domicile, comme la voiture ou la maison de campagne. L'utilisateur doit pouvoir bénéficier dans sa voiture des mêmes services que chez lui. De même, les extensions vers la chambre d'hôtel ou le bureau semblent naturelles. Cependant, ces extensions posent de nouveaux problèmes, surtout si la mobilité est un paramètre supplémentaire à prendre en compte. C'est dans cet objectif que des groupes de travail spécifiques, comme VANET (Vehicular Ad hoc Network), ont été mis sur pied par l'IETF. Nous les avons examinés au chapitre 17.

O

Annexe du chapitre 20 (Les réseaux Wi-Fi)

Cette annexe se penche sur un certain nombre de problèmes qui peuvent survenir en matière de supervision, de qualité de service, de contrôle de la mobilité ou de gestion de l'énergie avec le standard IEEE 802.11e.

Parmi les fonctionnalités examinées, nous aborderons successivement les solutions pour prendre en charge les stations cachées, les problèmes de fragmentation-réassemblage, l'introduction de priorités avec IEEE 802.11e, le contrôle des handovers et la gestion de la mobilité

La réservation RTS/CTS et le problème de la station cachée

Dans Wi-Fi, l'écoute du support se fait à la fois au niveau de la couche physique, avec le PCS (Physical Carrier Sense), et au niveau de la couche MAC, avec le VCS (Virtual Carrier Sense). Le PCS détecte la présence d'autres stations Wi-Fi en analysant toutes les trames passant sur le support hertzien et en détectant l'activité sur le support grâce à la puissance relative du signal des autres stations.

Le VCS est un mécanisme de réservation fondé sur l'envoi de trames RTS/CTS (Request to Send/Clear to Send) entre une station source et une station destination avant tout envoi de données. Une station source qui veut transmettre des données envoie un RTS. Toutes les stations du BSS entendant le RTS lisent le champ TTL du RTS et mettent à jour leur NAV. La station destination ayant reçu le RTS répond, après avoir attendu pendant un SIFS, en envoyant un CTS. Les autres stations entendant le CTS lisent le champ de durée du CTS et mettent à nouveau à jour leur NAV. Après réception du CTS par la station source, cette dernière est assurée que le support est stable et réservé pour sa transmission de données.

Cela permet à la station source de transmettre ses données ainsi que de recevoir l'ACK sans collision. Comme les trames RTS/CTS réservent le support pour la transmission d'une station, ce mécanisme est habituellement utilisé pour envoyer de grosses trames pour lesquelles une retransmission serait trop coûteuse en terme de bande passante.

La figure O.1 illustre le processus d'émission d'une trame lorsque la station destination est cachée.

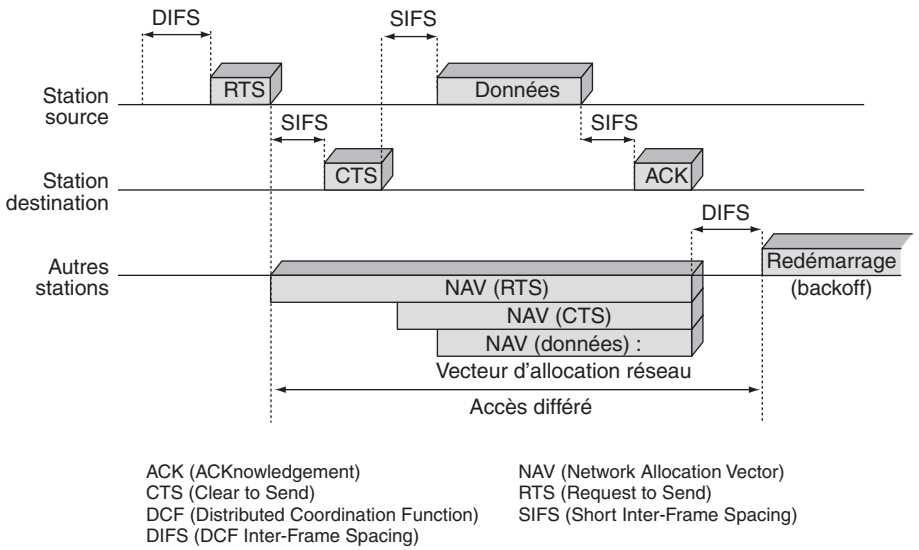


Figure O.1

Transmission en utilisant les trames RTS/CTS

Les stations peuvent choisir d'utiliser le mécanisme RTS/CTS ou de ne l'utiliser que lorsque la trame à envoyer excède une variable RTS_Threshold ou encore de ne jamais l'utiliser.

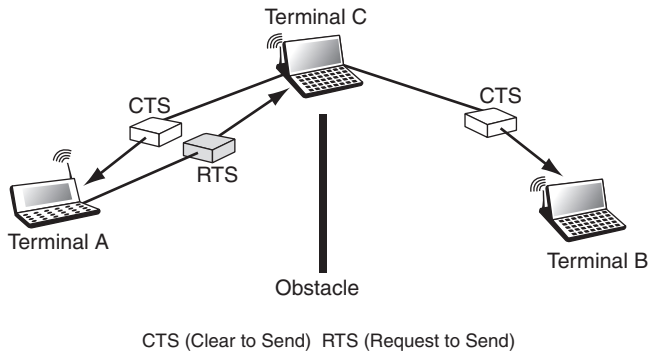
Le problème de la station cachée

Un problème spécifique du monde sans fil est le problème de la station cachée. Deux stations situées chacune à l'opposé d'un point d'accès (AP) ou d'une autre station peuvent entendre l'activité de cet AP mais ne pas s'entendre l'une l'autre du fait que la distance entre les deux est trop grande ou qu'un obstacle les empêche de communiquer entre elles. Le mécanisme de réservation RTS/CTS permet de résoudre ce problème.

La figure O.2 illustre une station B cachée de la station A mais pas de la station C. La station A transmet des données à la station C, mais la station B ne détecte pas l'activité de la station A. Dans ce cas, la station B peut transmettre librement, sans interférer avec la transmission de la station A. Toutefois, si A et C s'échangent des RTS et des CTS, la

station B, bien que n'écoutant pas directement la station A, est informée par l'envoi par la station C d'un CTS que le support est occupé. Elle n'essaie donc pas de transmettre durant la transmission entre A et C. Ce mécanisme ne permet pas d'éviter les collisions, puisque des RTS peuvent être envoyés simultanément par A et par B, mais une collision de RTS ou de CTS ne gaspille pas autant de bande passante qu'une collision de données, étant donné que les trames RTS et CTS sont relativement petites.

Figure O.2
Problème de la station cachée



En conclusion, le CSMA/CA permet de partager l'accès. Le mécanisme d'acquittement supporte en outre efficacement les problèmes liés aux interférences et, d'une manière générale, tous les problèmes liés à l'environnement radio. Le mécanisme de réservation RTS/CTS évite les problèmes de la station cachée. Tous ces mécanismes entraînent toutefois l'ajout aux trames Wi-Fi d'en-têtes, que les trames Ethernet ne possèdent pas. C'est pourquoi les réseaux Wi-Fi montrent toujours des performances plus faibles que les réseaux locaux Ethernet.

Fragmentation-réassemblage

Nous venons d'introduire le protocole CSMA/CA, qui permet à une station d'accéder au support hertzien pour émettre sa trame. Une question en suspens concerne la taille de la trame. Plus la taille d'une trame est importante, plus elle a de chance d'être corrompue. La fragmentation d'une trame en plusieurs trames de taille inférieure accroît la fiabilité de la transmission. Cette solution a pour effet de réduire le besoin de retransmettre des données dans de nombreux cas et d'augmenter ainsi les performances globales du réseau. La fragmentation est utilisée notamment dans les liaisons radio, dans lesquelles le taux d'erreur est important.

Wi-Fi utilise un système à saut de fréquence (Frequency Hop), dans lequel le support s'interrompt toutes les 20 ms pour changer de fréquence. Si la trame est petite, la probabilité pour que la transmission soit interrompue est faible. Pour savoir si une trame doit être fragmentée, on compare sa taille à une valeur seuil, appelée Fragmentation_Threshold.

Si la taille de la trame est plus grande que ce seuil, la trame est fragmentée. Les fragments ont une taille équivalente à la valeur du seuil Fragmentation_Threshold, sauf pour le dernier, qui peut avoir une taille plus petite.

Quand une trame est fragmentée, tous les fragments sont transmis de manière séquentielle. Le support n'est libéré qu'une fois tous les fragments transmis avec succès ou lorsque la station source ne réussit pas à recevoir l'acquittement d'un fragment transmis. La station destination acquitte chaque fragment reçu avec succès en envoyant un ACK à la station source. La station source garde le contrôle du support pendant toute la durée de la transmission d'une trame en attendant un temps SIFS après la réception d'un ACK ou après la transmission d'un fragment. Si un ACK n'est pas correctement reçu, la station source arrête la transmission et essaie d'accéder de nouveau au support. Lorsque la station source accède au support, elle commence à transmettre à partir du dernier fragment non acquitté.

Si les stations utilisent le mécanisme RTS/CTS, seul le premier fragment envoyé utilise les trames RTS/CTS pour réserver le support. Les autres stations dans le BSS maintiennent leur NAV en extrayant l'information de durée de vie dans les différents fragments et ACK.

La figure O.3 illustre le processus suivi par l'émetteur pour transmettre une suite de fragments provenant d'une même trame.

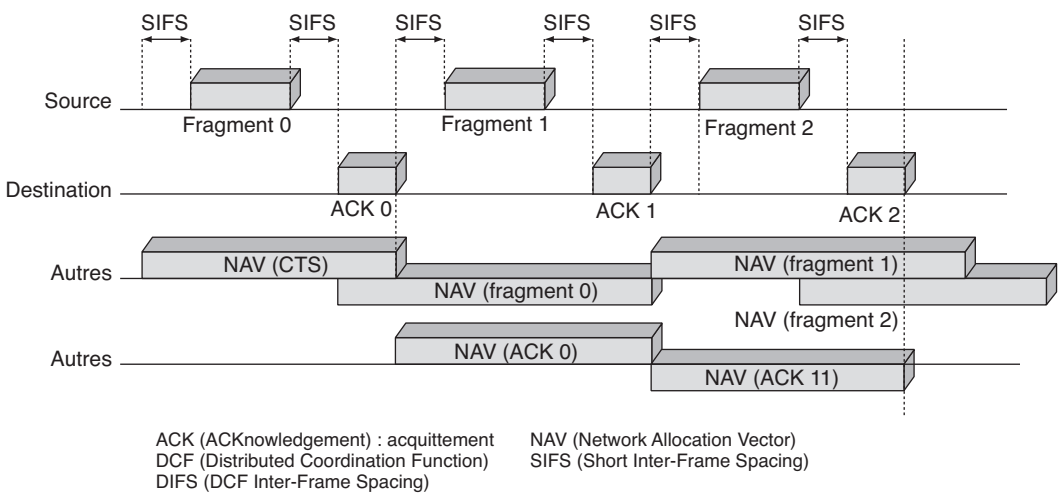


Figure O.3

Transmission d'une trame fragmentée

La trame est assemblée lorsque la station destination a reçu tous les fragments de la station source.

IEEE 802.11e

La qualité de service est indispensable pour assurer le transfert temps réel de données comme la voix ou la vidéo. De tels services demandent des transferts isochrones, c'est-à-dire des transferts de données qui permettent de faire varier le délai entre les différentes trames d'une même transmission. Dans le cas d'une application vidéo, par exemple, plus ce délai est important, plus la qualité se dégrade, qu'elle soit sonore ou visuelle. Pour minimiser ce délai, des mécanismes de priorité ont été introduits par une extension au standard 802.11, appelée 802.11e.

Wi-Fi et la qualité de service

Wi-Fi est utilisé comme un réseau local permettant d'échanger et de transmettre des données. Compte tenu des nombreux avantages apportés par ce type de réseau, il était normal de vouloir l'utiliser pour transmettre de la voix et même de la vidéo. Avec un débit théorique de 54 Mbit/s, IEEE 802.11g est capable de faire passer un trafic de type MPEG-4 ou même MPEG-2 sans aucun problème.

Il faut toutefois modérer cet optimisme, comme nous l'avons indiqué à la section précédente. Dans un tel cas, il faudrait qu'aucun autre trafic, par exemple de données, ne circule sur le réseau et que les stations qui utilisent l'application multimédia soient proches du point d'accès de façon que le mécanisme de variation de débit ne soit pas utilisé, évitant ainsi une chute de performance. Cela fait beaucoup de contraintes pour une simple transmission vidéo. Les mécanismes proposés par 802.11e améliorent justement la qualité de service.

Le taux de perte dans un réseau sans fil est de l'ordre de 10^{-3}, soit le taux de perte minimal pour appliquer une QoS. Le débit de Wi-Fi dépend du nombre de stations situées dans la cellule. La garantie de débit impose donc de limiter le nombre de stations connectées au point d'accès ainsi que de n'autoriser que des débits théoriques élevés. Le paramètre essentiel à prendre en compte est le délai entre les trames envoyées ainsi que sa variation, ou gigue.

La plupart des applications multimédias (voix et vidéo) demandent un trafic temps réel. Si les données d'une application multimédia n'arrivent pas à temps, cela peut stopper le processus de lecture ou engendrer des erreurs, que l'oreille et l'œil humain peuvent facilement voir ou entendre. L'oreille, par exemple, peut tolérer un temps de latence (délai) de 150 ms. Si ce temps augmente, la voix semble lointaine. Il en va de même de la vidéo. Si le délai n'est pas respecté, la vidéo peut apparaître pixellisée, ralentir, comporter des décalages entre le son et l'image, etc., la rendant difficile ou impossible à visionner.

Pour avoir un processus de lecture constant, l'instauration d'un système de priorité permettant de jouer sur le temps de réponse permet de mieux gérer ce type de trafic.

Les approches IntServ et DiffServ ne sont pas envisageables dans les réseaux Wi-Fi. En effet, ces mécanismes sont définis au niveau 3, niveau réseau, et il n'existe aucun lien, ou mapping, entre le niveau 3 et le niveau 2. Si l'on implémente DiffServ dans un réseau 802.11b souhaitant offrir à une station un débit de 3 Mbit/s, ce débit ne peut être

assuré que si la station est seule dans la cellule. Le débit maximal utile d'une station étant de 5 Mbit/s, en supposant un débit théorique de 11 Mbit/s, si une autre station essaye d'émettre sur le support, le débit est partagé entre les deux stations, soit 2,5 Mbit/s. Le débit de 3 Mbit/s ne peut plus être garanti, et DiffServ ne fonctionne pas.

Une solution à ce problème pourrait consister à appliquer un mécanisme de réservation en dehors du réseau Wi-Fi. Comme illustré à la figure O.4, il serait de la sorte possible de classifier le trafic entrant et sortant pour chaque station du réseau. Le problème est que la somme des débits alloués à chaque station ne devrait pas dépasser le débit maximal utile d'une cellule Wi-Fi. Dans l'exemple de la figure O.4, le réseau Wi-Fi étant en 802.11b, la somme des débits alloués aux trois stations (2, 2 et 1 Mbit/s) est égale à 5 Mbit/s, soit le débit maximal utile d'une cellule. Cette réservation, c'est-à-dire la classification des flux IP entrants et sortants du réseau Wi-Fi, ne peut donc se faire qu'à l'extérieur du réseau Wi-Fi par l'utilisation d'un classificateur. Une telle solution ne garantit toutefois que le débit et pas le délai, un paramètre important des trafics voix et vidéo.

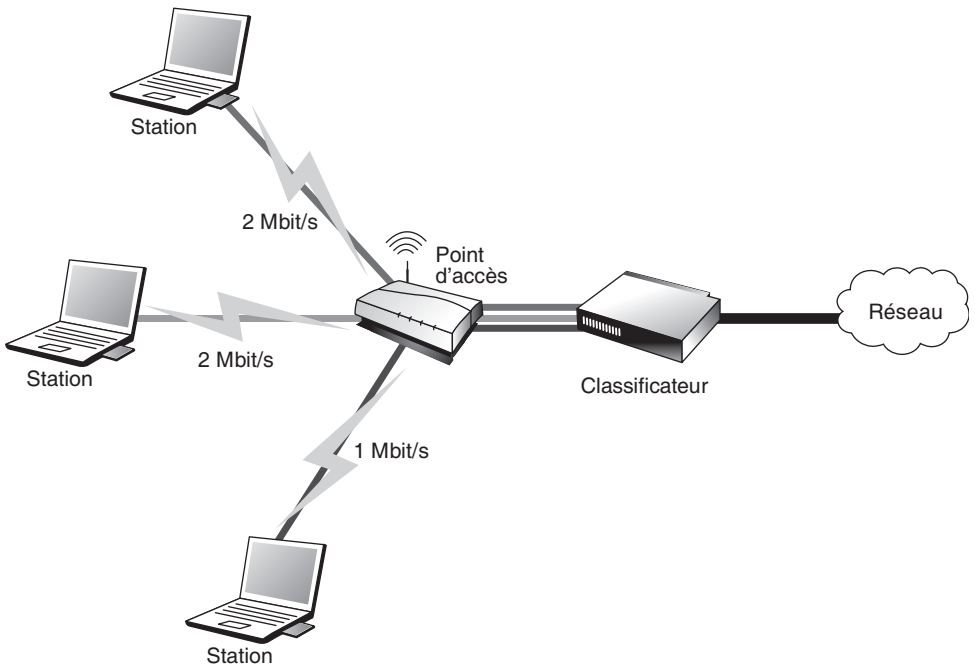


Figure O.4

Classification du trafic pour un réseau Wi-Fi 802.11b.

Cette solution est actuellement utilisée par de nombreux hotspots Wi-Fi ainsi que par certains FAI afin de garantir un débit moyen à l'utilisateur.

La téléphonie Wi-Fi, un marché en plein essor, ne peut utiliser un tel mécanisme qui ne garantit pas de délai. D'une manière générale, la téléphonie n'exige pas un débit

important. Le débit de la parole proprement dite est de 9,6 Kbit/s, ce qui donne un débit réel d'une cinquantaine de kilobits par seconde en tenant compte des éléments binaires introduits pour constituer le paquet puis la trame. Le délai et la gigue sont les paramètres principaux à prendre en compte. Ces derniers ne peuvent être assurés qu'en modifiant les paramètres d'accès définis dans 802.11, comme le propose l'amendement 802.11e.

Gestion des priorités

La norme IEEE 802.11e ajoute une nouvelle méthode, HCF (Hybrid Coordination Function), qui améliore la technique d'accès DCF. Cette méthode HCF est elle-même décomposée en deux algorithmes : l'EDCA (Enhanced Distributed Channel Access) et le HCCA (HCF Controlled Channel Access). Elles correspondent à l'introduction de classes, la première dans le DCF, la seconde dans le PCF. Comme l'EDCA est la seule utilisée, nous allons la décrire en détails.

L'EDCA est une évolution du DCF, qui ajoute un système de gestion de priorités lors de l'accès au support. Toujours à la manière du DCF, l'accès au support se fait selon le niveau de priorité de la trame. Les trames de même priorité ont la même probabilité d'accéder au support, tandis que celles de priorité supérieure ont une probabilité plus grande d'accéder au support.

Aujourd'hui, dans les réseaux Wi-Fi, les priorités sont les mêmes pour toutes les stations. Comme les trames de plus haute priorité ne peuvent interrompre le transfert des trames de plus faible priorité, il n'existe aucun moyen d'avoir une garantie sur la qualité de service d'une communication Wi-Fi.

L'EDCA fournit des accès différenciés pour différents types de trafic. Il définit huit niveaux de priorités par l'intermédiaire de catégories de trafic, ou TC (Traffic Categories). Chacune de ces catégories de trafic correspond à une file d'attente ayant, d'une part, un niveau de priorité et, d'autre part, des paramètres spécifiques, en fonction de ce niveau de priorité. Une station en mode EDCA équivaut à huit stations virtuelles traitant chacune différentes catégories de trafic.

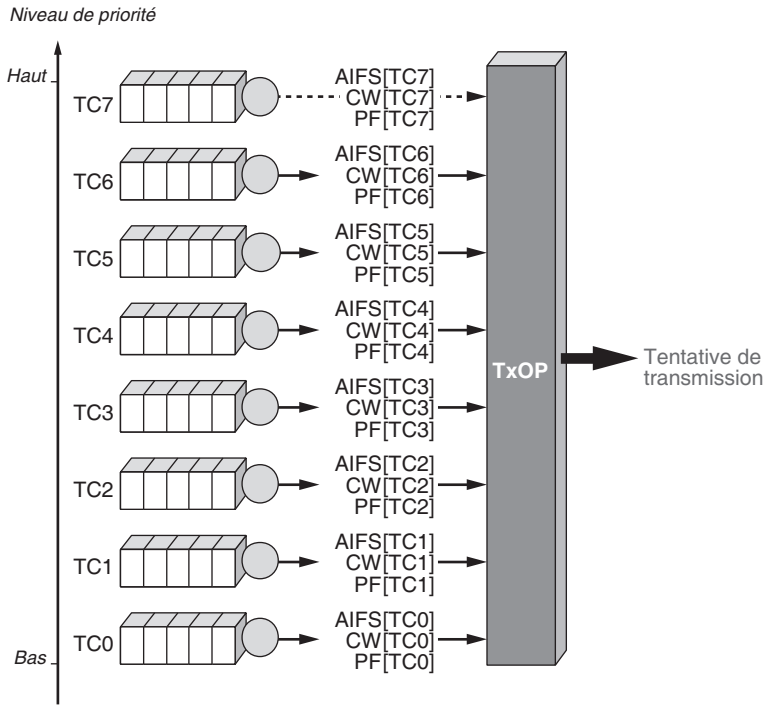
Chaque catégorie de trafic comporte des paramètres qui lui sont propres. Ces paramètres correspondent aux valeurs des différents temporisateurs utilisés (IFS, back-off), ainsi qu'aux paramètres utilisés dans le calcul de ces temporisateurs. La catégorie de trafic ayant la plus haute priorité est celle dont les valeurs de ces paramètres sont les plus faibles.

Les valeurs des temporisateurs ne sont pas fixes, comme dans le DCF. L'EDCA utilise toujours les IFS mais ajoute un nouveau temporisateur, l'AIFS (Arbitration IFS), qui joue le même rôle que le DIFS mais avec une valeur dynamique. De même, l'algorithme de back-off est toujours utilisé, mais la valeur de son temporisateur n'est plus fixe.

Le dernier apport de l'EDCA est l'ordonnanceur TxOP (Transmission Opportunities). Le TxOP détermine un temps, cette fois fixe, qui définit quand la station a le droit d'accéder au support et pendant quelle durée. Si plusieurs catégories de trafic veulent accéder au support au même instant, le TxOP encourage le TC de plus haute priorité.

Le fonctionnement de l'ECDF est illustré à la figure O.5.

Figure O.5
Les huit classes de trafics dans l'EDCA



L'EDCA fonctionne de la même manière que le DCF, les stations attendant en utilisant divers temporisateurs que le support soit libre avant toute transmission. La différence avec le DCF est que l'EDCA ne définit pas de valeurs fixes pour ces temporisateurs.

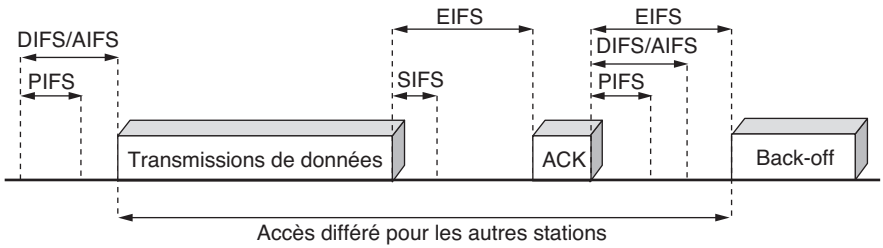
AIFS (Arbitration IFS)

Le DIFS est une durée d'attente utilisée par toutes les stations en mode DCF pour accéder au support. La valeur du DIFS est fixe et dépend de la couche physique utilisée. Seule la station arrivée la première sur le support — en supposant qu'il était auparavant libre — transmet ses données.

L'EDCA introduit un nouveau temporisateur, l'AIFS (Arbitration IFS), qui est utilisé de la même manière que le DIFS. Chaque station en mode EDCA attend un AIFS. Comme l'EDCA peut gérer jusqu'à huit niveaux de priorité, la valeur de l'AIFS n'est plus fixe mais dynamique. Elle varie en fonction du niveau de priorité requis par la station émettrice pour la transmission de sa trame. Cette valeur de l'AIFS est supérieure ou égale à celle du DIFS. Ainsi, la catégorie de trafic de priorité supérieure a une valeur d'AIFS égale à DIFS.

L'utilisation d'un tel système de priorité d'accès au support diminue le risque de collision. La figure O.6 illustre les différents temporisateurs utilisés lors de l'introduction de la qualité de service.

Figure O.6
Les relations entre les différents temporisateurs



L'algorithme de back-off

Dans le DCF, toute station accédant à un support occupé calcule un temporisateur grâce à l'algorithme de back-off. L'EDCA utilise toujours l'algorithme de back-off, mais, comme pour les temporisateurs IFS, son calcul est dynamique.

Le temporisateur de back-off est utilisé lorsqu'une ou plusieurs stations tente d'accéder au support alors que celui-ci est occupé ou qu'il y a eu des collisions. Pour accéder au support, ces stations attendent d'abord un DIFS. Si le support est toujours libre, elles attendent que le temporisateur de back-off expire. Ce temporisateur est calculé grâce à l'algorithme du même nom.

Cette variation opère sur la taille de la fenêtre de contention. Si cette taille est petite, la station virtuelle attend moins longtemps pour accéder au support par rapport à une station dont la taille de la fenêtre de contention est plus grande.

Pour chaque catégorie de trafic, la taille de la fenêtre de contention varie entre CWMIN [TCi] et CWMAX [TCi]. La formule permettant le calcul du temporisateur de back-off reste inchangée.

Lors d'une collision, un nouveau temporisateur est calculé. Cette fois, avec l'EDCA, on ne double pas la taille de la fenêtre de contention à chaque collision. La taille de la fenêtre de contention est calculée selon la formule suivante :

$CW_{new}\,[TCi] \geq (PF \times (CW_{old}\,[TCi] + 1)) - 1$

où PF (Persistent Factor) est le facteur persistant. Le paramètre PF est dépendant de la catégorie de trafic.

Si PF = 2, on retourne dans le mode DCF, où la fenêtre de contention est doublée après chaque collision, et l'on revient à l'algorithme de back-off exponentiel. Si PF = 1, la taille de la fenêtre de contention ne change pas. Ainsi, les catégories de trafic de priorités les plus hautes ont une valeur de PF plus petite comparées aux catégories de trafic de priorités les plus basses.

TxOP (Transmission Opportunities)

Une fois qu'une station accède au support et que son temporisateur de back-off expire, elle doit à nouveau retarder sa transmission. Comme expliqué précédemment, l'EDCA introduit un ordonnanceur de trafic, appelé TxOP (Transmission Opportunities), qui correspond à un temps fini dont la valeur est fonction de la classe de trafic utilisée.

Dans le cas où différentes catégories de trafic accèdent au support en même temps, c'est le TxOP qui détermine celle qui accède réellement au support en fonction de son niveau de priorité. Si deux classes de trafic voient leur temporisateur de back-off expirer au même instant, la valeur du TxOP détermine la classe de trafic qui peut émettre les données prioritairement. Étant donné que la classe de trafic de priorité la plus haute possède le TxOP le plus petit, c'est cette classe qui peut émettre en premier, respectant ainsi l'ordre des priorités.

Si une classe de trafic de priorité la plus haute (TC7) accède en même temps qu'une classe de trafic de priorité la plus faible (TC1) au TxOP, celui-ci favorise TC7, qui peut dès lors transmettre sur le support, et signifie à TC1 qu'une collision s'est produite. TC1 doit retransmettre ses informations en initiant l'algorithme de back-off avec ses paramètres caractéristiques : AIFS [TC1], CW[TC1] et PF[TC1].

En résumé, l'EDCA est la seule méthode d'accès qui permette d'affecter une certaine QoS au réseau Wi-Fi, même s'il n'empêche pas les collisions, obstacle majeur à la fourniture de services garantis. Par ailleurs, la classe de trafic de plus haute priorité utilise un AIFS égal au DIFS. Une classe de trafic TC7 ayant la même probabilité d'accéder au support qu'une station ne possédant pas ce mécanisme de QoS, certains paramètres de QoS ne peuvent donc être garantis. C'est pourquoi il est nécessaire de limiter l'accès au réseau aux stations 802.11e afin d'obtenir un vrai réseau Wi-Fi avec QoS.

802.11e ne spécifie pas non plus la manière dont sont choisies les applications qui ont la plus forte priorité et laisse cette tâche aux constructeurs. Le mapping le plus simple consisterait à affecter une des classes de trafic à un ou plusieurs numéros de port particulier. Chaque application possède un numéro de port permettant de le reconnaître au sein d'un flux de données. Malheureusement, cette notion de port est devenue assez obsolète depuis l'arrivée des réseaux peer-to-peer, qui utilisent des numéros de port dynamiques, voire des numéros de port déjà alloués, comme le port 80 pour HTTP, afin de passer outre les protections de type pare-feu des réseaux. On peut donc imaginer qu'un utilisateur puisse changer le numéro de port de son application afin que cette dernière passe en priorité sur un réseau Wi-Fi 802.11e.

IEEE 802.11f

La mobilité est une caractéristique essentielle d'un réseau sans fil. Elle permet aux utilisateurs du réseau de se déplacer à leur guise tout en maintenant leur communication en cours.

À l'origine, le standard 802.11 ne permettait pas de maintenir la communication lors d'un déplacement intercellulaire. Lucent, comme d'autres constructeurs, a développé un mécanisme apportant la mobilité au monde Wi-Fi. Ce protocole, appelé IAPP (Inter-Access Point Protocol), est déjà implémenté dans des équipements. Le groupe de travail IEEE 802.11f l'a désigné comme protocole de référence pour la gestion de la mobilité dans 802.11.

L'avenir de 802.11f

Le rôle premier de 802.11f est de permettre une interopérabilité entre points d'accès par le biais d'un mécanisme de gestion des handovers. Cet amendement n'est guère apprécié par les constructeurs du fait qu'il permettra l'utilisation de points d'accès hétérogènes dans un même réseau Wi-Fi. Les équipementiers proposent en effet des mécanismes de gestion des handovers propriétaires, qui nécessitent les mêmes points d'accès pour pouvoir fonctionner.

Dans Wi-Fi, une certaine mobilité n'est possible que si le réseau est en mode infrastructure. Dans le cas d'un réseau formé d'un seul BSS, c'est-à-dire d'une cellule unique contrôlée par un seul point d'accès, le point d'accès permet aux différentes stations d'avoir un service de mobilité restreint à la zone de couverture. Une fois la zone de couverture dépassée, aucune communication n'est possible. Pour un réseau en mode ad-hoc, la mobilité n'est possible que si les stations se voient.

Si le réseau est un ESS (Extended Service Set), c'est-à-dire un réseau composé d'un ensemble de BSS, les stations du réseau ont accès à une zone plus vaste. L'utilisation de certains mécanismes permet aux utilisateurs de se déplacer d'une cellule à une autre sans perte de communication.

Le standard 802.11 ne détaille pas ce mécanisme mais définit certaines règles de base, comme la synchronisation, l'écoute passive et active ou encore l'association et la réassociation, qui permettent aux stations de choisir le point d'accès le plus approprié pour communiquer.

Le groupe de travail 802.11f vise à standardiser un protocole permettant la gestion de la mobilité tout en apportant une certaine interopérabilité entre les points d'accès.

Synchronisation

Lorsque les stations se déplacent, c'est-à-dire lorsqu'elles changent de cellule ou qu'elles sont en mode économie d'énergie, elles doivent rester synchronisées pour pouvoir communiquer. Au niveau d'un BSS, les stations synchronisent leur horloge avec l'horloge du point d'accès.

Pour garder la synchronisation, le point d'accès envoie périodiquement une trame balise, ou Beacon Frame, qui contient la valeur d'horloge du point d'accès lorsque la transmission de cette trame a réellement lieu. Dès réception de cette trame, les stations mettent à jour leur horloge pour rester synchronisées avec le point d'accès. Les trames balises sont envoyés toutes les 32 µs. Cette période peut être toutefois configurable selon le matériel utilisé.

Association-réassociation

Lorsqu'une station entre dans un BSS ou un ESS, soit après une mise sous tension ou en mode veille, soit lorsqu'elle entre directement dans une cellule, elle doit choisir un point d'accès auquel s'associer. Le choix du point d'accès s'effectue selon différents critères,

tels que la puissance du signal, le taux d'erreur des paquets ou la charge du réseau. Si les caractéristiques du signal du point d'accès sont trop faibles, la station cherche un point d'accès plus approprié.

L'association, tout comme la réassociation, comporte les différentes étapes suivantes :

1. La station écoute le support.
2. Après avoir trouvé le meilleur point d'accès, elle s'authentifie.
3. Si cette phase réussit, la station s'associe avec le point d'accès et transmet ses données.

Le processus de réassociation est utilisé par une station qui veut changer de point d'accès. Bien qu'elle soit déjà associée à un point d'accès, la station essaye d'écouter le support afin de trouver un point d'accès ayant de meilleures caractéristiques. Si elle en trouve, la station se désassocie du point d'accès d'origine et se réassocie au nouveau point d'accès après s'être réauthentifiée.

L'écoute du support

Avant toute association avec un point d'accès, la station écoute le support sur tous les canaux radio inoccupés selon la réglementation en vigueur afin de découvrir les points d'accès disponibles.

Cette écoute peut se faire de deux manières différentes, active ou passive :

- **Écoute passive.** La station écoute sur tous les canaux de transmission et attend de recevoir une trame balise du point d'accès.
- **Écoute active.** Sur chaque canal de transmission, la station envoie une trame de requête (Probe Request Frame) et attend une réponse. Dès qu'un ou plusieurs points d'accès lui répond, elle enregistre les caractéristiques de ce dernier.

Une fois l'écoute terminée, la station trie les informations récupérées sur les points d'accès et choisit le plus approprié, essentiellement en fonction de la qualité du lien (rapport signal sur bruit).

L'authentification

Une fois le point d'accès choisi, la station doit s'authentifier auprès de lui.

Les deux mécanismes d'authentification suivants peuvent être utilisés pour cela :

- **Open System Authentication.** C'est le mode par défaut. Il ne fournit toutefois pas de réelle authentification car toutes les stations qui l'utilisent sont automatiquement authentifiées.
- **Shared Key Authentication.** Ce mécanisme d'authentification véritable n'est utilisé que si le protocole de sécurité WEP est implémenté sur le point d'accès et la station. Il s'appuie sur une clé secrète partagée, connue à la fois de la station et du point d'accès. Si la clé utilisée par la station est différente de celle du point d'accès, l'authentification échoue.

L'association

Dès qu'une station est authentifiée, elle peut s'associer avec le point d'accès. Elle envoie pour cela une trame de requête d'association, ou Association Request Frame, et attend que le point d'accès lui réponde pour s'associer.

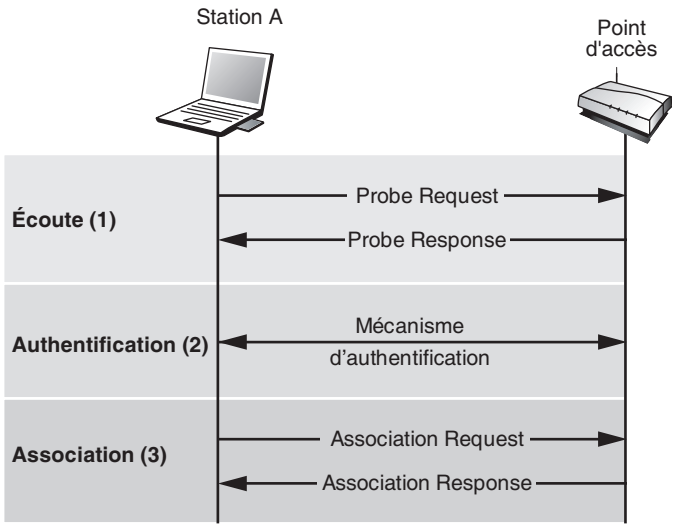
L'association se fait par le biais d'un identifiant, le SSID (Service Set ID). Cet identifiant est défini à la fois au niveau du point d'accès et des stations lorsqu'elles sont en mode infrastructure ou seulement au niveau des stations lorsqu'elles sont en mode ad-hoc. Le SSID définit en réalité le réseau lui-même, puisque c'est le nom du réseau. Il est périodiquement envoyé en clair par le point d'accès dans des trames balises dans toute la zone de couverture du réseau, ce qui permet aux stations en phase d'écoute de le récupérer.

Malheureusement, cette méthode présente une faille de sécurité, qui autorise n'importe qui à accéder au réseau. Une option permet cependant, au niveau du point d'accès, d'interdire la transmission du SSID dans les trames balises. Si la station n'est pas configurée correctement, avec le même SSID que le point d'accès, elle ne peut pas s'associer.

La figure O.7 illustre les étapes nécessaires que doit suivre une station pour s'associer à un point d'accès.

Figure O.7

Mécanisme d'association d'une station avec un point d'accès



Une fois la station associée avec le point d'accès, elle se règle sur le canal radio de ce dernier et peut commencer à transmettre et recevoir des données.

Périodiquement, la station surveille tous les canaux du réseau afin d'évaluer si un autre point d'accès ne possède pas de meilleures caractéristiques.

La réassociation

Le mécanisme de réassociation est similaire à celui décrit précédemment. Les réassociations s'effectuent lorsqu'une station se déplace physiquement par rapport au point d'accès d'origine, engendrant une diminution de la puissance du signal et entraînant une déconnexion.

Dans certains cas, les réassociations sont dues à des changements de caractéristiques de l'environnement radio ou à un trafic réseau trop élevé sur le point d'accès d'origine. Dans ce dernier cas, le standard fournit une fonction d'équilibrage de charge, ou load-balancing, qui répartit la charge de manière efficace au sein du BSS ou de l'ESS et évite les réassociations.

Les handovers

L'architecture d'un réseau sans fil peut comporter différentes cellules susceptibles de se recouvrir ou d'être disjointes. Dans un tel réseau, les utilisateurs sont généralement mobiles et doivent avoir la possibilité de se déplacer de cellule en cellule. Le déplacement intercellulaire, ou handover, ou encore handoff, est le mécanisme qui permet à tout utilisateur de se déplacer d'une cellule à une autre sans que la communication soit interrompue.

Cette technique est largement utilisée dans la téléphonie mobile. Lorsqu'on se déplace à pied, en voiture ou en train, la communication mobile n'est presque jamais coupée quand on passe d'une cellule à une autre.

La figure O.8 illustre un handover dans un réseau Wi-Fi. La station mobile connectée au point d'accès 1 doit, à un moment donné, s'associer au point d'accès 2. En d'autres termes, la communication qui passait par le point d'accès 1 doit, à un instant donné, passer par le nouveau point d'accès. La gestion du handover recouvre les mécanismes à mettre en œuvre pour réaliser la continuité de la communication, de sorte que le récepteur ne s'aperçoive pas que l'émetteur a changé de cellule.

Le standard d'origine ne supporte pas les handovers. Si une station se déplace dans un environnement couvert par de multiples points d'accès, et donc de multiples cellules, elle essaye de se connecter au point d'accès qui possède le meilleur signal. Cela assure à la station une bonne qualité du lien radio mais ne permet pas d'offrir la continuité de la communication dans un environnement cellulaire. Chaque fois qu'une station trouve un meilleur point d'accès, elle s'associe avec lui, toute communication en cours étant interrompue et non reprise par le nouveau point d'accès.

Le fait qu'il n'y ait pas de handover dans 802.11 est un facteur négatif pour le déploiement de ces réseaux et la vente des matériels correspondants. Certains constructeurs l'ont compris et n'ont pas attendu une éventuelle standardisation pour développer des protocoles de handover propriétaires. Pour en bénéficier, il faut que le réseau soit constitué d'équipements du même constructeur, ce qui présente d'autres contraintes. En l'absence de standard, il ne peut y avoir interopérabilité entre équipements de différents constructeurs.

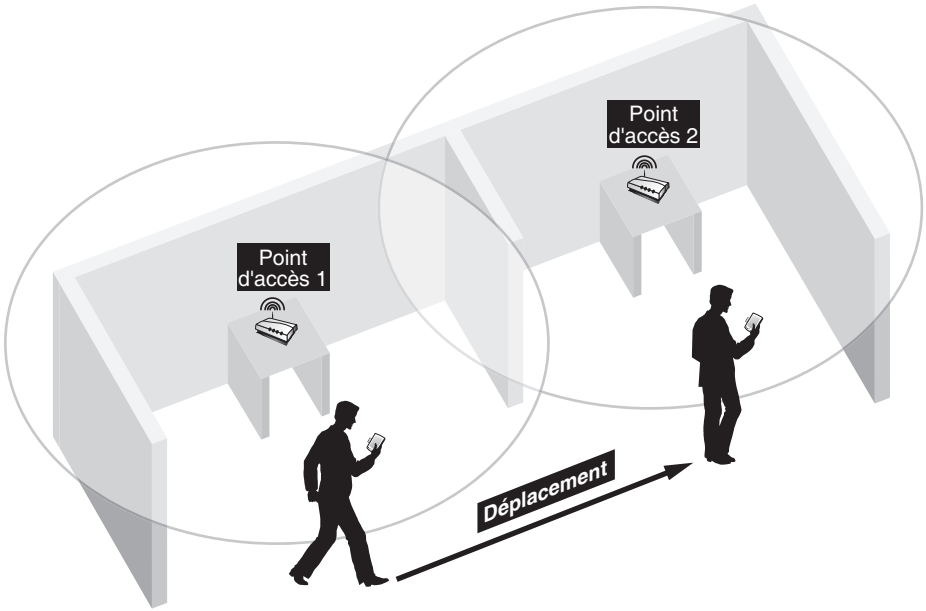


Figure O.8
Handover dans un réseau sans fil

IAPP (Inter-Access Point Protocol)

Comme expliqué précédemment, le groupe de travail 802.11f vise à la standardisation d'un protocole permettant de gérer les handovers et d'apporter ainsi l'interopérabilité entre des points d'accès de différents constructeurs. Le protocole retenu est l'IAPP (Inter-Access Point Protocol), développé à l'origine par Lucent.

IAPP fait communiquer les différents points d'accès d'un même réseau de façon à permettre à un utilisateur mobile de passer d'une cellule à une autre sans perte de connexion. Le seul lien entre les points d'accès du réseau étant le système de distribution (DS), c'est à ce niveau qu'est utilisé IAPP.

IAPP est un protocole de niveau transport (couche 4 du modèle OSI) qui se place au-dessus d'UDP (User Datagram Protocol). L'avantage d'utiliser UDP est que ce protocole de transport est sans connexion, à la différence de TCP (Transmission Control Protocol), les données étant envoyées directement.

Optionnel, IAPP ne fonctionne qu'avec les points d'accès qui l'implémentent. Il peut être désactivé à tout moment. Par ailleurs, aucun mécanisme de sécurité n'étant implémenté dans IAPP, cette tâche incombe au gestionnaire du système de distribution.

Le fonctionnement d'IAPP est illustré à la figure O.9.

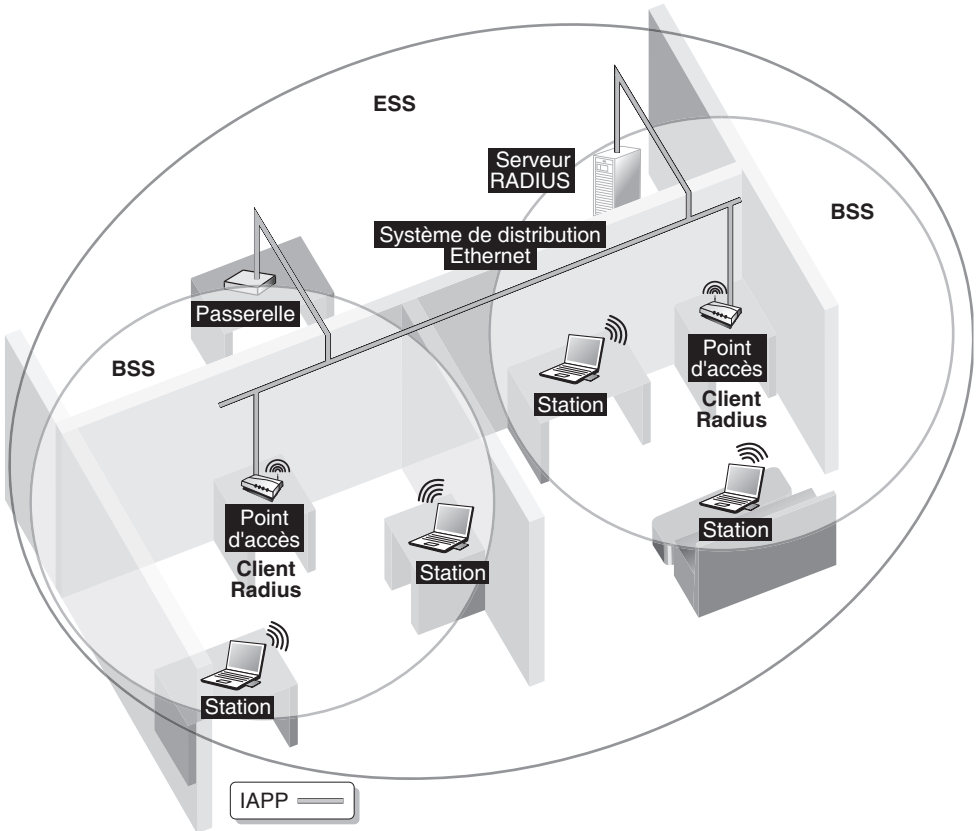


Figure O.9

Fonctionnement d'IAPP (Inter-Access Point Protocol)

Une caractéristique d'IAPP est qu'il définit l'utilisation du protocole client-serveur d'authentification RADIUS (Remote Authentication Dial-In User Server) afin d'offrir des handovers sécurisés. L'utilisation de ce protocole demande la présence d'un serveur centralisé ayant une vue globale du réseau. Le serveur RADIUS connaît la correspondance d'adresse entre l'adresse MAC des points d'accès et leur adresse IP. Par ailleurs, ce protocole permet de distribuer des clés de chiffrement entre points d'accès.

RADIUS est un protocole client-serveur, dans lequel le serveur est une entité se trouvant sur le système de distribution. Les clients ne sont pas les stations, mais les différents points d'accès du réseau. L'utilisation de RADIUS est optionnelle mais fortement conseillée, ne serait-ce que pour des raisons de sécurité.

IAPP ne résout pas la gestion de l'adressage des stations dans le réseau. L'utilisation de protocoles de niveau système de distribution, tels que DHCP (Dynamic Host Configuration Protocol) ou IP Mobile, est donc fortement recommandée.

Le protocole IAPP définit deux types de mécanismes, la configuration des points d'accès et les handovers proprement dits.

Configuration des points d'accès

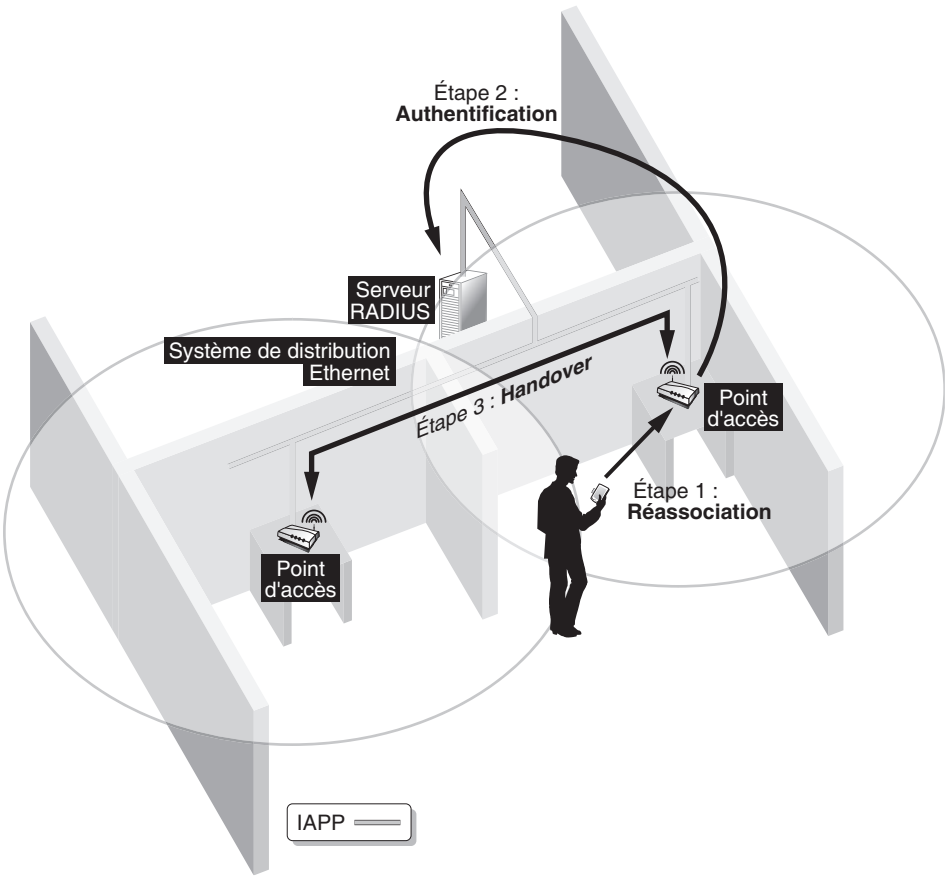
Le mécanisme de configuration permet d'instaurer un certain dialogue avec les points d'accès du réseau. Lorsqu'un nouveau point d'accès est installé, il informe les autres de sa présence et leur envoie des informations concernant sa configuration. De la sorte, tous les points d'accès se connaissent et peuvent s'échanger des attributs de configuration, voire les négocier.

