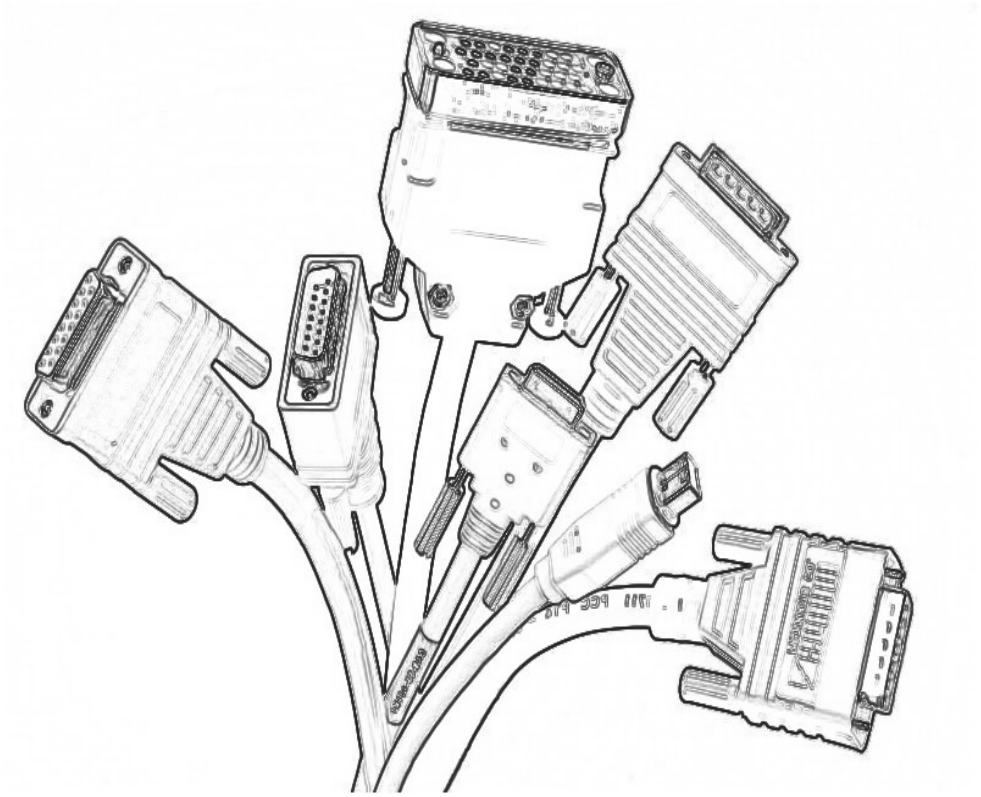
# LEXIQUE DE TERMES ET ACRONYMES RESEAUX & TELECOMMUNICATIONS



**Hervé FRENOT - Edition 04/2013**

http://lexique.reseaux.free.fr / lexique.reseaux@free.fr

**Pour toute remarque relative au présent document, merci d'adresser un message à l'adresse électronique ci-dessous :**

**lexique.reseaux@free.fr**

**Un site Internet permet de récupérer la dernière version mise en ligne du présent document.**

**http://lexique.reseaux.free.fr**



**Clins d'œil spéciaux : Comment ne pas citer deux personnages clefs ?**

**Jean STUMPF -** Responsable Exploitation Informatique de Monoprix - 1992. Jean m'a confié son réseau IBM en bon état pour que je le transforme en réseau IP/IPX/Decnet/SNA… Son soutien a été inconditionnel. J'ai découvert à son contact que le monde des réseaux étendus était une passion dévorante qui me rendrait malade de temps en temps et me procurerait de très belles satisfactions. Je me souviens de nos discussions, de son sourire vorace pour les bonnes choses de la vie.

**Franklin BOHBOT -** Directeur du développement de Infonie et Infosources. Franklin a tenu à relire le lexique pour le corriger à un moment de sa vie où la maladie le préoccupait plus que toute autre chose. Une belle leçon de vie à la lecture de ses commentaires, de nos échanges passionnants sur des concepts techniques.

# Introduction

L'objectif du "Lexique de Termes et Acronymes réseaux et Télécoms" était à l'origine de fournir une explication sur les termes ou les expressions utilisés dans le milieu des réseaux informatiques, de la télématique et des télécommunications. Au fil du temps et des versions, ce document s'est enrichi de compléments techniques plus ou moins complexes ainsi que de schémas d'explications permettant au lecteur de mieux appréhender le monde des "réseaux" dans son ensemble.

Le "réseau" est avant tout un immense vecteur de communication qui couvre des domaines techniques très vastes avec une terminologie particulière, souvent anglophone. D'où l'idée originale de ce document qui remonte à septembre 1992 pour les premières définitions.