Le mécanisme de handover

Un handover se produit chaque fois qu'une station passe d'une cellule à une autre. Pour cela, elle doit se réassocier avec le point d'accès contrôlant cette cellule. C'est la réassociation qui initie le mécanisme de handover.

La figure O.10 illustre le mécanisme de handover d'IAPP.

Figure O.10
Le mécanisme de handover d'IAPP



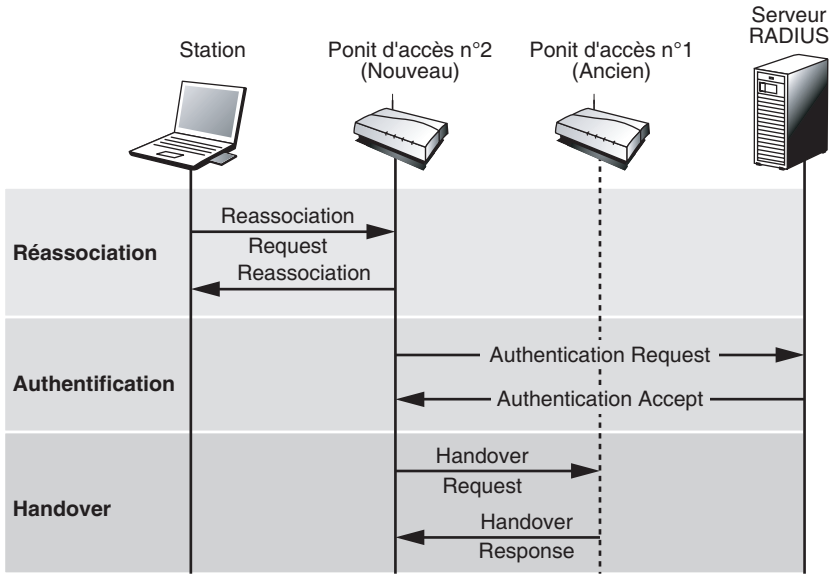
Dans les échanges d'informations entre le nouveau point d'accès et la station, le nouveau point d'accès connaît l'adresse de l'ancien. Il peut dès lors commencer à dialoguer avec celui-ci.

Avant tout handover, une authentification est nécessaire. L'utilisation de RADIUS entraîne une nouvelle phase d'authentification, qui se produit après chaque réassociation avec un nouveau point d'accès. La station envoie des informations au serveur par l'intermédiaire du point d'accès. Le serveur les vérifie, et, si les données sont correctes, authentifie la station auprès de ce point d'accès. Une fois authentifié, le nouveau point d'accès entre dans la phase de handover.

Pendant cette phase, le nouveau point d'accès envoie une requête à l'ancien par l'intermédiaire du système de distribution. L'ancien point d'accès lui répond et lui transmet toutes les informations nécessaires concernant la station. Ce processus est illustré à la figure O.11.

Figure O.11

Phase de négociation du handover



Une fois cette phase terminée, la station possède les paramètres réseau corrects et peut de la sorte soit continuer une communication, soit en commencer une nouvelle.

Économies d'énergie

Les réseaux sans fil peuvent être composés de stations fixes ou mobiles. Les stations fixes n'ont aucun problème d'économie d'énergie puisqu'elles sont directement reliées au réseau électrique. Les stations mobiles sont alimentées par des batteries, qui n'ont généralement qu'une faible autonomie (quelques heures selon l'utilisation).

Pour utiliser au mieux ces stations mobiles, le standard définit deux modes d'énergie, Continuous Aware Mode et Power Save Polling Mode :

- **Continuous Aware Mode.** C'est le mode de fonctionnement par défaut. L'interface Wi-Fi est tout le temps allumée et écoute constamment le support. Il ne s'agit donc pas d'un mode d'économie d'énergie.
- **Power Save Polling Mode.** C'est le mode d'économie d'énergie. Dans ce mode, le point d'accès tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie et stocke les données qui leur sont adressées dans un élément appelé TIM (Traffic Information Map).

Comme expliqué à la section précédente, les stations d'un BSS sont toutes synchronisées. Cette synchronisation, qui s'effectue par le biais des trames balises, permet d'établir le mécanisme d'économie d'énergie.

Les stations en veille s'activent à des périodes de temps régulières pour recevoir une trame balise contenant le TIM envoyé en broadcast par le point d'accès. Entre les trames balises, les stations retournent en mode veille. Du fait de la synchronisation, une trame balise est envoyée toutes les 32 µs. Toutes les stations partagent le même intervalle de temps pour recevoir les TIM et s'activent de la sorte au même moment pour les recevoir.

Les TIM indiquent aux stations si elles ont ou non des données stockées dans le point d'accès. Lorsqu'une station s'active pour recevoir un TIM et qu'elle s'aperçoit que le point d'accès contient des données qui lui sont destinées, elle lui envoie une trame de requête (PS-Poll) pour mettre en place le transfert des données. Une fois le transfert terminé, la station retourne en mode veille jusqu'à réception de la prochaine trame balise contenant un nouveau TIM.

Le mécanisme d'économie d'énergie ne peut être utilisé qu'au niveau des stations, lesquelles choisissent de l'utiliser ou non. Le fait d'utiliser ce mécanisme peut faire chuter les performances globales de débit du réseau de 20 à 30 %.

P

Annexe du chapitre 22 (VLAN et VPN)

Cette annexe introduit les VPN IP en commençant par les VPN personnels et les VPN de groupe avec identification du trafic. Elle examine ensuite les VPN des réseaux en mode avec connexion, c'est-à-dire les réseaux dans lesquels un paquet ne peut être envoyé qu'après une négociation avec le terminal distant. Les VPN des réseaux ATM et MPLS sont étudiés plus en détail à la section suivante.

Les VPN IP

Les VPN peuvent être implémentés selon six modèles différents. La figure P.1 illustre ces différents modèles. Parmi les nœuds, on trouve les équipements terminaux (End ou End Systems), les CE (Customer Edge) et les PE (Provider Edge). CE et PE sont généralement des routeurs qui se trouvent chez le client ou l'opérateur.

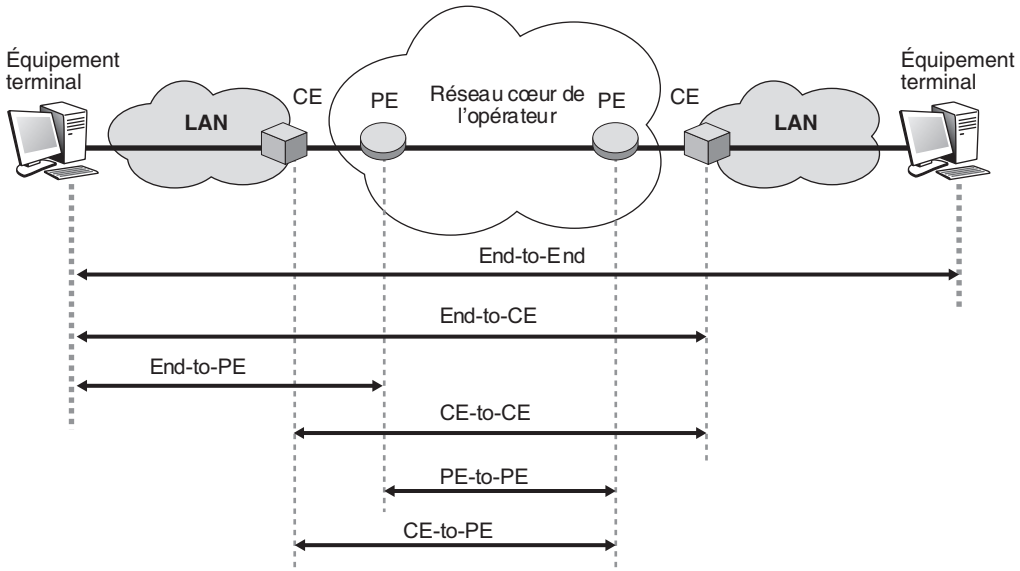


Figure P.1

Les six modèles de VPN

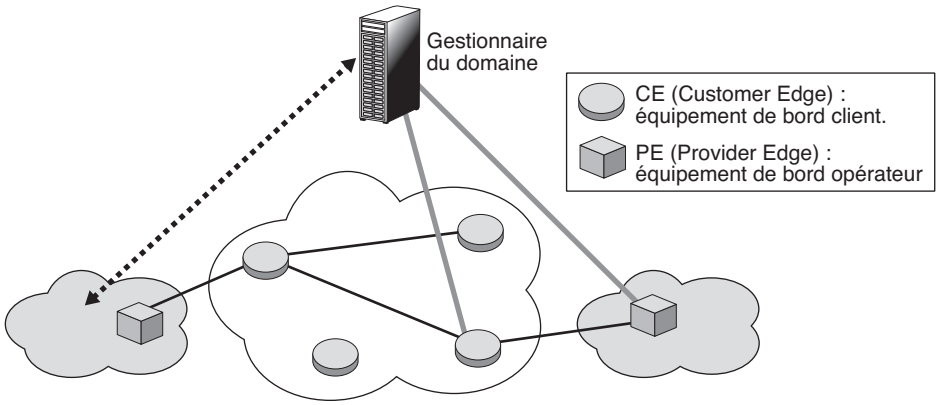
Parmi ces modèles, le cas du bout-en-bout (End-to-End) n'est pas applicable dans le cadre de la négociation de SLS avec un opérateur. Dans la suite de cette section, nous avons regroupé les modèles End-to-CE et End-to-PE dans la partie VPN personnels. Les modèles CE-to-CE, CE-to-PE et PE-to-PE sont regroupés dans la partie VPN de groupe.

VPN personnel (End-to-CE ou End-to-PE)

Le VPN personnel commence au niveau d'un terminal et prend fin au CE du LAN distant, dans lequel se trouvent les équipements terminaux, ou au PE, qui peut se situer dans un PoP (Point of Presence) de l'opérateur. Un équipement de VPN, associé à des fonctionnalités de VPN, disponible dans un CE ou dans un PE est responsable de l'application de services de sécurité entre lui et les équipements terminaux. L'approche End-to-PE peut éviter le besoin de déployer des matériels de VPN ou des fonctionnalités identiques dans le réseau du client. La plupart des VPN personnels sont implémentés selon le modèle End-to-CE.

Considérons un utilisateur distant qui demande la mise en place d'un VPN d'accès distant selon un certain niveau de service auprès du CE ou de l'opérateur du PE. Une négociation peut être mise en place entre le terminal et l'opérateur. Si cette négociation se finalise par un accord d'un certain niveau de service, l'activation du service n'est effective qu'après configuration de l'équipement terminal et du CE ou du PE. Ce schéma de fonctionnement est décrit à la figure P.2.

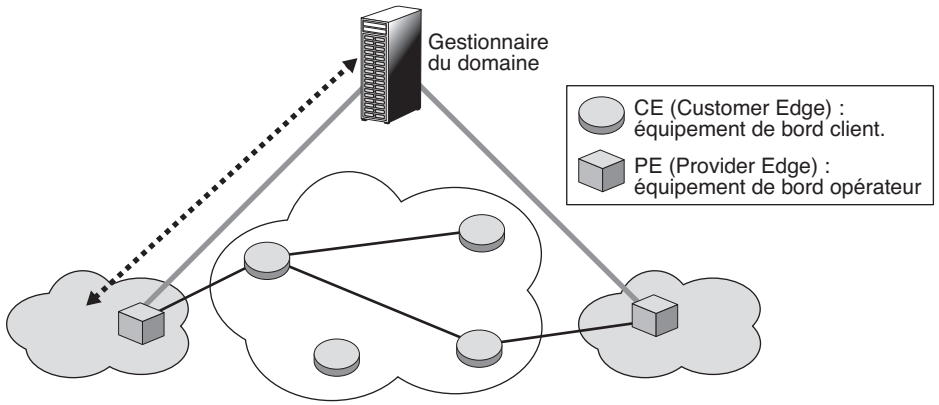
Figure P.2
Schéma de fonctionnement d'un VPN personnel



VPN:de groupe (CE-to-CE, CE-to-PE, PE-to-PE)

Avec un VPN de groupe, pour appliquer des services de sécurité, les équipements terminaux utilisent les équipements de VPN situés dans le périmètre du réseau d'entreprise (CE-to-CE ou CE-to-PE) ou dans le réseau de l'opérateur (CE-to-PE ou PE-to-PE). De cette façon, aucune fonction de sécurité n'a besoin d'être implémentée sur les terminaux. L'implémentation de services de sécurité leur est complètement transparente.

Figure P.3
Schéma de fonctionnement d'un VPN de groupe



Dans le cas d'une négociation intradomaine, par exemple CE-to-CE, les CE sont gérés par un même opérateur. La négociation du SLS a lieu entre un client situé au niveau d'un réseau d'entreprise et l'opérateur. Si nous prenons l'exemple d'un client situé dans le réseau d'entreprise de gauche de la figure P.3, le trait en pointillé indique la négociation du SLS pour un VPN à mettre en place entre le CE du réseau de gauche et le CE du réseau de droite.

Une fois la négociation terminée avec succès, l'opérateur peut mettre en place le service demandé en appliquant directement les politiques de sécurité adéquates sur les deux CE. Ce cas s'applique de façon similaire aux modèles CE-to-PE et PE-to-PE.

Le cas d'une négociation interdomaine, par exemple CE-to-CE, est illustré à la figure P.4. Les CE étant gérés par deux opérateurs différents, la négociation a lieu en plusieurs phases. La première phase de négociation se passe entre le client situé au niveau d'un réseau d'entreprise et l'opérateur qui gère son CE.

Prenons l'exemple d'un client situé dans le réseau d'entreprise de gauche. Le trait en pointillé sur la gauche de la figure indique la négociation du SLS pour un VPN à mettre en place entre le CE du réseau de gauche et le CE du réseau de droite. Une fois cette demande de négociation reçue, l'opérateur de gauche s'aperçoit qu'il ne gère pas le CE distant. Dès lors, il retransmet la demande de négociation du SLS à l'opérateur qui gère le CE distant (les pointillés du centre de la figure). Ce dernier traite la demande de négociation de service.

Deux situations se présentent alors :

- Si l'opérateur de droite l'accepte, une réponse favorable est transmise à l'opérateur de gauche puis au client initiateur de la demande. Les deux opérateurs transmettent les politiques adéquates à leur CE respectif, et ces derniers appliquent les politiques de sécurité.
- Si l'opérateur de droite refuse la négociation, deux possibilités se présentent :
  - L'opérateur distant (de droite) refuse catégoriquement la demande de négociation de service. Une réponse négative est transmise à l'opérateur de gauche puis au client. Le SLS ne peut être appliqué.
  - Le niveau de service demandé n'est pas applicable. Une renégociation du niveau du service de sécurité se met en place.

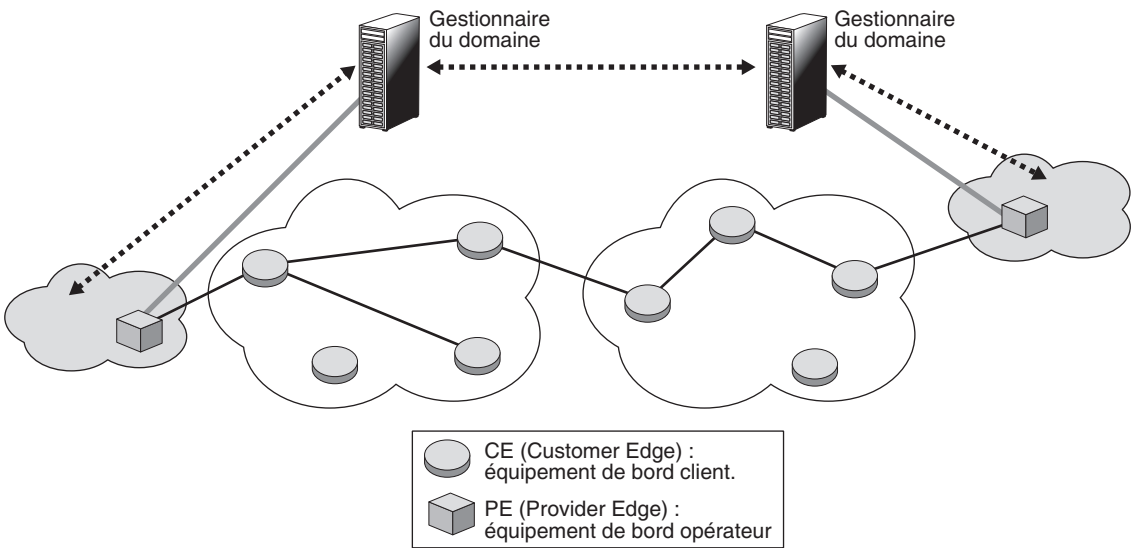


Figure P.4

Cas d'une négociation interdomaine

Identification du trafic

L'identification du trafic à sécuriser a lieu au point d'entrée de l'association de sécurité, ou SA (Security Association), IPsec. Cette information est stockée dans la base de données des politiques de sécurité SPD (Security Policy Database). À l'émission, une fois identifié, le trafic est encapsulé dans l'association de sécurité SA associée. Une SA est une connexion unidirectionnelle, ou simplex, qui apporte les services de sécurité au trafic qu'elle transporte. Deux SA sont nécessaires pour sécuriser une communication bidirectionnelle traditionnelle, une pour chaque direction. Dans ce cas, une identification du trafic à sécuriser a lieu au niveau des deux nœuds entre lesquels les SA sont mises en place.

Dans la réalité, le trafic à sécuriser entre deux points peut ne concerner que le trafic dans un sens, c'est-à-dire le trafic entrant ou sortant. On peut citer l'exemple d'un sous-réseau commercial dont la politique de sécurité est d'assurer le cryptage d'images en haute résolution à destination de ses clients. Dans ce cas, seuls les paquets IP sortants sont concernés. Les paquets IP entrants ne demandent aucune forme de cryptage. Dans ce cas, le client négocie auprès de son opérateur un niveau de service de sécurité pour le SA sortant. Aucun SA entrant n'est mis en place.

Les paramètres qui identifient le trafic à sécuriser, en unidirectionnel comme en bidirectionnel, sont les suivants :

- Adresse IP source (IPv4 ou IPv6) : peut être une adresse unique unicast, anycast ou broadcast (pour IPv4), un groupe multicast, une gamme d'adresses (valeurs inférieure et supérieure, adresse + masque de l'adresse) ou encore une adresse wildcard, c'est-à-dire une adresse réservée pour un invité.
- Adresse IP destination (IPv4 ou IPv6) : peut être une adresse unique unicast, anycast ou broadcast (pour IPv4), un groupe multicast, une gamme d'adresses (valeurs inférieure et supérieure, adresse + masque) ou une adresse wildcard.
- Nom : peut être un identifiant d'utilisateur ou un nom de système en fonction de la nature du nœud qui supporte IPsec. Le nom de système doit être applicable dans tout type de nœud IPsec. On peut se contenter d'un identifiant d'utilisateur au niveau des équipements terminaux, ainsi qu'au niveau des routeurs supportant IPsec pour le traitement du trafic entrant.

L'identifiant d'utilisateur et le nom de système peuvent être des noms d'utilisateur DNS ou des noms X.500.

Les réseaux en mode avec connexion

Les réseaux d'opérateurs sont généralement en mode avec connexion, la mise en place d'un chemin permettant de contrôler au mieux les ressources et de garantir la qualité de service. Au cours des années 1980, les opérateurs de télécommunications ont beaucoup utilisé les circuits, non seulement pour la téléphonie mais également pour les données. La première évolution après la commutation de circuits pure a été le RNIS (Réseau numérique à intégration de services), qui utilise le circuit aussi bien pour la parole téléphonique que pour le transfert de paquets.

Les opérateurs sont ensuite passés à la commutation de paquets sur des circuits virtuels. Les réseaux X.25 comme Transpac ont connu un grand succès dans les années 1980 et 1990. Ils étaient les premiers réseaux en mode avec connexion à permettre un partage des ressources entre tous les paquets acheminés dans le réseau. Les réseaux en relais de trames ont pris le relais. Ces réseaux ont à peu près les mêmes propriétés que les réseaux X.25, si ce n'est qu'au lieu de se servir de circuits virtuels au niveau 3, ils ouvrent des liaisons virtuelles de niveau 2, beaucoup plus simples et moins onéreuses. Ces liaisons virtuelles de niveau 2 permettent en outre de ne pas décapsuler les trames lors des traversées des nœuds de commutation, au contraire des réseaux X.25.

Après le relais de trames, les opérateurs ont choisi la technique de transfert ATM pour proposer des services avec garantie aux utilisateurs. Les réseaux ATM étant des réseaux de commutation de niveau trame, ils sont puissants et peuvent prétendre à des débits importants. Cette technologie a connu un grand succès sans toutefois réussir à s'imposer en raison de son système de signalisation, à la fois spécifique et relativement complexe. Cette complexité provient du choix qui a été fait d'étendre les signalisations précédentes, en particulier celle provenant du RNIS. De surcroît, l'UIT-T s'est trouvée dans l'incapacité de normaliser une interface standard que les équipementiers auraient pu intégrer dans les équipements de réseau. De ce fait, la technologie ATM n'a jamais pu s'imposer sur l'interface utilisateur, où elle a été supplantée par Ethernet et son allié de toujours IP. N'ayant pu s'imposer complètement, la technologie ATM a été remplacée par MPLS. La raison essentielle de cette nouvelle donne est l'introduction d'une signalisation permettant de mettre en place les chemins simplement avec une signalisation IP, puisque IP est un réseau de routage aux adresses universelles.

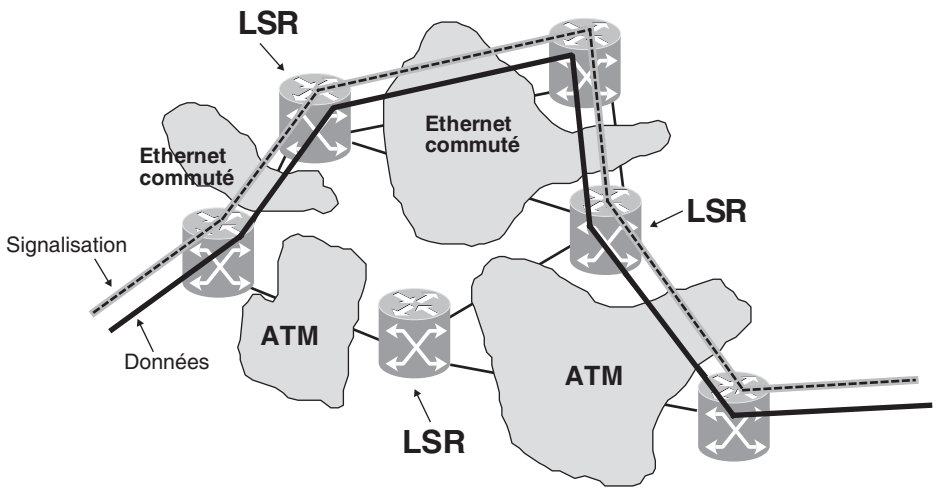
La technologie MPLS permet d'utiliser les anciens réseaux introduisant de la qualité de service, comme ATM. Le passage d'ATM à MPLS ne pose donc pas vraiment de problème. L'avantage de cette solution MPLS est l'utilisation d'un réseau de signalisation fondé sur IP, assez simple à mettre en œuvre. MPLS peut également utiliser des réseaux Ethernet à partir du moment où Ethernet emploie le mode commuté introduit avec le shim-label.

La figure P.5 illustre la traversée de plusieurs réseaux spécifiques formant un réseau MPLS afin d'illustrer la transition entre les réseaux de génération ATM et MPLS. La signalisation IP met en place un chemin de la façon suivante :

1. Lorsque le paquet de signalisation arrive au premier nœud, la technique de routage permet de déterminer le routeur suivant à atteindre après la traversée du réseau ATM. La traversée du réseau ATM par la signalisation est classique : un circuit virtuel ATM est ouvert en indiquant l'adresse ATM du routeur suivant, qui est obtenue par une traduction de l'adresse IP en une adresse ATM.
2. Une fois ouvert, le circuit virtuel ATM permet de transporter les différents fragments du paquet de signalisation, qui est reformé au nœud suivant.
3. Les fragments sont réassemblés au routeur suivant grâce à la couche AAL.
4. De nouveau, une fois déterminé le routeur suivant, il faut ouvrir un circuit virtuel ATM pour y transporter le paquet de signalisation IP.

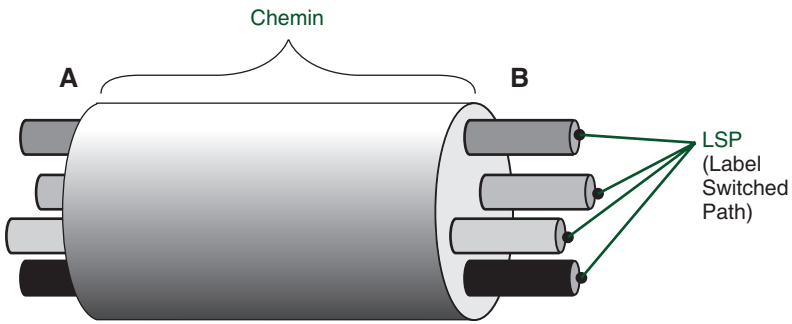
5. De même, pour traverser le réseau Ethernet, un chemin est mis en place, sur lequel les trames Ethernet sont commutées grâce aux références de type shim-label.

Figure P.5
Réseau MPLS de transition



La figure P.6 représente un réseau MPLS de façon conceptuelle. Les opérateurs n'attendent pas l'arrivée d'un client pour ouvrir un LSP mais l'ouvrent dès l'initialisation du réseau. De la sorte, lorsqu'un client se présente, il suffit de regarder l'adresse de sortie du réseau à partir de son adresse IP de destination et d'affecter le client au LSP approprié. Par exemple, entre les deux interfaces A et B, quatre circuits virtuels peuvent proposer un service EF, deux services AF, comme Gold et Bronze, et un service best-effort. Bien d'autres solutions peuvent être mises en œuvre pour affecter les chemins à des services particuliers. Par exemple, à chaque LSP pourrait correspondre une application particulière.

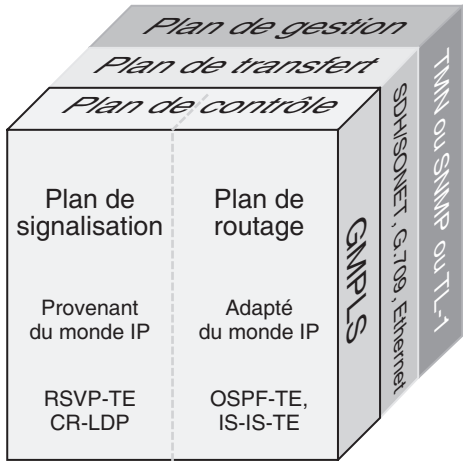
Figure P.6
Représentation conceptuelle d'un réseau MPLS



La figure P.7 représente un cas simple. Dans la réalité, MPLS fait appel à une solution de signalisation formant des FEC (Forwarding Equivalence Class). Toutes les communications qui ont une même destination se rassemblent sur un même circuit virtuel. Au

lieu d'être point-à-point, le chemin se présente sous la forme d'un arbre, dont la racine se trouve chez le destinataire et les feuilles chez les émetteurs.

Figure P.7
Architecture de GMPLS



Les réseaux MPLS seront eux-mêmes remplacés peu à peu par des réseaux GMPLS (Generalized MPLS), qui forment un surensemble de MPLS introduisant des techniques de commutation supplémentaires. L'architecture de GMPSL est illustrée à la figure P.7. Le plan de gestion utilise des standards classiques, comme SNMP ou le TMN de l'UIT-T. Le plan de transfert est issu principalement de l'UIT-T et de l'IEEE, avec SONET/SDH, G.709 et la commutation Ethernet. Le plan de contrôle provient quant à lui de l'IETF et comporte deux parties, le plan de signalisation, avec pour principaux protocoles RSVP-TE (Traffic Engineering) et CR-LDP (Constraint-based Routing/Label Distribution Protocol), et le plan de routage, avec pour principaux algorithmes de routage OSPF-TE (Traffic Engineering) et IS-IS-TE.

Les réseaux partagés

Les réseaux des opérateurs doivent être partagés entre les clients de telle sorte que chaque client puisse croire qu'il est seul à utiliser les ressources mises à sa disposition par l'opérateur et puisse avoir confiance dans la capacité de l'opérateur à sécuriser ses communications.

De ces principes sont nés les réseaux privés virtuels. Un réseau privé virtuel, ou VPN, est, du point de vue de l'entreprise cliente, un ensemble de réseaux de site reliés par un réseau d'opérateur garantissant une forte sécurité des communications. En particulier, aucun autre client que le personnel de l'entreprise ne peut y accéder de l'extérieur.

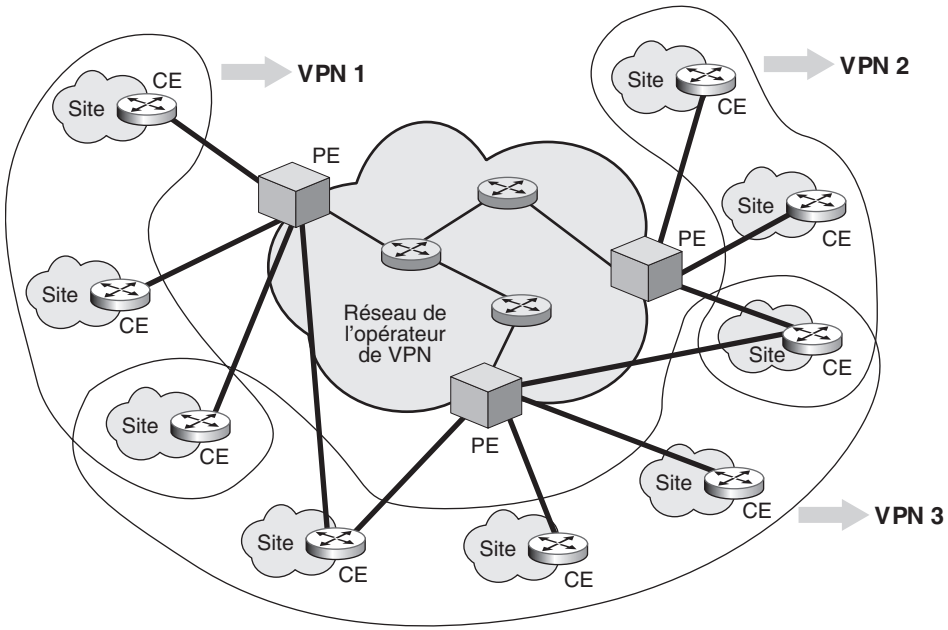
Du point de vue de l'opérateur, un VPN est un réseau dont les ressources sont partagées entre les différentes entreprises clientes de telle sorte que chaque client ait l'impression d'avoir un réseau dédié et non partagé. Pour l'opérateur, l'avantage de cette solution est énorme. Lorsque les entreprises n'utilisent les ressources qui leur sont affectées que

pendant un temps restreint, l'opérateur peut les réaffecter au fur et à mesure des besoins réels des autres entreprises clientes. En d'autres termes, nous avons un multiplexage statistique des équipements logiciels et matériels. Si la probabilité de manquer de ressources est parfaitement calculée, de façon à demeurer infime, le gain financier pour l'opérateur est très important.

Pour garantir le partage, il faut que le réseau se prête à une ingénierie simple, d'où le choix de MPLS et GMPLS.

Une structure de réseau VPN MPLS est illustrée à la figure P.8, dans laquelle trois VPN d'entreprise sont représentés. Un VPN MPLS est un ensemble de chemins, ou LSP, d'un réseau MPLS dédiés aux entreprises se connectant en VPN. Ces VPN d'entreprise sont connectés au réseau de l'opérateur par des points d'accès, ou PE (Provider Edge), appartenant à l'opérateur. Les réseaux d'entreprise sont raccordés au PE par un équipement CE (Customer Edge). Nous avons examiné ces éléments à la section précédente. Sur la figure P.8, on voit que certains sites peuvent appartenir à plusieurs VPN simultanément.

Figure P.8
Trois VPN d'entreprise sur un réseau d'opérateur

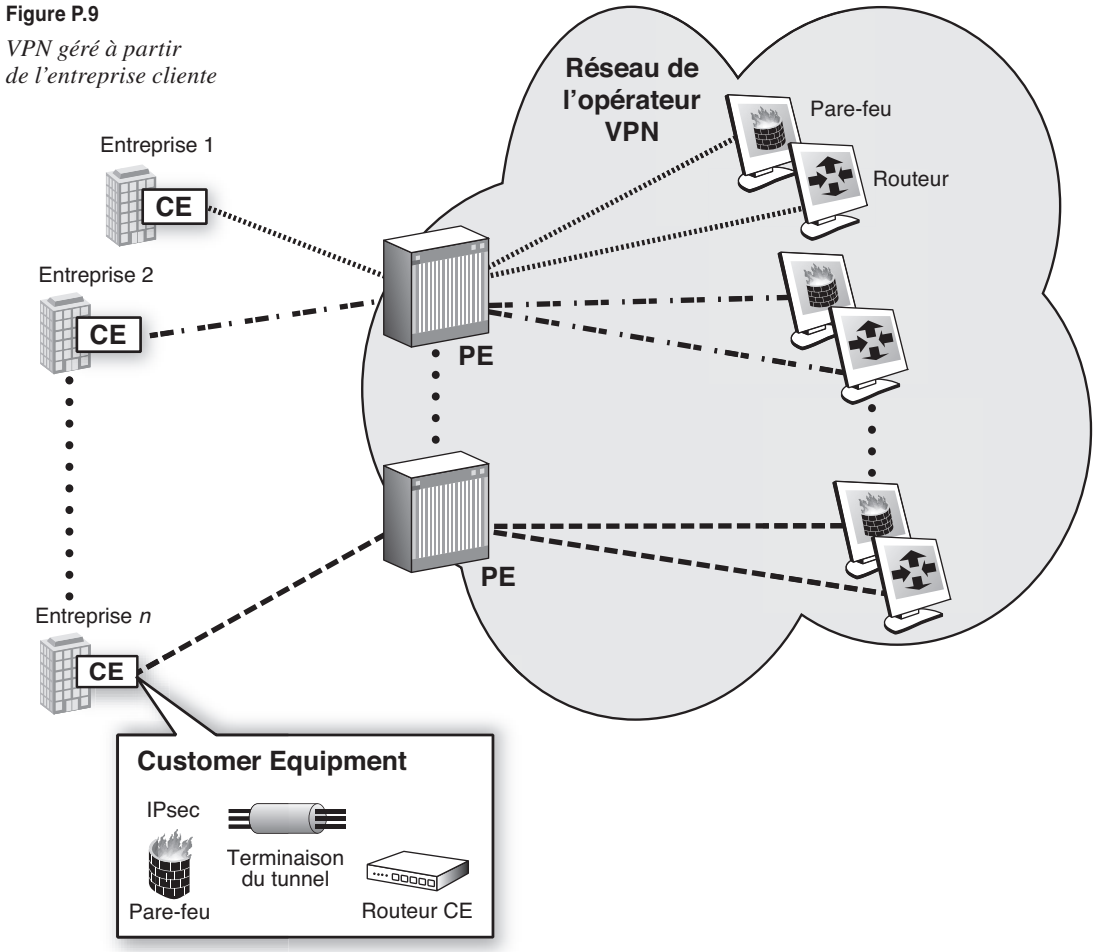


Les routeurs extrémité PE et CE peuvent gérer différents types de services. Le plus important pour les entreprises est la sécurité. Le VPN peut être sécurisé en chiffrant les paquets entrants dans le réseau de l'opérateur. Ce chiffrement peut s'effectuer dans le routeur extrémité de l'opérateur ou de l'entreprise. Bien que les opérateurs présentent cette solution comme une valeur ajoutée à leur offre de VPN, beaucoup d'entreprises préfèrent gérer elles-mêmes leur sécurité et chiffrer les données à l'entrée et à la sortie de leurs sites, en dépit du coût induit.

D'autres fonctionnalités peuvent être prises en charge par l'opérateur, notamment la qualité de service, la gestion de la mobilité ou d'autres types de services de sécurité que la simple confidentialité. Pour cela, la structure du VPN peut avoir son importance.

Deux structures de VPN MPLS peuvent être mises en place : un VPN selon le modèle overlay et un VPN selon le modèle peer. Dans le modèle overlay, les LSP sont ouverts directement de site à site, tandis que, dans le modèle peer, le routeur de bord se trouve chez l'opérateur. Dans le premier cas, les LSP sont ouverts directement entre CE, de telle sorte que le VPN de l'opérateur ne fasse que multiplexer les LSP sur son propre réseau. Le réseau de l'opérateur ne peut apporter de forte valeur ajoutée puisque l'information est chiffrée chez l'utilisateur. Dans le second cas, l'opérateur a à sa charge la gestion des extrémités des LSP et peut effectuer un multiplexage de plusieurs flots d'entreprise dans des LSP communs, garantissant au réseau de l'opérateur la scalabilité, ou passage à l'échelle.

Figure P.9
VPN géré à partir de l'entreprise cliente



La figure P.9 illustre le premier cas de figure, où le VPN démarre dans l'équipement extrémité, ou CE, de l'entreprise. Ce dernier gère les fonctionnalités de routeur, de sécurité IPsec, de terminaison de tunnel IPsec et de pare-feu mais peut aussi gérer des logiciels antivirus, antispam, etc. Le routeur PE de l'opérateur peut également jouer le rôle de pare-feu mais en proportion très limitée puisque les flots du client sont chiffrés. Seuls les paquets de gestion et de contrôle peuvent être vérifiés à ce niveau.

Cette solution revient relativement chère à l'entreprise, car elle doit gérer elle-même toutes les fonctionnalités de l'interconnexion de réseau.

La figure P.10 illustre un VPN géré par l'opérateur. Cette solution est beaucoup plus flexible puisque les équipements de routage, de pare-feu, de gestion d'IPsec, etc., sont partagés par les clients connectés au routeur PE.

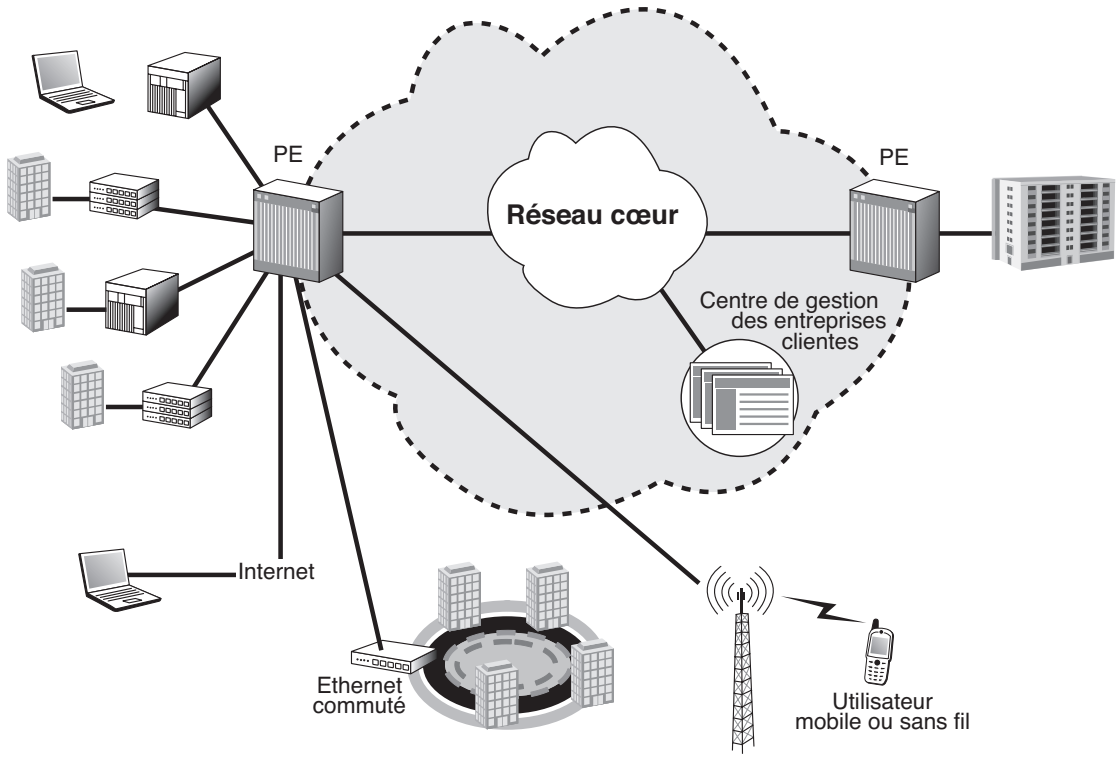


Figure P.10
VPN géré par l'opérateur

On voit que les machines de l'entreprise peuvent être connectées au routeur extrémité PE par un très grand nombre de solutions, alors que, dans la technique de raccordement au routeur CE, il faut que les matériels de l'entreprise soient connectés directement à l'entreprise. Dans la solution de gestion opérateur, les connexions peuvent s'effectuer par des

lignes *x*DSL, des liaisons spécialisées, des réseaux en relais de trames ou ATM ou même par des accès *via* des FAI permettant la connexion de terminaux mobiles ou sans fil. Des connexions Ethernet directes sont également possibles.

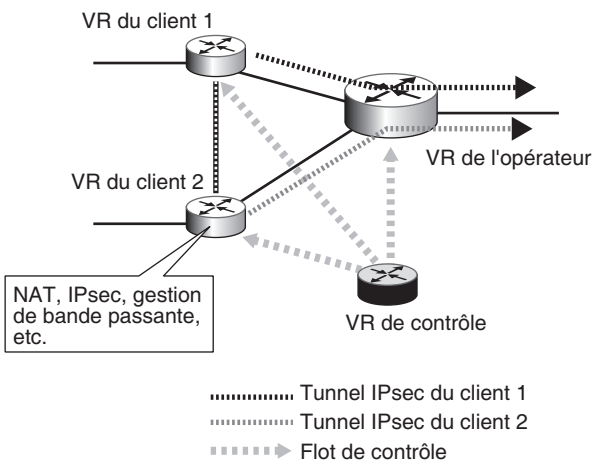
L'opérateur peut offrir des services supplémentaires, comme la gestion des équipements de l'entreprise cliente à partir de serveurs situés dans son réseau. Des services de gestion de messagerie électronique, d'impression, de gestion de logiciels ou de programmes métier peuvent être proposés à partir du réseau de l'opérateur. Cette solution apporte un gain à la fois au client et à l'opérateur. Le client n'a plus à gérer de façon privée un ensemble d'équipements. Il a de surcroît la possibilité de se connecter beaucoup plus facilement à ses sites par le biais de FAI intermédiaires et d'ajouter des clients mobiles ou nomades. Pour l'opérateur, le gain statistique est toujours le maître mot. Il est obtenu en partageant des équipements entre plusieurs clients.

Une autre solution qui se développe consiste, pour l'opérateur, à faire appel à des routeurs virtuels, ou VR (Virtual Router). Cette solution est illustrée à la figure P.11. Un routeur virtuel est l'équivalent d'un routeur matériel, mais avec ses propres algorithmes de routage et la possibilité de mettre en œuvre des fonctionnalités telles que NAT ou DHCP, des gestionnaires de bande passante, etc. Un routeur virtuel est donc un logiciel en technologie objet susceptible d'être implémenté sur une machine de sortie de l'entreprise ou plus généralement sur l'équipement PE de connexion de l'opérateur. Les fonctionnalités supplémentaires se présentent sous la forme d'objets spécifiques, qui peuvent être mis en route ou non. Plusieurs routeurs virtuels peuvent être créés à l'intérieur d'un même équipement. Si le routeur virtuel est situé sur le PE de l'opérateur, chaque client peut disposer de son propre routeur, avec ses propres fonctionnalités, même si, physiquement, l'équipement de réseau PE est unique.

L'opérateur peut agréger les flots sortant des différents routeurs virtuels sur des LSP uniques de façon à permettre la scalabilité de son réseau. L'opérateur possède un contrôleur de routeurs virtuels pour effectuer les modifications de configuration et la gestion du logiciel.

Figure P.11

Réseau d'opérateur à routeurs virtuels



Q

Annexe du chapitre 23 (La gestion et le contrôle de réseau)

La première partie de cette annexe apporte des précisions supplémentaires sur la gestion ISO et plus particulièrement sur la gestion système CMIS/CMIP. Elle aborde ensuite la gestion de réseaux à base de politiques, qui a été très à la mode dans les années 2000, mais qui perd de son intérêt avec les réseaux autonomiques. Cette partie s'achève par des compléments sur les SLA (Service Level Agreement).

La seconde partie de cette annexe est consacrée à la qualité de service, dont elle vise à donner une définition exacte. Elle détaille en outre les contrôles de flux dans le relais de trames et la commutation ATM, ainsi que la signalisation H.323, qui a été la principale signalisation de niveau application, avec une focalisation sur la parole téléphonique. La signalisation des « appliances » intermédiaires est ensuite abordée, avec le protocole MGCP, puis les signalisations COPS (Common Open Policy Service), qui permet de configurer un réseau de façon automatique, et CCITT n° 7.

Gestion ISO

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

Ces informations se présentent sous la forme d'objets dont la syntaxe est normalisée sous le nom d'ASN.1. D'autres choix auraient pu être faits, comme une entité de gestion,

à chaque niveau de la hiérarchie ISO, capable de prendre les décisions de gestion de ce niveau, mais tel n'est pas le cas. En outre, toutes les informations de gestion sont mémorisées dans une base de données, appelée MIB (Management Information Base). Cette MIB est, d'une part, remplie par les informations provenant des couches de protocoles à gérer et, d'autre part, consultée par le processus de gestion SMAP. L'entité SMAE récupère les informations demandées par le SMAP par une interface nommée SMI (System Management Interface). Cette architecture est illustrée à la figure Q.1, qui montre également la gestion de couche qui s'effectue, avec des processus de gestion associés à chaque couche.

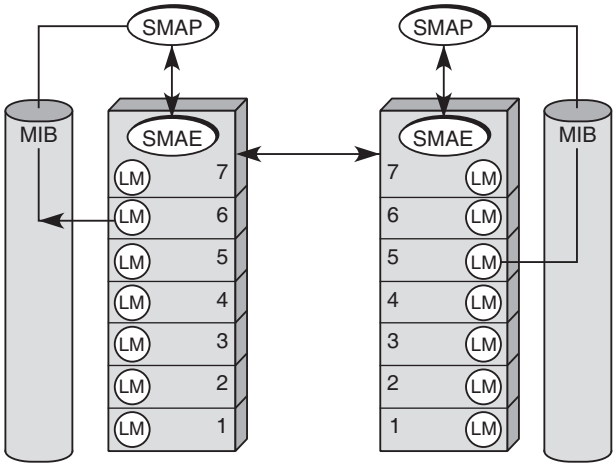


Figure Q.1

Modèle de gestion ISO

La gestion ISO comprend trois types d'activités :

- la gestion système, ou Systems-Management ;
- la gestion de couche, ou Layer Management (LM sur la figure Q.1) ;
- la gestion d'opération de couche (Layer Operation).

La gestion système définit l'échange de l'ensemble des informations de gestion concernant les ressources (objets gérés) utilisées dans un système ouvert. Ces échanges se font au niveau 7 de l'architecture du modèle de référence entre entités d'application pour la gestion système SMAE (System Management Application Entity), comme illustré à la figure Q.2.

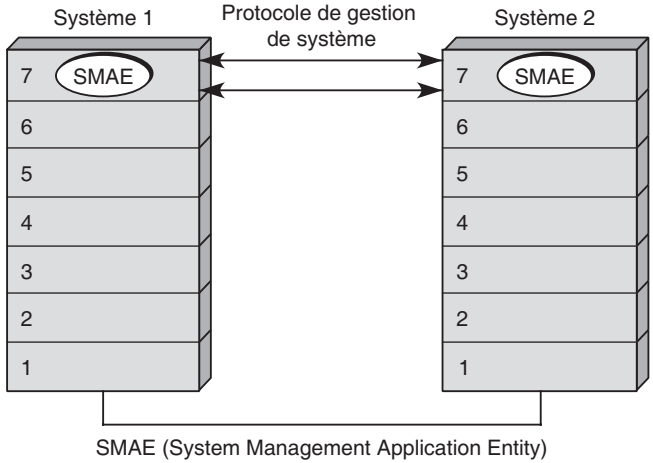


Figure Q.2

Échanges de niveau gestion de système

La gestion de couche, schématisée à la figure Q.3, définit les échanges d'informations concernant la gestion d'une couche *N* particulière. Ces informations ne concernent que les ressources propres à cette couche (mémoires tampons, temporisateurs, connexions, etc.). Cette gestion de couche correspond à des protocoles spécifiques, utilisés uniquement pour la gestion.

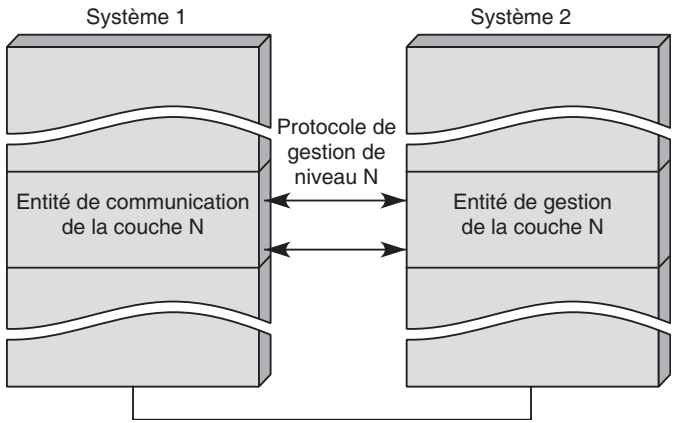


Figure Q.3

Échanges de niveau gestion de couche

Plusieurs instances de communication sont concernées par ces échanges, qui peuvent se faire soit *via* des protocoles de système (au niveau application), soit *via* des protocoles de gestion spécifiques de la couche concernée. On peut citer comme exemple de ces

derniers le NCMS (Network Connection Management Subprotocol), qui est un additif au protocole de transport OSI et qui spécifie un sous-protocole de gestion de connexions de réseau.

La gestion d'opération de couche couvre les échanges d'informations relatives à une instance de communication (une opération) dans une couche donnée. Cela englobe les données véhiculées par les protocoles de communication OSI. Ces échanges d'opération de couche sont illustrés à la figure Q.4.

En voici deux exemples :

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

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

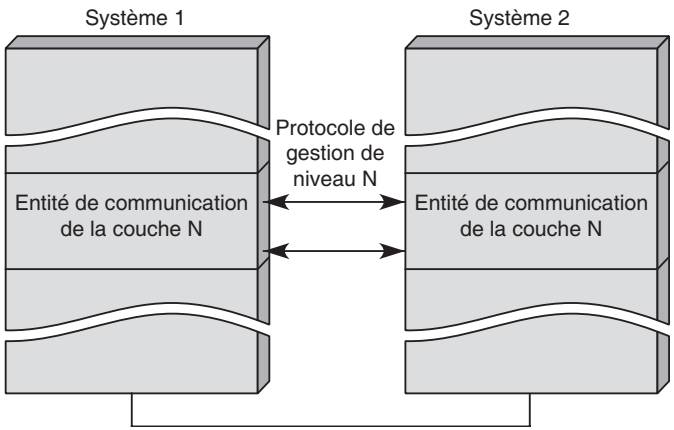


Figure Q.4

Échanges au niveau d'une opération de couche

Problématique de la gestion ISO

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

La figure Q.5 résume le fonctionnement de la gestion ISO. Les protocoles de couches viennent déposer leurs informations dans la MIB, qui peut être interrogée par les processus de gestion.

Cette architecture est conçue pour être générale, ce qui constitue son défaut par rapport à la simplicité de SNMP. En effet, les objets dans la gestion ISO peuvent devenir très complexes mais surtout spécifiques pour une implémentation donnée du modèle. De ce fait, la plupart des produits compatibles ISO ne sont que faiblement compatibles entre eux puisque les objets sont spécifiques, tout en étant conformes à la norme.

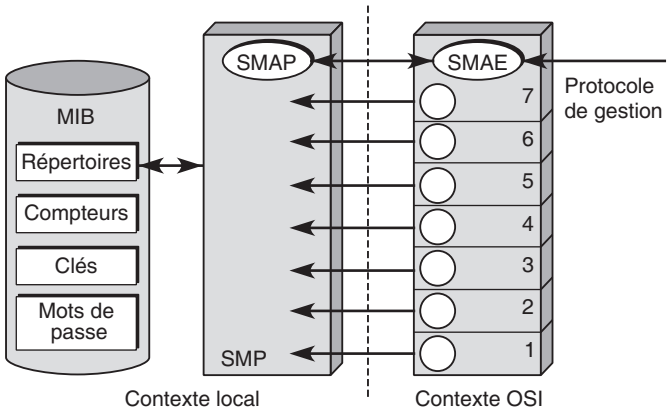


Figure Q.5
Architecture de la gestion ISO

TMN

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

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

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

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

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

- Business Management
- Service Management
- Network Management
- Element Management

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

Architecture du TMN

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

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

Architecture physique

Le TMN se fonde conceptuellement sur un réseau de communication de données, appelé DCN (Data Communication Network), séparé du réseau de télécommunications à gérer, comme illustré à la figure Q.6.

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

- OSF (Operations System Function), ou bloc fonctionnel des systèmes d'exploitation, traite les informations d'administration prises en charge et contrôle la réalisation des différentes fonctions d'administration de télécommunications. En d'autres termes, un bloc OSF offre des applications d'administration. Il existe trois types d'OSF : les OSF de base, qui gèrent les éléments de réseau, les OSF du réseau, qui réalisent les fonctions de TMN relatives au réseau en coopérant avec les OSF de base, et les OSF de service, qui fournissent les moyens de gérer les services de télécommunications.

- NEF (Network Element Function), ou bloc fonctionnel d'élément de réseau, qui communique avec un TMN dans le but d'être géré. Il peut être considéré comme un objet administré.
- MF (Mediation Function), ou bloc fonctionnel de médiation, qui opère sur l'information transitant entre les blocs NEF et OSF dans le but d'établir une communication entre les fonctions primitives et le stockage des données. Il doit également adapter, filtrer et condenser l'information du NEF d'une manière conforme à la demande de l'OSF. Parmi les exemples de MF, citons les convertisseurs de protocole, les contrôleurs de communication, les gestionnaires de prise de décision, les éléments de stockage des données, etc.
- DCF (Data Communication Function), ou bloc fonctionnel de communication de données, qui offre les moyens de transporter les informations relatives à l'administration des télécommunications entre les blocs fonctionnels. Son existence est souvent supposée implicite.
- WSF (Work Station Function), ou bloc fonctionnel du poste de travail, qui offre les moyens de communication entre les blocs fonctionnels et l'utilisateur.

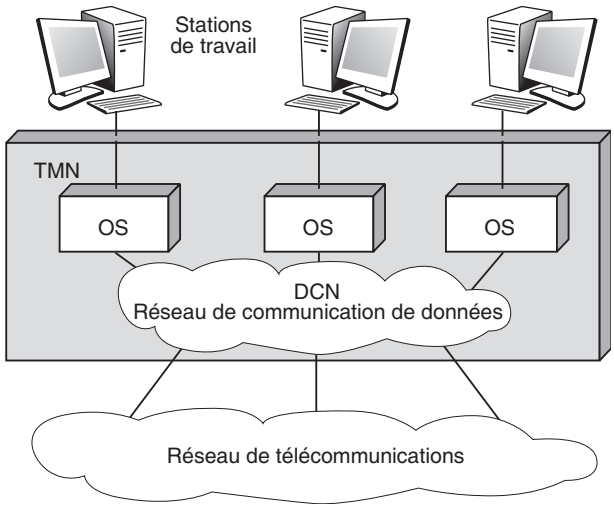


Figure Q.6

Architecture physique du TMN

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

Les blocs fonctionnels ci-dessus sont connectés de façon hiérarchique, comme illustré à la figure Q.7. Les points de référence de cette figure, indiqués par les valeurs f, g, q, x, sont expliqués dans la suite.

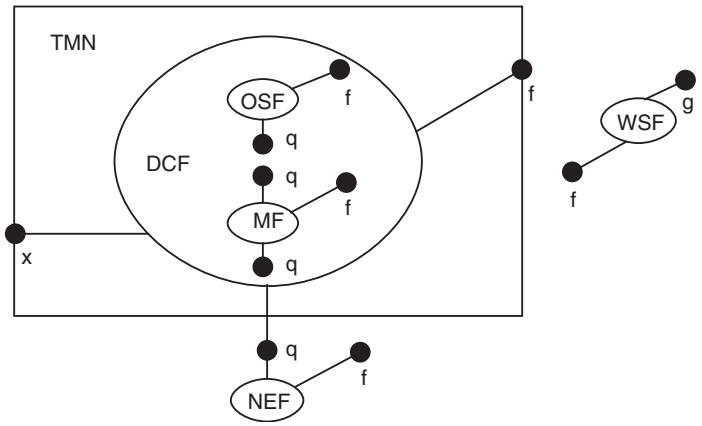


Figure Q.7

Architecture fonctionnelle du TMN

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

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

Comme illustré à la figure Q.8, l'architecture physique du TMN, schématisée ici avec les interfaces, est calquée sur l'architecture fonctionnelle.

Les interfaces normalisées sont définies en correspondance avec les points de référence. Elles sont signalées par des lettres majuscules pour les différencier des points de référence. L'interface Q est appliquée au point de référence q, F au point f, X au point x, etc. La figure Q.9 montre un exemple de relations entre une configuration physique et une configuration de référence dans laquelle le DCF est implicite.

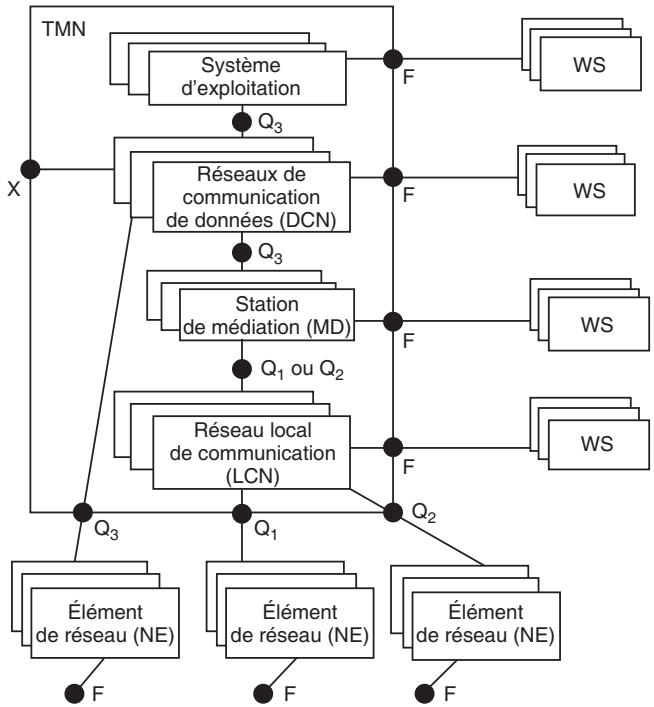


Figure Q.8

Architecture physique du TMN

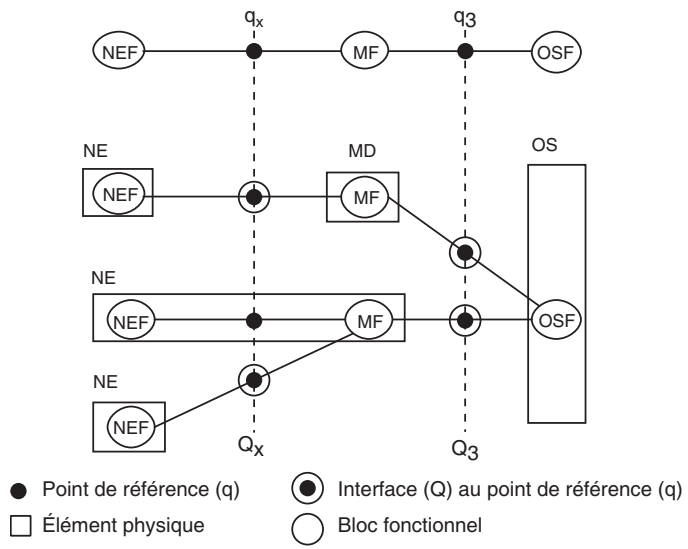


Figure Q.9

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

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

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

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

Architecture fonctionnelle

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

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

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

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

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

Le modèle informationnel de la gestion TMN

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

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

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

La gestion système CMIS/CMIP

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

Les services rendus par ces quatre ASE sont les suivants :

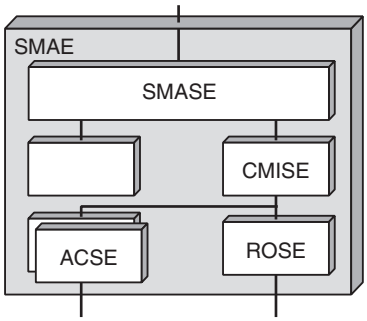
- SMAS (System Management Application Service), ou services d'application de la gestion système ;
- CMIS (Common Management Information Service), ou services communs à toutes les fonctions de gestion ;
- ACSE (Association Control Service Element), ou éléments de services de contrôle d'association ;
-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

Chacun de ces services repose sur un protocole spécifique :

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

La figure Q.10 illustre l'architecture de l'entité d'application SMAE avec ses quatre ASE.

Figure Q.10
Architecture de l'entité SMAE



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

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

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

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

Pour compléter cette architecture de gestion du modèle de référence de l'ISO, indiquons que le processus de gestion SMAP travaille sur treize fonctions administratives qui ont été regroupées dans cinq domaines fonctionnels, ou SMFA (Specific Management Functional Area) : la configuration (Configuration Management), la sécurité (Security Management), les pannes (Fault Management), l'audit de performances (Performance Management) et la comptabilité (Accounting Management). Ces fonctions sont détaillées à la section suivante, et les cinq domaines de gestion dans une section spécifique.

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

Le service SM

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

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

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

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

- pt-create
- pt-delete
- pt-event-report
- pt-get

- pt-set
- pt-action

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

Le service commun CMIS

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

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

Trois autres éléments de service concernent les associations :

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

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

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

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

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

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

La gestion et le contrôle par politique

Les opérateurs de télécommunications et les gestionnaires de réseau ont besoin d'automatiser le processus de configuration des nœuds et des équipements réseau. Cette automatisation vise à la fois à contrôler les flux d'information qui transitent dans ces nœuds et à gérer plus facilement les équipements réseau. De là est née la gestion par politique, à laquelle on peut ajouter le contrôle, qui en fait partie de façon intrinsèque. La terminologie anglo-saxonne correspondante est PBM (Policy-Based Management). Le mot *policy* est traduit dans ce livre par politique, mais on aurait aussi bien pu choisir règle.

Le propos de cette section est de présenter ce nouveau paradigme, consistant à gérer et contrôler les réseaux par l'intermédiaire de politiques. Nous commencerons par introduire les politiques puis détaillerons l'architecture associée au protocole de signalisation utilisé dans cet environnement.

Les politiques

Une politique s'exprime sous la forme « si condition alors action ». Par exemple, « si l'application est de type parole téléphonique, alors mettre les paquets en priorité Premium ». Cette section s'intéresse à la définition syntaxique et sémantique d'une politique puis examine en détail les politiques et leur utilisation pour le contrôle, ainsi que le protocole de signalisation permettant de transporter les paramètres des politiques et les différentes solutions pour mettre en œuvre le contrôle par politique.

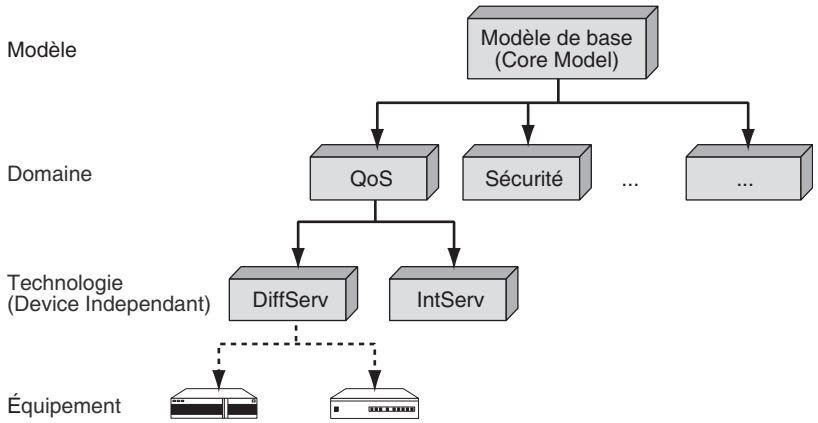
Une politique peut se définir à différents niveaux. Le niveau le plus haut correspond à celui de l'utilisateur, la détermination d'une politique s'effectuant par une discussion entre l'utilisateur et l'opérateur. On utilise pour cette discussion soit le langage naturel, soit des règles déjà préparées par l'opérateur du réseau. Dans ce dernier cas, l'utilisateur ne peut que choisir parmi ces règles la politique qu'il souhaite voir appliquer. On parle alors de politique définie au niveau business. Cette politique doit être traduite dans un langage de niveau réseau permettant de déterminer le protocole réseau de gestion de la qualité de service et son paramétrage. Enfin, il faut traduire ce langage de niveau réseau en un langage de bas niveau correspondant à la programmation des nœuds du réseau, ce que l'on peut appeler la configuration du nœud.

Ces différents niveaux de langage, business, réseau et configuration, sont pris en charge par un groupe de travail de l'IETF appelé Policy. Le modèle retenu provient d'un autre groupe de travail, le DMTF (Distributed Management Task Force) et porte le nom de CIM (Common Information Model). Les extensions sont aujourd'hui développées conjointement par les deux groupes de travail.

L'objectif de ce travail de normalisation des modèles d'information liés aux différents niveaux de langage est d'obtenir un modèle général qui puisse se décliner en modèles d'information par domaine, ainsi qu'une représentation indépendante des équipements et des implémentations. La figure Q.11 illustre le modèle le plus général possible à partir du modèle de base.

Figure Q.11

Structure du modèle CIM

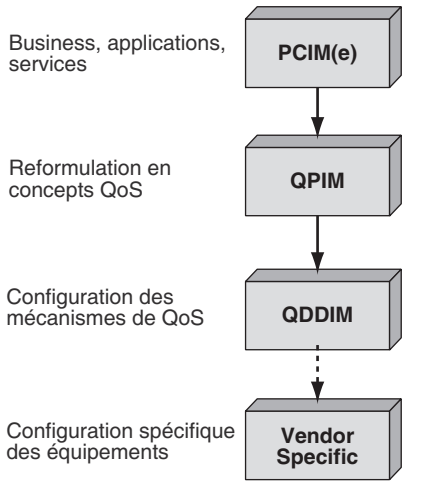


Si l'on ne se préoccupe que de la branche QoS, ou qualité de service, la structure des modèles successifs permet de passer de la définition générale d'une politique de qualité de service à la configuration d'un routeur.

La figure Q.12 illustre la succession de modèles allant vers de moins en moins d'abstraction et s'approchant de la description d'une configuration.

Figure Q.12

Structure des modèles associés à la QOS



PCIM (Policy Core Information Model)
QPIM (QOS Policy Information Model)
QDDIM (QoS Device Datapath Information Model)

PCIM (Policy Core Information Model)

PCIM définit le modèle de description des politiques, quel que soit leur domaine d'application. Le réseau est considéré comme une machine à états, c'est-à-dire un système qui ne peut prendre que des états définis à l'avance. Les politiques servent dès lors à contrôler les changements d'état en identifiant l'état courant et en définissant les transitions possibles.

Le modèle est fondé sur deux hiérarchies de classes, les classes structurelles, qui forment les éléments de base des politiques, et les classes d'association, qui déterminent les relations entre les éléments. Les politiques forment un ensemble de conditions vraies ou fausses qui peuvent être composées pour réaliser une politique plus complexe. Ces politiques forment à leur tour un ensemble d'actions associées aux conditions qui modifient la configuration d'un ou plusieurs éléments et qui introduisent des ordres d'exécution, comme la priorité des flots ou l'ordonnancement des paquets dans le réseau.

PCIMe (PCIM extension) a pour fonction de rendre le modèle PCIM plus flexible en permettant aux différents domaines d'homogénéiser leurs concepts. Les principales extensions concernent une meilleure gestion des priorités, l'ajout de variables et de valeurs, la définition de variables générales, l'ajout de règles simplifiées fondées sur les variables, la possibilité d'avoir des règles conditionnées par d'autres règles, la condition de filtrage de paquets IP à base de conditions, etc.

QPIM (QoS Policy Information Model)

Le rôle de QPIM est de fournir un format standard pour les politiques de QoS en intégrant les environnements IntServ et DiffServ, tout en restant indépendant des protocoles d'accès, des méthodes de stockage et des techniques de contrôle de QoS (files d'attente, etc.). QPIM doit en outre faciliter une représentation formelle de règles abstraites humaines.

Les actions possibles sur la définition de la QoS sont le classement par catégorie, l'adéquation par rapport aux fonctionnalités de RSVP, comme la modification de certains paramètres de RSVP, l'acceptation ou non d'une requête et la conformité au modèle COPS-RSVP et enfin les actions liées aux politiques de provisioning, comme le marquage, le lissage, la perte de paquets, l'ordonnancement, etc. D'autres extensions ont été ajoutées, notamment dix-sept variables liées à RSVP, ainsi que la définition formelle de profils de trafic pour DiffServ et IntServ.

QDDIM (QoS Device Datapath Information Model)

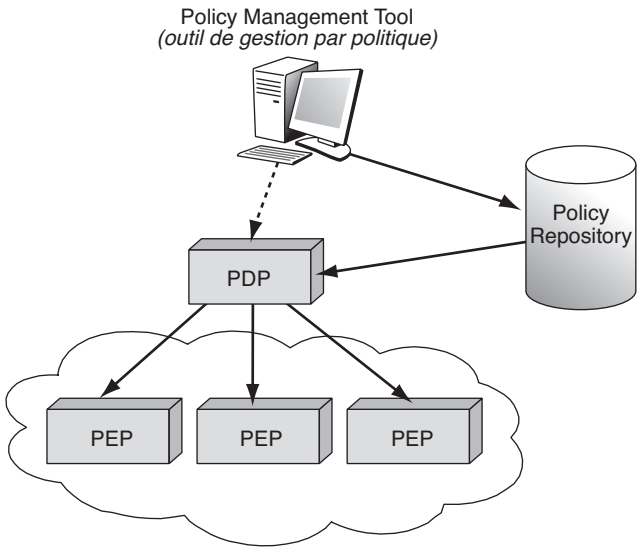
Le modèle QDDIM permet de s'approcher de la configuration des routeurs en étendant QPIM, qui définit des actions sur les paquets, par le biais d'actions sur les équipements tout en restant indépendant des implémentations. Le rôle de QDDIM est de permettre de programmer un routeur ou un équipement réseau, indépendamment de l'équipementier qui le commercialise. Pour cela, QDDIM utilise une syntaxe générale permettant de décrire précisément l'action que doit apporter la politique à appliquer sur les composants de l'équipement réseau.

Architecture d'un contrôle par politique

Le contrôle par politique implique plusieurs composants (voir figure Q.13). Les nœuds du réseau prennent le nom de PEP (Policy Enforcement Point). Les politiques y sont appliquées pour gérer les flux des utilisateurs. Le PDP (Policy Decision Point) est le point qui prend les décisions et choisit les politiques à appliquer aux PEP. La communication entre le PEP et le PDP s'effectue par le biais du protocole COPS (Common Open Policy Service). Le système comporte également une console utilisateur, qui contient des outils de gestion des politiques. Ces derniers permettent notamment d'entrer les politiques dans une base de données, nommée Policy Repository, qui entrepose les règles de politique que le PDP vient rechercher pour les appliquer aux nœuds du réseau.

Figure Q.13

Architecture d'un système géré par politique



Des variantes de ce schéma de base peuvent inclure plusieurs PDP susceptibles de gérer un même nœud de transfert du réseau. Dans ce cas, les PDP ont des rôles différents, comme nous le verrons par la suite. Une autre variante correspond à une décentralisation des fonctions du PDP dans des PDP locaux, appelés LPDP (Local Policy Decision Point). En règle générale, un PDP gère un seul domaine administratif, et les règles de politique sont communes à la configuration de l'ensemble des nœuds du domaine.

Un problème de cohérence se pose lorsque le client émetteur et le client récepteur ne se trouvent pas dans le même domaine administratif. Dans ce cas, les PDP des deux domaines doivent négocier pour se mettre d'accord sur les règles de politique à adopter pour que la communication se déroule de bout en bout avec la qualité voulue. Ce cas est illustré à la figure Q.14.

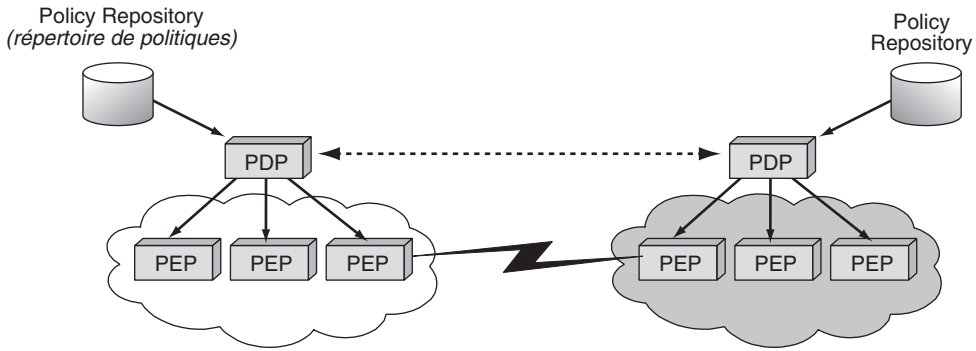


Figure Q.14

Architecture de gestion par politique sur une interconnexion de deux domaines administratifs

Le PDP (Policy Decision Point)

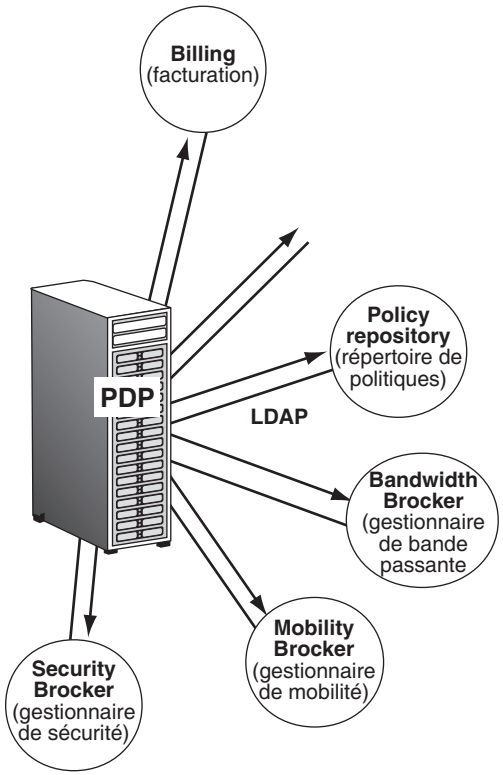
Le PDP est défini comme une entité logique prenant des décisions politiques pour elle-même ou pour d'autres éléments réseau qui demandent ses décisions. Le PDP, que l'on peut aussi appeler serveur de politiques, est donc le point central qui doit décider des politiques à appliquer dans le réseau. Il s'agit en quelque sorte d'un organe de décision, qui recherche les informations dont il a besoin dans de nombreux serveurs communiquant directement avec lui de façon à prendre une décision. Ces serveurs peuvent être locaux, ce qui est le cas le plus général, mais ils peuvent aussi être distants.

La figure Q.15 illustre un PDP et ses serveurs principaux.

Les principaux serveurs sont, dans l'ordre :

- Le Policy Repository, dans lequel le PDP vient rechercher les règles de politique. Cette mémoire communique avec le PDP par le biais du protocole LDAP, ce qui explique son nom de serveur LDAP.
- Un Bandwidth Broker, qui gère la bande passante disponible dans le réseau. Ce serveur de bande passante connaît la topologie et les caractéristiques du réseau, ce qui lui permet de distribuer les ressources du réseau à bon escient.
- Un Security Broker, ou serveur de gestion de la sécurité au moment de la connexion, qui est généralement un serveur AAA (Authentication, Authorization, Accounting). Ce serveur peut également gérer la sécurité du transport de l'information sur les supports physiques.
- Un Mobility Broker, ou serveur de mobilité, qui peut être apte à gérer la continuité de la qualité de service.
- Un serveur de facturation (Billing), qui se révélera essentiel dans les prochains réseaux Internet qui délivreront de la qualité de service.

Figure Q.15
Un PDP et ses serveurs



Il peut exister des serveurs complémentaires, comme la PIB (Policy Information Base), qui garde en mémoire les modèles informationnels pouvant être utilisés pour représenter une politique sous une syntaxe particulière. D'autres serveurs se révéleront sûrement très importants à l'avenir, comme le serveur de métrologie et de tuning, qui doit être capable de vérifier que les ressources mises à la disposition d'un utilisateur le sont effectivement.

Le rôle du PDP consiste à identifier les règles de politique qui sont applicables aux différents PEP et à déterminer les règles à appliquer stratégiquement à ces PEP. Le PDP doit également se préoccuper de la traduction des règles de politique dans des formats compréhensibles des nœuds comme les PIB. De plus, il doit pouvoir communiquer avec d'autres serveurs internes pour prendre ses décisions. Enfin, le PDP assure la distribution des configurations. En résumé, le PDP décide des règles à appliquer et envoie les ordres de configuration aux nœuds du réseau.

Les PEP (Policy Enforcement Point)

Les PEP sont des entités logiques qui appliquent les décisions politiques prises par le PDP dont elles dépendent. Les PEP sont généralement les nœuds du réseau, qui peuvent

être de différents types : routeur, commutateur ou LSR (Label Switched Router). Un PEP peut également être un pare-feu ou un équipement intermédiaire entre le client et le réseau. Le client peut lui-même posséder un client PEP sur son terminal. Dans les réseaux de mobiles à carte à puce, il est fréquent de considérer qu'un PEP d'accès se trouve sur la carte à puce. Son rôle est essentiellement réduit à la gestion de la sécurité et non de la qualité de service, mais il est imaginable d'implémenter la gestion de QoS dans les cartes à puce dès que celles-ci seront assez puissantes pour effectuer cette gestion.

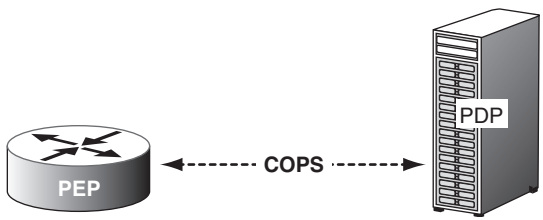
Un PEP doit être facilement accessible et paramétrable par le PDP de sorte qu'il soit possible de le configurer sans problème. Il peut être configuré par un message COPS mais aussi par une requête SNMP ou une commande CLI (Command Line Interface), qui est la commande la plus simple pour configurer manuellement un équipement de réseau. Le PEP fait le lien entre la représentation externe (PIB ou MIB) et la configuration interne de l'équipement et doit être capable de recevoir des requêtes de différents types provenant de l'utilisateur. En particulier, le PEP doit être apte à comprendre les requêtes RSVP. Le PEP s'assure de la cohérence des politiques locales et surveille leur bonne application. Enfin, il peut intégrer des fonctions d'ingénierie ou de facturation.

COPS (Common Open Policy Service)

COPS est le protocole de signalisation développé par l'IETF pour transporter les demandes de configuration et retourner les politiques à appliquer. Au départ, le protocole COPS devait permettre de prolonger RSVP vers le PDP et assurer les fonctions de contrôle d'admission au réseau en les fondant sur des politiques.

C'est un protocole requête-réponse simple pour l'échange d'informations de politiques entre un serveur de politique, ou PDP, et un client, ou PEP. La figure Q.16 illustre ce schéma de base.

Figure Q.16
Fonctionnement du protocole COPS



Le PEP peut être un routeur supportant RSVP ou un routeur supportant un service de gestion de la qualité de service, comme DiffServ, ou encore un nœud appliquant un contrôle quelconque. Le PEP fournit des informations au PDP concernant les décisions prises et les politiques installées. COPS transporte les messages d'erreur faisant suite à la détection d'un problème lors de l'installation d'une politique ou à un échec détecté lors de l'installation de la configuration sur le PEP.

Le PEP est responsable de la mise en place d'une connexion TCP avec le PDP. Il utilise cette connexion TCP pour envoyer des requêtes et recevoir les décisions du PDP. Le PEP doit rendre compte au PDP de l'exécution de ces décisions. De même, le PEP est responsable de la notification au PDP des modifications du PEP. Le PEP est en outre responsable de la suppression d'un état devenu inacceptable à la suite d'une modification demandée par le client ou d'une décision prise et envoyée par le PDP.

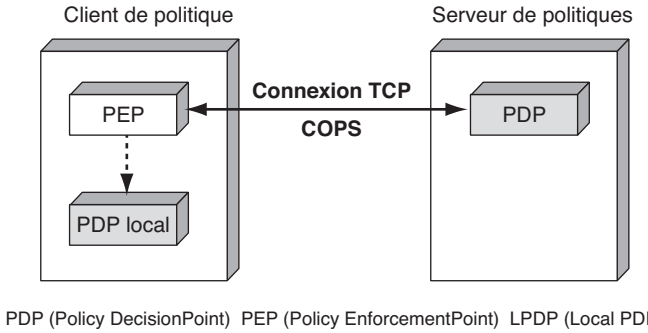
Le PEP peut être configuré et commandé par une décision locale *via* son LPDP (Local Policy Decision Point). Le PEP doit faire parvenir les caractéristiques de cette décision locale au PDP, lequel prend la décision finale. Si cette décision est différente de celle définie en local, le PDP l'envoie au PEP pour application.

La figure Q.17 décrit le système de communication entre un PDP et un PEP.

Le PDP est la composante de l'environnement PBN (Policy-Based Networking), qui contrôle directement le PEP. Le PDP choisit parmi les politiques disponibles dans la base, ou Policy Repository, contenant les informations de politique, la politique adaptée pour configurer le routeur.

Figure Q.17

Architecture de base d'un environnement contrôlé par politique



Les règles de politique utilisées par le PDP sont saisies par la console de gestion de l'opérateur puis mises à disposition du PDP par le Policy Repository où elles sont déposées. À l'intérieur des nœuds, le PEP peut être accompagné d'un LPDP (Local PDP), dont le rôle est de remplacer le PDP en cas de besoin. La présence du LPDP est facultative. Ce point de contrôle local est utilisé pour prendre une décision locale en l'absence du PDP.

Le PDP peut utiliser différents mécanismes et protocoles de communication avec des serveurs qui lui sont attachés pour réaliser des fonctions spécifiques, comme l'authentification, la facturation ou le stockage d'informations de politique.

Le fonctionnement général du modèle de gestion par politique est illustré à la figure Q.18.

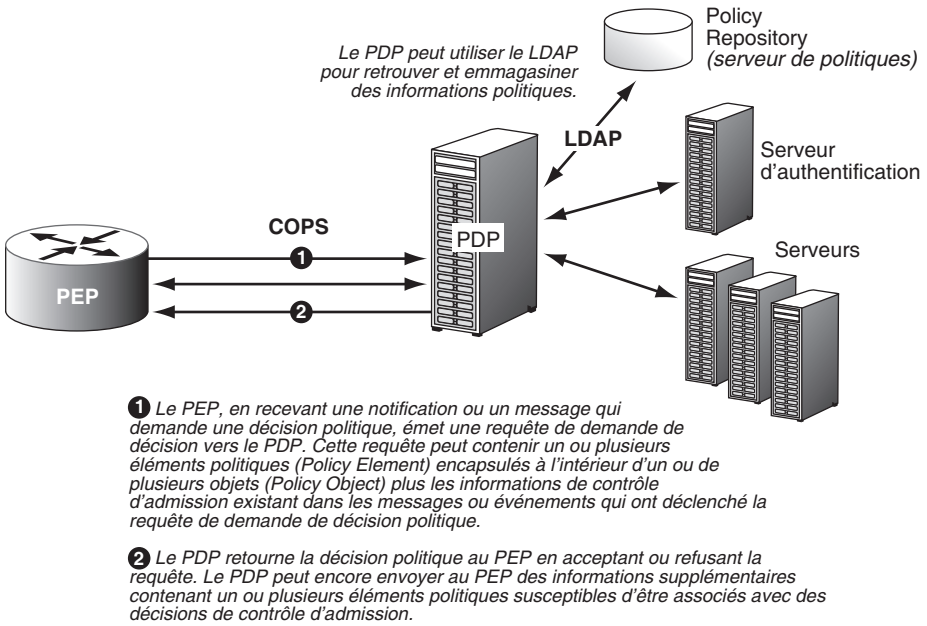


Figure Q.18

Fonctionnement global d'un environnement de contrôle par politique

Caractéristiques principales du protocole COPS

Le protocole COPS emploie un modèle client-serveur, dans lequel le PEP envoie des messages de requête (Request), de mise à jour (Update) et de suppression (Delete) au PDP. Le PDP retourne des messages contenant les décisions prises.

TCP est utilisé comme protocole de transport pour fiabiliser l'échange des messages entre le PEP et le PDP. Aucun mécanisme supplémentaire n'est à mettre en œuvre pour réaliser une communication fiable entre un PDP et un PEP. Le protocole est extensible, la communication pouvant prendre en charge plusieurs types d'information (Client Specific Information) sans exiger de modification de la part du protocole COPS.

Le protocole fournit les éléments de sécurité nécessaires pour l'authentification, la protection contre les attaques malveillantes et l'intégrité du message. COPS peut aussi utiliser d'autres protocoles spécifiques pour gérer les problèmes de sécurité. Ainsi, IPsec ou TLS (Transaction Layer Security) peuvent être mis en œuvre pour authentifier et sécuriser la connexion entre le PEP et le PDP.

Les états des configurations mises en place par la communication sous forme de requêtes-décisions sont partagés entre le PEP et le PDP. Les décisions du PDP peuvent être émises d'une manière asynchrone, c'est-à-dire à tout instant, pour modifier l'état du système installé. Le protocole permet au PDP d'envoyer l'information de configuration au PEP et permet au PDP de supprimer les états du PEP lorsqu'ils ne sont plus valides.

La figure Q.19 illustre un message COPS comprenant un en-tête avec différents champs de contrôle, suivi des champs objet. Chaque champ objet est composé de la même façon, en commençant par la longueur de l'objet, la définition de l'objet, le type d'objet et enfin le contenu et les valeurs associées de l'objet. La figure Q.20 décrit l'échange des messages dans une communication COPS.

Figure Q.19
Message COPS

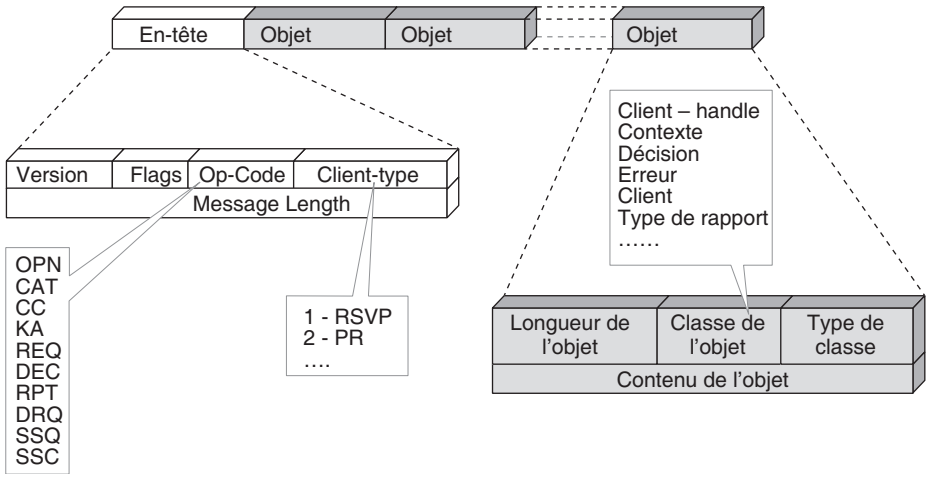
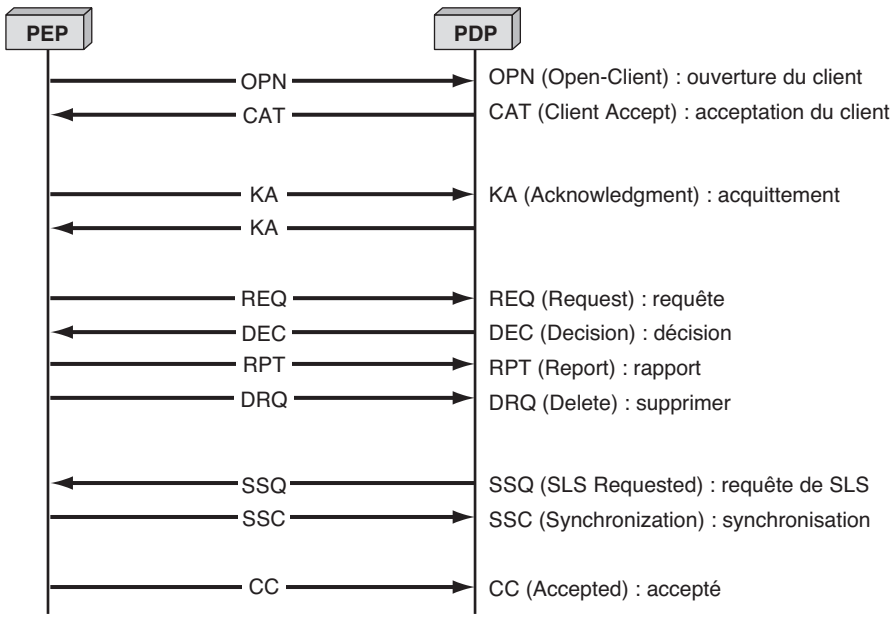


Figure Q.20
Échange de messages dans une communication COPS



COPS et les modèles de gestion par politique

Les deux modèles principaux de gestion et de contrôle par politique sont le provisioning et l'outsourcing.

Dans le cas de l'outsourcing (Outsourcing Policy Model), le PDP reçoit les requêtes (Policy Requests) de demande de configuration de la part des PEP et décide ou non d'autoriser la connexion en temps réel sans qu'un lien préalable soit tissé entre l'utilisateur et l'opérateur du réseau. Si la demande d'accès est acceptée, le PDP envoie la configuration proposée au nœud d'accès, qui la propose à son tour au client demandeur.

Le fonctionnement général de l'outsourcing est le suivant :

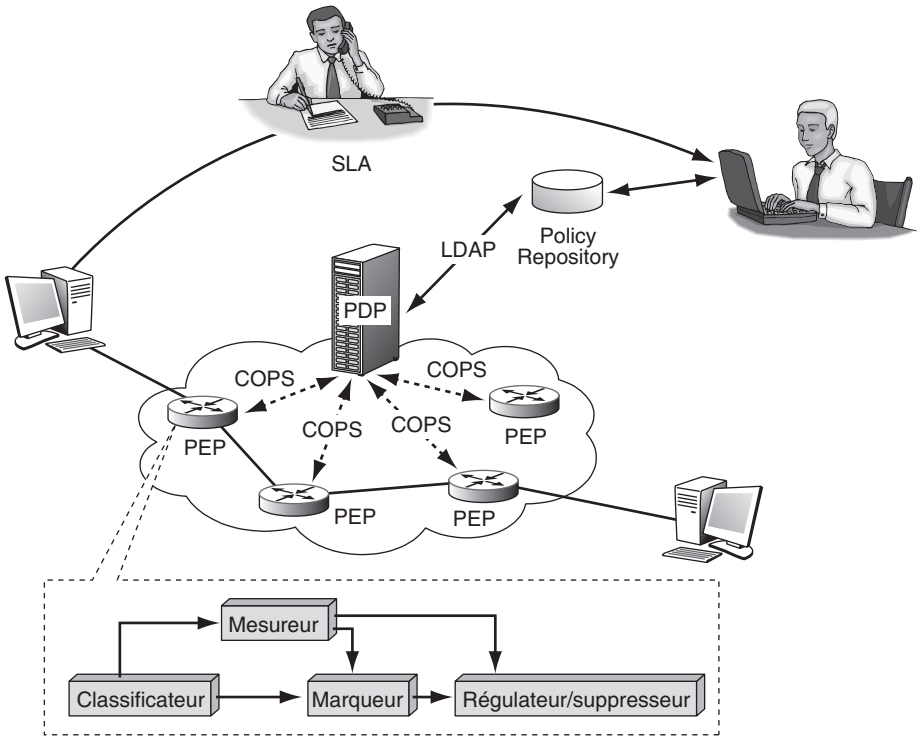
1. Le client effectue une demande de connexion à un réseau auquel il n'est pas abonné.
2. Cette demande appelle une décision concernant l'accès au réseau : l'opérateur accepte ou non la connexion du client.
3. Le client doit donc faire une requête au réseau. Le protocole RSVP est le vecteur le plus classique pour effectuer cette demande.
4. Celle-ci arrive au nœud d'entrée du réseau, ou edge router, qui la dirige vers le PDP grâce à une requête COPS.
5. Une fois la décision prise par le PDP, une réponse transitant par le protocole COPS indique au nœud d'entrée si la demande RSVP est acceptée ou non.
6. En cas d'acceptation, la requête RSVP peut continuer son chemin pour ouvrir une route satisfaisant la demande de l'émetteur.

Nous détaillons cette solution un peu plus loin dans cette annexe.

Dans le cas du provisioning (Provisioning Policy Model), les politiques sont entrées à la console de gestion de l'opérateur à la suite d'une discussion entre le client et l'opérateur. Cette discussion débouche sur un SLA (Service Level Agreement), qui correspond à un contrat entre l'utilisateur et le gestionnaire du réseau détaillant les caractéristiques du service qui doit être rendu par l'opérateur et les dispositions administratives en cas de problème. La partie technique du SLA s'appelle le SLS (Service Level Specification). Le SLS donne lieu à l'introduction de politiques dans la base de données de l'opérateur, politiques qui devront être appliquées dès que le client présentera un flux à l'entrée du réseau.

Les politiques sont distribuées en temps réel par le PDP. Le PDP décide si la politique doit être installée en permanence dans les PEP traversés par le client ou non, suivant les caractéristiques techniques de la demande du client. Si les politiques sont implémentées directement dans les nœuds, le PDP les envoie au travers d'une commande COPS. Les nœuds d'accès sont alors prêts à recevoir les demandes d'accès des flots négociés dans le SLA-SLS. Les nœuds d'accès sont capables de traiter en temps réel ces demandes. Le provisioning est souvent associé à la technique DiffServ, dans laquelle les flots peuvent être classifiés suivant diverses classes. Dans ce cas, les paquets des clients entrants sont marqués avec la priorité négociée dans le SLS et transmis aux routeurs par la politique correspondante. La figure Q.21 illustre le fonctionnement d'une politique de provisioning associée à DiffServ.

Figure Q.21
Fonctionnement d'une solution de provisioning



La figure Q.22 présente les requêtes échangées entre le PDP et le PEP pour une communication de provisioning (PR) avec un protocole COPS qui prend alors le nom de COPS-PR. Cette communication s'effectue par l'émission d'une requête REQ du PEP vers le PDP. Le PDP répond par une commande DEC précisant la configuration à mettre en œuvre dans le PEP.

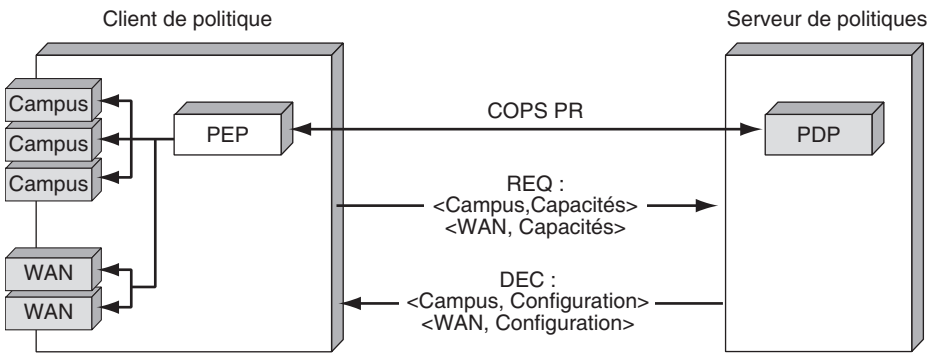


Figure Q.22
Fonctionnement de COPS-PR sous DiffServ

La pile du protocole COPS peut être divisée en trois couches conceptuelles distinctes : le protocole de base, les directives dépendant du type de client (client-type) et la représentation des données de politique (Policy Data Représentation).

L'IETF a proposé COPS comme protocole de communication pour faciliter l'échange des informations de politique entre le PDP et les PEP. Avant d'effectuer un échange de données de politique, le PEP doit initialiser la communication en ouvrant une connexion TCP avec le PDP. C'est là une des différences les plus importantes par rapport aux systèmes de gestion classiques de réseau, comme SNMP, dans lesquels le serveur initialise la communication avec le client avant d'envoyer l'information de configuration en utilisant une connexion UDP. L'utilisation d'une connexion TCP augmente la fiabilité du protocole COPS.

COPS-RSVP et le modèle d'outsourcing

RSVP a été choisi comme protocole de signalisation entre le client et le réseau pour gérer la QoS dans le modèle d'outsourcing. À la suite de l'arrivée d'un message RSVP dans le nœud d'accès, un protocole COPS spécifique, COPS-RSVP, est mis en jeu afin d'utiliser les objets de RSVP.

Quand le PEP reçoit un message RSVP sollicitant une décision pour la configuration des nœuds que son flot va traverser, les objets de RSVP sont encapsulés à l'intérieur de l'objet Signaled Client SI dans un message de requête COPS envoyé au PDP. Le PDP décide alors si ce message RSVP doit être accepté ou non puis envoie sa décision au PEP par un message de réponse. D'autres informations de supervision peuvent être envoyées par le PDP, suite à la même requête, si le PDP s'aperçoit que la décision politique originale a besoin d'être modifiée ou supprimée.

Dans le cas où le PDP détecte l'absence d'un objet RSVP essentiel dans la requête, il retourne un message d'erreur <Error> dans le message de décision, qui doit indiquer MANDATORY CLIENT-SPECIFIC INFO MISSING. Dans le cas où le PDP détecte l'absence d'un objet RSVP optionnel dans la requête, il retourne une décision négative.