A l'origine, un client m'avait demandé de lui expliquer en français et par écrit ce qu'étaient un "routeur", un "hub", et un "multiplexeur inverse". Il venait du monde IBM, avec un beau réseau SNA (fédérateur de son réseau en Token Ring). Je devais faire rentrer son réseau dans le monde IP, avec de l'Ethernet, des PC, des MACs, des AS400, des VAX, des RS6000, des stations SUN…

Il avait de quoi se poser des questions. ☺

Je lui ai fourni une documentation qui répondait à ses attentes et nous avons construit ensemble un réseau multi protocoles, multi supports & multi sites.

Evidemment, et vous l'aurez deviné, l'ensemble des informations contenues dans le présent document provient de sources aussi diverses que variées. Ces informations, pour la plupart collectées à l'occasion de projets ou au fil de mes lectures et recherches, ont été plus ou moins synthétisées avant d'être rassemblées et ordonnées dans le présent document.

**Remerciements :**

Il me faut ici citer tous les professionnels auprès desquels j'ai eu la chance d'apprendre, de collecter des informations techniques, marketing, linguistiques … Non pas que j'ai oublié les noms (enfin pas tous…), mais établir une liste sans en omettre un seul serait un exercice difficile et extrêmement risqué.

Sachez que seul je n'aurais pu accomplir cette synthèse. D'autres, beaucoup d'autres, m'ont aidé dans cette œuvre, par divers moyens et à divers moments.

**A tous, un grand merci !**

# Sommaire

# Numérique

**1000BaseCX -** Spécifications éditées par la task force 802.3z. Il s'agit d'une extension des spécifications réseau Ethernet vers le Gigabit Ethernet. Dans ce cas précis le Gigabit utilise un support de transmission sur paire cuivre blindée.

**1000BaseLX et 1000BaseSX -** Spécifications éditées par la task force 802.3z. Il s'agit d'une extension des spécifications réseau Ethernet vers le Gigabit Ethernet. Dans ce cas précis le Gigabit utilise un support de transmission optique.

**1000BaseT -** Spécifications éditées par la task force 802.3ab. Il s'agit d'une extension des spécifications réseau Ethernet vers le Gigabit Ethernet sur câble de cuivre en paire torsadée.

**100Base X -** Ethernet 100 Mb/s, bande de base, câble à 4 paires torsadées non blindé (100BaseT4) ou 2 paires blindé (100BaseTX) ou en fibre optique 2 fils (100BaseFX). Le câble à paires torsadées doit être de classe 5.

**100BaseFX -** Norme IEEE Fast Ethernet permettant d'utiliser la méthode d'accès Ethernet sur un câblage de type Fibre Optique à 100 Mbit par seconde.

**100BaseT -** Norme IEEE 802.3u Fast Ethernet permettant d'utiliser la méthode d'accès Ethernet sur un câblage de type téléphonique en étoile à 100 Mbit par seconde.

La fenêtre de collision (temps minimal pendant lequel une station émettrice doit écouter le réseau pour détecter la collision la plus tardive) est réduite à 5,12 µs, ce qui fait un silence inter-trame (IFG : InterFrame Gap) de 0,96 µs (96 bits). Ceci induit de fortes contraintes sur le temps de propagation du signal et donc sur la distance maximale entre les deux stations les plus éloignées du réseau. La longueur d'un segment ne peut excéder 100 mètres.

Le 100 base T4 utilise un codage de type 8B/6T (8 bits sur 3 temps d'horloge). Trois paires sont utilisées pour la transmission de données, la quatrième pour la détection de collision.

Le 100 base TX et 100 base FX utilise la signalisation 4B/5B (16 symboles parmi 32) sur une paire ou fibre d'émission et une paire ou fibre de réception.

**100BaseVG -** Technologie 100 Mb/s combinant les éléments Ethernet et Token Ring. Le 100VG Any LAN est standardisé dans la spécification IEEE 802.12.

L'appellation 100VG Any LAN provient de 100 Mbps, avec de 4 simples paires torsadées de qualité vocale (Voice Grade) et de sa double compatibilité Ethernet et Token Ring (Any LAN).

La topologie est identique à celle du 10 base T : une étoile hierarchisée autorisant jusqu'à 5 niveaux, soit 4 hubs . Le hub de tête est appelé « root hub ». Les distances maximum dépendent des câbles utilisés, soit 100 mètres pour les catégorie 3 et 4 et 150 mètres pour les câbles de catégorie 5 UTP.

Certains câbles particuliers autorisent des longueur de segment de 200 mètres. Les hubs utilisés sont particuliers à la norme et s'ils sont appelés hubs dans la spécification, ils se rapprochent plus du commutateur.

Principe de l'accès par scrutation (polling) :

Lorsqu'une station désire émettre, elle fait une requête auprès du hub qui lui alloue ou non le support (Demand Priority Access Method ou DPAM). Les collisions sont donc impossible et le délai d'attente du aux jetons sont supprimés.

Les stations informent le hub de leur disponibilité en lui transmettant le signal « Idle ». La station désirant émettre formule une requête avec un niveau de priorité. Les autres machines raccordées sont averties par le hub que quelqu'un va émettre et se mettent en état de recevoir (signal Incomming, INC). Lorsque toutes les stations ont cessé l'émission du Idle, cela signifie qu'elles sont prêtes à recevoir et la station émettrice transmet sa trame. Le hub l'analyse et la transmet à la station intéressée et reprend l'émission du Idle.

Les signaux de signalisation sont émis en basse fréquence (30 Mhz), ils se composent de 2 tonalités. La première tonalité correspond à la transmission de 16 bits à 1 suivis de 16 bits à 0, se qui donne un signal de 0.9375 Mhz, la seconde tonalité alternent la transmission de 8 bits à 0 et 8 bits à 1, se qui donne un signal de 1.875 MHz.

Cette méthode d'accès garantit que chaque station aura accès au support. Afin d'éviter un usage abusif des données prioritaires, le hub surveille les files d'attentes de requêtes de données normales et les transforment en priorité haute à l'échéance d'une temporisation (TTT : Target Transmission Time). Les stations sont donc sûre d'émettre après n.TTT secondes où n est le nombre de stations.

**10Base2 -** Norme IEEE 802.3 Ethernet utilisant pour support un câble coaxial fin. Longueur maximale d'un segment limitée à 185 mètres. Débit de 10 Mbit par seconde. Bande de base, câble coaxial fin. Un réseau 10Base2 peut comporter 5 segments de 185 m reliés par 4 répéteurs et dont 3 seuls desservent jusqu'à 30 stations chacun séparées de 50 cm.

**10Base5 -** Norme IEEE Ethernet utilisant pour support un câble coaxial jaune (épais, blindé et rigide). Longueur maximale d'un segment limitée à 500 mètres. Débit de 10 Mbit par seconde. Un réseau 10Base5 peut comporter 5 segments de 500 m reliés par 4 répéteurs et dont 3 seuls desservent jusqu'à 100 stations chacun séparées de 2,50 m.

**10BaseT -** Norme IEEE Ethernet permettant d'utiliser la méthode d'accès Ethernet sur un câblage de type téléphonique en étoile à 10 Mbit par seconde. Bande de base, câble à paires torsadées (100 m maximum) non blindé (UTP) ou blindé (STP) reliant les stations (1024 au maximum) aux concentrateurs

**10G base CX4 -** Norme IEEE 10 Gigabit permettant de transporter sur un support Cuivre le standard 10 gigabit. La distance se limite à 15 m environ.

**10GE -** 10 Gigabit Ethernet - Déclinaison à 10 Gbit/s du protocole Ethernet pour réseau local. Cette technologie a surtout prouvé son utilité chez les opérateurs et les fournisseurs de services. Les opérateurs le déploient directement sur fibre optique, quand les distances le permettent, sur les réseaux métropolitains ou au-dessus d'une couche WDM. Il leur permet d'offrir une bande passante plus importante.

En matière de réseaux locaux, le 10GE a fait ses premiers pas dans des structures aux besoins peu communs telles qu'universités et centres de recherche. Dans les entreprises plus traditionnelles, il commence à faire son apparition, principalement pour le déploiement d'applications très gourmandes en bande passante ne se satisfaisant pas du Gigabit Ethernet.

Le 10 Gigabit Ethernet fournit une bande passante théorique de 10 Gbit/s, soit dix fois plus que le Gigabit Ethernet. Correspondant à la norme IEEE 802.3ae, le 1OGE est totalement compatible avec les versions à plus bas débit du protocole. Il ne fonctionne qu'en duplex intégral : avec un seul équipement connecté sur le port d'un commutateur, les risques de collision de paquets sont supprimés, ce qui permet de s'affranchir du mécanisme CDMA/CD et rend l'utilisation de la bande passante optimale.

Le 10GE nécessite une infrastructure de câblage capable de supporter les très hauts débits. Seules les utilisations sur fibre optique (jusqu'à 40 km avec de la fibre optique monomode) et sur câble coaxial en cuivre (15 m au maximum) ont pour le moment été standardisées. La norme permettant l'utilisation de câblage de cuivre en paire torsadée catégorie 6a ou 7, sur une distance maximale de 100 m, devrait être validée en 2006.

**10PassTS -** Interface physique qui prévoit la transmission de trames Ethernet en mode symétrique sur une paire de cuivre. Elle utilise la modulation et l'interface du VDSL avec des débits de 100 Mbit/s en mode asymétrique et 50 Mbit/s en symétrique. La distance entre le réseau d'opérateur et l'abonné ne dépasse pas 1 km.