Pour chaque message de décision reçu, le PEP envoie un rapport au PDP, qui inclut les actions prises pour assurer que les politiques décidées par le PDP ont été convenablement installées et pour détecter d'éventuelles anomalies. De la sorte, le PDP reste bien informé de la politique installée dans le PEP.

Dans le protocole RSVP, l'objet Policy Data joue le rôle d'un conteneur de transport des messages RSVP qui arrivent au PEP, le PEP communiquant l'objet Policy Data au PDP. Le PDP prend alors une décision fondée sur le contenu de l'objet Policy Data. Le PDP peut aussi modifier ou remplacer le Policy Data par un message Outgoing RSVP, qui permet à RSVP de se propager dans le réseau.

COPS-PR et le modèle de provisioning

Le provisioning n'inclut pas de mécanisme de signalisation de QoS mais comporte un modèle de type push. La configuration des routeurs est effectuée par le PDP en poussant l'information de configuration dans les nœuds une fois le SLA négocié avec l'utilisateur.

Le mot *provisioning* (approvisionnement) provient de cette solution dans laquelle on réserve des ressources à l'avance, l'utilisateur les trouvant mises à sa disposition dans les nœuds du réseau lorsqu'il se connecte.

Au départ, le PDP choisit les règles de politique qu'il appliquera à un utilisateur en considérant les informations du SLA-SLS négocié au départ avec l'utilisateur. Ces décisions sont ensuite envoyées d'une manière asynchrone du PDP au PEP pour réaliser la configuration décidée par le PDP. Le PDP effectue un calcul de probabilité en fonction de tous les SLA-SLS des clients abonnés puis envoie l'information de configuration au PEP, telle que le changement de politique demandé directement par l'utilisateur en modifiant son abonnement, à une heure prédéterminée, à l'expiration d'un compte, etc. Le PEP confirme que l'installation de configuration est réussie à la suite du message de configuration.

Le protocole COPS-PR peut être utilisé pour mettre en place différentes configurations de gestion de la qualité de service, comme DiffServ, MPLS, etc. Les données transportées par COPS-PR forment un ensemble de données de politique. Ces données prennent le nom de PIB (Policy Information Base), ou base de données des informations de politique. La PIB est utilisée avec le protocole COPS et, dans le cas du provisioning, avec COPS-PR. Le modèle de description de l'information de politique décrit le format des informations de politique échangées entre le PEP et le PDP. La PIB contient des informations décrivant le service associé aux politiques et les techniques de classification des paquets. Elle est extensible, de sorte à permettre l'adjonction de nouveaux types de paramètres.

Interactions entre les PEP et le PDP

Au démarrage d'un PEP, celui-ci ouvre une connexion COPS avec son PDP. Une fois la connexion établie, le PEP envoie au PDP des informations à propos de lui-même sous la forme d'une requête de configuration. La requête inclut toutes les informations spécifiant le client, telles que les types de matériel et de logiciel utilisés, qui sont nécessaires à une configuration. Durant cette phase, le client peut spécifier la taille maximale du message COPS-PR.

Le PDP répond à la requête de configuration en transmettant l'ensemble des politiques acceptées par le PDP concernant ce PEP. À réception de ces politiques de configuration, le PEP les organise et les installe. Si le PDP change son comportement ou est averti par le PEP d'un changement de contexte, suite, par exemple, à une panne, le PDP envoie une nouvelle configuration avec les primitives INSTALL, UPDATE et DELETE pour modifier la configuration du PEP. Si la configuration du PEP doit changer de manière radicale, suite à une demande de configuration non disponible dans le nœud, le PEP envoie de façon asynchrone de nouvelles informations au PDP dans un message UPDATE REQUEST CONFIGURATION. À réception de cette requête, le PDP fait parvenir au PEP les informations nécessaires à la gestion de l'implantation de la nouvelle politique et, bien sûr, à l'effacement des politiques qui ne sont plus nécessaires.

Nous avons vu que COPS utilisait une connexion TCP entre le PEP et le PDP. La connexion TCP est initialisée par le PEP. Chaque serveur PDP écoute la connexion sur le port 3288. Il existe au moins un PDP par domaine administratif. Le PEP peut obtenir

l'adresse du PDP par le service de gestion du réseau ou par le mécanisme de localisation de service, ou SRVLOC (Service Location). Un PEP peut supporter plusieurs types de clients. Dans ce cas, il doit envoyer plusieurs messages CLIENT-OPEN, de façon que chaque connexion spécifie un type de client particulier.

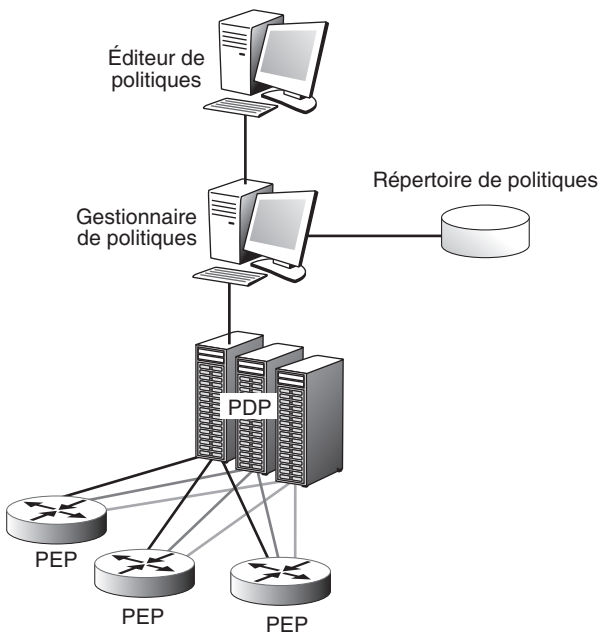
Le PEP effectue sa requête à un ou plusieurs PDP au travers d'une ou de plusieurs connexions TCP. Un PDP qui a une adresse et un numéro de port peut supporter plusieurs types de clients. Il est donc possible qu'un PEP ouvre plusieurs connexions avec plusieurs PDP. C'est le cas lorsque plusieurs PDP physiques séparés, et non logique dans un seul PDP, supportent différents types de clients. Il est important de noter que, pour une classe de clients donnée (client type), il ne peut exister qu'un PDP par domaine administratif. La figure Q.23 illustre ce type d'architecture. L'éditeur de politique est généralement un ordinateur personnel qui permet d'entrer les politiques par l'intermédiaire d'un clavier.

Pour distinguer les différents types de clients, le client est identifié dans chaque message. Les classes de clients peuvent se servir de données propres à leur classe et réclamer l'application de politiques spécifiques.

Le PEP doit passer par les étapes suivantes pour arriver à une décision politique :

1. Un événement local ou un message demande au PEP de se configurer suivant une politique particulière.
2. Le PEP créé une requête COPS contenant les informations provenant du message de demande d'admission et les éléments de politique à appliquer.

Figure Q.23
Architecture à plusieurs PDP



3. Le PEP peut consulter une base de données de configuration locale (Local Configuration Database) pour identifier un ensemble d'éléments de politique (Policy Element) qui peuvent être évalués localement. Le PEP passe alors la requête au LPDP (au cas où il en possède un), lequel, à son tour, renvoie une décision, appelée résultat partiel.
4. Le PEP émet une requête contenant tous les éléments de politique, accompagnés du résultat partiel du LPDP, vers le PDP, lequel prend la décision finale.
5. Le PDP retourne la décision finale au PEP et indique la politique à implémenter dans le nœud.

Le PDP doit éventuellement être informé de l'échec du LPDP en ce qui concerne la décision locale à prendre ainsi que de l'échec de l'admission, par manque de ressources, par exemple. Le PDP peut à tout moment envoyer des notifications au PEP pour demander une modification concernant une décision, générer une erreur de politique (Policy Error) ou envoyer un message d'avertissement (Warning Message).

La sécurité dans COPS

La sécurité dans COPS est négociée une fois pour toutes au début de la connexion et couvre ainsi toutes les communications utilisant cette connexion. Si une sécurité particulière est demandée pour une connexion, elle doit être négociée durant l'échange initial, pendant la phase CLIENT-OPEN/CLIENT-ACCEPT, en spécifiant un CLIENT-TYPE égal à zéro (CLIENT-TYPE = 0 est réservé à la négociation de la sécurité).

Si un PEP n'est pas configuré pour utiliser la version COPS Security avec un PDP, le PEP envoie tout simplement au PDP un message CLIENT-OPEN pour un CLIENT-TYPE disponible. Le PEP envoie sa demande de sécurité au PDP à l'aide d'un message CLIENT-OPEN possédant un CLIENT-TYPE = 0 avant même d'ouvrir un autre CLIENT-TYPE. Si le PDP reçoit un message CLIENT-OPEN avec un CLIENT-TYPE = 0 après qu'un autre CLIENT-TYPE a été ouvert avec succès, le PDP retourne un message CLIENT-CLOSE avec CLIENT-TYPE = 0 pour ce PEP.

Le premier message CLIENT-OPEN doit spécifier un CLIENT-TYPE = 0 et indiquer le PEP ID (identité du PEP) et l'objet d'intégrité de COPS. Cet objet d'intégrité contient un numéro de séquence initialisé par le PEP, que le PDP incrémente durant la communication suivant l'échange du message initial CLIENT-OPEN/CLIENT-ACCEPT. La valeur de l'ID identifie l'algorithme et la clé utilisés pour sécuriser la communication. Le PDP accepte l'algorithme et la clé de sécurité du PEP en validant le message reçu par le biais de la clé identifiée par la valeur de l'ID. Le PDP envoie alors au PEP un message CLIENT-ACCEPT avec un CLIENT-TYPE = 0 en portant un champ d'intégrité pour vérifier la correction de l'information. Cet objet d'intégrité contient le numéro de séquence initialisé par le PDP, numéro que le PEP doit incrémenter durant toute la communication avec le PDP. Ce numéro permet de bien séquencer les différents messages que s'échangent le PEP et le PDP.

Disponibilité d'un réseau d'opérateur

Dans un réseau d'opérateur, la fiabilité est une qualité essentielle. Nous avons représenté au tableau Q.1 les temps d'indisponibilité d'un réseau en fonction du taux de disponibilité, c'est-à-dire la proportion du temps pendant lequel le réseau est disponible. La première colonne indique le taux de disponibilité et les colonnes suivantes le temps d'indisponibilité du réseau par mois et par an.

Tableau Q.1 • Taux d'indisponibilité d'une ligne ou d'un réseau

1	90 %	36,5 j/an	3 j/m	
2	99 %	3,65 j/an	7,3 h/m	
3	99,9 %	8,8 h/an	44 min/m	Bon ISP
4	99,99 %	53 min/an	4,4 min/m	
5	99,999 %	5 min/an	25 s/m	Téléphone
6	99,9999 %	32 s/an	3 s/m	

Les réseaux de télécommunications pour la téléphonie sont actuellement des réseaux « cinq neuf », c'est-à-dire avec un taux de disponibilité de 99,999. Ce taux représente des coupures du service téléphonique égales au total à 5 minutes par an. Actuellement, les réseaux des FAI n'offrent que « trois neuf » et donc un temps de panne de l'ordre de 9 heures par an, un temps beaucoup trop important pour un service téléphonique de qualité. Les opérateurs de télécommunications en mode IP doivent donc faire un énorme effort pour atteindre des taux de deux ordres supérieurs.

Plusieurs solutions pour atteindre des taux de disponibilité acceptables pour les applications utilisateur sont envisageables et même déjà en grande partie implémentées dans les grands réseaux d'opérateurs. La solution la plus utilisée est la réservation de chemins supplémentaires, ou chemins de back-up. Les chemins supplémentaires peuvent être soit réservés et disponibles en permanence, soit réservés mais utilisés par des flots qui cèdent leur place aux flots à sauvegarder.

Une protection 1:*N* indique qu'une ligne en back-up est réservée pour *N* lignes en cours d'utilisation, la ligne en back-up pouvant elle-même être utilisée. Une protection 1+*N* indique qu'une ligne en back-up est réservée pour *N* lignes en cours d'utilisation, la ligne en back-up ne pouvant être utilisée que par les lignes à protéger. Plus généralement, une protection *M*:*N* ou *M*+*N* indique que *M* lignes en back-up sont réservées pour *N* lignes actives.

Pour arriver au « cinq neuf » dans un grand réseau où les paquets doivent passer par plusieurs routeurs, il faut protéger très fortement les chemins. En effet, le taux de panne pour une liaison en fibre optique de 1 000 kilomètres est de l'ordre de 0,3 p. 1000. Les pannes peuvent avoir de nombreuses raisons, dont la plus importante est la coupure pour travaux de génie civil. Si l'on compte un temps de réparation de 12 heures par panne, qui est déjà une valeur excellente, une redondance de 1:1 ne suffit pas à atteindre les « cinq neuf » car la probabilité que les chemins primaire et secondaire

soient tous deux en panne est supérieure à 5 minutes par an. Il faut donc que la ligne de protection soit elle-même protégée.

Dans les réseaux traditionnels, la boucle locale est protégée dans le cadre de SONET par une reconfiguration qui s'effectue en 50 ms. Dans le réseau cœur, il y a toujours un chemin de rechange pour un chemin en panne. Quant à la partie entre le réseau métropolitain et l'utilisateur, sa fiabilisation s'effectue comme pour la téléphonie classique par le biais d'une alimentation indépendante du réseau électrique. Dans ce cas, il est facile d'atteindre les 99,999 %. Cependant, le prix de revient de cette fiabilisation du réseau est assez important, et les opérateurs IP hésitent du fait de la concurrence acharnée sur les prix.

SLA/SLS

Les opérateurs ont pour objectif de satisfaire les besoins de leurs clients en matière de réseau. C'est la raison pour laquelle leur première tâche est de connaître le plus précisément possible les demandes des clients. Ces demandes s'effectuent par le biais de SLA (Service Level Agreement).

Les réseaux d'opérateurs doivent en outre être en mesure de transformer ces demandes en une configuration des équipements et des lignes de transmission. Afin d'adapter leur réseau à la demande, les opérateurs ont presque tous opté pour des architectures avec signalisation. Cela consiste, avant d'envoyer le moindre paquet d'un utilisateur, à mettre en place des chemins, éventuellement avec réservation explicite de ressources. Parmi les différentes techniques de signalisation, MPLS est la plus populaire.

Une autre caractéristique importante de ces réseaux concerne l'interconnexion avec les autres opérateurs pour desservir tous les points du globe. C'est normalement le rôle de la normalisation de l'UIT-T. Cependant, cette normalisation est moins bien respectée aujourd'hui, compte tenu de la suprématie de l'IETF, qui ne spécifie pas toujours parfaitement certaines options, rendant les interconnexions entre opérateurs plus délicates.

L'objectif des opérateurs est de vendre un maximum de services à leurs clients. Les premiers d'entre eux sont évidemment la bande passante et les temps de réponse, ainsi que, de plus en plus, la sécurité, la gestion de la mobilité, l'optimisation, etc. Les réseaux privés virtuels, ou VPN (Virtual Private Network), font partie de la panoplie de solutions proposées par les opérateurs.

Le rôle d'un SLS de sécurité est de fournir les paramètres techniques du SLA pour la négociation de services de sécurité liés à la protection des données de l'utilisateur.

Comme pour le SLS de QoS, le temps de service (schedule) correspond à la durée en seconde pendant laquelle le service est assuré. Ici, le schedule peut aussi être défini en termes de quantité de trafic bénéficiant du service. Il s'exprime sous la forme de la durée divisée par la quantité d'information transportée.

Ce paramètre détermine les nœuds dans le réseau où l'opérateur peut appliquer le service de sécurité. La mise en place d'une association de sécurité, ou SA (Security Association), entre deux nœuds nécessite la configuration d'un service de sécurité sur ces deux nœuds.

La qualité de service (QoS)

Selon ces définitions, le contrôle de flux peut être considéré comme un cas particulier du contrôle de congestion. Tous deux permettent d'assurer une qualité de service, ou QoS (Quality of Service).

La qualité de service est définie par la recommandation E.800 de l'UIT-T de la façon suivante : « Effet collectif du service de performance qui détermine le degré de satisfaction d'un utilisateur du système. » Cette définition très générale est précisée dans la recommandation I.350, qui définit la QoS et la performance de réseau, ou NP (Network Performance).

La performance de réseau NP s'évalue en fonction de paramètres qui ont une signification pour l'opérateur du réseau et qui sont utilisés pour jauger le système, sa configuration, son fonctionnement et sa maintenance. La NP est définie indépendamment des performances du terminal et des actions de l'utilisateur. La qualité de service se mesure à l'aide de variables d'état, qui peuvent être directement observées et mesurées à l'endroit où l'utilisateur accède au service.

La figure Q.24 illustre comment les concepts de QoS et de NP peuvent être appliqués dans un environnement réseau. De son côté, le tableau Q.2 établit les distinctions entre QoS et NP.

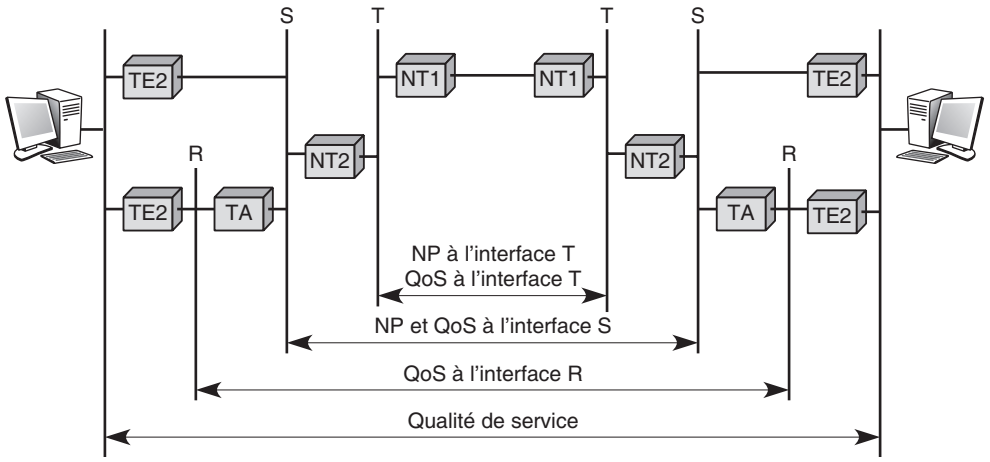


Figure Q.24

Qualité de service (QoS) et performance du réseau (NP)

Tableau Q.2 • Distinction entre QoS et NP

Qualité de service (QoS)	Performance du réseau (NP)
Orientée client	Orientée réseau
Attribut du service	Attribut de l'élément de connexion
Effet observable par l'utilisateur	Influe sur la planification, la gestion de performance et la maintenance.
Entre les points d'accès	Entre les deux points de la connexion réseau

Une matrice 3×3 a été développée par l'UIT-T dans l'annexe à la recommandation I.350 pour déterminer les paramètres à prendre en compte dans la valeur de la QoS et de la performance de réseau. Cette matrice est illustrée à la figure Q.25. Elle détermine six zones, qui doivent être définies explicitement. Par exemple, si l'on examine la première colonne, il faut déterminer la capacité des accès, celle du transfert d'informations utilisateur et enfin la capacité maximale susceptible d'être gérée lors du désengagement d'un utilisateur. La deuxième colonne correspond aux paramètres qui permettent d'assurer la validité des actions d'accès, de transfert et de désengagement. La dernière colonne se préoccupe des paramètres qui assurent le fonctionnement sécurisé de l'accès, du transfert et du désengagement.

Figure Q.25
Matrice 3×3 définissant QoS et NP

	Capacité	Validité	Sécurité de fonctionnement
Accès			
Transfert d'informations utilisateur			
Désengagement			

Le contrôle de flux est une des fonctionnalités essentielles du transfert de trames ou de paquets. Il s'agit de gérer les paquets de façon qu'ils arrivent au récepteur dans le laps de temps le plus court et surtout en évitant les pertes, en cas de surcharge, par écrasement dans les mémoires tampons des nœuds intermédiaires.

Le contrôle de congestion a pour objectif de sortir d'une congestion lorsque le contrôle de flux n'a pas permis de l'empêcher.

Le contrôle de flux s'effectue par une contrainte sur le nombre de paquets qui circulent dans le réseau. Cette limitation s'exerce soit sur le nombre de paquets en transit d'une entrée à une sortie ou sur l'ensemble du réseau, soit sur le nombre de paquets ayant le droit d'entrer à l'intérieur du réseau par unité de temps. À ces contrôles peuvent s'ajouter des techniques d'allocation des ressources, de façon à garantir qu'il n'y aura pas de congestion. Les sections qui suivent détaillent quelques-uns de ces contrôles de flux.

Le contrôle de flux dans le relais de trames

Le contrôle de flux dans le relais de trames est assuré par un contrat de trafic qui détermine en premier lieu un débit moyen à respecter par l'utilisateur, le CIR (Committed Information Rate). Ce contrôle très simple consiste à demander à l'utilisateur d'émettre un flux de débit constant, ou presque. Ainsi, l'opérateur connaît les flux qui transitent dans les nœuds de commutation et peut planifier l'ouverture ou le refus de nouvelles demandes de liaisons virtuelles. Précisons que le CIR doit être garanti pour des périodes de longueur *T.* Si *T* est relativement long, le trafic peut excéder le CIR pendant une partie de ce temps *T* et être en dessous dans une autre partie. Pour respecter cette moyenne, la quantité maximale d'informations que l'émetteur peut envoyer pendant le temps *T* est indiquée par $T \times \text{CIR} = \text{CBS}$ (Committed Burst Size).

Il est toutefois possible d'émettre des trames au-delà de la moyenne déterminée dans le contrat. Pendant une courte période de temps, le débit peut être supérieur à celui précisé dans le CIR. Cependant, le débit ne peut pas dépasser la valeur EIR (Excess Information Rate). Les trames engendrant un débit supérieur sont automatiquement détruites à l'entrée du réseau. Sur la période *T,* le trafic supplémentaire peut atteindre en moyenne la valeur EBS (Excess Burst Size), qui est égale à $T \times (\text{EIR} - \text{CIR}) = \text{EBS}$. En résumé, sur la période de longueur *T,* la quantité totale d'informations peut atteindre $T \times \text{EIR}$.

Comme nous venons de le voir, durant cette période *T,* l'utilisateur peut dépasser le trafic négocié dans le CIR, mais, à chaque dépassement de la valeur CIR, l'utilisateur se sert du bit DE (Discard Eligibility) pour indiquer les trames supplémentaires qui forment la quantité EBS. L'utilisateur qui dépasse son contrat de trafic a intérêt à marquer les trames qui ne sont pas très importantes par rapport à la qualité de service, de façon que l'opérateur puisse les détruire dans le réseau en cas de surcharge. Le bit DE = 1 indique que la trame peut être détruite.

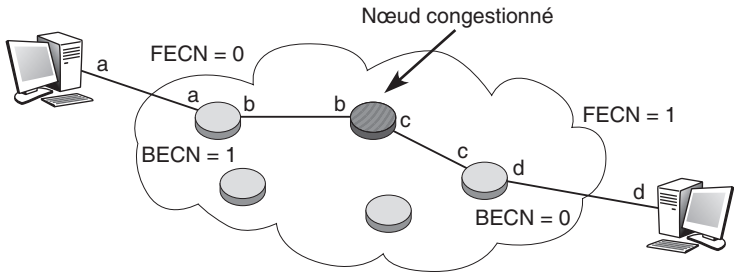
Deux bits supplémentaires ont été introduits dans la structure de trames pour permettre la mise en place d'un contrôle de flux :

- le bit FECN (Forward Explicit Congestion Notification) ;
- le bit BECN (Backward Explicit Congestion Notification).

Le premier de ces bits permet à un nœud congestionné de faire connaître son état au récepteur. Quant au second, il a pour fonction de faire remonter la connaissance de l'état de congestion d'un nœud à l'émetteur. La figure Q.26 illustre l'utilisation de ces deux bits. Le bit FECN est mis à 0 en sortant de l'émetteur avec la référence a. Lorsqu'il transite dans le nœud congestionné, il passe à la valeur 1 et arrive au récepteur avec la référence d en portant la valeur FECN = 1, qui indique au récepteur qu'un des nœuds traversés dans le circuit virtuel est congestionné. Dans l'autre sens, un processus analogue se produit : le bit BECN est mis à 0 en sortant de la station terminale. Ce bit est modifié par le nœud congestionné, qui le transforme en la valeur 1. À l'arrivée au récepteur, celui-ci prend conscience que la route sur lequel il envoie des trames possède un nœud congestionné.

Figure Q.26

Contrôle de congestion dans le relais de trames



Les bits FECN et BECN sont toujours mis à 0, respectivement par l'émetteur et le récepteur, dans la structure de la trame émise sur la liaison virtuelle. Lorsque ces bits passent par un nœud congestionné, ils sont automatiquement mis à 1. Le récepteur et l'émetteur sont donc informés de l'état de congestion d'un nœud par la réception de ces deux bits à 1.

L'information concernant une congestion sur la liaison virtuelle est assez sommaire, puisque la seule chose qu'on sache est qu'un nœud a dépassé un certain seuil de trafic ou un nombre de mémoires tampons utilisées sur la liaison virtuelle. Les actions que doivent entreprendre l'émetteur et le récepteur sont totalement laissées à l'initiative de l'opérateur ou de l'utilisateur.

Il existe des intervalles de temps pendant lesquels aucune trame ne transite du récepteur vers l'émetteur. Dans ce cas, une trame de supervision, appelée CLLM (Consolidated Link Layer Management), est utilisée pour transporter des informations de supervision. Cette trame permet à un nœud congestionné de diffuser vers ses voisins son état de congestion. Les nœuds voisins peuvent à leur tour avertir leurs voisins, et ainsi de suite. Cette trame de supervision est émise sur un circuit virtuel de numéro 1023 lorsque le DLCI est sur 2 octets.

Le contrôle de flux dans les réseaux ATM

Les réseaux ATM doivent pouvoir prendre en charge toutes les catégories de demandes de service possibles. Les récents progrès dans les domaines techniques de la commutation, du multiplexage et de la transmission par fibre optique ont rendu possible l'intégration de tous les types de services de communication, tels les services à haut débit et haute qualité, comme la TVHD ou le transfert de grands volumes de données à haute vitesse, mais aussi les services à faible débit et sans contrainte au niveau des erreurs, comme la parole téléphonique.

Les difficultés du contrôle de flux ATM proviennent des différentes qualités de service requises par tous ces services. L'efficacité de la gestion de la bande passante réalisée par le multiplexage statistique des services constitue l'un des avantages des réseaux ATM. Cependant, ce multiplexage à débit irrégulier peut créer des congestions internes.

Le multiplexage statistique et le contrôle des réseaux ATM

Dans un multiplexage statistique, une ligne du réseau peut être partagée par plusieurs circuits virtuels. L'allocation des ressources est réalisée de façon statistique. Le total des débits crêtes (Σp_i) des connexions se partageant la même liaison peut dépasser la bande passante (B) de la ligne :

- B : bande passante disponible ;
- p_i : débit crête de la connexion i ;
- n : nombre de connexions simultanées sur la ligne.

Le total des débits moyens (Σa_i) ne doit pas dépasser la bande passante de la source :

a_i = débit moyen de la connexion i.

Le gain réalisé par le multiplexage statistique peut être défini de la façon suivante :

L'augmentation du SMG est réalisée au prix d'une réduction de la qualité de service, exprimée sous la forme d'un délai de transit, d'un taux de perte ou d'une gigue (variation du délai de transfert par cellule). En règle générale, le SMG dépend du nombre de connexions et de la bande passante du conduit virtuel.

Prenons comme exemple les résultats de statistiques sur le comportement de la vidéoconférence, où le débit moyen est de 5 Mbit/s et le débit crête de 15 Mbit/s. Quand 16 connexions de vidéoconférence sont établies sur une ligne à 155 Mbit/s, le taux de perte est négligeable si 10 Mbit/s sont alloués à chaque connexion au lieu de 15 Mbit/s. Dans ce cas, la valeur du SMG est 1,5. Dans le cas d'un multiplexage de 30 sources, la bande passante requise s'approche de la somme des débits moyens, et la valeur du SMG atteint 3, mais avec un taux de perte de paquets important et des images projetées sérieusement endommagées. Le contrôle d'admission de connexion, ou CAC (Connection Admission Control), doit décider si une nouvelle demande de connexion est acceptable ou non en considérant la charge du réseau, la bande passante disponible, les descripteurs de trafic de la nouvelle connexion et la QoS requise.

De très grands débits sont possibles dans les réseaux ATM grâce aux fonctions simplifiées des nœuds intermédiaires. En fait, il n'y a pas de contrôle de flux au niveau de la couche ATM, ce qui nécessite l'application de certaines stratégies de contrôle pour limiter des trafics entrants dans le réseau. On peut dire que les stratégies de contrôle de congestion pour les réseaux ATM sont plutôt préventives que réactives.

Pour certains types de données sensibles aux pertes mais peu exigeants en délais de propagation (données de types 3/4 ou 5 de la couche AAL), on peut utiliser un mécanisme de contrôle de flux au niveau de la couche AAL ou d'une couche supérieure. Ce mécanisme peut être utilisé soit comme une méthode de reprise des cellules erronées ou perdues, soit comme une méthode de contrôle de flux réactive sur une congestion, soit encore comme une méthode de synchronisation entre l'émetteur et le récepteur. Dans le cas où une méthode de contrôle de flux réactive est utilisée, un nombre suffisant de tampon est exigé pour les services de données dans les nœuds intermédiaires. Ainsi, les cellules éventuellement bloquées lors des débordements peuvent être reçues. Pour les services temps réel, un nombre trop important de tampons peut dégrader le temps de réponse.

Même pour ce type de service, le contrôle de flux de bout en bout peut améliorer l'utilisation des ressources et le taux de perte des cellules.

La mise en œuvre des techniques de contrôle de congestion dépend des types de commutateurs utilisés. Par exemple, l'ordonnancement des priorités dans un commutateur est inutile si ce dernier ne dispose pas de mémoire tampon. Même s'il existe des mémoires tampons dans le commutateur, les performances sont influencées par plusieurs facteurs, tels que la taille de la mémoire, l'architecture du commutateur, le type de mémoire, etc.

Un développement réussi des méthodes de contrôle du réseau ATM exige des interactions douces entre les méthodes de contrôle de congestion, les fonctions OAM (Operations And Maintenance), les mécanismes de transport VC/VP, les commutateurs ATM, etc.

La qualité de service et le contrôle d'admission

Le groupe d'étude XVIII de l'UIT-T a énormément travaillé sur le problème du contrôle de flux dans les réseaux ATM, car c'était un élément stratégique pour le succès de cette technique de transfert.

Rappelons que le mode de transfert temporel asynchrone ATM (Asynchronous Transfer Mode) est le mode de transfert cible pour le RNIS large bande. L'information est transmise dans des blocs de taille fixe (53 octets), appelés cellules, chacune d'elles étant constituée d'un en-tête de 5 octets et d'un champ d'information de 48 octets. Les cellules sont transmises dans un circuit virtuel, et le routage se fonde sur l'identificateur de voie virtuelle VCI (Virtual Channel Identifier) et l'identificateur de conduit virtuel VPI (Virtual Path Identifier) de l'en-tête de la cellule. Le réseau ATM adopte une architecture simplifiée, fondée sur une commutation de cellules en mode avec connexion. Il n'y a ni contrôle d'erreur, ni contrôle de flux au niveau de la couche ATM. L'acheminement des cellules n'est pas dynamique. Les cellules appartenant à une même connexion sont transportées en séquence à travers le réseau, le long d'un circuit virtuel.

L'ATM a été choisi comme mode de transfert pour le RNIS large bande au détriment de son concurrent, le mode de transfert temporel synchrone, ou STM (Synchronous Transfer Mode), en raison du gain économique qu'il apporte grâce au multiplexage statistique. Cependant, le multiplexage statistique de trafic en rafale peut provoquer des problèmes de congestion. Les travaux de l'UIT-T visent à minimiser cette congestion et à maximiser le taux d'utilisation du réseau, tout en garantissant la qualité de service spécifiée par l'utilisateur. Ces efforts ont abouti à la définition d'un contrat de trafic dépendant de la qualité de service requise par l'utilisateur et à la normalisation des fonctions de gestion de trafic.

Avant d'examiner plus avant ces fonctions, définissons la qualité de service. Une classe de qualité de service peut préciser des paramètres de performance (QoS spécifiée) ou non (QoS non spécifiée). Dans ce dernier cas, on parle de service best-effort, c'est-à-dire du meilleur effort possible de la part du réseau pour satisfaire la demande de l'utilisateur.

L'utilisateur et l'opérateur du réseau ATM négocient, *via* l'interface UNI, un contrat de trafic. Ce contrat de trafic doit contenir une classe de QoS, un descripteur de trafic sur la connexion demandée et une définition de la conformité.

Le descripteur de trafic est un sous-ensemble des paramètres de trafic qui servent à décrire les caractéristiques du trafic des cellules sur la connexion. Ce descripteur contient un nombre de variable qui diffère selon qu'il s'agit des recommandations de l'UIT-T ou des propositions de l'ATM Forum.

Les variables UITT sont les suivantes :

- Descripteur du trafic source, qui peut lui-même contenir :
  - le débit crête PCR (Peak Cell Rate) ;
  - le débit projeté SCR (Sustainable Cell Rate).
- Durée des rafales tolérées BT (Burst Tolerance).
- Tolérance de gigue CDV (Cell Delay Variation).
- Algorithme du taux de génération des cellules GCRA (Generic Cell Rate Algorithm), qui définit la conformité du trafic. Deux paramètres sont utilisés : le temps minimal entre deux émissions de cellule et une capacité de mémorisation maximale. Lorsqu'une cellule se présente et que la capacité maximale est atteinte (cellule non conforme), soit cette cellule est détruite, soit elle est émise en surplus, soit elle prend la place d'une autre cellule, qui, elle-même, peut être détruite ou envoyée en surplus. C'est là que le bit CLP devient opérationnel : si la cellule est envoyée en surplus, elle est marquée par le bit CLP = 1, qui permet à un nœud interne du réseau de la détruire en cas de congestion. Il y a donc deux classes de priorité : CLP = 0, qui correspond aux cellules les plus prioritaires, et CLP = 1, pour les cellules pouvant être détruites dans le réseau.
- Paramètres expérimentaux, qui permettent de faire passer dans la demande des caractéristiques spécifiques, correspondant le plus souvent à des propriétés propres à des constructeurs.

L'ATM Forum a déterminé un ensemble de combinaisons de paramètres de trafic pour simplifier les demandes. Le bit CLP est égal soit à 0, soit à 0 ou 1, ce que nous indiquons respectivement par CLP = 0 et CLP = 0 + 1 :

- PCR pour CLP = 0 et PCR pour CLP = 0 + 1 ;
- PCR pour CLP = 0 et PCR pour CLP = 0 + 1 avec un marquage demandé par le réseau en cas de cellule non conforme ;
- SCR pour CLP = 0 et PCR et BT pour CLP = 0 + 1 ;
- SCR pour CLP = 0 et PCR et BT pour CLP = 0 + 1 avec marquage ;
- PCR pour toutes les cellules CLP = 0 + 1 ;
- PCR, SCR et BT pour toutes les cellules CLP = 0 + 1 ;
- Best-effort service, PRC pour toutes les cellules CLP = 0 + 1.

Le contrôle d'admission de connexion

On désigne par contrôle d'admission de connexion, ou CAC, l'ensemble des actions exécutées par le réseau au cours de la mise en place de la connexion pour déterminer si cette demande de connexion doit être acceptée ou refusée. La demande d'ouverture de

la connexion fait partie de la demande CAC. C'est la principale méthode de contrôle de congestion préventive dans les réseaux ATM.

Cette méthode permet d'accepter ou de rejeter une nouvelle demande de connexion en considérant la bande passante disponible, le descripteur de trafic de la nouvelle connexion et son exigence en terme de qualité de service. L'objectif du CAC est d'accepter une nouvelle connexion si les ressources sont suffisantes et d'assurer la qualité de service demandée pour les connexions déjà ouvertes.

Dans les réseaux de type STM, la décision est simple. Si la somme des débits crête, comprenant le débit crête de la nouvelle demande de connexion sur un VP ou sur une liaison donnée, ne dépasse pas la bande passante disponible comme l'indique la formule suivante :

$$\sum_{i=1}^{N} pi < B$$

la demande d'une nouvelle connexion est acceptée.

Cette approche simple peut être adoptée pour toutes les sources de trafic de VBR, ou débit binaire variable, et de CBR, ou débit binaire constant. Cependant, il est possible d'obtenir une utilisation optimisée des ressources par le multiplexage statistique de sources de trafic VBR.

Puisque le réseau ATM doit supporter des VC avec des exigences diverses de QoS (délai d'établissement d'une connexion, taux de perte des cellules, délai de transmission, etc.), la conception de méthodes CAC efficaces est complexe. La méthode la plus simple pour s'attaquer à ce problème, tout en satisfaisant les diverses demandes de QoS, consiste à classer les sources de trafic en fonction de leurs caractéristiques, des exigences de QoS, etc. Ensuite, la bande passante d'une liaison ou d'un VP est allouée pour chaque classe et contrôlée indépendamment.

Les techniques de contrôle de flux ATM

De nombreuses techniques de contrôle de flux ont été définies par l'UIT-T pour l'ATM :

- Le contrôle des paramètres de l'utilisateur et du réseau UPC/NPC (Usage Parameter Control/Network Parameter Control) regroupe l'ensemble des actions exécutées par le réseau pour surveiller et gérer le trafic offert à l'accès utilisateur et à la conformité de la connexion ouverte à l'accès réseau. Le principal objet de cette technique est de protéger le réseau contre des violations du contrat de trafic pouvant conduire à une dégradation de la qualité de service sur des connexions d'autres utilisateurs.
- La gestion de priorité par l'utilisateur peut employer deux classes de services pour la perte des cellules. Si le bit CLP est à 0, la cellule est prioritaire. Si cet élément binaire est 1, la cellule est moins prioritaire et peut être détruite dans un nœud congestionné.
- La gestion des ressources du réseau NRM (Network Resource Management) regroupe les prévisions d'attribution des ressources du réseau pour optimiser la séparation des trafics en fonction des caractéristiques du service.
- Les techniques de rétroaction (feed-back) forment l'ensemble des actions exécutées par les usagers et le réseau pour réguler le trafic sur les connexions ATM.

Parmi les méthodes de gestion de trafic permettant d'éviter les surcharges du réseau, on trouve les mécanismes de contrôle de trafic visant à rendre le trafic conforme au contrat de trafic (traffic shaper), les protocoles de réservation rapide FRP (Fast Reservation Protocol) et EFCI/BCN (Explicit Forward Congestion Indication/Backward Congestion Notification).

Le défi est toujours de concevoir des mécanismes de contrôle de flux qui permettent d'utiliser efficacement les ressources du réseau et de satisfaire la qualité de service requise. Dans les réseaux traditionnels, c'est le mécanisme de contrôle de flux par fenêtre qui est surtout utilisé. Dans les réseaux ATM, en revanche, du fait que le délai de propagation est très long par rapport au temps d'émission, les protocoles de type « envoyer et attendre » ne sont pas performants. Plusieurs autres méthodes de contrôle de flux adaptatif peuvent également être implémentées au niveau de la couche AAL ou à un niveau supérieur. En règle générale, ces contrôles travaillent sur la taille de la fenêtre, ou sur le débit, la valeur des paramètres étant décidée par le nœud destinataire en fonction de l'état du réseau.

Les hypothèses implicites à ce système, telles que la connaissance de l'état du réseau ou le temps de propagation suffisamment court pour faire un aller-retour de l'information sur l'état du réseau, posent toutefois problème. Même si une congestion dans le réseau est détectée, il est difficile de prévoir sa durée, de localiser à temps le nœud congestionné, de mesurer l'importance de la congestion et donc d'en déduire la taille de la fenêtre.

Plusieurs contrôles d'accès et de trafic ont été définis par l'UIT-T. Le rôle du contrôle des paramètres de l'utilisateur et du réseau UPC/NPC est de protéger les ressources réseau contre des utilisateurs malveillants et des fonctionnements involontaires susceptibles de dégrader la qualité de service des connexions établies auparavant. L'UPC/NPC a pour fonction de détecter les violations des contrats et d'exécuter les fonctions appropriées.

Pour éviter les pertes de cellules causées au niveau UPC/NPC, l'émulation de l'UPC/NPC peut être réalisée au niveau de l'émetteur. Cette fonction est appelée STS (Source Traffic Smoothing) pour la distinguer de l'UPC/NPC. Du point de vue de l'utilisateur, la fonction STS présente des inconvénients puisqu'elle introduit un délai supplémentaire et nécessite des mémoires tampons supplémentaires.

L'algorithme VSA (Virtual Scheduling Algorithm) recommandé dans la norme I.371 représente une première possibilité pour détecter les situations irrégulières et redonner un flux acceptable par le contrat de trafic. Il a pour rôle de surveiller le débit crête d'une connexion ATM tout en garantissant une limite sur la gigue. En termes simplifiés, si une cellule arrive plus tôt que prévu, elle est mise en attente jusqu'à l'instant où elle aurait dû arriver. À ce moment seulement, elle est émise sur le réseau et est conforme. Si la cellule arrive plus tard que prévu, soit elle arrive dans un intervalle suffisamment court pour rester conforme à la gigue — elle est alors conforme —, soit elle arrive trop tard pour rester dans la limite acceptable et est jugée non conforme. Les cellules conformes sont indiquées par CLP = 0, et les cellules non conformes par CLP = 1.

Le leaky-bucket est un autre mécanisme de l'UPC/NPC et du STS. Il est composé d'un compteur (c), d'un seuil (t) et d'un taux de vidage, le leaky-rate (l). Le compteur est incrémenté chaque fois qu'une cellule arrive dans le tampon et décrémenté par le leaky-rate. Si une cellule arrive au moment où la valeur du compteur est égale au seuil, elle n'est pas mémorisée dans le tampon. En d'autres termes, quand le tampon est plein, la cellule qui arrive est rejetée.

Si le débit crête de la source est *p* et la durée de la rafale *b,* le compteur est augmenté à la fin de la rafale de la façon suivante :

$c = c + b\ (p - 1)$ si cette valeur est inférieure à *t,* sinon $c = t$.

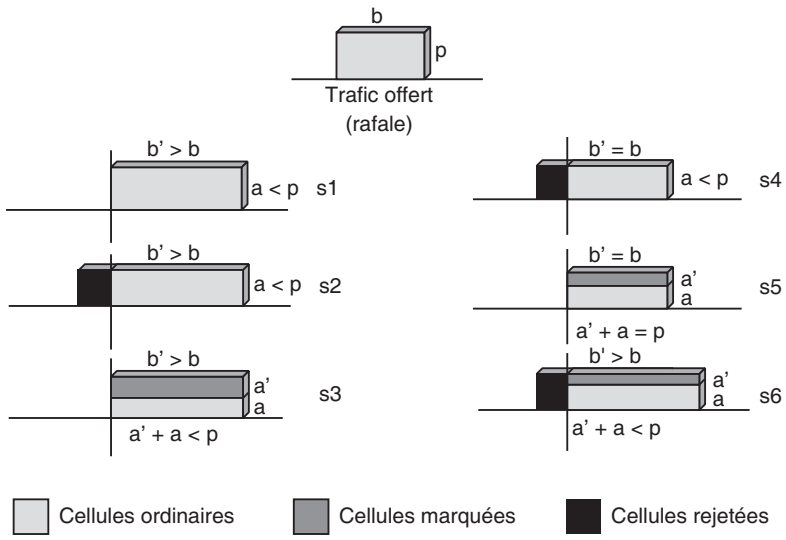
Pendant la durée d'un silence de longueur *s,* le compteur est diminué comme suit :

$c = c - sl$ si cette valeur est supérieure à 0, sinon c = 0.

Un trafic en avalanche peut être transformé en l'une des formes illustrées à la figure Q.27. Ces formes sont dessinées sans qu'il soit tenu compte de la séquence réelle des cellules détruites ou marquées. Les hauteurs a et a' correspondent respectivement au débit conforme (cellules ordinaires) et au débit non conforme (cellules marquées). La longueur b' correspond à la durée de la rafale après la mise en forme par le leaky-bucket. Les paramètres b et p représentent respectivement la longueur de la rafale et le débit crête du trafic offert au leaky-bucket. Un choix approprié des valeurs des paramètres l et b permet de redonner au trafic la forme désirée. Par exemple : un service de données sensible aux pertes mais qui tolère des délais peut être remis en forme (*s*1 sur la figure). Cette fonction peut être exécutée dans un terminal afin de respecter le contrat de trafic. Dans ce cas, un tampon suffisamment grand est nécessaire pour le terminal. Si l'état du réseau est connu à temps, la perte des cellules peut être évitée grâce au contrôle dynamique du débit du leaky-bucket (leaky-rate).

Un délai inacceptable peut provenir d'une attente trop longue dans une grande mémoire tampon. Pour les services sensibles au délai, comme la vidéo ou la parole téléphonique, le choix des formes s2, s3, s4 ou s5 est préférable.

Figure Q.27
Effet de contrôle du leaky-bucket



Le contrôle de flux des classes de services ATM étant détaillé à l'annexe G, nous ne le reprenons pas ici.

La signalisation H.323

En 1996, l'UIT (Union Internationale des Télécommunications) proposa la famille de protocoles H.32x, très fortement soutenue par Microsoft et Intel. L'UIT parvint rapidement à convaincre les différents équipementiers et fournisseurs de services de la nécessité d'adopter pour norme commune ces protocoles H.32x.

Sans être précurseurs ni de la téléphonie, ni de la vidéo, ni même de la conférence, ces protocoles constituent l'initiative la plus aboutie et la plus marquante des débuts de la signalisation multimédia. La généralisation progressive et systématique de H.323 a fini par faire céder les plus récalcitrants des acteurs du multimédia, qui ont abandonné leurs solutions propriétaires, pourtant très évoluées. La ToIP (Telephony over IP) trouvait là son protocole fédérateur et pouvait prendre son envol.

Les premiers travaux sur H.323 ont débuté en mai 1995. Depuis lors, six versions standardisées se sont succédé, apportant leurs lots de nouveautés et d'améliorations.

Initialement prévue dans le cadre très restreint des réseaux locaux n'apportant aucune garantie de qualité de service, la version 1 de la recommandation H.323 de l'IUT-T prit le nom de « Systèmes et équipements visiophoniques pour réseaux locaux offrant une qualité de service non garantie ». Il faudra attendre les versions suivantes pour qu'elle soit renommée « Système de communication multimédia fonctionnant en mode paquet ». Tout porte à croire que ses concepteurs n'avaient pas imaginé rencontrer un tel succès auprès des industriels, et que le protocole a ensuite évolué pour adresser des réseaux plus étendus, de type Internet.

Cette version balbutiante présentait de sévères limitations, notamment des performances, illustrées, par exemple, par la lenteur de la mise en place d'une communication ou la sécurité, totalement absente. Surtout, la spécification était imprécise quant à la manière d'implémenter le protocole, ce qui entraîna d'importants problèmes d'interopérabilité entre les différents constructeurs.

Remarquable à bien des égards, la version 2 (1998) améliora considérablement un protocole encore instable et perfectible, en particulier les délais d'établissement d'une communication grâce à la procédure de FastConnect, qui permettait de paralléliser les annonces.

Une autre nouveauté fut incarnée par la procédure H.245 tunneling, qui permettait d'encapsuler des messages H.245 dans des messages H.225.0 (Q.931). De nouveaux services étaient supportés par le protocole, dont les classiques services de renvoi et de transfert d'appel, et des mécanismes de sécurité étaient rassemblés dans la spécification H.235. Cette dernière couvrait la plupart des mécanismes de sécurité, incluant l'authentification et le cryptage des flux de données.

Des paramètres de gestion de la qualité de service étaient ajoutés dans les messages de signalisation, permettant de s'intégrer dans une architecture de type DiffServ ou RSVP, par exemple. Néanmoins, la gestion elle-même de la qualité de service ne faisait pas partie du protocole, H.323 n'offrant aucune garantie de réservation de ressources. Seuls des paramètres de qualité de service pouvaient être ajoutés dans la structure des paquets

et pouvaient être utilisés par les terminaux. Au niveau du réseau cœur, ces paramètres devaient être exploités et traités par des mécanismes externes au protocole.

Plus généralement, la manière d'ajouter des services supplémentaires était décrite dans le document H.450.1, qui définissait une plate-forme générique.

Les documents suivants, numérotés H.450.x (x > 1) décrivent de tels services :

- H.450.2 détaille le service de transfert d'appel, qui transforme une communication entre deux postes A et B en une communication entre A et un autre poste C. Elle est classiquement utilisée dans les entreprises pour mettre l'appelant en relation avec la personne souhaitée.
- H.450.2 détaille le service de redirection d'appel, qui remplace un poste appelé par un autre, avec ou sans condition.

Grâce au support du DTMF (Dual-Tone Multi-Frequency), le protocole H.323 version 2 permettait la création de nouveaux services vocaux. Au contraire de la téléphonie par impulsion, les codes DTMF correspondent à des fréquences. En assignant à chaque touche du terminal un code DTMF unique, il devenait possible à un serveur d'interpréter les saisies de l'utilisateur appelant et de lui fournir un service adéquat en retour. Auparavant, les messages de signalisation ne transmettaient qu'une partie de ces informations DTMF, ce qui ne permettait pas d'interpréter pleinement ces signaux.

Enfin, la recommandation H.323 permettait d'utiliser des alias à la place des adresses IP afin d'identifier les utilisateurs. Ces alias respectent le format des URL traditionnellement utilisées pour désigner une ressource unique sur Internet.

Globalement, la version 3 de H.323 (1999) a apporté moins de nouveautés fondamentales que la précédente. Si la version 2 corrigeait en profondeur plusieurs imperfections de la norme initiale, la 3 contribuait à l'amélioration du protocole, sans le bouleverser en profondeur.

Retenons notamment les trois améliorations suivantes de cette version :

- Gestion de nouveaux services complétant la gamme existante, tels que les suivants :
  - CLIP (Connected Line Identification Presentation), ou présentation de l'identification de l'appel, aussi connu par son appellation commerciale d'affichage du numéro, qui permet à l'appelé de connaître le numéro d'appel de l'appelant.
  - CLIR (Connected Line Identification Restriction), ou restriction de l'identification de l'appel, plus connu sous son appellation commerciale de masquage du numéro, qui permet à l'appelant de limiter les possibilités d'identification de son numéro.
- Ajout de services destinés à compléter la série H.450.x, tels que la mise en attente ou la notification d'appel ou de message en attente.
- Intégration avec la signalisation SS7, utilisée classiquement dans les réseaux téléphoniques commutés.

L'annexe E de la norme prévoyait l'utilisation du protocole de transport UDP au lieu de TCP, les deux protocoles pouvant être utilisés au choix.

La version 4 (2000) a axé ses développements sur la robustesse, à la fois en terme de passage à l'échelle (scalabilité), de flexibilité et de fiabilité. Le protocole confirmait ainsi

sa suprématie par une technologie solide et véritablement en phase avec les besoins et les usages de tous types, y compris professionnels. La recommandation proposait pour cela des changements radicaux par rapport aux versions précédentes.

Afin d'offrir un cadre de développement stable à la norme, cette version 4 proposait de formaliser les améliorations sous forme d'extensions au protocole, mais sans modifier ses fondations. Autrement dit, les améliorations ne remettaient plus en cause le principe de fonctionnement du protocole mais se présentaient sous la forme de modules génériques, appelées GEF (Generic Extensibility Framework).

Le protocole H.323 devenait de la sorte stable, tout en autorisant des enrichissements progressifs. Il offrait en outre un bon niveau de souplesse puisque les équipementiers étaient libres d'implémenter certaines extensions des GEF et pas d'autres, tout en restant compatibles avec le socle du standard. De fait, le protocole atteignait une certaine maturité, et ses acteurs n'étaient plus obligés de suivre en permanence les évolutions et de mettre à jour la norme pour garantir la compatibilité.

La notion de *gatekeeper alternative,* permettant le basculement des appels en cas de panne d'un gatekeeper, ou « garde-barrière », était explicitée dans le document. À cette fin, l'annexe R proposait des mécanismes permettant de modifier dynamiquement le routage des appels en cas de panne.

Dans cette version, le protocole H.323 se rapprochait du protocole MGCP (Media Gateway Control Protocol), dont les travaux étaient menés en parallèle. Il offrait en effet une nouvelle conception architecturale, qui décomposait l'équipement de passerelle originale, jugé trop lourd, en deux sous-parties. Cette nouvelle répartition reprenait le modèle proposé conjointement entre le groupe de travail numéro 16 de l'IUT-T et le groupe de travail MEGACO de l'IETF. L'IUT en proposera une nouvelle recommandation, numérotée H.248.

Le protocole RTP (Real-time Transport Protocol) permet de séparer les flux audio et vidéo, ce qui offre aux récepteurs une plus grande flexibilité en leur permettant de choisir indifféremment de recevoir l'un ou l'autre, avec un système de priorité. L'inconvénient de ce système est que le récepteur doit synchroniser les deux flux pour transmettre de façon parfaitement homogène la diffusion du son avec la vidéo en simultané. Cela suppose des capacités complémentaires, à la fois de l'émetteur, qui sépare la voix de la vidéo, et du récepteur, qui assure la synchronisation des deux flux.

Avec la version 4 de H.323, le protocole proposait une solution de rechange facultative permettant de multiplexer la voix et la vidéo dans un même flux, de manière que l'émetteur n'ait plus à se soucier de la synchronisation de la vidéo par rapport à la voix et qu'il puisse jouer les données sans que des décalages du son et de l'image soient perceptibles.

En plus de proposer la gestion de nouveaux services, la version 4 permettait la mobilité de l'utilisateur et l'intégration avec les réseaux GSM et UTMS. En outre, le concept « d'enregistrements additionnels » donnait aux utilisateurs la possibilité de s'enregistrer plusieurs fois auprès des gatekeepers avec plusieurs pseudonymes différents. Les paquets UDP étant trop courts pour permettre de spécifier dans une même requête tous les pseudonymes à enregistrer, ce mécanisme d'enregistrements additionnels permettait de générer à la suite plusieurs courtes requêtes venant compléter les précédents enregistrements.

L'adressage H.323 était fixé, et une URL H.323 pouvait désormais prendre la forme *h323:utilisateur@domaine*, où le préfixe *h323* spécifiait qu'il s'agissait d'une adresse à interpréter par le protocole H.323, la partie *utilisateur* était un identifiant de l'utilisateur (ou éventuellement d'un service) et la partie *domaine* désignait l'entité capable de traduire cette URL, classiquement le gatekeeper susceptible de prendre en charge la résolution de cette adresse. La façon de résoudre effectivement cette adresse ne sera donnée que dans la version suivante.

La version 5, de 2002, est mineure par rapport aux précédentes. On peut la considérer comme une version de maintenance, qui répondait à un certain nombre de demandes et besoins. Reprenant la philosophie de stabilité initialisée par la version 4, avec le cadre générique des GEF, cette version 5 proposait des améliorations, avec la série de recommandations H.460.x, dont le tout premier document, H.460.1, expliquait ce nouveau dispositif. La recommandation H.460.9 permettait quant à elle aux terminaux de fournir les statistiques RTCP.

L'annexe O expliquait comment utiliser les serveurs de domaines DNS (Domaine Name Server) pour effectuer les résolutions de noms des adresses (URL) utilisées dans les identifications des abonnés H.323. L'interrogation des serveurs DNS pouvait s'effectuer selon différents procédés, tel ENUM (tElephone NUmber Mapping), qui associe un nom identifiant un utilisateur (par exemple l'utilisateur dont l'identifiant est *albert@exemple.com*) avec un numéro de téléphone conventionnel (au format à dix chiffres, comme 0102030405), ou A Record (Address Record), qui associe un nom d'utilisateur avec une adresse IP (192.168.1.15 pour une adresse en réseau local, par exemple).

La version 5 gérait le protocole SCTP (Stream Control Transmission Protocol) comme solution de rechange aux protocoles de transport TCP et UDP.

Au centre de la version 6, de 2006, on retrouve une philosophie modulaire, avec de multiples perfectionnements et des procédures simplifiées et épurées, destinées à rendre H.323 encore plus accessible. Quelques améliorations sont aussi proposées, comme des supports plus larges, par exemple, de codecs (GSM, iLBC et H.264 sont pris en charge) ou de spécifications de QoS (H.361 notamment).

Le concept de *gatekeeper affectée,* imposant un gatekeeper fixe à un terminal, complète celui de *gatekeeper alternatif* offert depuis la version 4. En termes de sécurité, les mécanismes sont complètement refondus. Le document de référence H.235 est restructuré et décomposé en plusieurs recommandations, numérotées de H.235.0 à H.235.9.

Les recommandations H.460.17, H.460.18 et H.460.18 répondent au problème de la traversée des réseaux avec translation d'adresse IP, ou NAT (Network Address Translation) et des filtres pare-feu, qui pénalisaient le protocole H.323. Pendant longtemps, les communications H.323 ne pouvaient en effet être mises en place dans les entreprises utilisant un plan d'adressage privé et des solutions de pare-feu, car le protocole H.323 utilise des ports dynamiques qui ne sont généralement pas supportés par les pare-feu ordinaires.

La translation des adressages privés et logiciels des pare-feu est une solution déployée aujourd'hui presque systématiquement dans les entreprises, ainsi que bien souvent chez les particuliers. Si certains pare-feu perfectionnés et onéreux proposent des méthodes

propriétaires pour permettre aux flux H.323 d'être filtrés correctement, la solution générale n'est véritablement donnée que dans ces nouvelles recommandations H.460.

Ces dernières spécifient les procédures à implémenter dans les gatekeepers et les terminaux pour passer les translations d'adresses et traverser les pare-feu. Le principe de ces procédures est de conserver une connexion persistante TCP entre les terminaux et le gatekeeper pour assurer les communications.

Une nouvelle entité est introduite pour permettre aux terminaux n'implémentant pas encore les procédures de la version 6 de H.323 de traverser quand même les réseaux nattés et filtrés. Il s'agit en ce cas d'un proxy particulier auquel s'adressent les terminaux et qui agit comme un intermédiaire pour relayer les messages de signalisation vers leur destinataire. En quelque sorte, si les terminaux n'arrivent pas à joindre leurs correspondants parce que leurs flux sont difficilement interprétés, le proxy interprète et reformate les flux avant de les envoyer vers leur destinataire. Ces derniers utilisent eux aussi le proxy afin que leurs flux soient conformes à ce qu'attendent les émetteurs.

Architecture et fonctionnalités du protocole H.323

Le protocole H.323 s'articule autour d'une architecture particulière décrite dans ce qui suit. Cette architecture concentre les fonctionnalités autour d'entités, et, pour cette raison, le protocole H.323 est considéré comme fortement centralisé. Nous allons définir et détailler chacune des entités introduites par le protocole H.323.

Les quatre entités d'une architecture H.323

Le protocole H.323 axe très fortement ses communications sur une typologie d'équipements en proposant une architecture sur laquelle se fonde son fonctionnement.

La terminologie anglaise étant couramment employée dans les documentations françaises, il convient de la connaître. Dans ce qui suit, les premiers termes donnés peuvent être considérés comme les plus courants.

Une architecture H.323 est généralement composée des quatre catégories d'entités suivantes :

- Terminaux (au minimum deux). Ce sont les équipements de traitement destinés aux utilisateurs, leur permettant d'émettre et de recevoir des appels. Deux terminaux doivent au minimum être présents pour qu'une communication ait lieu.
- Gatekeeper, ou garde-barrière. C'est l'équipement permettant la localisation des utilisateurs. Ces derniers peuvent s'identifier entre eux par des noms, auxquels il faut attribuer l'adresse IP correspondante dans le réseau ou, si l'appelé n'est pas situé dans un réseau IP, la localisation de l'entité intermédiaire à joindre pour l'appel. Outre cette fonction primordiale, un gatekeeper remplit tout un ensemble de fonctions complémentaires de gestion et de contrôle des communications, certaines étant indispensables et d'autres facultatives.
- Passerelle, ou gateway. C'est l'équipement permettant à des utilisateurs du réseau IP de joindre les utilisateurs qui sont actifs sur d'autres types de réseaux téléphoniques,

RTC, RNIS ou RTC. On peut avoir autant de passerelles différentes que nécessaire, suivant la nature des réseaux non-IP à interconnecter.

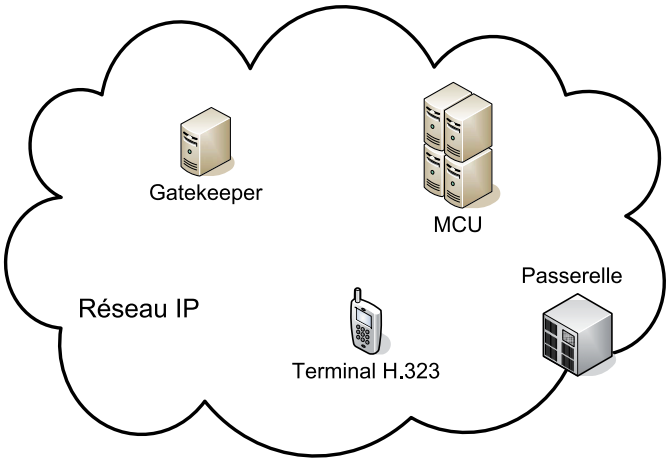
- MCU (Multipoint Control Unit), ou unité de contrôle multipoint, parfois appelée pont multipoint. C'est l'équipement permettant la gestion des conférences, c'est-à-dire les communications multimédias mettant en jeu plus de deux interlocuteurs. Ces derniers doivent préalablement se connecter à la MCU, sur laquelle s'établissent les demandes et négociations des paramètres à utiliser lors de la conférence.

Ces quatre entités sont illustrées à la figure Q.28.

Avant de détailler chacune de ces entités, les deux définitions suivantes doivent être connues :

- **Points de terminaison.** Terminaux, gateway et MCU sont des entités auxquelles les émetteurs peuvent s'adresser directement pour communiquer. Contrairement au gatekeeper, qui joue un rôle intermédiaire de contrôle et de gestion, ces entités sont des points de terminaison des appels (aussi appelés endpoints).
- **Zone et système H.323.** La nomenclature H.323 définit deux notions qu'il convient de bien connaître et différencier :
  - Un système H.323 est défini comme un ensemble de deux terminaux au minimum, d'autres éléments pouvant être ajoutés.
  - Une zone H.323 est un ensemble de deux terminaux avec un gatekeeper au minimum, d'autres éléments pouvant être ajoutés.

Figure Q.28
Architecture de H.323

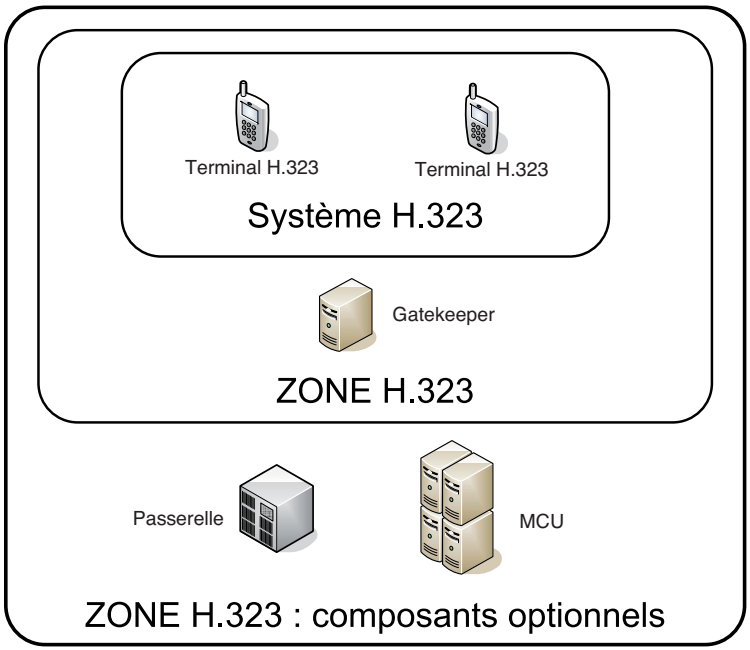


Autrement dit, une zone H.323 est un système H.323 associé à un gatekeeper et éventuellement, mais pas nécessairement, à des entités additionnelles, comme une MCU ou une gateway. Chaque entité peut être présente en grand nombre.

La figure Q.29 illustre ces notions de manière hiérarchique. Système et zone correspondent à des considérations logiques. Cela signifie que plusieurs réseaux locaux peuvent

être regroupés dans une même zone H.323 et dépendre d'un même gatekeeper. À l'inverse, il est possible d'avoir plusieurs zones H.323 et de les faire communiquer entre elles.

Figure Q.29
Système et zones H.323



Le terminal H.323

Équipement de base des interlocuteurs, le terminal peut prendre la forme d'un téléphone IP, en apparence semblable à n'importe quel autre appareil téléphonique utilisé dans la téléphonie RTC, ou d'un logiciel téléphonique installé sur un ordinateur ou un assistant personnel de type PDA équipé d'un micro et d'une sortie audio. On parle dans ce cas de softphone.

Pour qu'un terminal soit de type H.323, il doit respecter les prérequis fonctionnels suivants :

- Support des protocoles H.225.0 et H.245 (obligatoire). Ces protocoles, dont le premier utilise des protocoles hérités du RNIS, avec Q.931 et RAS, ont à leur charge d'effectuer la partie signalisation proprement dite dans un système H.323. C'est pourquoi leur gestion est requise par les terminaux.
- Support des protocoles RTP/RTCP (obligatoire). Une fois la liaison établie entre les interlocuteurs, la session multimédia peut commencer. Le transport des données recourt au protocole RTP, auquel est associé le protocole RTCP afin que l'application téléphonique H.323 utilisée dans le terminal puisse réguler son débit selon l'état du réseau. Ces deux protocoles sont donc aussi nécessaires au terminal H.323.
- Support du codec G.711 (obligatoire). Un terminal H.323 doit être capable de gérer l'audio et, suivant les usages, les textes, images et éventuellement vidéos. Pour cela,

il doit nécessairement supporter au moins le codec audio G.711, selon l'une de ces deux variantes : PCM (Pulse Code Modulation), la loi μ utilisée en Amérique du Nord et en Asie, et MIC (modulation, impulsion et codage), la loi A utilisée dans le reste du monde. Le support des autres codecs audio et de l'ensemble des codecs vidéo est laissé libre et optionnel dans la spécification du protocole H.323.

- Support de liaisons asymétriques (optionnel). Les terminaux peuvent être disposés de façon à établir des communications asymétriques, pour lesquelles la réception de données se fait avec un codec différent de celui utilisé pour l'envoi. Par exemple, un même terminal peut utiliser le codec G.222 en réception et le codec G.711 en émission. Cela permet d'affiner les débits selon les capacités des terminaux.

  À titre d'exemple, considérons deux terminaux A et B, dont le premier a un débit descendant (en réception, ou *download*) fort, mais un débit montant (envoi, ou *upload*) faible, et le second a un débit montant et descendant fort. Le terminal A peut utiliser un codec de très bonne qualité pour la réception et un codec de moins bonne qualité pour l'envoi. Parallèlement, le terminal B doit s'adapter aux capacités de son correspondant en utilisant le même codec de bonne qualité pour l'envoi et le même codec de moins bonne qualité pour la réception. Les liaisons sont de la sorte asymétriques.
- Support du multicast (optionnel). Si le terminal doit servir à la mise en place de conférences, le multicast doit être géré par le terminal. Il permet de dialoguer sans l'intervention d'une entité spécialisée, telle qu'une MCU, en diffusant ses messages dans le réseau, sous réserve que ce dernier dispose de routeurs qui autorisent la diffusion en multicast.

Comme l'illustre la figure Q.30, des terminaux peuvent parfaitement communiquer entre eux en utilisant le protocole H.323 sans l'intervention d'autres éléments architecturaux. Ils forment ainsi un système H.323 autonome, mais leurs communications ne peuvent profiter de la gamme de services fournis par les autres entités. En particulier, les utilisateurs doivent impérativement connaître l'adresse IP de leur correspondant pour pouvoir les joindre. En outre, ils restent cloisonnés dans un réseau purement IP, ce qui représente une contrainte très limitative pour H.323, qui vise à offrir une large communication entre différents types de réseaux.

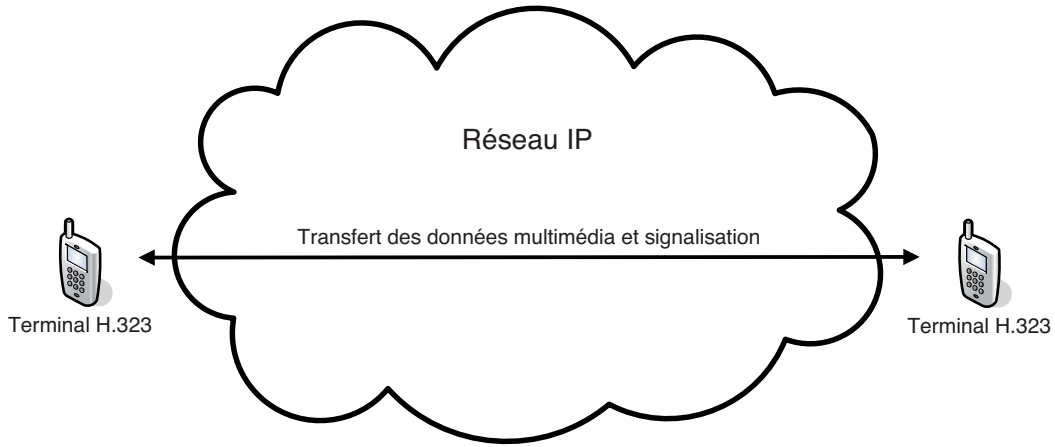


Figure Q.30
Communication entre deux terminaux H.323

Le gatekeeper

Facultatif de manière générale, le gatekeeper est requis pour toutes les opérations de contrôle et de gestion des communications. Il offre de la valeur ajoutée aux communications en proposant plusieurs fonctions, dont la première consiste à assurer la localisation des abonnés. Progressivement, le gatekeeper est devenu un élément central, dans lequel se concentrent toutes les fonctionnalités additionnelles, offrant une gamme de services complémentaires. L'architecture de H.323 est donc fortement centralisée autour de lui.

Si un gatekeeper est présent dans une zone H.323, tous les terminaux doivent nécessairement s'y enregistrer et y solliciter l'autorisation d'effectuer des appels, en émission comme en réception.

Localisation des abonnés

Pour permettre la localisation des utilisateurs dans un réseau IP utilisant H.323, le gatekeeper effectue la conversion d'un alias en une adresse IP.

Un alias est un identifiant associé à un utilisateur. Chaque utilisateur est localisé dans le réseau IP par une adresse IP, mais cette adresse peut être attribuée dynamiquement. Pour être joignables, les utilisateurs ne sont pas identifiés par cette adresse IP, qui est impropre à les qualifier pleinement et univoquement, mais par un alias qui les représente et que les utilisateurs peuvent s'échanger pour se contacter.

Le gatekeeper se charge d'effectuer la correspondance entre les alias et les adresses IP. Les utilisateurs qui ne sont pas situés dans un réseau IP doivent aussi pouvoir être joignables par les utilisateurs du réseau IP. C'est à nouveau le gatekeeper qui permet de les localiser.

Un alias peut être défini de plusieurs façons :

- une adresse de type e-mail, éventuellement préfixée de l'indication *h323:* spécifiant qu'il s'agit d'un alias H.323 ;
- une adresse de type numéro de téléphone (recommandation E.164 de l'UIT-T) ;
- une chaîne de caractères Unicode quelconque ;
- une adresse de type URL ;
- une adresse IP, éventuellement suffixée du numéro de port à utiliser.

Les adresses suivantes sont donc des alias H.323 valides : *albert@domaineH323.com, albert323, 132.227.55.155:1720, 0323323323,* etc.

La translation d'un alias vers une adresse IP est illustrée à la figure Q.31. Lors de sa connexion au réseau IP, Bertrand indique au gatekeeper sa localisation dans le réseau (étape 1), comme tout utilisateur qui se connecte. Le gatekeeper a sauvegardé cette association de l'alias avec l'adresse IP correspondante dans sa base de données. Lorsqu'Alice souhaite joindre Bertrand, elle ignore sa localisation mais dispose de son alias. En sollicitant le gatekeeper (étape 2), Alice peut donc déterminer la localisation de Bertrand (étape 3) puis initialiser un appel vers ce dernier (étape 4).

Autres fonctionnalités du gatekeeper

Initialement chargé d'assurer seulement la traduction d'adresses, le gatekeeper est progressivement devenu un équipement de point de contrôle dans lequel se concentre l'ensemble des fonctionnalités complémentaires du réseau.

Parmi elles, les fonctionnalités suivantes sont spécifiées dans la norme comme indispensables et implémentées systématiquement dans tous les gatekeepers :

- Contrôle d'admission. Si la bande passante ne permet pas d'établir un nouvel appel dans une zone H.323, la gateway est habilitée à interdire de nouveaux appels et à établir une liste de priorités d'appels licites.
- AAA (Authentication, Authorization, Accounting), ou authentification, autorisation et comptabilisation. L'authentification permet de connaître l'identité de la personne connectée, tandis que l'autorisation indique quels sont les droits (et éventuellement les conditions) attribués à la personne qui s'est authentifiée.
- Gestion des flux. Le gatekeeper peut implémenter un gestionnaire de bande passante pour décider de l'allocation de bande affectée aux terminaux. Il est en outre possible de limiter le nombre d'intervenants dans une conférence et de rejeter certaines demandes de flux (par exemple en n'autorisant que la voix à un utilisateur qui réclame l'audio et la vidéo).

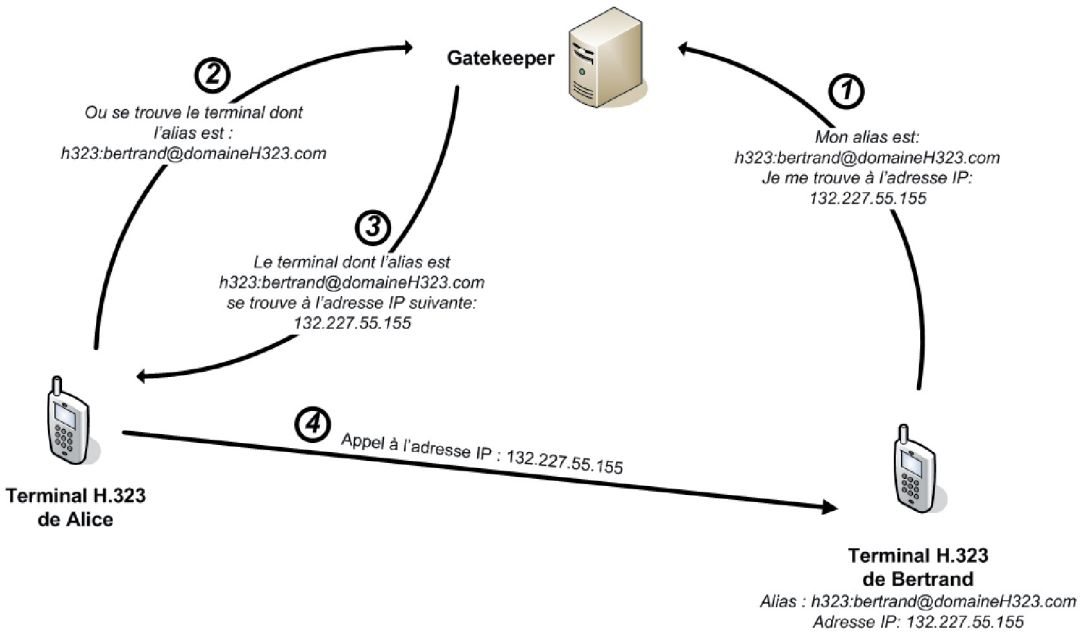


Figure Q.31
Traduction d'adresses par le gatekeeper

Signalisation routée et directe

Pour mettre en relation deux utilisateurs, il est possible d'utiliser deux moyens différents pour faire transiter la signalisation dans le réseau :

- un mode indirect, ou routé, la signalisation entre les correspondants passant par le gatekeeper ;
- un mode direct, la signalisation entre les correspondants ne faisant intervenir que ces correspondants, sans entité intermédiaire.

Dans le mode indirect, toute la signalisation passe systématiquement par le gatekeeper. Ce dernier garde donc la supervision totale de la communication et peut intervenir ensuite lors des négociations entre les utilisateurs, en interdisant certains flux vidéo, par exemple, ou en sauvegardant les paramètres négociés lors de l'appel, ce qui peut être utilisé à des fins de facturation notamment.

Comme l'illustre la figure Q.32, l'inconvénient immédiat de cette méthode est que le gatekeeper, déjà fortement sollicité dans une zone H.323, l'est davantage encore puisqu'il fait transiter l'ensemble des messages de signalisation.

Seule la partie signalisation de l'appel est concernée par cette redirection vers le gatekeeper, la transmission des flux multimédias eux-mêmes ne faisant pas intervenir le gatekeeper mais seulement les utilisateurs finaux.

Figure Q.32
Signalisation en mode indirect

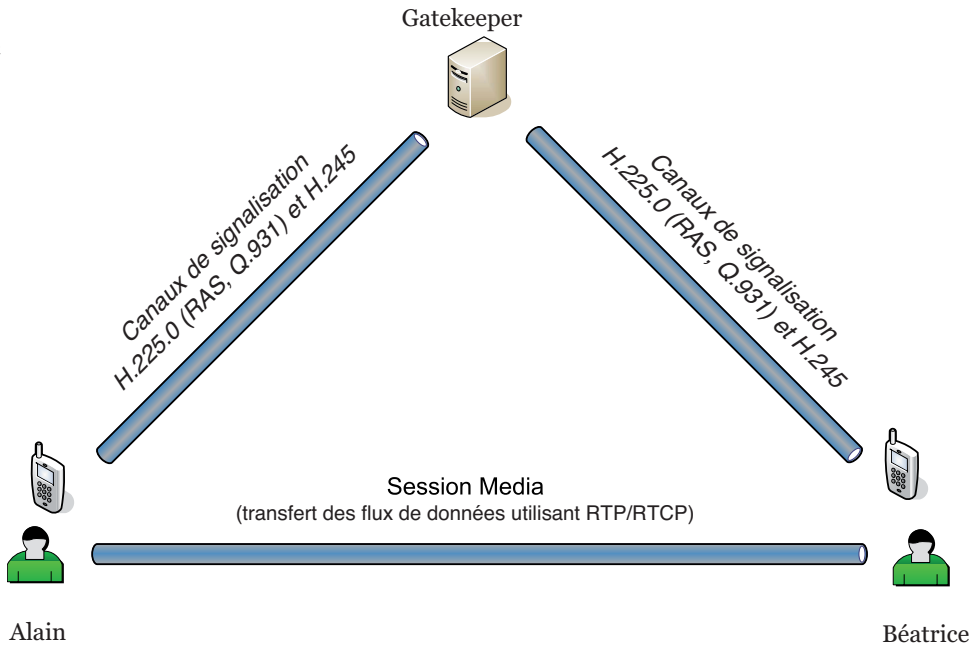
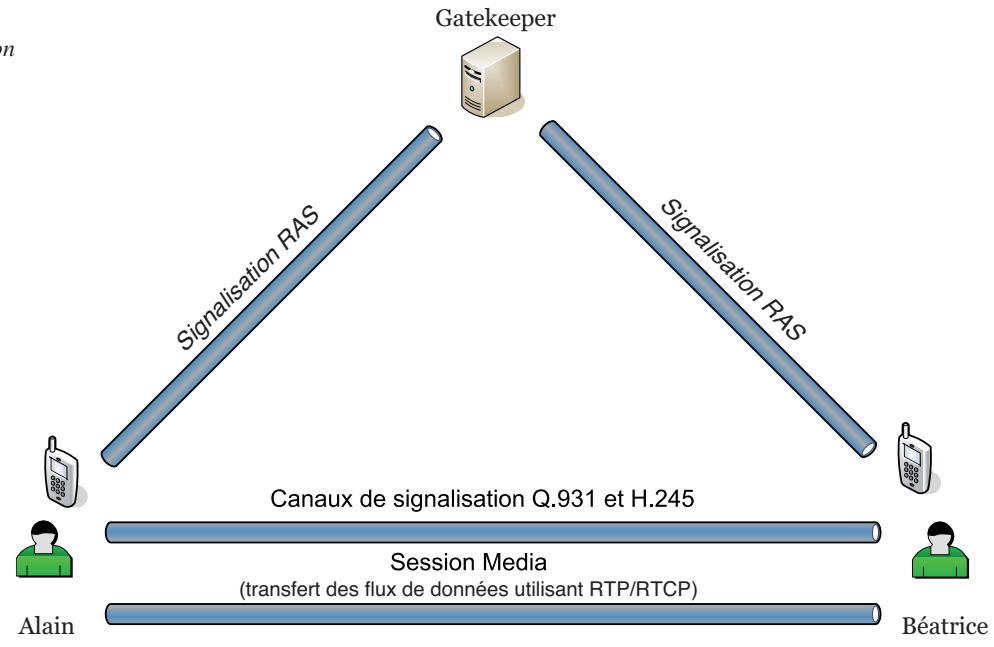


Figure Q.33
Signalisation en mode direct



Dans le mode direct, les interlocuteurs s'échangent la signalisation entre eux, comme l'illustre la figure Q.33. Le gatekeeper joue cependant toujours son rôle, et les intervenants l'utilisent pour effectuer préalablement à l'appel la traduction d'adresse permettant de localiser le terminal appelé puis pour s'y authentifier et être soumis au contrôle d'admission ainsi qu'à toutes les fonctionnalités dont dispose le gatekeeper. Ce n'est qu'ensuite que les informations de signalisation sont envoyées uniquement entre les correspondants, exactement comme pour un appel dans un système H.323 ne faisant pas intervenir de gatekeeper.

Les messages H.323

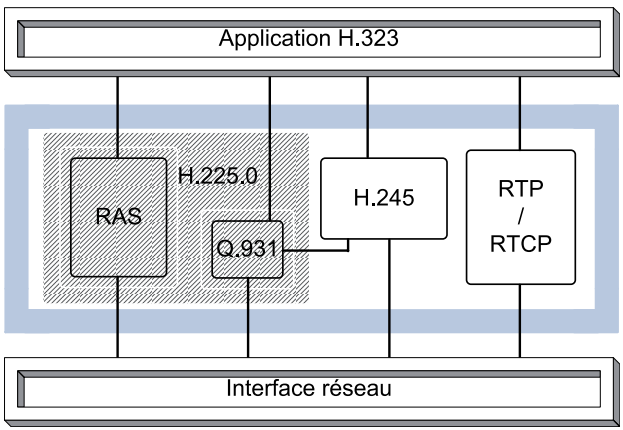
Bien plus qu'un protocole, H.323 renvoie à une plate-forme complète décrivant comment des protocoles se combinent pour assurer la signalisation. Pour être fonctionnel, H.323 doit impérativement utiliser d'autres protocoles, qui forment son ossature. Les plus importants d'entre eux sont les standards fondamentaux H.225.0, qui exploite les protocoles RAS, Q.931, hérité du RNIS, et H.245.

Le protocole H.225.0 met en place un canal de signalisation d'appel et d'enregistrement afin d'assurer la mise en relation des interlocuteurs. Le protocole H.245 permet quant à lui de créer un canal de contrôle pour la négociation des paramètres de la communication (codeur utilisé, contrôle de flux, etc.).

Les couches protocolaires de ce modèle sont illustrées à la figure Q.34.

Figure Q.34

Couches protocolaires de H.323



Initialement, les protocoles H.245 et Q.931 ne supportaient que le protocole de transport TCP, mais, depuis la version 3 de H.323, ils supportent indifféremment TCP et UDP.

Le protocole H.245, la signalisation de contrôle de connexion

Le protocole H.245 gère l'ouverture du canal de contrôle, l'établissement du canal de transmission, la négociation des paramètres (comme le codec utilisé) et le contrôle de flux ainsi que la fermeture du canal de contrôle. Comme pour le protocole Q.931,

tous les messages H.245 ne sont pas exploitables dans le protocole H.323, qui n'en utilise qu'une faible proportion.

Initialement, les messages H.245 ne devaient être diffusés qu'après le message Q.931 SETUP. Pour optimiser les temps d'établissement d'une communication, les versions suivantes de H.323 ont fortement suggéré que les échanges H.245 s'établissent en parallèle ou même avant le message Q.931 SETUP.

Les autres protocoles

Bien d'autres protocoles sont utilisés dans la spécification H.323. Le tableau Q.3 récapitule les principaux d'entre eux.

Tableau Q.3 • Principaux protocoles de H.323

Protocole	Description
RTP (Real Time Transport Protocol)	Assure l'horodatage des paquets au niveau de l'émetteur pour permettre la synchronisation au niveau du récepteur.
RTCP (Real Time Transport Control Protocol)	Retourne des informations statistiques sur la qualité de la connexion du récepteur vers l'émetteur, afin que ce dernier puisse adapter ses envois en conséquence.
H.235.x	Les protocoles de sécurité à utiliser dans un système H.323 sont décrits dans les documents H.235 sous dix sections référencées de H.235.0 à H.235.9.
H.450.x	La série H.450.x définit un ensemble de protocoles pour la mise en œuvre de services supplémentaires. Alors que la spécification H.450.1 propose simplement un cadre générique, les suivantes spécifient la fourniture de services divers, comme le transfert d'appel (H.450.2), la mise en attente d'appel (H.450.4), l'indication d'un appel pendant un autre appel (H.450.6), la présentation de l'appelant (H.450.8), le renvoi d'appel (H.450.9), etc.
H.460.x	La série H.460.x définit un ensemble d'extensions qu'il est possible d'apporter au protocole de base. Par exemple, le document H.460.9 détaille comment un point de terminaison peut envoyer des informations de qualité de service pour permettre à ce dernier d'optimiser le routage des appels.
X.680	C'est le document de référence pour la syntaxe ASN.1 qui est utilisée dans le codage des données H.323.
X.691	Ce document définit les règles d'encodage des paquets (Packet Encoding Rules) pour la transmission réseau.
T.120	Spécification pour l'échange de données lors des conférences, offrant la fiabilité des échanges et l'interopérabilité entre les constructeurs, tout en préservant une indépendance vis-à-vis du type de réseau utilisé.
T.38	Définit la manière de relayer les communications pour les fax.
V.150.1	Définit la manière de relayer les communications pour les modems.
H.26x	Ces documents détaillent les codecs normalisés pour les transmissions multimédias. Les deux plus utilisés sont H.261 pour le codage vidéo à débits multiples de 64 Kbit/s par seconde et H.263 pour le codage vidéo à faible débit.
H.510	Ce document décrit un support pour la mobilité des utilisateurs en leur fournissant des services analogues quel que soit le terminal qu'ils utilisent.

Le dispositif middle box et l'architecture MIDCOM

Une *middle box* est un dispositif de réseau intermédiaire permettant d'implémenter des services divers tels qu'un filtrage de paquets, un VPN, une détection d'intrusion, une

translation d'adresse NAT ou un pare-feu. Une middle box est donc une appliance située entre deux équipements de réseau, d'où son nom de middle box. En fait, middle box et appliance sont deux noms désignant pratiquement les mêmes équipements. Middle box est le terme utilisé par l'IETF, appliance étant surtout le terme des industriels commercialisant des boîtiers intermédiaires.

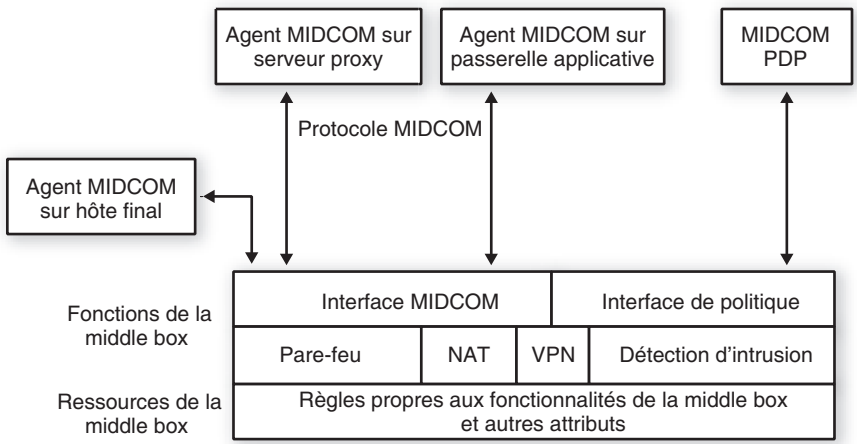
Ces boîtiers nécessitent de l'intelligence pour faciliter la traversée du flux applicatif. Cela rend leur maintenance difficile et dégrade leur performance. D'où l'idée de déplacer l'intelligence de ces boîtiers dans des agents MIDCOM communiquant avec le boîtier à l'aide du protocole MIDCOM. Les agents MIDCOM exécutent des fonctions ALG (Application Level Gateway), qui examinent le flux applicatif et aident la middle box à remplir ses fonctions.

Le protocole MIDCOM s'exécute en trois phases : établissement de la session, session et rupture de la session. La communication entre le boîtier et l'agent se déroule de façon transparente pour l'utilisateur final. Les agents peuvent résider dans les hôtes finals, des serveurs proxy des applications, des passerelles applicatives ou dans la middle box.

Seuls des agents MIDCOM autorisés peuvent influencer le fonctionnement du boîtier. L'autorisation d'un agent requiert une inscription, pendant laquelle les agents suppléent leur profil à la middle box ou au MIDCOM PDP que la middle box consulte. Ce profil détermine les opérations autorisées. L'inscription est souvent une opération manuelle.

L'architecture d'une middle box est illustrée à la figure Q.35.

Figure Q.35
Architecture d'une middle box



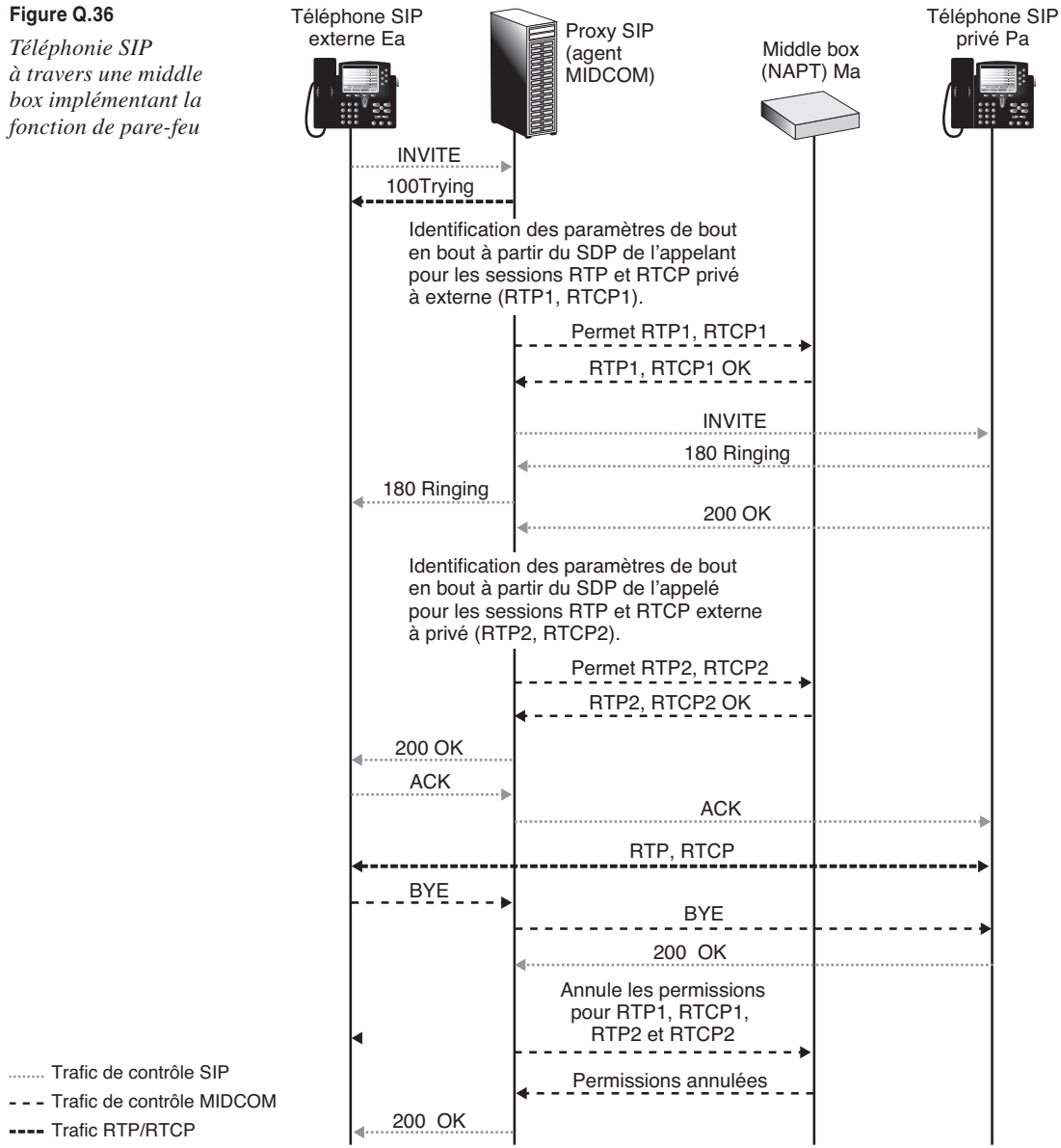
Un agent MIDCOM assistant un pare-feu, par exemple, peut lui demander d'autoriser l'accès au trafic d'une application.

Les sections suivantes illustrent le fonctionnement temporel d'une *middle box* par des exemples d'applications temps réel, notamment avec l'implémentation de fonctionnalités de pare-feu et de NAT dans une middle box pour la téléphonie SIP.

Implémentation d'une fonction de pare-feu dans une middle box

Prenons le cas d'un téléphone SIP externe au réseau qui souhaite communiquer avec un téléphone interne. L'agent MIDCOM résidant dans le SIP proxy demande à la middle box pare-feu du réseau de débloquer les ports nécessaires aux flux RTP (Real-time Transport Protocol) et RTCP (Real-Time Control Protocol) dans les deux sens. La figure Q.36 en illustre le fonctionnement.

Figure Q.36
Téléphonie SIP à travers une middle box implémentant la fonction de pare-feu



Implémentation de NAT dans une middle box

La middle box est configurée pour rediriger les appels SIP entrants vers l'adresse privée du téléphone SIP. La commande INVITE est destinée à l'adresse NAT externe. Les appels SIP sont des sessions TCP/UDP sur le port 5060.

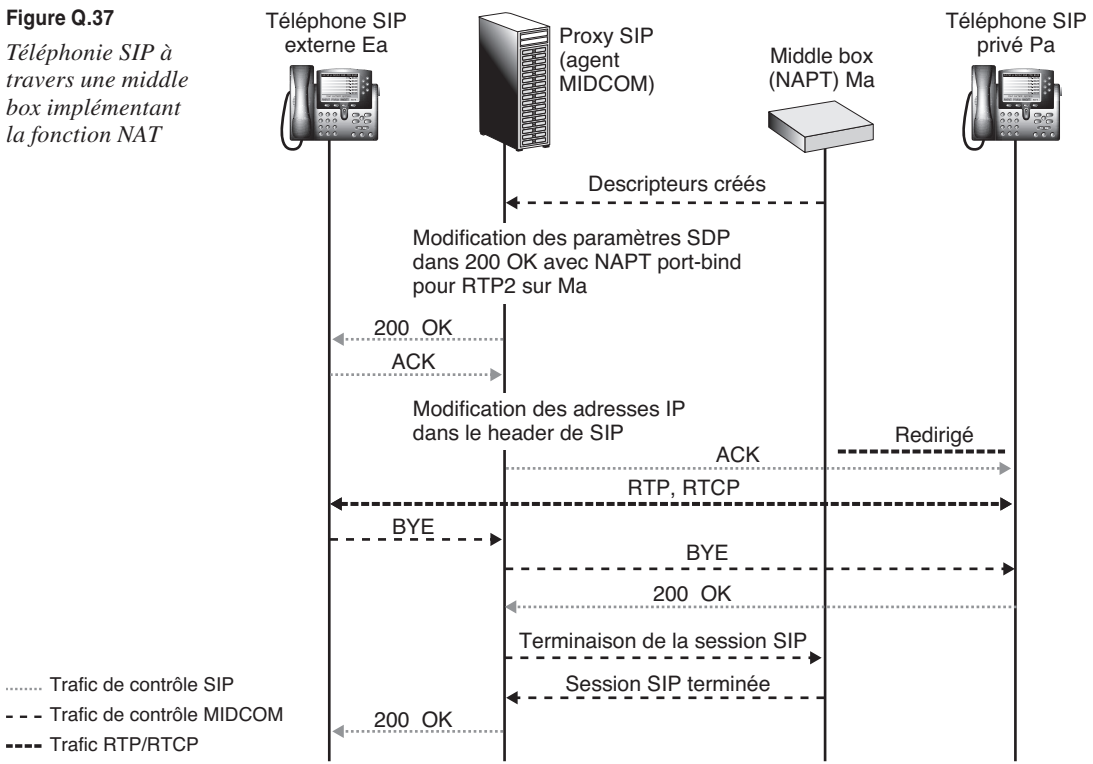
Nous utilisons la notation suivante :

- Ma : adresse externe de la middle box ;
- Pa : adresse interne du téléphone SIP ;
- Ea : adresse du téléphone SIP externe.

Le proxy SIP demande les descripteurs de la session NAT pour les deux flux entrant et sortant. Les ports dynamiques utilisés pour le flux média sont contenus dans la partie SDP du message SIP. Après le 200 OK reçu par le proxy du téléphone privé, l'agent demande à la middle box d'allouer des descripteurs de session NAT pour le trafic entrant de sorte que les ports réservés pour RTP2 et RTCP2 soient contigus. Bien que les flux média entrants et sortants soient indépendants, ils sont liés à la même session SIP. Quand le message BYE est envoyé, toutes les ressources sont libérées.

La figure Q.37 illustre l'interaction entre un proxy SIP et une middle box implémentant la fonctionnalité NAT.

Figure Q.37
Téléphonie SIP à travers une middle box implémentant la fonction NAT



La signalisation MGCP

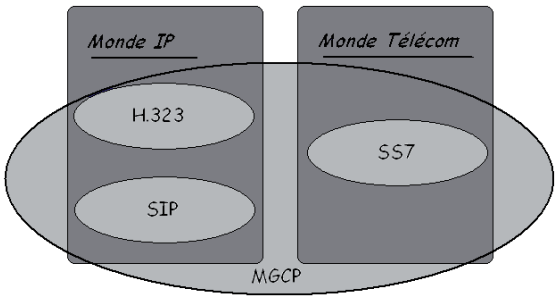
L'une des raisons ayant expliqué l'émergence et le succès du protocole H.323 est le besoin de regrouper les différents acteurs du multimédia, qu'ils soient équipementiers ou fournisseur de services, autour de normes communes. La concurrence engendrée par le protocole SIP a réduit cet effet d'universalité puisque les réseaux IP ont désormais une solide solution de rechange à H.323. Dès lors, se pose la question de la communication entre des réseaux de nature différente (ATM, RNIS, RTC ou IP) ou bien de même nature mais exploitant des protocoles de signalisation différents (H.323, SIP ou autre).

Si les passerelles ont déjà été introduites avec le protocole H.323, elles demeurent des entités complexes, onéreuses et non administrables, qui plus est fortement sollicitées alors qu'elles tiennent difficilement la montée en charge. Pour combler ce nouveau besoin, le protocole MGCP (Media Gateway Control Protocol), ou protocole de contrôle des passerelles multimédias, a été proposé.

Il fonctionne au niveau applicatif et permet d'offrir une couverture plus large en fédérant toutes les signalisations, qu'elles soient de type IP ou RTC entre autres. C'est le maître d'œuvre de l'interopérabilité entre tous les protocoles de signalisation et tous les réseaux, de quelque nature qu'ils soient.

Comme l'illustre la figure Q.38, qu'il s'agisse de la signalisation CCITT n° 7 (SS7), utilisée dans un réseau commuté, H.323 ou SIP, le protocole MGCP est conçu pour relier et faire communiquer l'ensemble de ces réseaux.

Figure Q.38
Rôle fédérateur du protocole MGCP



MGCP est aujourd'hui utilisé par les FAI pour assurer le contrôle et l'administration à distance des InternetBox mises à disposition de leurs abonnés.

Les travaux ont débuté après que le protocole H.323 eut été proposé par l'UIT. Très vite, il est apparu que l'initiative H.323 était insatisfaisante pour relier à grande échelle des réseaux de natures différentes. Les passerelles (gateways) proposées dans l'architecture H.323 sont des éléments complexes et coûteux, ce qui pose problème dans le monde IP. Plus le nombre de réseaux à traverser pour établir une communication est important, plus l'est aussi celui des passerelles sollicitées.

Progressivement, un certain nombre d'initiatives ont été lancées, dont l'idée-force est de disposer d'un réseau dont toutes les passerelles multimédias soient des composants simples. Ces passerelles sont reliées à un contrôleur maître concentrant toute l'intelligence

du réseau et centralisant les décisions. C'est le modèle maître-esclave. L'architecture générale qui conceptualise les entités de contrôleur et de passerelle multimédia, et plus généralement le modèle maître-esclave, fut initialement proposée dans le projet TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) de l'ETSI. La première tentative de protocole de communication entre ces entités fut SGCP (Simple Gateway Control Protocol), en 1997. Proposée par Telcordia (anciennement BellCoRe, acronyme de Bell Communications Research), elle reçut le soutien de Cisco. TIPHON est le protocole précurseur de MGCP.

En 1998, l'opérateur de télécommunications Level 3 Communications (groupe XCOM Technologies) a mis en place un comité consultatif technique, ou TAC (Technical Advisory Council), réunissant une douzaine d'industriels renommés, comme Ericsson, Lucent, Nortel, Alcatel, 3Com et Cisco. Avec ces membres fondateurs, le TAC sera à l'origine de la conception d'un protocole de contrôle des entités réseau sur Internet, nommé IDCP (Internet Device Control Protocol). Ses spécifications seront présentées à ITU, l'IETF et l'ETSI.

En octobre 1998, avec le soutien d'importants constructeurs, tels que Cisco et Alcatel, le protocole MGCP a été standardisé à l'IETF par le groupe de travail MEGACO (Media Gateway Control). Celui-ci réalisait la fusion des initiatives SGCP et IDCP. MGCP s'inscrit dans la droite ligne de la version 1.1 du protocole SGCP, qui servira de socle principal à MGCP.

En plus de dériver de SGCP, MGCP s'est enrichi de nombreuses fonctionnalités proposées dans IDCP. En octobre 1999, la RFC 2705 présentait la première version de MGCP. Elle sera rendue obsolète en janvier 2003 par la RFC 3435, qui sera complétée par la RFC 3661, en décembre 2003.

Architecture et fonctionnement de MGCP

Pour communiquer entre deux réseaux de nature différente, il est nécessaire d'utiliser une passerelle. Cette entité prend en charge à la fois la signalisation pour l'établissement, la gestion et la terminaison de la communication, mais aussi la conversion des signaux pour l'adaptation des flux d'un réseau vers un autre. MGCP sépare ces deux aspects en entités distinctes, l'une pour contrôler les appels, l'autre pour appliquer le contrôle ordonné par la première entité.

MGCP fonctionne selon une architecture centralisée permettant de faire communiquer et de contrôler différentes entités appartenant à des réseaux distincts. Il se fonde sur l'hypothèse que les terminaux des utilisateurs peuvent être des composants de base peu coûteux et sans aucune intelligence, réduits à des fonctionnalités élémentaires.

Les passerelles sont également des entités simples. En fournissant un service générique, elles restent indépendantes de leur constructeur. Pour leur donner des directives permettant le traitement des services, ces passerelles multimédias sont reliées à une entité centrale. Le protocole MGCP assure le contrôle et l'échange de messages de signalisation entre ces passerelles, réparties dans un réseau IP, et le contrôleur de passerelles, chargé de l'administration et de la gestion dynamique des passerelles.

MGCP fait éclater le modèle architectural proposé avec H.323 en décomposant le rôle des passerelles et en externalisant toute leur intelligence sur une entité centrale.

Pour réaliser cette distinction, MGCP définit les entités suivantes :

- Le Call Agent, qui sert à piloter et administrer les passerelles de manière centralisée.
- Les passerelles, qui maintiennent la connectivité entre réseaux de nature différente.

Le Call Agent

Le Call Agent, également appelé contrôleur de passerelles multimédias ou encore SoftSwitch, selon une terminologie non officielle mais courante, a pour fonction de contrôler les passerelles et de concentrer toute l'intelligence ainsi que la prise de décision dans le réseau.

Entité logique, pouvant être localisée n'importe où sur le réseau, le Call Agent est spécifiquement responsable de l'établissement, de la maintenance et de la terminaison des appels établis entre des terminaux appartenant à des réseaux de nature différente.

Comme ces opérations sont initialisées au niveau des passerelles multimédias, le Call Agent intervient pour contrôler l'activité de ces dernières et leur donner les directives de traitement de ces opérations. Il est en quelque sorte le maître d'œuvre et d'opération des communications entre les réseaux.

Dans la mesure où il contribue à centraliser le réseau autour de lui, le Call Agent est une entité fortement sollicitée. De ce fait, il devient un élément sensible dans le réseau, particulièrement en cas de panne. Néanmoins, cette centralisation n'intervient que pour arbitrer et assurer la maintenance et la gestion des échanges de signalisation. Elle n'entre pas en jeu dans les communications intra-réseau. En outre, pour gérer les pannes, il est plus simple de mettre en place des doublures, sous forme de Call Agents redondants, que de rendre toutes les passerelles multimédias redondantes.

Il est possible d'avoir plusieurs Call Agents, chacun ayant en charge un parc de passerelles multimédias. Par exemple, chaque opérateur peut gérer ses propres passerelles par un Call Agent propriétaire. Le protocole MGCP ne définissant pas de mécanisme de synchronisation entre Call Agents, on doit considérer indépendamment chaque Call Agent et les passerelles qu'il contrôle.

Fondamentalement, MGCP repose sur un modèle maître-esclave, et il n'est pas dans son objectif de fournir des mécanismes de communication entre les agents de contrôle, qui sont des entités de même nature, auxquelles le modèle maître-esclave ne convient pas. Pour faire communiquer entre eux plusieurs Call Agents, un protocole tel que SIP peut être utilisé afin de négocier les paramètres de communication.

Les passerelles multimédias

Selon le protocole MGCP, la notion de passerelle est assez floue et couvre un vaste ensemble de définitions, notamment les suivantes :

- Passerelle d'opérateur téléphonique, pour faire le lien entre un réseau téléphonique et un réseau IP. Les opérateurs de téléphonie alternatifs, par exemple, utilisent souvent le réseau RTC de l'abonné comme réseau de base puis basculent les flux de l'abonné

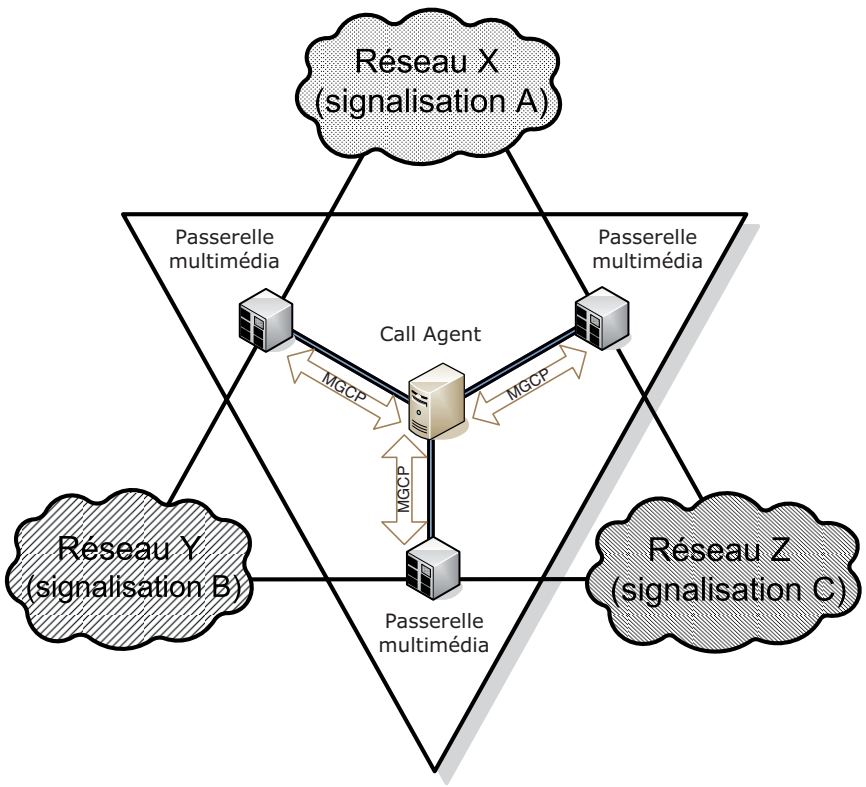
vers un réseau IP (lequel présente l'avantage d'être à commutation de paquets, donc sans réservation de ressources, et ainsi moins coûteux qu'un réseau à commutation de circuits) sur de longues distances internationales, avant de basculer à nouveau les flux de l'appelant vers le réseau RTC auquel le terminal du destinataire est connecté.

- Passerelle résidentielle de type box (boîtier exploitant le modem, le câble ou les technologies xDSL), généralement mise à disposition par le FAI. Ce boîtier fait la liaison entre le réseau IP des utilisateurs et le réseau d'accès téléphonique de l'opérateur.
- PBX d'entreprise faisant la liaison entre le réseau IP de l'entreprise et le réseau téléphonique RTC de l'opérateur. Au sein de l'entreprise, des téléphones IP ou des softphones peuvent être utilisés en interne pour exploiter les services complémentaires qu'offre le réseau IP et permettre la convergence des flux sur un support unique. Comme le réseau de l'entreprise est connecté à une liaison RTC, une passerelle est toutefois nécessaire.

Par rapport aux passerelles initialement prévues dans le protocole H.323, les passerelles multimédias sont simplement dépourvues de la fonctionnalité de traitement des appels. Elles s'en remettent pour cela au Call Agent. Néanmoins, elles conservent intact leur emplacement physique, à la frontière entre les deux réseaux de nature distincte, alors que le Call Agent peut être situé n'importe où, comme l'illustre la figure Q.39.

Figure Q.39

Places des passerelles et du Call Agent dans l'architecture MGCP



X, Y ou Z représentent des réseaux quelconques (RNIS, ATM, IP, RTC, etc.). Sur chacun de ces réseaux, le protocole de signalisation intra-réseau de son choix peut être utilisé, par exemple SIP ou H.323 dans un réseau IP, ou SS7 dans un réseau RTC. MGCP ne peut s'appliquer au sein de ces réseaux, mais seulement à leur périphérie afin d'assurer la gestion et le traitement des communications inter-réseau.

On observe deux niveaux de communications : l'un qui fait intervenir les réseaux et les passerelles multimédias et l'autre les passerelles multimédias et le Call Agent. Le protocole MGCP s'applique exclusivement à transmettre de la signalisation entre le Call Agent et les passerelles. Les flux de données multimédias (voix, vidéo, données) entre deux terminaux appartenant à des réseaux différents ne transitent jamais par le Call Agent. Une fois que le Call Agent en a donné l'autorisation, ces flux sont véhiculés de poste terminal à poste terminal, en passant uniquement par la passerelle.

Le rôle de la passerelle multimédia est donc réduit à l'acheminement cohérent des données, ce qui implique qu'elle accomplisse les tâches suivantes :

- conversion du signal ;
- adaptation au support ;
- compression des données ;
- conversion de la signalisation ;
- multiplexage ;
- mise en paquets.

Les passerelles multimédias se retrouvent ainsi réduites à leur fonctionnalité première et fondamentale de transmission : elles travaillent au niveau du média lui-même et assurent les traitements des données, sans la logique de traitement. Toutefois, ces actions ne sont réalisables qu'en accord avec le Call Agent, dont les passerelles sont les exécutants.

Globalement, le mode de fonctionnement des passerelles est donc allégé par rapport à H.323 et le réseau devient constitué d'éléments simples et configurables.

Les communications MGCP passent systématiquement par le protocole UDP, choisi pour optimiser les délais de traitement des envois.

S'il n'est pas mentionné, le Call Agent utilise par défaut le port 2727 pour ses communications, tandis que les passerelles utilisent le port 2427.

Principes d'établissement d'une communication

On appelle *endpoint* un équipement dit de terminaison, qui représente soit la source soit la destination d'un message multimédia.

Un routeur réseau n'est pas un endpoint puisqu'il se contente d'acheminer des données, sans être à l'origine de l'envoi. Le Call Agent n'est pas non plus un endpoint, puisqu'il ne traite pas des messages multimédias.

Dès lors qu'une entité participe aux échanges de médias et se place comme source ou destinataire de ces échanges, même si elle n'est pas la source initiale ou le destinataire

final et qu'elle ne joue qu'un rôle d'intermédiaire dans ces échanges, elle est considérée comme en endpoint. Les terminaux des utilisateurs sont des endpoints de référence.

Supposons que nous souhaitions connecter deux terminaux, appelés des endpoints. Chacun d'eux se trouve localisé derrière une passerelle multimédia. Ces deux passerelles sont elles-mêmes contrôlées par un Call Agent, comme l'illustre la figure Q.40.

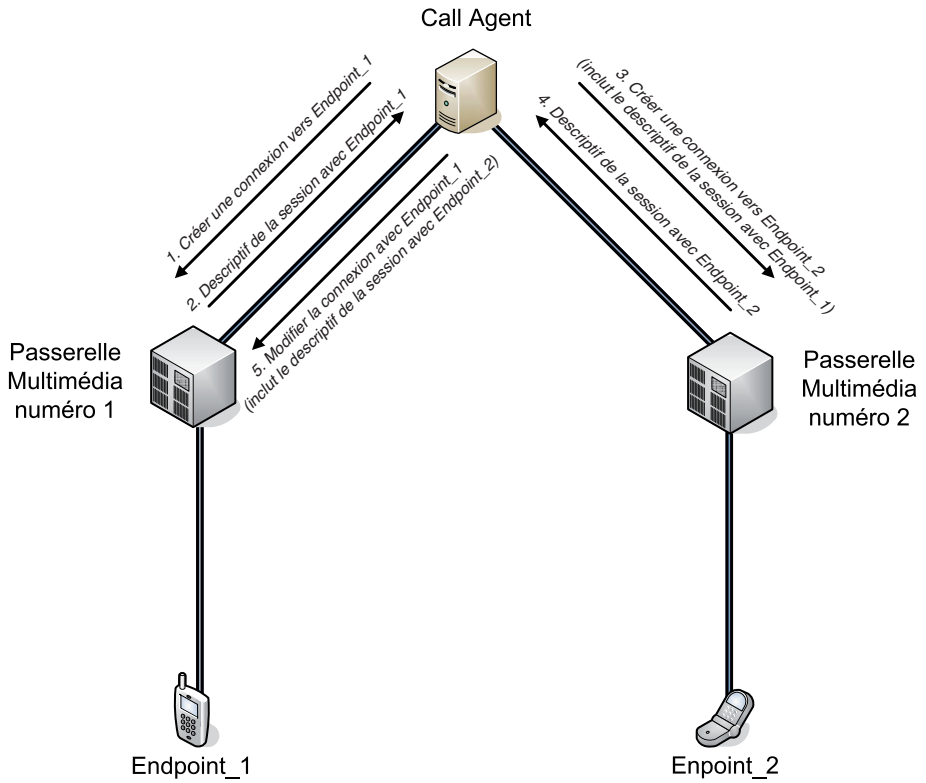


Figure Q.40

Mise en relation de deux endpoints

Pour mettre en relation les deux endpoints, les cinq étapes suivantes sont nécessaires :

1. **Requête de création de connexion vers la première passerelle.** Le Call Agent sollicite la création d'une connexion avec un endpoint auprès de la passerelle concernée.
2. **Réponse de la première passerelle.** Celle-ci se charge de joindre le endpoint et lui attribue les ressources nécessaires à la communication : une session est créée entre la passerelle et le endpoint. En retour, la passerelle envoie au Call Agent un descriptif de la session créée. Ce descriptif contient l'ensemble des paramètres permettant de joindre le endpoint, incluant l'adresse IP de ce dernier, le port UDP sur lequel la communication est en attente et les codecs supportés.

3. **Requête de création de connexion vers la seconde passerelle.** Le Call Agent procède de la même façon pour le second endpoint et sa passerelle : il sollicite cette dernière en lui envoyant un message pour la création d'une connexion avec le second endpoint. En plus, et dans le même message, le Call Agent lui fait parvenir le descriptif de session que lui a retourné la première passerelle.
4. **Réponse de la seconde passerelle.** La seconde passerelle joint le endpoint concerné et alloue les ressources nécessaires à cette communication. En retour, elle transmet au Call Agent un descriptif de session contenant les paramètres permettant de joindre le second endpoint.
5. **Mise en relation des deux endpoints.** Le Call Agent contacte la première passerelle et lui transmet le descriptif de la session retournée par la seconde passerelle. Comme une connexion existe déjà avec le endpoint, il n'est pas nécessaire de créer une nouvelle connexion. Il suffit de modifier celle qui existe et de la compléter. C'est donc une commande de modification qui est effectuée par le Call Agent.

Une fois ces étapes achevées, la communication débute dans les deux sens. Elle peut être modifiée à tout moment par le Call Agent, qui peut imposer, par exemple, un changement de codec, d'adresse IP ou de port. De même, le Call Agent peut mettre fin à la communication à tout moment en envoyant un message aux passerelles, qui doivent alors rompre les connexions.

On peut résumer tous les états possibles d'une passerelle multimédia comme illustré à la figure Q.41.

Les messages MGCP

La communication avec MGCP obéit à un modèle de type client-serveur. Un message MGCP est soit une requête soit une réponse à une requête. Il est constitué sous forme textuelle, ce qui simplifie son usage (traitement sans compilateur, donc plus rapide, et débogage immédiat), et présente plusieurs analogies avec le protocole SIP. Ainsi, une transaction MGCP est-elle constituée d'une requête et de la réponse à cette requête, éventuellement précédée de réponses temporaires. Le format d'un message MGCP est illustré à la figure Q.42.

Dans ce message, on distingue trois parties :

- Ligne de requête ou de réponse : notifie la commande à exécuter (s'il s'agit d'une requête) ou le résultat de la commande (s'il s'agit d'une réponse). C'est une partie indispensable.
- En-tête : spécifie la liste des paramètres du message. C'est une partie facultative.
- Corps du message : décrit les paramètres de la session à établir. C'est une partie facultative.

Plusieurs lignes peuvent constituer chacune des parties. On sépare chaque ligne par des retours chariot, ou CR (Carriage Return), et des sauts de ligne, ou LF (Line Feed), ou par des retours chariot seulement.

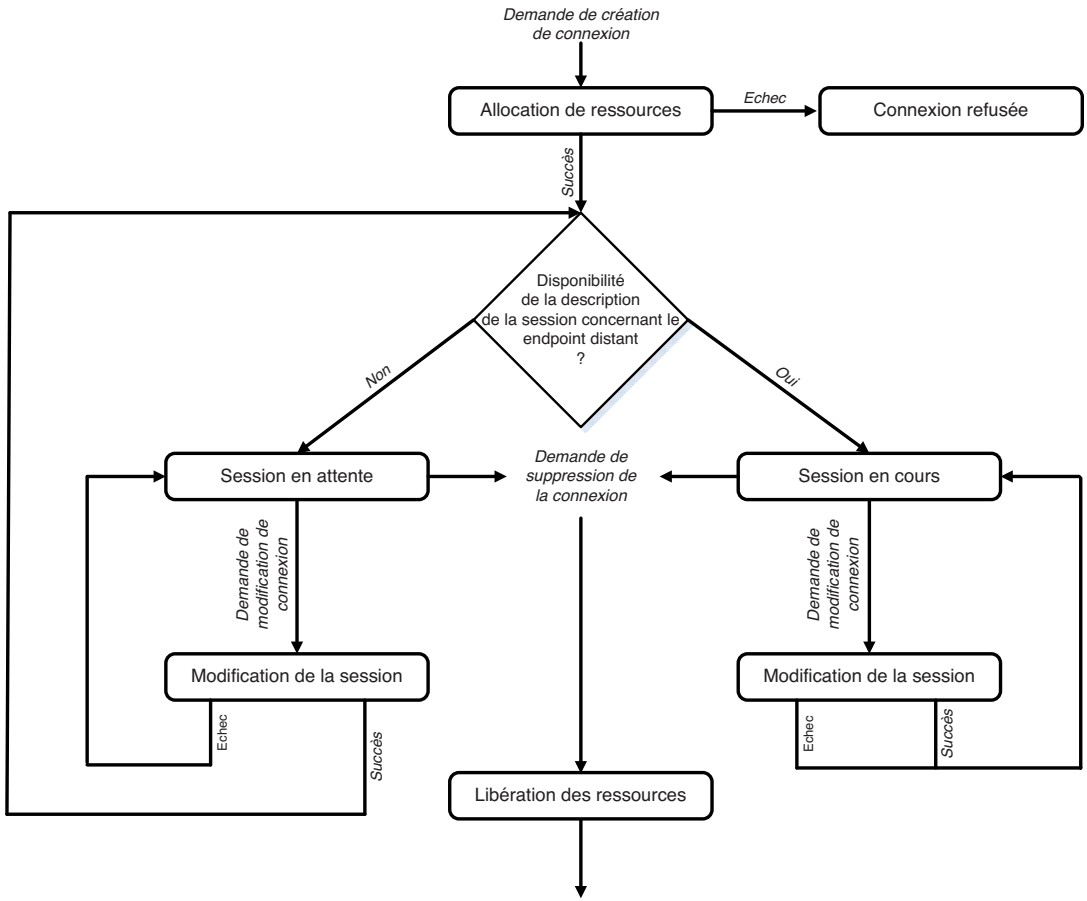


Figure Q.41
Diagramme d'états d'une passerelle

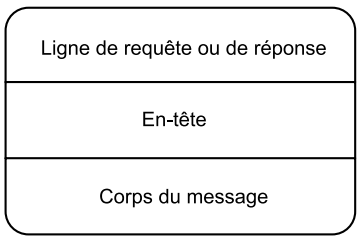


Figure Q.42
Format d'un message MGCP

Notons que, dans la RFC 3435, la partie spécifiant la ligne de requête ou de réponse et celle spécifiant l'en-tête sont regroupées.

Les requêtes

Le protocole MGCP définit neuf requêtes permettant de spécifier l'action à entreprendre. Les commandes sont lancées entre le Call Agent et les passerelles (Media Gateway). Comme MGCP est un protocole de type maître-esclave, toutes les entités n'ont pas des possibilités comparables, et ces commandes ne peuvent être lancées qu'à l'initiative de l'une de ces entités, soit le Call Agent, soit la Media Gateway.

On distingue donc deux catégories de commandes : celles qui sont lancées par le Call Agent vers une ou plusieurs passerelles et celle qui vont dans l'autre sens, de la passerelle vers le Call Agent.

À chaque requête correspond un code en quatre lettres de caractères ASCII, qui permet de condenser la taille de la requête. Les neuf requêtes et leur code respectif sont récapitulés au tableau Q.4.

Tableau Q.4 • Les 9 requêtes MGCP et leur format abrégé

Format complet	Format abrégé
AuditConnection	AUCX
AuditEndpoint	AUEP
CreateConnection	CRCX
DeleteConnection	DLCX
EndpointConfiguration	EPCF
ModifyConnection	MDCX
NotificationRequest	RQNT
Notify	NTFY
RestartInProgress	RSIP

La signalisation COPS (Common Open Policy Service)

COPS est un protocole d'échange de politiques. Il a été introduit dans la première partie de cette annexe, en même temps que l'architecture globale du contrôle par politique. Cependant, nous ne sommes pas entrés dans le détail du protocole COPS en tant que signalisation, et c'est ce que nous allons faire ici.

Le protocole COPS est issu de travaux démarrés en 1996 dans le contexte de la réservation de ressources. COPS a été étendu en 1999 dans un contexte plus large dans le groupe de travail RAP (Resource Allocation Protocol) de l'IETF et normalisé par la RFC 2748 de janvier 2000.

Dans sa version actuelle, COPS a pour objectif l'échange d'informations de politiques réseau entre un PDP (Policy Decision Point) et un PEP (Policy Enforcement Point). Le PDP et le PEP font partie de l'architecture de gestion de réseau à base de politique définie par les groupes PFWG (Policy Framework Working Group) et DMTF (Distributed Management Task Force) de l'IETF. Le rôle du PDP est de prendre des décisions sur les politiques réseau, tandis que celui du PEP est d'appliquer les décisions que lui a communiquées le PEP.

Deux modes de signalisation sont actuellement standardisés au sein de l'IETF :

- COPS-Outsourcing, issu des premiers travaux, intègre COPS dans un réseau où existe un protocole de signalisation tel que RSVP. Les événements déclencheurs d'échanges COPS sont les messages de signalisation arrivant au PEP. Le PDP est alors sollicité pour prendre la décision sur la politique à appliquer. La première RFC qui se réfère à ce mode est COPS-RSVP (COPS usage for Resource ReserVation Protocol), que nous examinons un peu plus loin.
- COPS-Configuration, aussi appelé COPS-Provisioning, permet l'intégration de COPS dans un réseau où les politiques sont transmises au préalable par le PDP au PEP et engendrent la configuration du PEP. La RFC qui se réfère à ce mode est COPS-PR (COPS usage for Policy Provisioning), que nous étudions également plus loin.

Le mode d'échange de COPS est de type client-serveur, avec une relation maître à esclave. Le PDP est le maître et le PEP l'esclave. Il n'y a pas de classification de message de type requête/réponse. COPS ne peut fonctionner qu'au-dessus de TCP. Une connexion persistante TCP est établie entre le PEP et le PDP. La fiabilité est donc assurée par TCP.

COPS définit un fonctionnement général, qui peut être étendu pour générer des fonctionnements plus spécifiques, propres à la politique ou au mode de gestion de la politique. Ces fonctionnements spécifiques sont définis hors de COPS dans des extensions que nous verrons ultérieurement.

Dans le protocole COPS, le mode de communication est unique et direct entre le PEP et le PDP, et il n'y a pas d'entités intermédiaires. Dans COPS et ses deux extensions COPS-RSVP et COPS-PR, le PEP est une entité logique, qui représente un équipement actif du réseau. Le PDP est une entité logique qui représente un équipement de management du réseau. En retour des requêtes du client, il envoie des décisions. C'est le fonctionnement naturel dans le mode outsourcing. Le PEP et le PDP conservent l'état des requêtes/décisions échangées, selon un fonctionnement « stateful ». L'architecture complète dans laquelle s'insère COPS est illustrée à la figure Q.43.

Les messages COPS

Les messages COPS ont tous la même structure générale : un en-tête commun donnant les informations sur le type du message et un corps transportant les objets spécifiques. Cette structure est représentée à la figure Q.44.

Figure Q.43
Architecture de gestion de réseau par politique

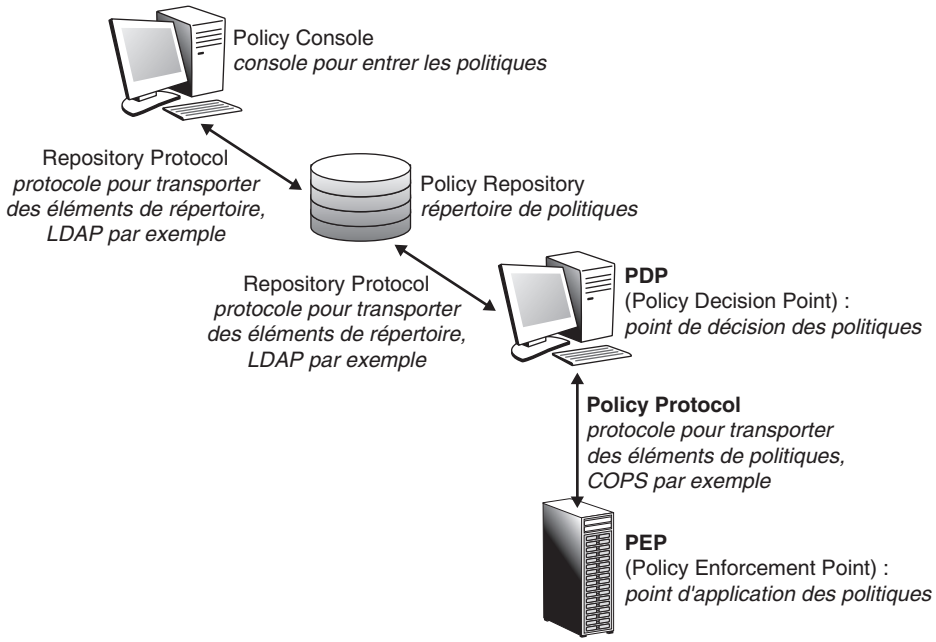
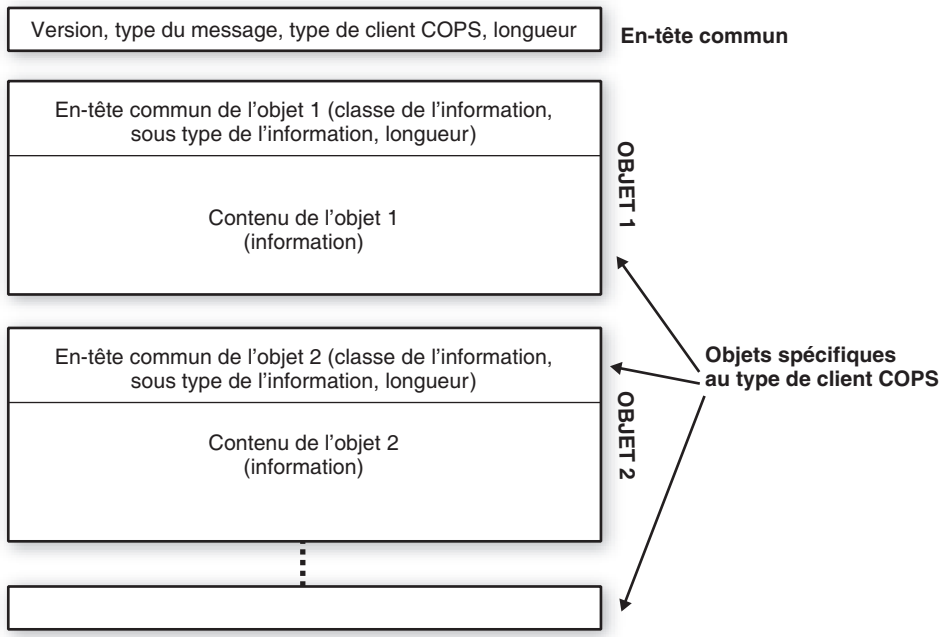


Figure Q.44
Format général des messages COPS



COPS comporte les 16 classes d'objets, ou plutôt classes d'information de contenu d'objets, récapitulées au tableau Q.5. La structure des objets est soit précisée dans la RFC, soit étendue et définie dans les extensions du protocole.

Tableau Q.5 • Classes d'objets de COPS

C-Num	Classe de l'objet	C-Type	Objet
1	Handle (Handle)	1	Client – Handle
2	Context (Context)	1	Context
3	In Interface (IN-Int)	1 2	IPv4 address + Interface IPv6 address + Interface
4	Out Interface (OUT-Int)	1 2	IPv4 address + Interface IPv6 address + Interface
5	Reason Code (Reason)	1	Reason Code
6	Decision (Decision)	1 2 3 4 5	Decision Flags Stateless Data Replacement Data Client Specific Decision Data Named Decision Data
7	LPDP Decision (LPDPDecision)	1 2 3 4 5	Decision Flags Stateless Data Replacement Data Client Specific Decision Data Named Decision Data
8	Error (Error)	1	Error
9	Client Specific Info (ClientSI)	1 2	Signaled ClientSI Named ClientSI
10	Keep-Alive Timer (KATimer)	1	Keep-alive Timer value
11	PEP Identification (PEPID)	1	PEP Identification
12	Report Type (Report-Type)	1	Report Type
13	PDP Redirect Address (PDPRedirAddr)	1 2	IPv4 + TCP port IPv6 + TCP port
14	Last PDP Address (LastPDPAddr)	1 2	IPv4 Address IPv6 Address
15	Accounting Timer	1	Accounting timer value
16	Message Integrity	1	HMAC digest

Dans COPS-RSVP, la classe d'objets Context object est utilisée pour transporter le type de message RSVP et la classe Client specific information pour transporter les objets RSVP.

Dans COPS-PR, de nouveaux objets sont encapsulés dans les sous-types Named Client-Specific Information object et Named Decision Data Object. Les objets spécifiques sont issus d'une base d'information de politiques, ou PIB (Policy Information Base), relative à chaque type de client COPS. L'ensemble de ces PIB réunies compose la PIB générale. Cette PIB suit la même convention que la MIB SNMP. Les formats d'encodage actuellement définis pour le stockage des informations et leur transport sont ASN.1 (Abstract Syntax Notation 1) et BER (Basic Encoding Rule).

Les messages sont définis d'une manière générale dans la RFC COPS, leur utilisation spécifique étant précisée dans les RFC d'extension. Le tableau Q.6 récapitule les 10 messages COPS regroupés par sens de circulation.

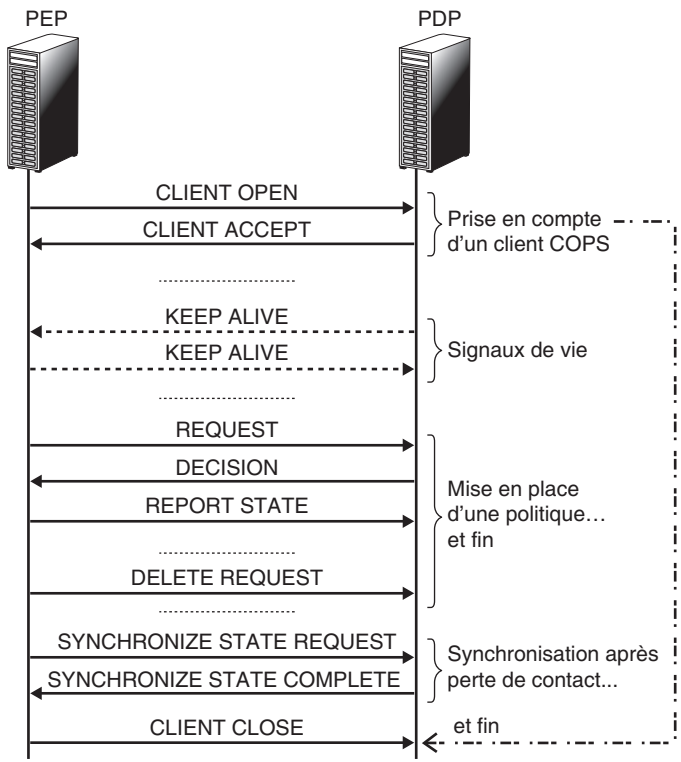
Tableau Q.6 • Messages COPS

Message PEP → PDP	Message PDP → PEP	Message PDP ↔ PEP
REQUEST (demande de politique)	DECISION (envoi de politique)	CLIENT CLOSE (fin de prise en compte de client COPS)
REPORT STATE (résultat d'installation de politique)	SYNCHRONIZE STATE REQUEST (demande de synchronisation)	KEEP ALIVE (Signal d'existence)
DELETE REQUEST STATE (fin d'application de politique)	CLIENT ACCEPT (prise en compte de client COPS)	
CLIENT OPEN (demande de prise en compte de client COPS)		
SYNCHRONIZE STATE COMPLETE (fin de synchronisation)		

Scénarios de contrôle de politique

Les scénarios de contrôle de politique COPS dépendent du mode de contrôle de politique. Cependant, on peut illustrer les échanges de messages COPS par la décomposition en étapes de la figure Q.45.

Figure Q.45
Échanges COPS



Les extensions de COPS

Le protocole COPS peut être étendu en introduisant de nouveaux types de clients. Nous ne décrivons ici que les deux extensions les plus répandues, COPS-RSVP et COPS-PR.

COPS-RSVP (COPS usage for RSVP)

La RFC 2749 de janvier 2000 précise les directives d'usage pour le support de COPS dans un environnement RSVP. C'est dans cette première optique que COPS a été développé par le groupe de travail RAP (Resource Allocation Protocol) afin de fournir un mécanisme de contrôle d'admission à partir de requêtes sur les ressources réseau. Cela a donné lieu à la création d'une extension pour RSVP permettant de prendre en charge le contrôle d'admission par politique, qui spécifie notamment l'objet POLICY-DATA transporté par les messages RSVP et utilisé pour le contrôle par politique par les PEP et le PDP. La RFC 2750 décrit cette extension.

Comme expliqué précédemment, le mode de fonctionnement de COPS-RSVP est l'outsourcing, dans lequel les événements déclencheurs sont les messages RSVP.

Les détails de l'architecture COPS-RSVP sont peu développés dans les RFC 2749 et 2750. On peut cependant déduire les informations suivantes :

- Un PEP est un client RSVP.
- Un client RSVP n'est pas forcément un PEP.
- Un client RSVP sur un routeur extrémité du domaine est forcément un PEP.

L'architecture COPS-RSVP est illustrée à la figure Q.46.

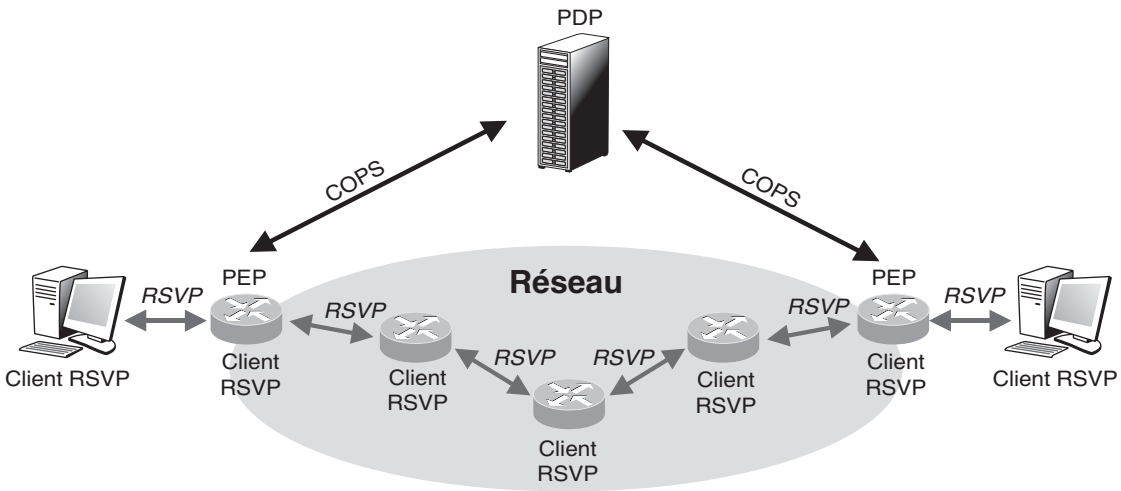


Figure Q.46
Architecture COPS-RSVP

Les types de messages RSVP générant des requêtes COPS sont Path, Resv, PathErr et ResvErr. Tous les objets reçus dans ces messages sont encapsulés dans les requêtes COPS. Trois contextes objet sont définis pour la génération de requêtes COPS du PEP vers le PDP en fonction des événements/actions RSVP :

- Incoming-Message request : lors de l'arrivée d'un message RSVP, une sollicitation pour l'accepter ou le rejeter est envoyée du PEP au PDP.
- Resource-Allocation request : lors de l'arrivée d'un message RSVP Resv, une sollicitation pour injecter (commit) les ressources dans le flux RSVP est envoyée du PEP au PDP.
- Outgoing-Message request : lorsque le PEP doit faire suivre un message RSVP sortant, il sollicite le PDP, qui accepte ou refuse cette sortie et fournit l'objet POLICY-DATA qui sera encapsulé dans le message RSVP.

Lors de l'établissement d'une réservation RSVP, plusieurs sollicitations sont déclenchées. Le nombre de messages COPS engendrés dépend de nombreux paramètres. Dans un fonctionnement normal d'une réservation pour une session point-à-point (unicast), le nombre de ces messages peut être minimisé par regroupement de plusieurs contextes objet dans une même requête COPS. C'est le cas avec le contexte objet combiné In & Allocation & Out pour traiter l'arrivée d'un message Resv et l'affectation des ressources associées et pour le faire suivre.

COPS-PR (COPS usage for Policy Provisioning)

La RFC 3084 de mars 2001 précise les directives d'usage pour la prise en charge de COPS dans un environnement à base d'approvisionnement de politiques. Cette prise en charge est indépendante du type de la politique devant être approvisionnée (QoS, sécurité, etc.) et développe les mécanismes et conventions utilisés pour l'échange d'information en mode provisioning entre des PEP et des PDP.

Le mode provisioning se différencie du mode outsourcing par le fait qu'il n'y a plus de corrélation entre un événement se produisant dans un PEP et la décision relative du PDP. Le PDP peut envoyer directement des informations de provisionnement au PEP suite à une sollicitation externe ou à un ensemble d'événements s'étant produits dans le PEP ou encore à toute autre combinaison.

Le provisionnement des ressources dans un réseau est souvent fondé sur les SLA et s'opère aux frontières du réseau. Cela confère un aspect statique au modèle COPS-PR, où les échanges entre PEP et PDP sont espacés par des temps longs comparativement au modèle dynamique du mode outsourcing.

Les événements externes susceptibles de déclencher des décisions directes du PDP vers le PEP peuvent être les suivants :

- Utilisateur sollicitant des services réseau *via* une interface Web de l'application centrale de gestion.
- Serveur H.323 sollicitant des ressources pour le compte d'un utilisateur voulant établir une visioconférence.

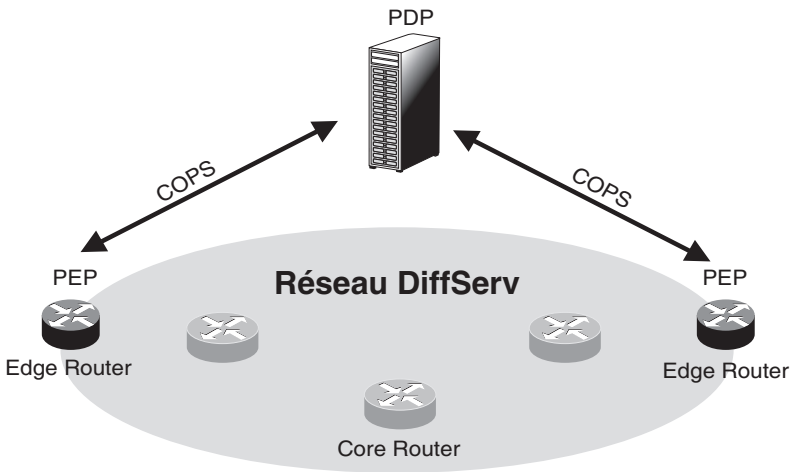
Ces sollicitations externes arrivent directement au PDP. Cependant, la RFC ne décrit pas le mode de communication entre le serveur H.323 et le PDP. D'un autre côté, le PEP peut lui aussi solliciter directement le PDP. Dès l'ouverture de la connexion globale entre PEP et PDP, c'est-à-dire juste après l'échange Client Open ↔ Client Accept, le PEP sollicite le PDP pour obtenir l'ensemble des politiques à approvisionner en son sein. Il peut ensuite le faire à chaque modification de sa configuration, telle que le retrait d'une carte d'interface.

Pour représenter les informations de politique approvisionnée à échanger entre les PEP et le PDP, une base d'information de politiques PIB (Policy Information Base) est introduite. La PIB est représentée par un arbre, dans lequel les branches identifient les classes de politiques, ou PRC (Provisioning Class), et les feuilles les instances de ces PRC, ou PRI (Provisioning Instance), qui sont échangées entre PEP et PDP. Ces PIB sont stockées à la fois dans les PEP et le PDP.

Si l'on regarde l'application du modèle provisioning à la gestion des politiques de QoS, on voit tout de suite son adéquation avec le modèle DiffServ. Dans le modèle DiffServ, les équipements du réseau sont configurés au préalable pour appliquer des mécanismes de qualité de service à l'ensemble des flux du réseau. L'architecture DiffServ définit deux catégories d'équipements, les routeurs extrémité (edge routers) et les routeurs internes. Les premiers doivent classifier les flux et leur affecter un DSCP (DiffServ Code Points), qui sera utilisé dans la suite par tous les seconds pour traiter les paquets avec le comportement associé à ce DSCP particulier. La mise en place de politiques de contrôle de QoS dans cette architecture se fait par l'implantation d'un PEP COPS-PR au niveau de chaque routeur extrémité.

L'architecture de l'environnement COPS-PR pour un réseau DiffServ est décrite à la figure Q.47.

Figure Q.47
Architecture COPS-PR pour un réseau DiffServ

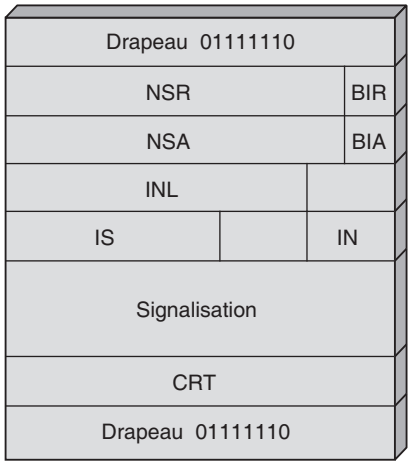


La signalisation CCITT n° 7 (SS7)

Le protocole CCITT n° 7 (SS7 en anglais) a été mis au point par l'UIT-T dans le cadre de la transmission de la signalisation sur les réseaux publics. Le protocole LAP-D, que nous verrons par la suite, véhicule la signalisation sur la terminaison d'abonnés. Au moment de leur passage dans le réseau public proprement dit, les informations de supervision sont prises en charge par un réseau spécifique de type datagramme, le réseau sémaphore, qui suit la recommandation CCITT n° 7 décrivant les couches du protocole. Cette architecture est compatible avec le modèle de référence.

Le protocole de niveau 2 est de type HDLC. Il a été légèrement modifié pour prendre en compte les contraintes temps réel de la signalisation. Tous les algorithmes sont semblables à ceux de HDLC, excepté celui des reprises sur erreur. La détection se fait toujours par la zone de contrôle. La structure de la trame CCITT n° 7 est illustrée à la figure Q.48.

Figure Q.48
La trame CCITT n° 7



Trois types de trames sont disponibles dans la procédure :

- Les PDU de signalisation sans champ d'information.
- Les PDU avec un champ d'information, qui servent aux contrôles de la procédure elle-même. C'est par ce type de trame que le contrôle de flux de la liaison est effectué. Lorsque la procédure n'a pas de signalisation utilisateur à transmettre, elle émet en continu des trames de ce type, en acquittant la dernière trame bien reçue. On a ainsi une duplication des acquittements, ce qui est très utile en cas de perte d'acquittement. Un autre avantage de ces trames est qu'elles détectent presque instantanément une rupture de la liaison.
- Les PDU avec un champ d'information, qui transportent la signalisation de bout en bout. Pour cette catégorie, on trouve un numéro de trame sur 7 bits situé dans le deuxième octet de la trame, juste derrière le drapeau, ainsi qu'un deuxième numéro

de séquence dans le troisième octet de la trame. Ces deux numéros, associés aux bits BIR (indicateur de bit arrière) et BIA (indicateur de bit avant), permettent un contrôle avant et arrière de la procédure.

Les trames contiennent encore un indicateur de longueur sur 6 bits, le champ INL, un indicateur de service dans le champ IS sur 4 bits et un indicateur national IN sur 2 bits.

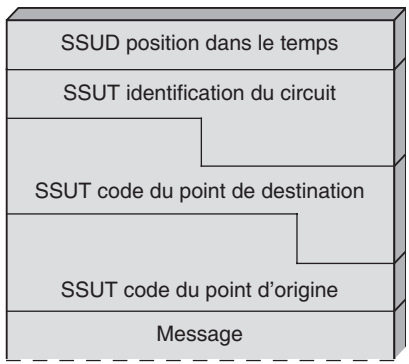
Deux techniques de reprise sur erreur sont disponibles. La première est conforme à la procédure HDLC. La seconde permet une récupération plus rapide et une duplication des réémissions. Cette seconde technique est particulièrement appréciable dans les réseaux où le temps de propagation est très long, comme les réseaux satellite. À chaque réémission, si le support est libre, on retransmet toutes les trames depuis la trame en erreur, et l'on recommence jusqu'à ce qu'il y ait une nouvelle signalisation à émettre. Cette politique permet de dupliquer ou tripliquer, c'est-à-dire faire trois copies, les reprises et de prévoir, le cas échéant, plusieurs trames successives erronées.

Pour compléter les caractéristiques de la procédure CCITT n° 7, indiquons que les coupleurs extrémité possèdent des compteurs d'erreur, qui comptabilisent le nombre de trames erronées par unité de temps. Si le compteur dépasse une valeur déterminée par le gestionnaire du réseau, la liaison est fermée.

Le niveau réseau de la recommandation CCITT n° 7 spécifie un réseau datagramme puisque les données à transmettre sont extrêmement courtes, de l'ordre de quelques octets. Nous allons décrire brièvement le protocole de niveau réseau.

Les avis Q.702 à Q.704 de l'UIT-T décrivent le protocole CCITT n° 7. Le niveau 3 prend surtout en charge le problème de l'adressage. Celui-ci est décrit dans les recommandations Q.711 à Q.714. En particulier, la norme 84 définit le sous-système de commande des connexions sémaphore SCCP (Signaling Connection Control Part). Le paquet de niveau 3 est illustré à la figure Q.49.

Figure Q.49
Paquet de niveau 3 du protocole CCITT n° 7



SSUT (sous-système utilisateur téléphonique)
SSUD (sous-système utilisateur informatique)

Deux sous-systèmes ont été normalisés : le sous-système correspondant aux applications téléphoniques, dans les avis Q.721 à Q.725, et celui correspondant aux applications

informatiques. Ils sont appelés respectivement TUP (Telephone User Part) et DUP (Data User Part).

Le service de transport de la recommandation CCITT n° 7 assure pour le compte du niveau session un transport de bout en bout des TSDU. Il offre cinq classes de services spécifiques suivant le type de relation entre les deux extrémités.

R

Annexe du chapitre 24 (La sécurité et l'identité)

Cette annexe passe en revue des exemples de protocoles EAP utilisés part divers grands équipementiers des réseaux. Elle aborde ensuite la sécurité de la messagerie électronique.

Exemples de protocoles EAP (Extensible Authentication Protocol)

Cette section présente les protocoles LEAP, EAP-FAST, EAP-SIM et PEAP.

LEAP (Lightweight Extensible Authentication Protocol)

L'architecture LEAP s'appuie sur la procédure d'authentification disponible sur les plates-formes Windows.

L'authentification LEAP fonctionne de la façon suivante (*voir figure R.1*) :

1. À partir du mot de passe utilisateur, on calcule une empreinte MD4 de 16 octets. Cette dernière est complétée par cinq octets nuls. On obtient ainsi une suite de 21 octets interprétée sous la forme de trois clés DES de 7 octets, soit 56 bits. Le mécanisme d'authentification, de type CHAP, consiste à chiffrer un nombre aléatoire de 8 octets à l'aide des trois clés DES associées à un utilisateur, ce qui produit une réponse de 24 octets. LEAP est associé au type EAP 17 (0x11) pour réaliser une double authentification, entre le serveur d'authentification et le supplicant (utilisateur du réseau), d'une part, et entre l'authenticator (point d'accès) et le serveur d'authentification, d'autre part.

2. Au terme d'un scénario d'authentification réussi entre supplicant et serveur RADIUS (correspondant aux phases 1 à 5 de la figure R.1), les deux entités déduisent une clé de session SK (unicast), qui est transportée à l'aide d'un attribut propriétaire (CISCO-AVPAIR, LEAP SESSION-KEY) du protocole RADIUS. LEAP supporte également des mécanismes de mise à jour de clés WEP, soit par la négociation d'une session RADIUS limitée (Session Timeout), soit par des demandes périodiques de réauthentification par le supplicant à l'aide des trames EAP LOGOFF et EAP START.

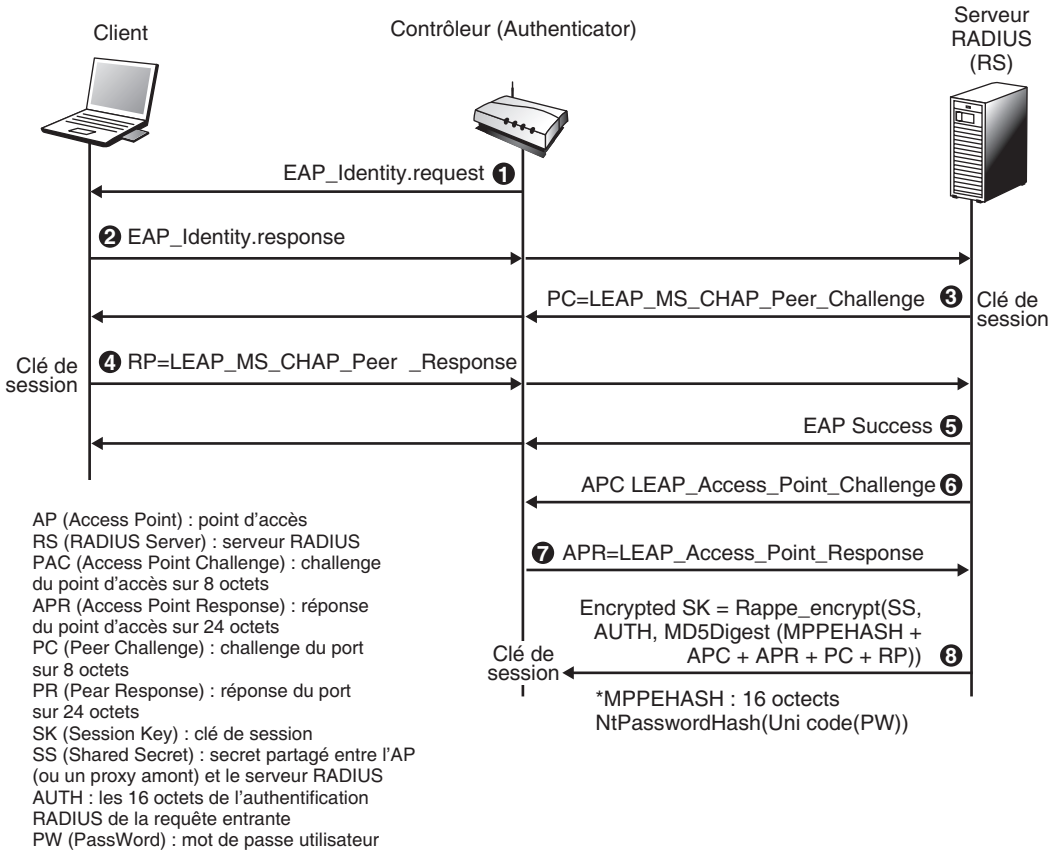
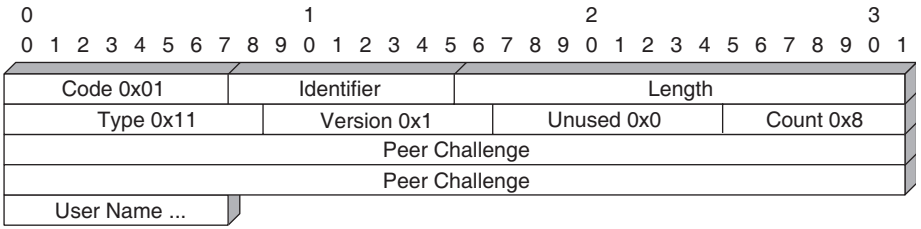


Figure R.1

Processus d'authentification LEAP

Le format du paquet LEAP est illustré à la figure R.2.

Figure R.2
Paquet LEAP



EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)

EAP-FAST a été développé par Cisco Systems pour résoudre une faille de sécurité de son protocole propriétaire LEAP (Lightweight EAP), que nous venons d'examiner, lorsque les mots de passe ne sont pas assez sophistiqués.

Ce protocole vise notamment à contrer les attaques par dictionnaire utilisées avec succès contre LEAP. Contrairement à PEAP, que nous verrons un peu plus loin dans cette annexe, qui est le fruit d'une alliance entre Cisco, Microsoft et RSA Security, EAP Fast ne requiert pas la mise en place d'une infrastructure complexe de distribution de certificats pour l'établissement de tunnels sécurisés entre machines terminales.

EAP FAST est intégré dans l'ensemble des produits Aironet de Cisco ainsi que dans son serveur VPN Cisco Secure ACS. Les partenaires de Cisco auront aussi accès au standard dans le cadre de la spécification Cisco Compatibility Extensions 3.0.

De façon plus précise, EAP-FAST est une architecture de sécurité de type client-serveur, qui chiffre les transactions EAP au moyen d'un tunnel TLS. Cette solution est assez semblable à PEAP, à la différence essentielle près que le tunnel EAP-FAST est établi à l'aide de secrets forts, qui appartiennent aux utilisateurs. Ces secrets sont appelés PAC (Protected Access Credentials). Ils sont générés par le serveur Cisco Secure ACS à l'aide d'une clé maître connue uniquement du serveur Cisco Secure ACS. Les handshakes réalisés par des secrets partagés étant beaucoup plus rapides à mettre en œuvre qu'une PKI, EAP-FAST est plus simple à mettre en place que les solutions qui chiffrent les transactions EAP, comme EAP-TLS ou PEAP.

EAT-FAST s'exécute en trois phases :

- La phase 0, spécifique d'EAP-FAST, consiste à ouvrir un tunnel sécurisé entre les machines terminales en utilisant les certificats PAC. Le tunnel est établi par un échange de clés au moyen d'une procédure de type Diffie-Hellman. Si l'authentification EAP-MSCHAPv2 réussit, le serveur Cisco Secure ACS donne un certificat PAC à chaque client. Cette phase 0 est optionnelle si les certificats sont introduits par une autre méthode assurant le secret des certificats.
- En phase 1, le serveur Cisco Secure ACS et les machines terminales établissent des tunnels TLS grâce aux PAC présents dans les machines terminales. La façon dont le PAC a été introduit dans la machine terminale est indépendante de la phase 1.

- En phase 2, le serveur Cisco Secure ACS authentifie les certificats des machines terminales par l'intermédiaire d'un EAP-GTC, qui est protégé par le tunnel TLS créé à la phase 1. Le protocole EAP-FAST ne supporte pas d'autre type d'EAP. Cisco Secure ACS autorise un service réseau au travers du point d'accès si la phase 2 s'est déroulée avec succès.

Cette solution est présentée par Cisco comme étant aussi simple que LEAP et aussi sécurisée que PEAP. En fait, EAP-FAST est un compromis entre les deux. Le fait de ne pas utiliser de PKI semble plus simple mais est en réalité aussi difficile à mettre en œuvre pour obtenir une bonne sécurité. De plus, la sécurité n'est pas aussi bonne qu'avec PEAP car la phase 0 peut conduire à des attaques décisives si elle n'est pas aussi sécurisée que peut l'être une PKI.

EAP-SIM (Subscriber Identity Module)

Une solution classique d'authentification est proposée par les opérateurs de téléphones mobiles de deuxième génération, ou GSM, selon une procédure d'authentification réalisée entre le serveur de l'opérateur et la carte SIM (Subscriber Identity Module) située dans le terminal de l'utilisateur. Cette authentification utilise non pas le protocole EAP mais des protocoles provenant de l'ETSI effectuant un travail comparable.

Les sections qui suivent décrivent ce mécanisme avant de présenter EAP-SIM, une extension normalisée d'EAP pour le monde IP que les opérateurs peuvent, par exemple, utiliser dans les hotspots.

L'authentification du GSM

Le GSM est un standard de téléphonie mobile défini par l'ETSI (European Telecommunications Standards Institute). Il supporte des opérations de sécurité telles que l'authentification de l'utilisateur et le chiffrement entre le réseau nominal, où l'abonné est inscrit, et la carte SIM de l'abonné.

Les éléments du réseau GSM intervenant dans ces fonctions de sécurité sont les suivants :

- AuC (Authentication Center), ou centre d'authentification du réseau de l'opérateur.
- HLR (Home Location Register), ou base de données des abonnés de l'opérateur, qui mémorise les données de chaque abonné, telles que son identité internationale, ou IMSI (International Mobile Subscriber Identity), son numéro de téléphone, son profil d'abonnement, etc. Il stocke aussi pour chaque abonné le numéro de VLR courant.
- VLR (Visitor Location Register), ou base de données des seuls abonnés localisés dans la zone géographique gérée.

Les données d'authentification sont stockées dans la carte SIM et ne sont pas chargées dans le terminal mobile. La procédure d'authentification consiste donc en un échange de messages entre la carte SIM et le réseau.

Lors de l'inscription d'un nouvel abonné, une clé Ki (jusqu'à 128 bits) lui est attribuée. Cette clé est secrète et n'est stockée que sur sa carte SIM et sur l'AuC de l'opérateur.

La procédure d'authentification se déroule de la façon suivante :

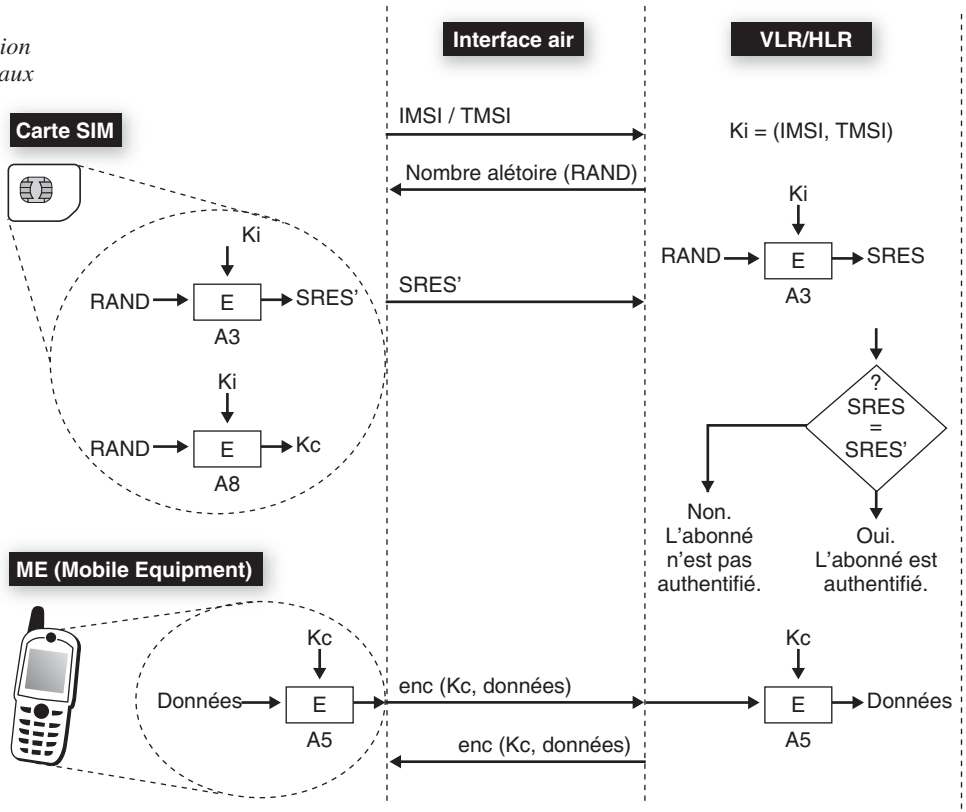
1. Le réseau transmet au mobile un nombre aléatoire RAND, codé sur 128 bits.
2. La carte SIM du mobile calcule la signature de RAND grâce à l'algorithme d'authentification A3 et sa clé Ki. Le résultat, SRES (32 bits), est envoyé par le mobile au réseau.
3. Le réseau compare SRES avec le résultat calculé de son côté. Si les deux coïncident, l'abonné est authentifié.

Une fois l'abonné authentifié, le chiffrement est effectué selon l'algorithme A5. Il utilise la clé Kc, de 64 bits, calculée à partir de la clé secrète Ki et du nombre aléatoire RAND, selon l'algorithme A8.

Il suffit au réseau de disposer d'un triplé (RAND, SRES, Kc) pour authentifier un abonné et activer le chiffrement de ses communications. Cependant, le réseau ne calcule pas ces données en temps réel. L'AuC prépare des triplés pour chaque abonné et les transmet à l'avance au HLR, qui les stocke. Le VLR qui a besoin d'un triplé en effectue la demande le moment venu.

La procédure d'authentification entre l'équipement mobile et le VLR/HLR est illustrée à la figure R.3.

Figure R.3
Authentification dans les réseaux GSM



L'algorithme A5 est implémenté dans chaque terminal et dans le réseau. Les implémentations des algorithmes A3 et A8, aussi appelés COMP128, existent sur Internet, mais aucun standard n'a encore été publié.

L'authentification EAP-SIM

Les hotspots, ou zones publiques à forte densité de population, telles que gares, aéroports, etc., peuvent être vus par les opérateurs de mobiles comme une extension possible de leur réseau. Il existe pour ces hotspots un mécanisme d'authentification mutuelle fondé sur le module SIM, appelé EAP-SIM. Ce protocole complète les procédures d'authentification utilisées par le GSM en fournissant une authentification entre le centre d'authentification de l'opérateur mobile et chaque module SIM. Les algorithmes d'authentification sont présents à la fois dans le réseau et dans toutes les cartes à puce SIM.

La solution EAP-SIM interagit directement avec les cartes à puce existantes. Sur le terminal, le composant logiciel qui implémente le protocole EAP-SIM peut utiliser PC/SC (Personal Computer/Smart Card), un environnement défini par un groupe d'industriels mené par Microsoft, pour communiquer directement avec la carte à puce de l'abonné. Une telle configuration ne nécessite aucune modification du réseau cœur GSM pour implémenter EAP-SIM. Par contre, il est nécessaire d'implémenter les communications entre le serveur d'authentification et le HLR/AuC, côté serveur, et entre le logiciel EAP-SIM et la carte SIM, côté client.

Une solution innovante a également été mise en place par un des fabricants majeurs de téléphones portables, permettant à une carte réseau 802.11 de communiquer directement avec un module SIM intégré, sans passer par le terminal, renforçant ainsi la sécurité.

L'identité (EAP-ID) est obtenue par la concaténation du caractère 1 de la valeur, exprimée en une suite de chiffres ASCII, de l'IMSI, du caractère @ et du nom de domaine de l'opérateur (EAP-ID = 1IMSI@operator.com).

L'authentification EAP-SIM se déroule de la manière suivante (*voir figure R.4*) :

1. Soit C le client et A le point d'accès. Dans ce processus, A utilise trois triplés d'authentification (RAND, Kc, SRES) :

   $$C \rightarrow A: RC$$

   Lors de cette première étape, le client C envoie au point d'accès A un défi aléatoire Rc.

2. A répond au client par la liste des trois nombres aléatoires RAND1, RAND2 et RAND3 provenant de trois triplés. Il envoie aussi le MAC calculé sur ces 3 nombres et sur Rc (MACk) :

   $$A \rightarrow C: RAND1, RAND2, RAND3, MACk[\ldots, RAND1, RAND2, RAND3, Rc]$$

3. La clé K, permettant le calcul de MACk, a été préalablement calculée par le point d'accès par dérivation d'une clé maître MK=SHA[…,Kc1,Kc2,Kc3,Rc,…], où Kc1, Kc2 et Kc3 sont les clés Kc des 3 triplés.

   $$C \rightarrow A: MACk[\ldots, SRES1, SRES2, SRES3]$$

4. Quand C reçoit MACk et la liste de nombres aléatoires RAND, il vérifie le MACk. Pour ce faire, C utilise Ki (présente sur la carte à puce de l'utilisateur et partagée avec le serveur d'authentification) pour retrouver les clés Kc1, Kc2 et Kc3. Ces dernières lui permettent de générer MK, qu'il utilise pour calculer K par dérivation.
5. Avec cette même clé K, C calcule le MAC sur les trois valeurs SRES des triplés et envoie le résultat au point d'accès. À son tour, A vérifie le MAC et la liste de SRES qu'il a reçus du réseau GSM. Si les résultats obtenus sont identiques, C est authentifié.

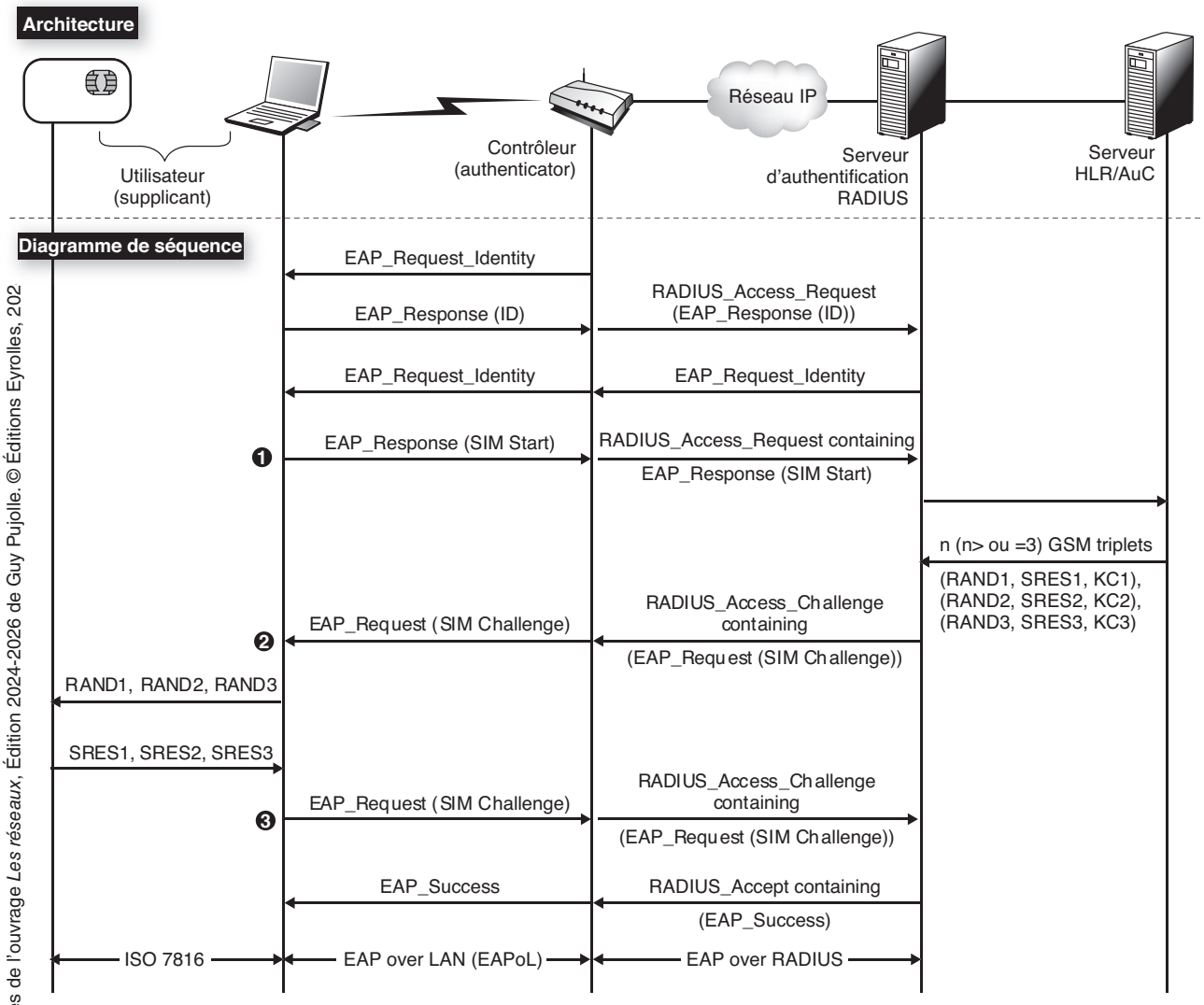


Figure R.4
Authentification EAP-SIM

Grâce à la technologie EAP-SIM, les opérateurs de téléphonie peuvent utiliser leur base de données client (HLR) pour assurer la facturation des services sans fil.

PEAP (Protected Extensible Authentication Protocol)

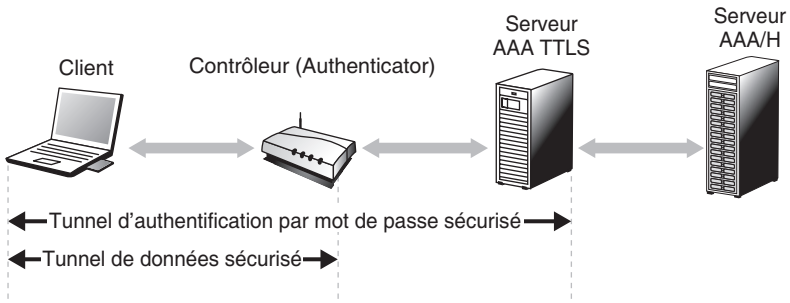
Les installations sans fil actuellement déployées utilisent des protocoles d'authentification hétérogènes. De ce fait, la mobilité du client est difficile à gérer. Pour une entreprise, EAP offre l'avantage de réutiliser dans son environnement sans fil des mécanismes déjà adoptés dans l'environnement filaire.

La sélection d'une méthode d'authentification est une décision stratégique pour le déploiement sécurisé d'un réseau. La méthode d'authentification conduit au choix du serveur d'authentification, qui, à son tour, conduit au choix du logiciel client. Dans le cas où une infrastructure PKI n'est pas déjà déployée, il existe d'autres méthodes d'authentification, présentant un niveau de sécurité équivalent à celui obtenu avec les certificats numériques et permettant de s'affranchir des barrières liées à la mise en place d'une infrastructure PKI. Ces méthodes permettent aussi de protéger les procédures d'authentification du client fondées sur des mots de passe.

Par exemple, EAP-TTLS (Tunneled Transport Layer Security) et PEAP conservent les fortes fondations cryptographiques de TLS et d'EAP mais utilisent d'autres mécanismes pour authentifier le client.

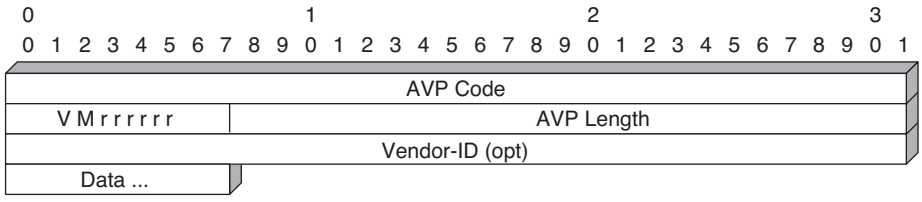
Ces protocoles établissent d'abord un tunnel sécurisé TLS, après quoi le client authentifie le serveur (*voir figure R.5*).

Figure R.5
Tunnels PEAP et EAP-TTLS



Dans une seconde étape, des paquets d'authentification sont échangés. TTLS échange des AVP (Attribute-Value Pairs) avec un serveur, qui les valide pour tout type d'authentification. Le format des paires de valeurs d'attributs est illustré à la figure U.6.

Figure U.6
Format des paires de valeurs d'attributs



PEAP utilise le canal TLS pour protéger un second échange EAP. MS-CHAP-V2 peut être utilisé pour les clients n'ayant pas de PKI. Pour les clients ayant une PKI, EAP-TLS peut être utilisé. L'avantage de PEAP par rapport à l'EAP-TLS classique est que l'identité du client est protégée lors de l'échange.

La figure R.7 illustre le principe de fonctionnement de PEAP.

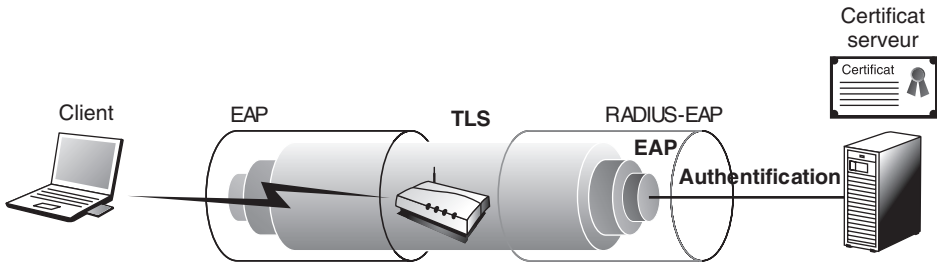


Figure R.7

Principe de fonctionnement de PEAP

La sécurité dans les protocoles

Conçus avant les années 2000, les protocoles du monde IP n'ont pas intégré de fonctions de sécurité. De nombreuses failles de sécurité existent donc, qui sont comblées régulièrement par des RFC spécifiques.

Les attaques sur les protocoles de gestion ou de contrôle peuvent facilement arrêter le fonctionnement d'un réseau. Il suffit, par exemple, de faire croire aux accès que le réseau est saturé ou que les nœuds sont en panne pour que les performances du réseau s'effondrent totalement.

La sécurité dans SNMP

La RFC 2274 définit le modèle USM (User-based Security Model) de sécurité de SNMP, qui offre à la fois une authentification et un service de sécurité.

Les principales attaques dont SNMP peut être l'objet sont les suivantes :

- Modification de l'information : une entité peut altérer un message en transit généré par une entité autorisée pour modifier une opération de type comptabilité, configuration ou opération.
- Mascarade : une entité prend l'identité d'une entité autorisée.
- Modification à l'intérieur d'un flot de messages : SNMP est construit pour gérer un protocole de transport en mode sans connexion. Les messages peuvent être réordonnés d'une façon différente de celle d'origine et détruits ou rejoués d'une autre manière. Par exemple, un message qui redémarre une machine peut être copié puis rejoué ultérieurement.

- Ordre de secret : une entité peut observer les échanges entre un manager et son agent et apprendre les valeurs des objets gérés. Par exemple, l'observation d'un ensemble de commandes capables de modifier un mot de passe permettrait à un utilisateur de modifier le mot de passe et d'attaquer le site.

Le modèle de sécurité USM ne prend pas en compte les deux fonctionnalités suivantes :

- Refus de service : un attaquant interdit l'échange d'informations entre un manager et son agent. Nous avons vu au chapitre 23, consacré à la gestion de réseau, que les échanges d'information de gestion s'effectuaient entre un manager de gestion et ses agents. Si le manager ne reçoit plus les informations du réseau et *vice versa,* les agents ne reçoivent plus les commandes du manager, et le processus de gestion du réseau ne peut plus s'effectuer. On appelle cette attaque un refus de service, puisque le service de gestion refuse de travailler.
- Analyse de trafic : un attaquant observe le type de trafic qui s'effectue entre un manager et son agent. L'analyse permet de détecter les ordres qui sont passés et les remontées d'information. Après analyse du trafic, le pirate peut faire croire au manager que le trafic est totalement différent de ce qu'il est effectivement dans le réseau.

Pour contrer ces différentes attaques, deux fonctions cryptographiques ont été définies dans USM : l'authentification et le chiffrement. Pour les réaliser, le moteur SNMP requiert deux valeurs : une clé privée et une clé d'authentification. Ces valeurs sont des attributs de l'utilisateur qui ne sont pas accessibles par des primitives SNMP.

Deux algorithmes d'authentification sont disponibles : HMAC-MD5-96 et HMAC-SHA-96. L'algorithme HMAC utilise une fonction de hachage sécurisée et une clé secrète pour produire un code d'authentification du message. Ce protocole fortement utilisé dans Internet est décrit en détail dans la RFC 2104.

S

Complément ToIP et IPTV

Cette annexe détaille la téléphonie sur ATM et le relais de trames. En particulier, elle se penche sur la technologie AAL2, utilisée sur le RAN (Radio Accès Network) de l'UMTS, et examine l'évolution des PABX et l'intégration téléphonie-informatique.

Les applications de téléphonie et de télévision sont devenues les applications dominantes du monde des réseaux, et elles le resteront pendant de nombreuses années en raison notamment de l'émergence de nouveaux et immenses marchés, comme celui de la Chine. Proportionnellement, le débit de la téléphonie décroît, même si l'ensemble des communications devrait être en VoIP (Voice over IP) en 2015. Au contraire, le débit des applications vidéo, en particulier de la télévision, augmente fortement au point que cette application est devenue prépondérante sur Internet.

La parole téléphonique a été traditionnellement prise en charge par les réseaux à commutation de circuits, mais le passage vers les réseaux à transfert de paquets, essentiellement de type IP, est inéluctable. En 2010, quasiment l'ensemble des communications téléphonique s'effectuent en mode paquet. Le passage au tout-IP permet d'intégrer les services de données et de téléphonie dans un même réseau. Beaucoup d'entreprises intègrent leur environnement téléphonique dans leur réseau à transfert de paquets pour, d'une part, faire baisser les coûts des communications, mais aussi, d'autre part, simplifier la maintenance en passant de deux réseaux à gérer (téléphonie et données) à un seul (données).

La télévision sur IP (IPTV) ne cesse de s'étendre, de même que le nombre de chaînes. Nous examinerons les principes du transport de la télévision sur Internet.

L'annexe commence par examiner l'évolution de la téléphonie vers les réseaux Internet et intranet puis traite de l'arrivée massive de la télévision et plus généralement de la vidéo sur IP.

L'application téléphonique

La difficulté de faire de la téléphonie par paquet provient de la très forte contrainte temporelle résultant de l'interaction entre individus. Le temps de latence doit être inférieur à 300 ms si l'on veut garder une interaction humaine acceptable. Si l'on souhaite une bonne qualité de la conversation, il ne faut pas que la latence soit supérieure à 150 ms. Un cas encore plus complexe se produit lorsqu'il y a un écho, c'est-à-dire un signal qui revient à l'oreille de l'émetteur. L'écho se produit lorsque le signal rencontre un obstacle, comme l'arrivée sur le combiné téléphonique. L'écho qui repart en sens inverse est numérisé par un codec et traverse sans problème un réseau numérique. La valeur normalisée de la latence de l'écho étant de 56 ms, pour que l'écho ne soit pas gênant à l'oreille, il ne faut pas que le temps aller dépasse 28 ms, en supposant un réseau symétrique qui prend le même temps de réponse à l'aller et au retour. Il faut donc que, dans les équipements terminaux, les logiciels extrémité soient capables de gérer les retards et de resynchroniser les octets qui arrivent. En règle générale, les équipements modernes, comme les terminaux GSM, possèdent des suppresseurs d'écho évitant cette contrainte temporelle forte.

La voix simple en paquet n'est pas aussi contraignante que la parole téléphonique, car elle n'implique aucune contrainte temporelle. Dans le cas d'IP, il ne faut donc pas confondre la téléphonie sur IP (ToIP) et la voix sur IP (VoIP).

L'application de téléphonie est donc complexe à prendre en charge en raison de son caractère interactif et de sa forte synchronisation. Rappelons les trois opérations successives nécessaires à la numérisation de la parole, qu'elle soit téléphonique ou non :

1. **Échantillonnage.** Consiste à prendre des points du signal analogique au fur et à mesure qu'il se déroule. Il est évident que plus la bande passante est importante, plus il faut prendre d'échantillons par seconde. C'est le théorème d'échantillonnage qui donne la solution : il faut échantillonner à une valeur égale à au moins deux fois la bande passante.
2. **Quantification.** Consiste à représenter un échantillon par une valeur numérique au moyen d'une loi de correspondance. Cette phase consiste à trouver la loi de correspondance de telle sorte que la valeur des signaux ait le plus de signification possible.
3. **Codage.** Consiste à donner une valeur numérique aux échantillons. Ce sont ces valeurs qui sont transportées dans le signal numérique.

La largeur de bande de la voix téléphonique analogique est de 3 200 Hz. Pour numériser ce signal correctement sans perte de qualité, puisqu'elle est déjà relativement mauvaise, il faut échantillonner au moins 6 400 fois par seconde. La normalisation a opté pour un échantillonnage de 8 000 fois par seconde. La quantification s'effectue par des lois semi-logarithmiques. L'amplitude maximale permise se trouve divisée en 128 échelons positifs pour la version américaine PCM, auxquels il faut ajouter 128 échelons négatifs dans la version européenne MIC. Le codage s'effectue donc soit sur 128 valeurs, soit sur 256 valeurs, ce qui demande en binaire 7 ou 8 bits de codage. La valeur totale du débit de la numérisation de la parole téléphonique s'obtient en multipliant le nombre d'échantillons par le nombre d'échelons, ce qui donne :

- 8 000 × 7 bit/s = 56 Kbit/s en Amérique du Nord et au Japon ;
- 8 000 × 8 bit/s = 64 Kbit/s en Europe.

Beaucoup d'autres solutions ont été développées par rapport aux qualités et aux défauts de l'oreille :

- AD-PCM (Adaptive Differential-Pulse Code Modulation), ou MIC-DA (Modulation par impulsion et codage-différentiel adaptatif) ;
- SBC (Sub-Band Coding) ;
- LPC (Linear Predictive Coding) ;
- CELP (Code Excited Linear Prediction).

La section suivante fait un tour d'horizon des principaux codeurs audio.

Les codeurs audio

Les codeurs audio associés aux différentes techniques citées précédemment sont nombreux. On trouve notamment les codecs classiques mais aussi de nouveaux codeurs bas débit. La figure S.1 illustre les vitesses de sortie des différentes normes de codeurs de la voix téléphonique fondées sur un échantillonnage standard à 8 kHz. L'ordonnée représente la qualité du son en réception, qui est évidemment un critère subjectif. Nous avons aussi représenté les codeurs utilisés dans les réseaux de mobiles GSM et les normes régionales.

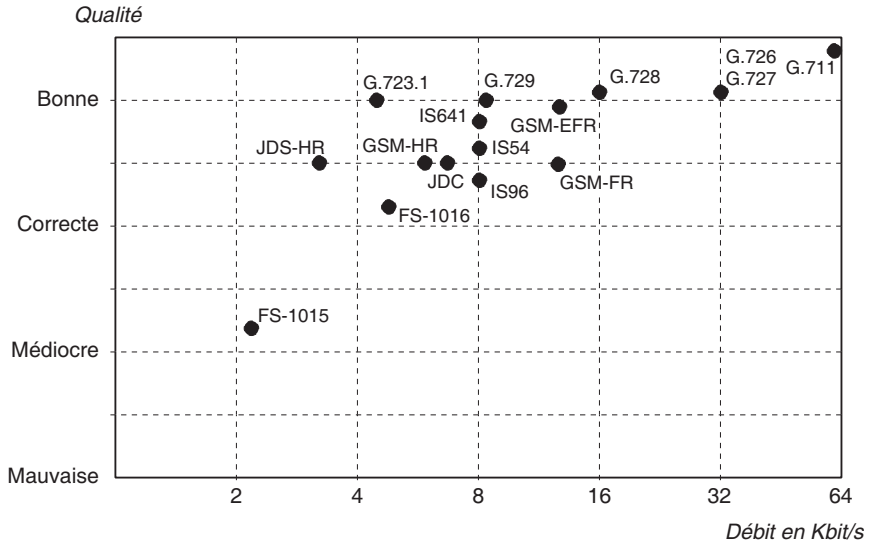


Figure S.1

Codeurs audio

Pour l'audio haute définition, on considère une bande passante plus importante puisque l'oreille humaine est sensible aux fréquences de 20 à 20 000 Hz. L'échantillonnage s'effectue sur 40 kHz, et c'est la valeur de 44,1 kHz qui a été choisie. Le codage effectué sur un CD tient sur 16 bits par échantillon, ce qui donne 705,6 Kbit/s.

Parmi les nombreux codeurs propriétaires qui existent sur le marché, citons :

- StreamWorks à 8,5 Kbit/s
- VoxWare à 2,4 Kbit/s avec le codeur RT24
- Microsoft à 5,3 Kbit/s avec la norme G.723
- VocalTec à 7,7 Kbit/s

La recommandation G.711 correspond à la numérisation classique à 64 Kbit/s en Europe ou 56 Kbit/s en Amérique du Nord. G.723 est une compression de la parole utilisée par de nombreux industriels, entre autres Microsoft, qui l'utilise dans l'environnement Windows. Le débit descend à presque 5 Kbit/s. G.726 est la norme adoptée pour la compression de la parole en codage différentiel adaptatif en 16, 24, 32 ou 40 Kbit/s. Dans ce cas, au lieu de coder l'échantillon en entier, on n'envoie que la différence avec l'échantillon précédent, ce qui permet un codage sur beaucoup moins d'éléments binaires. G.727 utilise aussi un codage différentiel, qui apporte des compléments au codage précédent. Cette recommandation indique comment changer, en cours de numérisation, le nombre de bits utilisés pour coder les échantillons. Elle est particulièrement utile dans le cadre des réseaux qui demandent à l'application de s'adapter en fonction de la charge du réseau. G.728 est une compression à 16 Kbit/s utilisant une technique de prédiction, qui consiste à coder la différence entre la valeur réelle et une valeur estimée de l'échantillon à partir des échantillons précédents. On comprend que cette différence peut être encore plus petite que dans la technique différentielle. Si l'estimation est bonne, la valeur à transporter avoisine toujours 0. Très peu de bits sont alors nécessaires pour acheminer cette différence. Les standards FS proviennent du ministère américain de la Défense.

Les codeurs les plus récents sont G.723.1, G.729 et G.729.A. Le codeur G.723.1 permet un débit compris entre 5,3 et 6,4 Kbit/s. Les deux codeurs G.729 donnent un débit de 8 Kbit/s, mais la qualité de la communication est meilleure. Ce codec a été choisi pour compresser la voix dans l'UMTS.

La parole téléphonique est une application très contraignante, comme nous l'avons vu à plusieurs reprises dans cet ouvrage. La première contrainte provient de l'interactivité entre les deux utilisateurs, qui limite le temps aller-retour à une valeur de 600 ms au maximum. Les normes de l'UIT-T portent cette valeur à 800 ms. Cependant, pour avoir une bonne qualité de la communication, il faut descendre à 300 ms aller-retour. Suivant les protocoles sous-jacents, plusieurs méthodes permettant de satisfaire à ces contraintes ont été développées à la fin des années 1990, que nous allons examiner.

La téléphonie sur IP

La problématique du transport de la parole téléphonique dans des environnements IP est assez différente suivant que l'on est sur un réseau IP non contrôlé, comme Internet, ou sur un réseau permettant l'introduction d'un contrôle, comme le réseau privé d'une compagnie, de type intranet, ou celui d'un FAI.

Sur l'Internet de première génération, il faut que le réseau soit peu chargé pour que la contrainte de 300 ms soit respectée. Sur les réseaux intranet et ceux des fournisseurs

d'accès à Internet, mais aussi ceux des opérateurs, le passage de la parole est possible à condition de contrôler le réseau pour que le temps total de transport, y compris la paquétisation et la dépaquétisation, soit limité.

De nombreuses solutions ont été proposées, comme VoIP (Voice over IP) de l'IMTC (International Multimedia Teleconferencing Consortium). Dans ces solutions, il a d'abord fallu définir un codeur normalisé. Le choix s'est généralement porté sur G.723, mais d'autres solutions sont opérationnelles, comme le codeur G.711. Le paquet IP doit être le plus court possible, et il faut multiplexer plusieurs voies de parole dans un même paquet, de façon à raccourcir le temps de remplissage et à limiter les temps de transfert dans le réseau. Si les routeurs peuvent gérer des priorités, ce qui est possible en utilisant des services de type DiffServ, la parole téléphonique est acheminée beaucoup plus facilement dans le laps de temps demandé.

Plusieurs organismes de normalisation, de droit ou de fait, ont fortement travaillé sur ce sujet. Dans les organismes de droit, l'ETSI, l'organisme de normalisation européen, a mis sur pied le groupe TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks). Ce groupe a défini la parole et le fax entre utilisateurs connectés, en particulier sur des réseaux IP. Le cas où un utilisateur travaille sur un réseau IP et un autre sur un réseau à commutation de circuits, qu'il soit téléphonique, RNIS, GSM ou UMTS, entre également dans le cadre des études de TIPHON. Les activités de TIPHON concernent en outre la validation de solutions pour transporter la parole téléphonique par le biais de démonstrateurs.

L'UIT-T travaille de son côté activement sur le problème de la téléphonie sur IP dans trois groupes du SG 16 : le WP1 pour les modems (série V), le WP2 pour les codecs (série G) et le WP3 pour les terminaux (série H). L'objectif de l'UIT-T est de finaliser un environnement complet et non pas simplement un terminal ou un protocole.

Au sein de l'IETF, de nombreux groupes de travail se sont attaqués à cette problématique, parmi lesquels :

- AVT (Audio Video Transport), qui utilise le protocole RTP (RFC 1889 et 1890) pour effectuer la communication en temps réel.
- MMUSIC (Multiparty Multimedia Session Control), qui utilise le protocole SIP.
- IPTel (IP Telephony), qui définit un protocole de localisation des passerelles et un langage permettant de mettre en communication des circuits et des flots IP.
- PINT (PSTN IP Internetworking), qui utilise également le protocole SIP.
- FAX (Fax over IP), qui stocke et émet des fax par l'intermédiaire de messages électroniques.
- MEGACO (Media Gateway Control), qui détermine un protocole entre une passerelle et son contrôleur.
- SIGTRAN (Signal Translation), qui propose l'utilisation du passage des commandes de la signalisation CCITT n° 7 dans des paquets IP.
- ENUM (E.164/IP translations), qui gère les translations d'adresses E.164 vers des adresses IP.

Respecter la contrainte temporelle est une première priorité pour le transport de la parole téléphonique. Une seconde priorité concerne la mise en place d'une signalisation pour mettre en connexion les deux utilisateurs qui veulent se parler.

Les protocoles de signalisation utilisés pour le transport et la gestion de la parole sous forme de paquets IP regroupent essentiellement H.323 et SIP (Session Initiation Protocol). La signalisation H.323 a été définie dans un environnement de télécommunications, à la différence de SIP, qui provient de l'informatique et plus spécifiquement du Web. SIP peut utiliser le code HTTP ainsi que la sécurité qui y est liée. Il peut en outre s'accommoder des pare-feu de protection. SIP met en place des sessions, qui ne sont que des appels téléphoniques entre un client et un serveur. Comme nous l'avons vu, six primitives HTTP sont utilisées pour cela : INVITE, BYE, OPTIONS, ACK, REGISTER et CANCEL.

La VoIP est devenue une application classique grâce aux possibilités de numérisation et à la puissance des PC, qui permettent d'annuler les échos. L'élément le plus contraignant reste le délai, surtout lorsqu'il faut traverser des terminaux de type PC, des modems, des réseaux d'accès, des passerelles, des routeurs, etc.

On peut considérer que le PC demande un temps de traversée d'une centaine de millisecondes, le modem de quelques dizaines de millisecondes, la passerelle également d'une centaine de millisecondes et le réseau IP de quelques dizaines de millisecondes. Le total montre que la limite des 300 ms pour avoir une interactivité est rapidement atteinte. Si l'on dépasse les 150 ms de transit et que l'on s'approche des 300 ms, la qualité de la communication s'en ressent, comme lors d'une conversation par satellite.

Détaillons la mise en place de la communication. Il faut utiliser une signalisation pour mettre en place la session. Premier élément, la localisation du récepteur (User Location) s'effectue par une mise en correspondance de l'adresse du destinataire (adresse IP ou téléphonique classique) en une adresse IP. Le protocole DHCP et les passerelles spécialisées sont des éléments de solution pour déterminer les adresses des récepteurs. L'établissement de la communication passe par une acceptation du terminal destinataire, que ce soit un téléphone, une boîte vocale ou un serveur Web. Comme nous l'avons vu, plusieurs protocoles de signalisation peuvent être utilisés, comme SIP, de l'IETF, ou H.323, de l'UIT-T.

Les protocoles de signalisation

Nous avons déjà examiné en détail le protocole SIP au chapitre 23. Rappelons quelques éléments de ce protocole avant d'aborder SDP et surtout RTP-RTCP.

Comme son nom l'indique, SIP (Session Initiation Protocol) est utilisé pour initialiser la session. Une requête SIP contient un ensemble d'en-têtes qui décrivent l'appel, suivis du corps du message, contenant la description de la demande de session. SIP est un protocole client-serveur, qui utilise la syntaxe et la sémantique de HTTP. Le serveur gère la demande et fournit une réponse au client.

Trois types de serveurs gèrent différents éléments : un serveur d'enregistrement (Registration Server), un serveur relais (Proxy Server) et un serveur de redirection (Redirect Server). Ces serveurs travaillent à trouver la route. Le serveur proxy détermine le prochain serveur (Next-Hop Server), qui, lui-même, trouve le suivant, et ainsi de suite. Des

champs supplémentaires de l'en-tête précisent les options, comme le transfert d'appel ou la gestion de conférence téléphonique.

Le protocole SDP (Session Description Protocol) est utilisé pour décrire les sessions multimédias pour la partie téléphonique mais aussi pour d'autres applications distribuées, comme la radio sur Internet.

SDP permet le transfert de nombreuses informations, notamment les suivantes :

- flots correspondant aux médias de l'application ;
- pour chaque flot, adresse de destination, unicast ou multicast ;
- pour chaque flot, numéro de port UDP ;
- type de charge transportée ;
- instants de synchronisation (par exemple, l'instant de début d'un programme de télévision diffusée) ;
- origine de la demande de communication.

Le protocole RTP (Real-time Transport Protocol) prend le relais pour le transport de l'information proprement dite. Son rôle est d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie pour reformer le flot avec ses caractéristiques (synchronisme, perte, etc.). C'est un protocole qui travaille au niveau transport et essaye de corriger les défauts apportés par le réseau.

Les fonctions de RTP sont les suivantes :

- Le séquencement des paquets par une numérotation permettant de détecter les paquets perdus, ce qui est essentiel pour la recomposition de la parole. La perte d'un paquet n'est pas en soi un problème, s'il n'y en a pas trop de perdus. En revanche, repérer qu'un paquet a été perdu est impératif car il faut en tenir compte et éventuellement le remplacer par une synthèse déterminée en fonction des paquets précédant et suivant.
- L'identification de ce qui est transporté dans le message pour permettre, par exemple, une compensation en cas de perte.
- La synchronisation entre médias, grâce à des estampilles.
- L'indication de tramage. Les applications audio et vidéo sont transportées dans des trames dont la dimension dépend des codecs effectuant la numérisation. Ces trames sont incluses dans les paquets pour être transportées et doivent être récupérées facilement au moment de la dépaquétisation afin que l'application soit décodée simplement.
- L'identification de la source. Dans les applications en multicast, l'identité de la source doit être déterminée.

RTP utilise le protocole RTCP (Real-Time Control Protocol) pour transporter les informations supplémentaires suivantes pour la gestion de la session :

- Retour de la qualité de service lors de la demande de session. Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs des rapports sur la QoS. Ces rapports comprennent le nombre de paquets perdus, la gigue et le délai aller-retour. Ces informations permettent à la source de s'adapter, c'est-à-dire, par exemple, de modifier le degré de compression pour maintenir la QoS.

- Synchronisation supplémentaire entre médias. Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix et l'image, ou même une application numérisée sur plusieurs niveaux hiérarchiques, peuvent voir les flots générés suivre des chemins distincts.
- Identification. Les paquets RTCP contiennent des informations d'adresse, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Contrôle de la session. RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement une indication de leur comportement.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement ces informations. La périodicité est calculée en fonction du nombre de participants à l'application.

Un autre protocole utilisable est RTSP (Real-Time Streaming Protocol), dont le rôle est de contrôler une communication entre deux serveurs où sont stockées des informations multimédias audio et vidéo. RTSP offre des commandes assez semblables à celles d'un magnétoscope, telles qu'avance, avance rapide, retour, pause, etc. Ce protocole peut être très utile dans le cadre de la téléphonie sur IP en permettant l'enregistrement d'une téléconférence pour la réentendre ultérieurement, la vision d'une séquence vidéo, l'enregistrement de message téléphonique, etc.

Un autre point important pour réaliser la communication de l'émetteur vers le récepteur concerne les fonctionnalités de la passerelle permettant de passer d'un réseau à transfert de paquets à un réseau à commutation de circuits, avec les problèmes d'adressage, de signalisation et de transcodage que cela pose. Ces passerelles se démultiplient entre FAI et opérateurs télécoms.

Pour finaliser l'ouverture d'un appel, le protocole SIP envoie une requête à la passerelle. Le premier problème est de déterminer quelle passerelle est capable de réaliser la liaison circuit pour atteindre le destinataire. En théorie, chaque passerelle peut appeler n'importe quel numéro de téléphone. Cependant, pour réduire les coûts, il vaut mieux choisir une passerelle locale.

Les réseaux de téléphonie IP d'entreprise

Les réseaux de téléphonie d'entreprise utilisant le protocole IP sont disponibles sur le marché depuis le début des années 2000. L'objectif de ces réseaux est d'intégrer le réseau de données et le réseau téléphonique en un seul et même réseau. La norme IP est bien sûr à la base de cette intégration.

La parole téléphonique est numérisée, et les octets sont mis dans des paquets IP les plus courts possibles afin qu'il n'y ait pas trop de perte de bande passante. La compression de la parole avec G.729, par exemple, qui est très utilisé, donne naissance à des trames de 16 octets toutes les 16 ms. Si l'on veut de la qualité, il faut s'arrêter à cette valeur de 16 octets par paquet IP. Les paquets IP sont transportés avec la contrainte de 150 ms de délai jusqu'au poste du destinataire.

Dans l'entreprise, on utilise des trames Ethernet pour effectuer le transport. On place donc le paquet IP dans une trame Ethernet, qui possède une longueur de 64 octets. Au débit de 8 Kbit/s du codec G.729 correspond un débit de 32 Kbit/s sur le réseau Ethernet. Si l'on utilise un réseau Gigabit Ethernet, la trame minimale est de 512 octets, et le débit d'une seule parole téléphonique devient de 256 Kbit/s.

Pour la contrainte temporelle à respecter, il ne faut perdre aucun temps. Le premier point où des pertes de temps sont possibles provient potentiellement du traitement du son, effectué par une carte son dans un PC si le PC est utilisé comme téléphone. Ces cartes son ont généralement un temps de réaction très lent, de l'ordre d'une quarantaine de millisecondes, ce qui est inacceptable. Il faut donc utiliser des téléphones spécifiques, que l'on appelle téléphones IP. Un téléphone IP est un routeur qui encapsule directement les octets dans un paquet IP. Ce routeur possède des sorties Ethernet de façon que le téléphone puisse se connecter directement sur le réseau de l'entreprise. La figure S.2 illustre un téléphone IP.

Figure S.2
Téléphone IP

Toujours pour perdre le moins de temps possible dans le transport, le réseau ne doit posséder aucun réseau Ethernet partagé, le partage engendrant une perte de temps importante. Il faut donc utiliser uniquement des réseaux Ethernet commutés, si possible au débit de 100 Mbit/s, pour être sûr que le débit des paroles superposées ne pose pas de problème. Enfin, il faut que les paquets IP ou les trames portant les paquets IP de parole soient prioritaires partout dans le réseau d'entreprise. Pour cela, il faut se servir, par exemple, des priorités de type DiffServ au niveau paquet et des priorités de niveau trame dans Ethernet. Les priorités de niveau 2 correspondent à la norme IEEE 802.1p, qui définit un champ de 3 bits pour gérer jusqu'à huit classes de priorités.

Mise en œuvre de la téléphonie sur IP

Après avoir évoqué les caractéristiques principales des protocoles supportant la téléphonie sur IP, nous décrivons dans cette section le processus à suivre pour installer une téléphonie sur IP, ou ToIP (Telephony over IP), dans une entreprise possédant plusieurs sites. Les éléments à prendre en compte doivent suivre une architecture à quatre niveaux, comme illustré à la figure S.3.

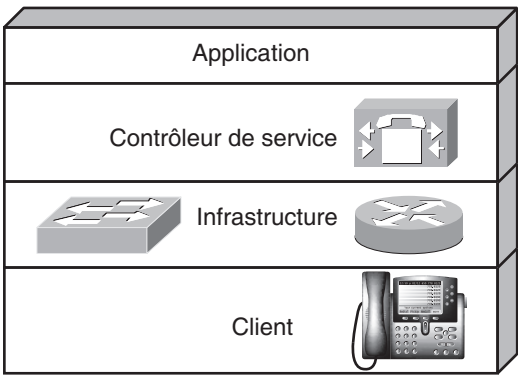


Figure S.3
Architecture d'un réseau de téléphonie sur IP

Un réseau d'entreprise assez standard est décrit à la figure S.4. Il contient deux sites, l'un principal et l'autre secondaire. Le réseau est composé d'un réseau local dans chaque site. Les deux réseaux locaux sont reliés par un réseau WAN, qui peut-être, par exemple, un réseau privé virtuel. Ce réseau est composé de commutateurs Ethernet formant un réseau local Ethernet commuté. Sur ce réseau local, on trouve aussi bien des téléphones IP que des stations de travail. Les stations de travail peuvent être connectées aux téléphones IP ou directement au commutateur Ethernet. Les deux réseaux locaux Ethernet commutés sont connectés à des routeurs d'entrée-sortie de l'entreprise, et les deux routeurs sont reliés entre eux par un réseau étendu, par exemple un réseau privé virtuel d'opérateur.

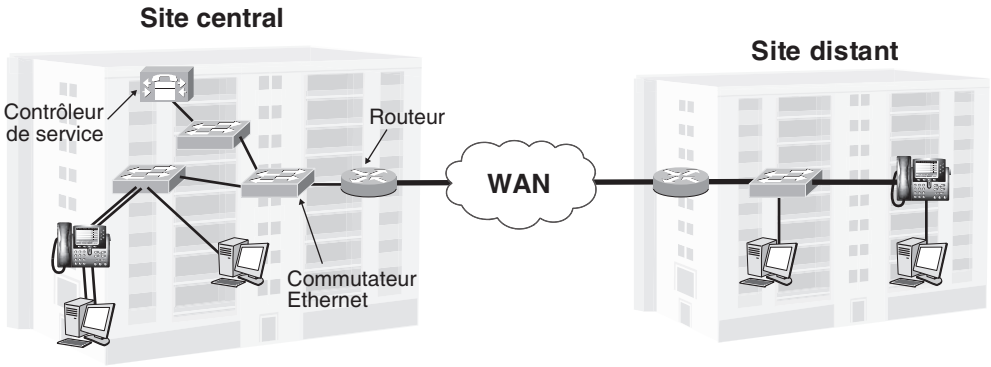


Figure S.4
Réseau intégrant la téléphonie sur IP

En remontant l'architecture par le bas, nous trouvons tout d'abord les téléphones IP. Ce sont des routeurs de niveau paquet capables d'encapsuler des octets de téléphonie. Les postes de travail peuvent également être utilisés comme téléphones, mais il faut faire attention à ce que la carte son soit de bonne qualité pour ne pas trop retarder la mise en paquet des octets téléphoniques. Ces postes de travail un peu spécifiques sont connectés par Ethernet, généralement à 100 Mbit/s, avec la priorité disponible la plus haute.

La zone DSCP du paquet IP est positionnée sur la classe de service EF (Expedited Forwarding), et le paquet est encapsulé dans une trame Ethernet de priorité la plus haute, cette priorité étant indiquée par la zone IEEE 802.1p. Les autres machines, qui ne produisent pas de la parole, ou plus précisément les autres applications positionnent le DSCP à une valeur AF ou BE moins forte que celle utilisée pour la téléphonie sur IP. L'entreprise doit donc se munir de routeurs DiffServ capables de traiter la priorité au niveau IP et de commutateurs Ethernet capables de gérer les classes de priorités IEEE 802.1p.

Si la valeur du DSCP est normalisée, celle du champ IEEE 802.1p l'est beaucoup moins. Tout d'abord, ce champ ne contient que 3 bits de priorité, ce qui donne naissance à 8 classes de priorités, alors que DiffServ en comporte 14. Ensuite, il faut vérifier que les équipementiers suivent les mêmes règles pour déterminer la valeur du champ IEEE 802.1p. Toujours au niveau du transport, il faut faire une évaluation du temps maximal de transit dans chaque site afin d'en déduire le temps maximal de traversée du réseau WAN. Une fois cette valeur connue, il est possible de déduire le temps maximal de transit dans le réseau. L'entreprise doit alors négocier un SLA avec son opérateur et lui demander que cette contrainte soit satisfaite dans la partie technique, c'est-à-dire le SLS. La valeur maximale du temps de transit se situe généralement autour de 50 ms.

En passant à la couche supérieure, il faut introduire un contrôleur de service capable de déclencher les processus de recherche du correspondant et d'initialiser la signalisation permettant l'ouverture de la session. Le contrôleur de service peut être centralisé sur un seul site, même si les deux sites sont assez distants. Ce contrôleur de service peut gérer un grand nombre de services, tels que la téléphonie, les passerelles, les ports TAPI (Telephony API) et JTAPI (Java TAPI), la messagerie, les conférences, etc. Ce contrôleur de communication peut éventuellement prendre en charge des terminaux analogiques de générations précédentes ou des lignes de sortie plus classiques allant vers un opérateur de téléphonie fixe.

Les applications de téléphonie sur IP grand public

Une première application de téléphonie sur IP grand public est proposée par les opérateurs de téléphonie pour offrir des communications internationales à tarif local. Elle consiste à rassembler un grand nombre de voies téléphoniques classiques et à les encapsuler dans un même paquet IP, qui peut devenir assez long. L'utilisateur se connecte en local sur un point de présence d'un opérateur IP, lequel multiplexe toutes les voies téléphoniques sur une même liaison IP, transatlantique par exemple. À la sortie de la liaison IP transatlantique, la parole recouvre sa composition normale et est envoyée de façon classique au destinataire.

Des applications grand public telles que Skype ou MNS (Microsoft Network Service) proposent de la téléphonie sur IP de bout en bout. Pour cela, il faut généralement passer par un modem ADSL aux deux extrémités de la communication afin que le débit soit accepté sur la boucle locale. Skype fait appel à une technique P2P pour rester le plus simple possible et ne pas avoir de contrôle centralisé. La signalisation de MNS est quant à elle gérée par une base de données centralisée mais qui peut être distribuée sur plusieurs sites.

Skype

Avec plus de 100 millions d'utilisateurs dans le monde, Skype, leader mondial de la téléphonie sur Internet et pionnier des offres de téléphonie grand public sur Internet, bouleverse l'industrie des télécommunications en modifiant en profondeur les habitudes des consommateurs.

Chaque jour, 150 000 nouveaux utilisateurs téléchargent cette solution de téléphonie sur Internet qui utilise la technologie peer-to-peer (P2P) qui propose deux services différents : une offre gratuite entre utilisateurs équipés du logiciel pour une exploitation purement Internet et une offre payante, qui permet de joindre et d'être joint *via* Internet tandis que les correspondants utilisent la téléphonie traditionnelle RTC.

Skype est l'un des premiers logiciels grand public à avoir permis la jonction entre la téléphonie du monde Internet et celle du monde RTC. C'est sans doute là la clé de son succès. Grâce à une qualité d'écoute excellente, une facilité d'utilisation ne nécessitant généralement aucune configuration (y compris dans les infrastructures réseau déployant des pare-feu), une mobilité accrue, une gamme de services complémentaires et un prix incomparablement moins cher que la téléphonie traditionnelle, Skype s'est répandu de manière virale.

Skype a été lancé le 29 août 2003 à l'initiative de Niklas Zennström, un Suédois de 36 ans, et Janus Friis, une Danois de 26 ans, tous deux experts en technologies de peer-to-peer puisqu'ils avaient fait frémir l'industrie des loisirs au début des années 2000, avec le logiciel KaZaA qu'ils avaient conçu.

Microsoft et Google d'abord, puis Yahoo! et News Corporation (la société de Rupert Murdoch), s'intéressent à Skype, mais, en 2005, ses deux fondateurs créent la surprise en vendant la société à eBay, un acteur pour le moins inattendu dans le domaine des télécoms.

Architecture de Skype

Comme expliqué précédemment, Skype fonctionne selon un mode décentralisé et une architecture peer-to-peer (P2P), c'est-à-dire de poste à poste, ou point à point, ou encore de pair en pair ou d'égal à égal, dans lequel chaque poste intermédiaire est susceptible de jouer le rôle de relais et de participer de manière dynamique au processus d'acheminement des paquets.

Le client logiciel n'est pas seulement utilisé par le possesseur du logiciel. Il est mis à contribution pour les besoins d'autres utilisateurs et sert de support de transmission aux flux de ces derniers. Chaque élément du réseau (on parle de nœuds) constitue à la fois un client, qui peut demander un service, et un serveur, qui peut agir pour le compte d'un

autre client. Ce modèle distribue ainsi totalement ses traitements, à l'opposé du traditionnel modèle client-serveur, dans lequel chaque entité joue exclusivement le rôle de serveur ou de client, ce qui nécessite de centraliser les flux vers des centres de contrôles.

Le terme peer-to-peer est parfois utilisé pour désigner toute communication directe entre un poste et un autre, indépendamment du mode de routage des données utilisé. C'est là un abus de langage, puisque le routage caractérise la technologie P2P et définit un moyen de transporter des informations faisant intervenir des terminaux intermédiaires de proche en proche jusqu'au véritable destinataire.

Limiter les ressources

Le modèle décentralisé peer-to-peer proposé par Skype fait reposer l'intelligence de son réseau sur les utilisateurs eux-mêmes, et non sur des serveurs centraux. Dès lors, le passage à l'échelle est permis à moindres frais, puisque chaque nouvel utilisateur est potentiellement une source de traitement pour l'ensemble du réseau. Skype a ainsi pu s'étendre sur toute la planète sans avoir à s'intéresser directement aux ressources de traitement de la montée en charge. C'est l'un des secrets de sa réussite.

Traverser les pare-feu

Une condition essentielle de la réussite de ToIP est la possibilité de traverser les pare-feu. Les communications de ce type exploitent des ports dynamiques qui ne sont généralement pas ouverts par ces pare-feu. Par ailleurs, le réseau sur lequel se trouve l'utilisateur peut mettre en œuvre un mécanisme de NAT (Network Address Translation), ou translation d'adresse réseau, qui donne à l'utilisateur une adresse IP non routable sur Internet. Pour ces deux raisons, la communication directe entre correspondants est impossible.

Skype a trouvé la parade en exploitant différentes techniques. L'une d'elle consiste en l'utilisation de ports standards, qui sont étrangers à la téléphonie sur IP, mais qui présentent l'avantage d'être le plus souvent ouverts par les pare-feu. C'est le cas du port 80, associé généralement au Web pour le protocole HTTP.

Skype permet en outre d'utiliser des ressources situées à l'extérieur de la zone protégée par le pare-feu. Cette ressource peut être un utilisateur parmi d'autres, choisi pour accomplir cette tâche selon un algorithme propriétaire. Les flux IP de Skype suivent ainsi un chemin détourné lorsque le chemin direct est impossible. Ce sont de tels chemins qu'empruntent les communications entre utilisateurs de Skype, lesquels se prêtent à la fonctionnalité de routage sans en avoir conscience et pour les besoins d'autres clients.

Ce type de connexion s'effectue aux dépens des utilisateurs intermédiaires, mais à un débit faible, de 0,5 kg-octet par seconde, qui ne perturbe que très peu ces derniers. Ceux-ci sont en outre sélectionnés en fonction de la bande passante dont ils disposent afin d'assumer la charge supplémentaire induite par ces communications. L'idée du transfert relayé est d'avoir une communication, fût-elle de qualité médiocre, plutôt que pas de communication du tout.

Si l'architecture de Skype est globalement décentralisée, il existe cependant des serveurs centralisés, qui assurent un ensemble de fonctionnalités annexes indispensables à la

communication. Par exemple, pour savoir si un utilisateur est connecté ou non, le logiciel se connecte à l'un de ces serveurs, qui informe de la disponibilité de tous les contacts.

Skype et la sécurité

Si aucune attaque ou vulnérabilité critique concernant le logiciel n'a encore été recensée, de nombreux spécialistes déplorent la facilité avec laquelle le logiciel parvient à traverser et se jouer des pare-feu censés bloquer les flux non autorisés. De ce fait, ces experts recommandent d'interdire l'utilisation du logiciel dans un cadre professionnel.

De leur côté, les autorités s'inquiètent du manque de transparence du logiciel, qui se comporte comme une boîte noire. Il n'est donc pas possible de savoir s'il contient une porte dérobée, accessible à partir d'Internet, pas plus qu'il n'est possible de savoir si des données sensibles sur les utilisateurs ne sont pas envoyées à leur insu.

Quant au fondement même du logiciel, le peer-to-peer, puisque les communications peuvent être acheminées *via* des ordinateurs intermédiaires, elles peuvent faire l'objet d'écoutes clandestines par ces mêmes intermédiaires.

De même, les pièces jointes transmises par l'outil de transfert de fichiers de Skype ne sont pas soumises à des contrôles d'antivirus. Même si l'on peut supposer que les interlocuteurs sont dignes de confiance, il n'est va pas forcément de même des fichiers qu'ils transfèrent qui peuvent avoir été corrompus.

Selon un raisonnement paranoïaque, on pourrait imaginer que toutes les communications soient relayées vers des serveurs centraux qui les enregistreraient, agissant comme un système automatisé de profiling des utilisateurs. Techniquement, ce serait parfaitement réalisable. Dans le doute, et dans la mesure où Skype refuse d'ouvrir les spécifications de son protocole, on comprend la méfiance de certains.

Chez Skype, on garantit que le logiciel est parfaitement sécurisé et ne présente aucun risque pour l'internaute. Le cryptage se fait de bout en bout, au moyen de l'algorithme de chiffrement symétrique AES (Advanced Encryption Standard), le standard utilisé par les organisations gouvernementales aux États-Unis. AES utilise un cryptage sur 256 bits. La négociation des clés symétriques AES s'effectue par un RSA de 1 536 à 2 048 bits.

Si les spécifications générales du protocole ne sont pas rendues publiques, explique-t-on chez Skype, c'est uniquement pour offrir au logiciel une protection supplémentaire et éviter de donner aux pirates l'occasion d'y chercher des failles.

En entreprise, même si des administrateurs souhaitent bloquer l'utilisation de Skype chez les utilisateurs de leur réseau, dans la pratique il est très difficile de mettre en place une politique de sécurité qui prenne en compte les spécificités du logiciel. Le cryptage rendant impossible le filtrage, il n'est même pas possible de protéger le logiciel d'attaques malicieuses ou de le rendre compatible avec un système de détection d'intrusion IDS (Intrusion Detection System) puisque les échanges ne sont pas analysables.

Plusieurs sociétés proposent des logiciels qui détectent et bloquent les flux de Skype. Appelés SkypeKiller, ces logiciels poussent la reconnaissance de l'analyse protocolaire jusqu'au niveau applicatif, et pas uniquement en se fondant sur les protocoles de transport ou les ports, afin d'empêcher les flux Skype de traverser le réseau.

IPTV

Cette section est dévolue à la télévision sur Internet, ou IPTV. Le décollage de cette application à tarder principalement par manque de débit des infrastructures. Avec le déploiement de la fibre optique et des composants haute capacité associés, la télévision et plus généralement la vidéo, l'IPTV devient une application standard. Nous allons regarder dans un premier temps les caractéristiques de cette application.

Trois grandes catégories d'IPTV ont été définies :

- la télévision classique ;
- la télévision en temps différé ;
- la vidéo à la demande ou VoD (Video on Demand).

Contrairement à la télévision des diffuseurs, qui utilisent les voies hertziennes ou le CATV (Community Antenna TeleVision), l'IPTV arrive par la boucle locale que ce soit terrestre ou hertzienne. L'ADSL ou le modem câble pour la partie terrestre et la 3G/4G pour la partie hertzienne.

Deux architectures sont acceptables : centralisée ou distribuée. Dans le cas centralisé, le serveur de distribution des programmes est comme le nom l'indique centralisé. Cette solution est assez simple à mettre en œuvre mais elle ne passe pas l'échelle. Le cas distribué demande un service de distribution des contenus adapté aux grands réseaux.

La distribution chez l'utilisateur s'effectue via la Home Gateway. Cependant, la partie traitement est repoussée vers l'utilisateur dans la set-top-box. Dans l'ordre à partir de l'accès opérateur il y a la Home Gateway, la set-top-box et le téléviseur. La direction, poussée en particulier par DLNA (cf. chapitre 19 et annexe N), est d'intégrer la set-top-box dans le téléviseur avec la terminaison de réseau. Les paquets IP transportant le canal de télévision vont jusqu'au terminal.

Le codage des flots TV s'effectue en MPEG-2 et surtout MPEG-4. Les protocoles utilisés sont :

- IGMP version 2 ou IGMP version 3, pour prendre en charge un flot multimédia en multicast, c'est-à-dire une diffusion du canal de télévision vers l'ensemble des utilisateurs voulant regarder la même chaîne.
- RTSP (Real Time Streaming Protocol) pour la vidéo à la demande.
- NPVR (Network-based Personal Video Recorder).

Une des particularités, comme dans la téléphonie, concerne le temps réel de l'application de télévision en direct et de streaming en général. L'application de streaming est plus ou moins facile en fonction des qualités de service du réseau.

La téléphonie sur ATM et le relais de trames

La technique de transfert ATM a été conçue pour transporter de la parole téléphonique de type G.711 à 64 Kbit/s. La raison de la petite taille de la cellule se trouve dans cette

fonctionnalité. Les 48 octets de données de la trame sont remplis en 48 fois 125 µs, c'est-à-dire 6 ms, ce qui reste acceptable, même lorsqu'il y a des échos et que le temps de transit doit rester inférieur à 28 ms. Si la parole téléphonique est compressée par un codeur G.729 à 8 Kbit/s, il faut un temps de 48 ms de remplissage des 48 octets de données puisque le signal donne naissance à 1 octet toutes les 1 ms. Cette section examine la technique AAL-2 introduite dans la commutation ATM pour réaliser le transport de la voix téléphonique et plus particulièrement la téléphonie UMTS. Avant d'aborder l'AAL-2, introduisons les techniques préalables, qui sont encore utilisées dans les réseaux ATM.

L'émulation de circuit CES (Circuit Emulation Service) a été la première solution pour transporter de la téléphonie en paquet. Cette émulation de circuit utilise l'AAL-1 de l'environnement ATM, et plus précisément le service CBR (Constant Bit Rate), présenté à l'annexe G. Les PABX interconnectés par cette solution utilisent des interfaces E1 normalisées (G.703 et G.704). Le service ATM est de type circuit virtuel permanent. La signalisation sur l'interface est portée dans l'IT16 de l'interface E1.

Une autre solution, VTOA (Voice and Telephony Over ATM), ne privilégie pas de protocole AAL spécifique mais demande le support du service VBR-rt (Variable Bit Rate-real-time). Le PABX est relié au nœud d'accès du réseau de l'opérateur par un canal de type E1 structuré. La signalisation utilise encore l'IT16 de l'interface ou un circuit virtuel permanent dédié. Des normes classiques, comme le CCITT n° 7 ou Q-SIG (Q-Interface Signaling Protocol), une signalisation développée par l'UIT-T, sont utilisées. La parole elle-même est transportée par des liaisons permanentes ou commutées.

AAL-2

L'AAL-2 (ATM Adaptation Layer de type 2) correspond à la troisième couche du modèle ATM. C'est la couche qui s'occupe de la fragmentation et du réassemblage des messages pour obtenir des blocs à la dimension des cellules ATM. Comme nous allons le voir, l'AAL-2 détermine des fragments qui peuvent être tout petits de façon à ne pas perdre de temps à attendre des octets téléphoniques et à envoyer les fragments aussi vite que possible.

Les solutions précédentes concernent essentiellement la parole numérique sous forme de flux à 64 Kbit/s. En réalité, la parole est de plus en plus souvent compressée, comme nous l'avons vu au début de cette annexe. Lorsque la compression est forte, comme lors de l'utilisation du codeur G.723.1, qui diminue le débit du flot à 6,3 Kbit/s, le temps de remplissage d'un paquet ATM devient très long, même pour une petite cellule.

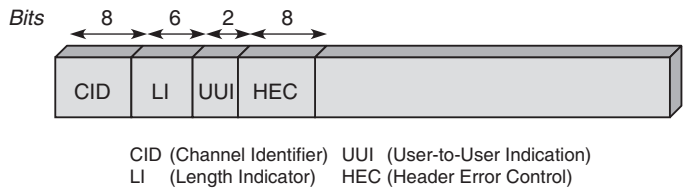
Un calcul simple montre que, pour remplir une cellule de 48 octets à la vitesse de 6,3 Kbit/s, il faut plus de 60 ms. Ce temps est inacceptable si la communication génère des échos ou si d'autres temps d'attente incompressibles s'ajoutent. C'est notamment le cas de la parole numérique dans les réseaux de mobiles, où, au temps de remplissage de la cellule, s'ajoute un temps d'accès important sur l'interface air. Une solution possible, mais guère enthousiasmante, à ce problème est de ne remplir que partiellement les cellules. En supposant,

par exemple, une compression de 50 %, amenant le débit à 32 Kbit/s, si l'on veut garder les mêmes contraintes que pour des flux à 64 Kbit/s, il ne faut remplir les cellules qu'à moitié. Cette solution induit un flux à 64 Kbit/s de cellules à moitié remplies.

Le rôle de l'AAL-2 est de remplir une cellule d'octets provenant de plusieurs connexions de parole, mais avec des débits variables pour les différentes voies basse vitesse. La solution du multiplexage de voies de débit constant est simple, puisqu'il suffit de connaître le numéro de l'octet pour récupérer le numéro de la connexion. Lorsque les flux sont variables, il faut ajouter une information pour savoir à quelle voie de parole appartient le segment.

Dans l'AAL-2, ce multiplexage de plusieurs voies de parole est effectué par des minitrames, appelées paquets CSP (Common Part Sublayer). La minitrame AAL-2 est illustrée à la figure S.5.

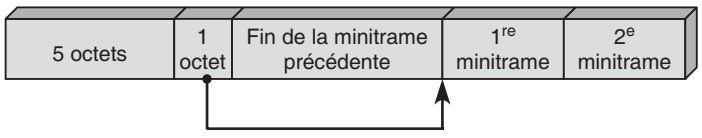
Figure S.5
Minitrame de l'AAL2



L'en-tête de la minitrame tient sur 3 octets. La zone CID (Channel IDentifier) est un identificateur de la voie de parole. Sa longueur de 1 octet permet de multiplexer jusqu'à 248 voies de parole (les valeurs 0 à 7 sont réservées). Le champ LI (Length Indicator) indique la longueur de la minitrame. Le champ UUI (User-to-User Indication) permet de transmettre de l'information d'une extrémité à l'autre de la connexion. Le champ HEC (Header Error Control) permet la détection et la correction des erreurs sur les deux octets précédents de l'en-tête. La longueur maximale d'une minitrame est de 64 octets, si bien que le transport d'une minitrame requiert parfois plus d'une seule cellule. Exactement 44 octets de longueur maximale sont nécessaires à son encapsulation dans une cellule ATM.

Les minitrames sont donc encapsulées dans les cellules ATM, et des bits de bourrage complètent la cellule pour arriver à une longueur de 47 octets, un octet étant réservé, comme dans l'AAL-1, pour transmettre des informations de contrôle. La cellule AAL-2 est illustrée à la figure S.6.

Figure S.6
Cellule AAL-2



L'octet de contrôle permet de pointer sur le début de la première minitrame encapsulée. En effet, il se peut que le début d'une minitranche ait été transporté dans une cellule précédente. Pour trouver cette valeur, il faut connaître la longueur de la dernière minitrame et compter les octets déjà envoyés dans la fin de la cellule précédente. Le pointeur est utile lorsqu'une cellule est perdue et qu'il faut retrouver le début d'une minitrame. Le pointeur requerrant 6 bits, il reste 2 bits, qui permettent d'effectuer une numérotation modulo 2 et une vérification de parité.

En conclusion, malgré la surcharge engendrée par l'en-tête des minitrames, l'AAL-2 est beaucoup plus efficace que l'utilisation d'une connexion unique pour une voie de parole.

Le relais de trames

Le problème du transport de la parole dans le relais de trames est similaire à celui que l'on trouve dans les réseaux ATM. Sur une liaison virtuelle, où les paquets peuvent atteindre plus de 4 000 octets, il est indispensable de multiplexer sur une même liaison plusieurs voies de parole. La proposition FRF.11 du Frame Relay Forum décrit une solution de minitrame semblable à celle de l'AAL-2 pour transporter les voies de parole.

La possibilité d'avoir un commutateur occupé par la transmission d'une longue trame LAP-F crée toutefois une difficulté supplémentaire. Il faut donc un mécanisme de priorité pour laisser passer les petits paquets portant de la parole téléphonique.

Évolution des PABX

Les PABX sont les autocommutateurs téléphoniques qui gèrent les communications téléphoniques de type circuit. Leur évolution s'est accélérée au cours des quinze dernières années pour aboutir aujourd'hui à la quatrième génération. Ces différentes générations se sont enrichies d'une multitude de services et offrent désormais la possibilité de transmettre des données. Après un développement assez anarchique, la mise en place d'un réseau de communication entre PABX hétérogènes est devenue indispensable aux grandes entreprises. Cette communication entre PABX s'est concrétisée par la normalisation des échanges entre autocommutateurs.

L'environnement PABX s'est enrichi d'une extension lui permettant de prendre en charge des services évolués, comme le télémarketing ou la gestion des appels par menu grâce à l'association de processeurs informatiques. Nous présentons à la fin de cette annexe cette intégration de la téléphonie et de l'informatique, appelée CTI (Computer Telephony Integration).

Les autocommutateurs privés

Un autocommutateur assure une liaison temporaire entre deux lignes d'abonnés (communication locale) ou entre une ligne d'abonné et une jonction allant vers un autre autocommutateur. L'autocommutateur se subdivise en deux sous-ensembles principaux : le

réseau de connexion, à travers lequel s'effectue la connexion, et les organes de commande, qui effectuent les différents dialogues permettant l'établissement de la communication.

Fonctionnellement, on peut distinguer :

- les équipements individuels de ligne permettant le raccordement des postes téléphoniques ou des circuits ;
- le réseau de connexion ;
- l'unité de commande qui gère la traduction, la maintenance, les équipements de signalisation, etc. ;
- les organes de collecte et de distribution de la signalisation voie par voie ;
- les organes de collecte et de distribution de la signalisation par canal sémaphore.

Le numéro de l'appelé est la seule source d'information pour l'autocommutateur. Ce numéro doit être analysé, ou traduit, en fonction du plan de numérotation. En règle générale, un premier chiffre indique que l'appelé est sur le même PABX que l'appelant. Les chiffres suivants désignent la ligne correspondant à l'appelé. Si le premier chiffre ne correspond pas au chiffre de l'autocommutateur, cela signifie que l'appelé est situé sur un autre autocommutateur. Dans ce cas, les premiers chiffres représentent le numéro de l'autocommutateur de l'appelé, et les derniers la ligne correspondant à l'appelé.

Cette architecture peut devenir plus complexe si l'on ajoute de nouvelles fonctionnalités, telles que des interfaces avec les réseaux locaux, des applications de messagerie vocale, etc. Un exemple de PABX IP avec des fonctionnalités de connexion à de la téléphonie classique est détaillé à la figure S.7.

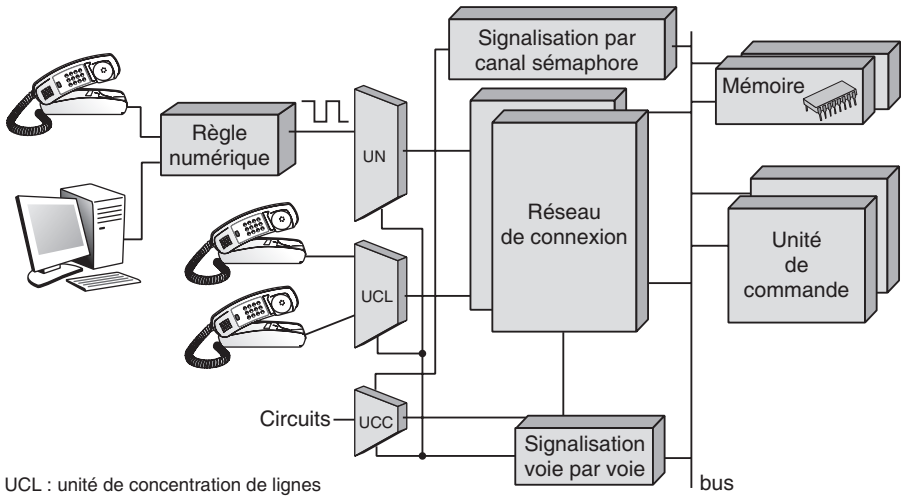


Figure S.7

Architecture générale d'un PABX

Un commutateur temporel permet d'émettre des voies entrantes dans un ordre quelconque sur les voies du multiplex de sortie. Il est constitué d'une mémoire tampon réceptionnant les IT (intervalles de temps) entrants et d'une mémoire de commande gérant la mémoire tampon. On distingue les commutateurs à commande aval et ceux à commande amont.

En mode de commande aval, les IT sont inscrits au fur et à mesure dans la mémoire tampon. La mémoire de commande contient à chaque instant l'adresse, en mémoire tampon, de l'échantillon à transmettre sur le multiplex de sortie. Si l'ITi entrant doit être connecté à l'ITj sortant, les octets de données entrant sur l'ITi doivent être envoyés sur l'ITj en sortie.

En mode de commande amont, les IT entrants sont inscrits dans la mémoire tampon, sous le contrôle de la mémoire de commande, dans l'ordre où ils sont lus avant d'être envoyés sur le multiplex de sortie. Ainsi, le mot i de la mémoire de commande contient l'adresse j où inscrire l'ITi entrant.

Les différentes générations de PABX

Issu de la technologie électromécanique, le type le plus ancien de commutateur privé a duré près de cent ans. La première génération de commutateurs électroniques est apparue dans les années 1960. La commutation est pilotée par un calculateur universel, et le réseau de connexion est de type spatial. Le raccordement au réseau public s'effectue *via* des groupements de lignes analogiques.

Dans un commutateur spatial, électronique ou électromécanique, l'établissement et la libération d'une communication se font respectivement par la mise en place et la rupture d'un certain nombre de points de connexion. Une fois un itinéraire établi, il sert de support exclusif à une seule communication.

La deuxième génération, datant du milieu des années 1970, offre la commutation de données, mais la voix et les données se trouvent sur des lignes séparées. L'interface avec les terminaux reste analogique. Si le calculateur intégré gérant la commutation offre certaines fonctionnalités nouvelles, telles que la numérotation abrégée ou l'interdiction d'appeler l'international, ces dernières restent largement sous-employées (IBM 3750 et TBX de Philips) en raison d'une ergonomie médiocre. Le réseau de connexion est temporel, et les abonnés sont reliés entre eux par l'intermédiaire d'une ligne multivoie. Un intervalle de temps est régulièrement affecté à chaque connexion, ce qui simplifie le réseau.

La troisième génération correspond à l'avènement des réseaux numériques à intégration de services, au début des années 1980. Elle est caractérisée par le multiplexage de la voix et des données sur la même porte du PABX, soit sur une même paire torsadée, soit sur deux. La transmission est généralement analogique. Le PABX étant entièrement numérique, des codecs équipent ses portes. La commutation est de type temporel, mais les voix et les données sont traitées différemment dans le PABX. Ces commutateurs offrent également des interfaces numériques à 64 Kbit/s, où peuvent se connecter divers terminaux et téléphones numériques. Le raccordement au réseau public devient lui aussi numérique grâce à des liaisons MIC (modulation par impulsion et codage) à 2 Mbit/s.

Ces liaisons autorisent la sélection directe à l'arrivée et permettent aux centraux publics d'envoyer au PABX des informations relatives au coût de la communication (taxation), qui peuvent donc être retransmises à l'utilisateur au cours de la communication.

Une troisième génération et demie, de conception modulaire, est apparue au début des années 1990. Elle associe un commutateur de circuits à 64 Kbit/s et un commutateur de paquets X.25 ou relais de trames, chacun ayant son propre processeur. Ainsi, les variations du trafic de données ne pénalisent pas la qualité des services téléphoniques.

La quatrième génération est intervenue avec les PABX-IP, au milieu des années 1990, pour gérer des flux de paquets IP. Il est possible de connecter à la fois des téléphones numériques, les octets étant paquétisés dans des paquets IP, et des téléphones IP, qui envoient directement des paquets IP.

Une cinquième génération est à l'étude avec un cœur complètement IP. Cette génération ressemble à maints égards aux routeurs IP avec des signalisations SIP ou H.323.

PABX et transmission de données

Le débat en cours depuis quelques années sur les rôles respectifs des PABX et des LAN (réseaux locaux) dans la communication d'entreprise est aujourd'hui clos, les deux réseaux étant considérés comme complémentaires. Le PABX est parfaitement adapté au transport de la voix (64 Kbit/s/ligne), mais il peut également transporter des données à faible débit (jusqu'à 256 Kbit/s par ligne en interne). Le réseau local est adapté au transfert de données haut débit (10 Mbit/s pour un réseau Ethernet) mais pas à celui de la voix, du fait de contraintes temporelles trop strictes, sauf exception. Le tableau S.1 récapitule les caractéristiques comparées des PABX et des réseaux locaux.

Tableau S.1 • Comparaison des PABX et des réseaux locaux

	PABX	Réseau local
Architecture	Étoile	Étoile/bus/anneau
Support	Paire téléphonique	Paire téléphonique, coaxial, fibre
Mode de transmission	Analogique, numérique	Bande de base, large bande
Méthode d'accès	Circuit, paquet	CSMA/CD, jeton (bus/anneau)
Débit maximal	64 et 144 Kbit/s	De 50 à 1 000 Mbit/s
Capacité	10 à 6 000 terminaux	10 à 10 000 terminaux
Connexion aux réseaux publics	Multifréquence, numérique	Problèmes d'interface
Normalisation	De fait	Ethernet, Token-Ring

Pour satisfaire les besoins des utilisateurs, les deux techniques de commutation, paquet et circuit, doivent pouvoir être offertes sur les PABX. La première optimise les circuits physiques en y multiplexant plusieurs communications tandis que la seconde permet des débits élevés.

Les communications en mode circuit se font soit par modem, soit par intégration dans un raccordement numérique. L'accès d'un système informatique au service de circuits s'effectue par le biais d'un adaptateur de terminal chargé d'adapter la vitesse du terminal à celle du circuit (64 Kbit/s) et de supporter la fonction d'établissement de la communication. Les normes V.110 ou ECMA 102 sont utilisées pour l'adaptation de la vitesse et X.21 pour l'interface d'accès.

De même, les communications en mode paquet se font soit par modem, soit par intégration dans un raccordement numérique. Les relations entre terminaisons de standards différents sont automatiquement établies. Le PABX peut aussi établir en mode circuit une relation entre un terminal et un équipement de passerelle, lequel, selon les modèles, est situé dans le PABX.

Aujourd'hui, on distingue deux types d'architecture de PABX. Le premier privilégie la commutation de circuits pour le raccordement de terminaux. Les accès en transmission de données sont traités comme des communications téléphoniques, le PABX ayant alors surtout un rôle de concentrateur de terminaux. L'optimisation du câblage est atteinte par l'utilisation des câbles téléphoniques pour le transfert des données.

Cette solution est plutôt destinée aux entreprises ayant peu de postes de travail informatiques par rapport aux téléphones ou qui emploient des applications à faible taux d'utilisation. Elle nécessite la mise en place d'un réseau local en cas de transmission de données importantes.

Certains commutateurs peuvent accéder à des réseaux locaux. C'est le cas des autocommutateurs munis d'une URM (unité de raccordement multiservice). Celle-ci peut recevoir des cartes d'interface pour permettre à un terminal asynchrone d'accéder à un réseau. De même, certains PABX sont dotés d'un interfaçage Ethernet. Chaque carte Ethernet peut supporter 24 connexions, et plusieurs cartes peuvent être installées en parallèle. Cet équipement permet le raccordement d'un système, *via* un câblage en paire torsadée, à un débit à 10 ou 100 Mbit/s.

Le second type d'architecture entraîne également la cohabitation PABX-LAN, les deux étant fournis cette fois par le même équipementier. Le LAN et le PABX sont alors reliés par une passerelle. Celle-ci permet à un utilisateur occasionnel, connecté au PABX, d'accéder à l'ensemble des ressources informatiques raccordées au LAN. De même, un utilisateur du LAN atteint les serveurs connectés au PABX et les réseaux publics raccordés à celui-ci. Ce type d'architecture profite pleinement de la complémentarité PABX-LAN et du plan de câblage unique.

La signalisation entre PABX

La signalisation entre les PABX peut se faire voie par voie ou par canal sémaphore. Jusqu'à présent, la première méthode est la plus utilisée. L'information utile et la signalisation empruntent les mêmes circuits physiques dans le réseau. Une bande de fréquences est réservée en mode spatial et 1 octet en mode temporel. Dans ce mode temporel, les paroles téléphoniques sont transportées dans des octets, et un octet particulier est réservé

à la signalisation, par exemple l'octet transporté dans l'intervalle de temps Numéro 16 d'une communication en mode MIC (modulation, impulsion et codage).

La seconde méthode est caractérisée par l'utilisation d'un réseau de signalisation séparé du réseau transportant le trafic utile. Les informations relatives à chaque appel sont échangées sous forme de messages transportés par un canal annexe de transmission de données, commun à tout un groupe de circuits. Il y a quelques années, cette signalisation était propre à chaque constructeur. On compte aujourd'hui une centaine de types de signalisation privée inter-PABX, dont aucune n'est normalisée. Les organismes de normalisation ont par la suite proposé le protocole D, du nom du canal de signalisation dans lequel il est mis en œuvre, pour permettre la communication entre PABX hétérogènes et une gestion du réseau (réacheminement et reconfiguration en cas de surcharge de trafic ou de défaillance d'un commutateur, etc.). Adapté par l'ECMA (European Computer Manufacturers Association), ce protocole a été normalisé par l'ETSI sous le nom de Q-SIG (141 et 143). Cette norme s'aligne sur le protocole Q.932 de l'UIT-T utilisé pour l'interconnexion des autocommutateurs privés et des centraux publics.

Les caractéristiques principales du protocole de signalisation, que ce soit Q-SIG ou Q.932, sont les suivantes :

- Gestion des communications de type circuit ou paquet.
- Capacité à transmettre des informations de nature différente (signalisation, téléaction, maintenance, etc.).
- Fiabilité, due à l'emploi de méthodes efficaces de détection et de correction d'erreur grâce à l'utilisation d'une signalisation de type transmission de données.
- Extension du vocabulaire de la signalisation : il suffit pour toute nouvelle application d'indiquer aux logiciels des calculateurs l'élaboration et l'interprétation des nouveaux messages.

Parallèlement aux travaux de l'ECMA, un groupe de constructeurs, mené par Alcatel et Siemens, a fondé le forum IPNS (ISDN PBX Networking Standard), dont l'objectif est la normalisation des compléments de services offerts par les protocoles propriétaires. L'utilisation d'un protocole normalisé tel que Q-SIG devrait permettre de rassembler au sein d'un même réseau des PABX de constructeurs différents. Rappelons que la procédure CCITT n° 7 est le protocole choisi pour la signalisation entre commutateurs du RNIS. Ce protocole de signalisation n'est pas accessible par l'utilisateur, l'interfonctionnement avec le protocole Q-SIG se faisant dans les commutateurs d'abonnés.

L'intégration téléphonie-informatique

L'intégration de la téléphonie et de l'informatique n'est pas une nouveauté. Prévue depuis longtemps, la nécessité de cette alliance a commencé à se faire sentir dans les produits à partir de 1995. Cette intégration, qui a pris le nom de CTI, est née d'un groupe de travail sur le CSTA (Computer Supported Telephony Applications), et c'est l'ECMA qui a pris les choses en main en créant le groupe de travail TG11.

Un premier rapport a décrit les objectifs du CSTA :

- téléphonie évoluée (messagerie vocale, accès divers au réseau, téléconférence téléphonique, etc.) ;
- télémarketing ;
- service de clientèle ;
- micro-ordinateur comme centre de communication ;
- service de contrôle et d'alarme ;
- accès aux données de l'entreprise.

Ces services s'obtiennent par l'adjonction d'un équipement supplémentaire, qui s'interconnecte au PABX par une liaison CTI. Les terminaux sont connectés à ce serveur de téléphonie, tandis que les combinés téléphoniques continuent, bien sûr, à être connectés au PABX.

Éditeurs de logiciels et constructeurs de produits CTI

Les principales entreprises qui commercialisent des interfaces de programmation ou des produits de CTI sont les suivantes :

- Microsoft et Intel, avec l'interface TAPI (Telephony API) ;
- Novell, avec l'interface TSAPI (Novell Telephony Server API) ;
- Dialogic's, avec Dialogic's CT-Connect ;
- IBM Callpath ;
- Sun XTL Teleservice ;
- Hewlett Packard ACT ;
- Tandem CAM.

Tous ces produits de CTI visent à permettre au client qui téléphone d'atteindre l'agent capable de lui répondre par une synthèse vocale, par fax ou par toute autre solution viable. Ils visent également à mettre en mémoire les réponses d'un utilisateur.

Regardons d'un peu plus près l'interface de programmation TAPI de Microsoft-Intel, qui fait partie de l'architecture WOSA (Windows Open Services Architecture) de Microsoft. Plus exactement, WOSA est une plate-forme qui intègre les différents logiciels destinés aux applications du système d'information d'une entreprise. Outre l'application TAPI, WOSA contient ODBC (Open DataBase Connectivity), MAPI (Messaging Application Programming Interface), LSAPI (Licensing Server Application Program Interface), ainsi que des services de communication, comme le RPC de Microsoft.

TAPI est une interface générique d'appel de services. Trois objets ont été définis :

- L'objet ligne, qui caractérise la configuration et les numéros d'appel.
- L'objet appel, qui représente la mise en liaison avec le correspondant.
- L'objet téléphone, qui définit la configuration statique et les caractéristiques des combinés.

L'évolution de la CTI consiste en son intégration dans un environnement Internet permettant une connectivité totale de tous les éléments nécessaires à la vie d'une entreprise. Il devient dès lors possible de mettre en place des stratégies extrêmement évoluées d'utilisation des communications téléphoniques arrivant dans l'entreprise. De plus, il est relativement simple d'évoluer vers le multimédia.

Une des avancées immédiates provient des boîtes aux lettres universelles, capables de gérer toutes sortes de messages, de paroles, de fax, d'e-mail, etc. Il est possible, par exemple, d'effectuer une synthèse de parole à partir d'un e-mail ou d'un fax, de traduire une parole en fax, etc.

En résumé, l'association de la téléphonie et de l'informatique est en train de s'imposer par le biais de logiciels grand public. Cette intégration commence à faire partie de la vie de tous les jours.

Index

Symboles

A

B

C

D

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z