**1394 (IEEE 1394) -** ou FireWire le monde PC ou i.LinK chez Sony - Grâce à ses transferts à haut débit 400 Mégabits par secondes (Mbps) et maintenant 800 Mégabits par secondes (Mbps) et à ses capacités Plug & Play à chaud, FireWire est l'interface idéale des équipements vidéo et audio numériques actuels, mais aussi des disques durs externes et d'autres périphériques haute performance. Il donne la possibilité de gérer simultanément jusqu'à 63 périphériques.

**2,5G -** Système mobile intermédiaire entre la 2G et la 3G (débits inférieurs à 100 kbit/s - GPRS, CDMA 2000 1x).

**2BaseTL -** Interface physique qui prévoit la transmission de trames Ethernet en mode symétrique sur une paire de cuivre. Fonctionnant en bande de base, elle réutilise l'interface physique définie par l'UIT pour l'E-SHDSL (débit nominal de 5,7 Mbit/s par paire). En fonction du nombre de paires utilisées, la transmission court de 1 à 3,5 km.

**2G -** Système mobile de seconde génération (GSM- CDMA- TDMA (IS 136) - PDC). Voir GSM

**3G -** Système mobile de troisième génération labellisé IMT 2000 par l'UIT. Voir UMTS

**3G Third Generation -** Méthode pour envoyer des informations provenant d'internet sur des téléphones mobiles, jusqu'à une vitesse de 2 mégabits par seconde, ce qui est nettement plus rapide que le GPRS.

**3GPP -** Third Generation Partnership Project - Organisation de normalisation internationale issue d'une collaboration entre les membres de l'ETSI et des instances de normalisation américaines, japonaises et coréennes, afin de parvenir à la détermination d'une norme unique pour les systèmes mobiles de troisième génération (UMTS), notamment par la définition d'une interface radio commune. L'ETSI a transféré les activités du comité SMG pour l'UMTS au 3GPP.

**3GPP2 -** Third generation partnership project 2 - Structure de standardisation qui élabore les spécifications du CDMA 2000 et de l'évolution de l'IS 41 (protocole cœur de réseau) ainsi que l'interface entre les accès radio du 3 GPP et l'évolution de l'IS 41, regroupant les membres des instances de normalisation régionales suivantes : TIA (Etats-Unis), ARIB et TTC (Japon), TTA (Corée), CWTS (Chine).

**3ivx -** Codec vidéo à l'instar du MPEG et de DivX;-). Il est multi plate-forme.

**3RD -** Réseau radioélectrique réservé aux données.

**448 -** IEEE 448 - Interface utilisée principalement pour la mesure.

**4G -** Fondé sur un cœur de réseau IP, le futur système de téléphonie 4G fournira un accès haut débit aux données, permettant un passage sans interruption de service entre plusieurs points d'accès radio.

Le futur réseau 4G, à la convergence de plusieurs réseaux, ne devrait pas provoquer de rupture technologique avec le réseau 3G (UMTS). Le 4G sera caractérisé par un cœur de réseau IP et par la gestion de nombreuses technologies d'accès radio. Où qu'il soit, l'utilisateur pourra accéder à toutes ses données, mais une décennie de patience sera nécessaire.

Certains opérateurs et équipementiers travaillent déjà sur le prochain réseau 4G. Parmi les premiers à avoir réalisé des tests et des maquettes de réseaux, nous pouvons citer l'opérateur japonais NTT DoCoMo, l'équipementier Alcatel (centre de recherche de Shanghai) ou le fabricant sud-coréen Samsung. Plus qu'une réelle rupture technologique comme l'UMTS par rapport aux réseaux 2G et 2.5G, le réseau 4G sera à la convergence du réseau 3G et de diverses technologies radio complémentaires (Wifi, WiMax,…)

Le réseau 4G devrait également assurer des débits nettement supérieurs : entre 20 et 100 Mbit/s dans les réseaux à longue portée (UMTS) et jusqu'à 1 Gbit/s dans les réseaux locaux comme les hot spots Wifi. Ces débits assureront la transmission de contenus multimédias de plus en plus riches et permettront d'établir plusieurs sessions en parallèle (une session de vidéoconférence de haute qualité avec accès en temps réel à des contenus multimédias par exemple)

Avec le réseau 4G, un utilisateur accédera à ses données où qu'il se trouve : à son domicile ou dans son entreprise (Bluetooth, UWB ou Wifi), dans la rue (UMTS) ou même dans les lieux publics équipés de hot spots. Passer d'un réseau à l'autre deviendra transparent. Enfin, les débits (jusqu'à 100 Mbit/s en déplacement et 1 Gbit/s dans les environnements fermés) permettront d'accéder à plusieurs applications multimédias en parallèle.

**802.1 -** GMRP - Garp Multicast Registration Protocol - Standard du comité IEEE 802.1, il requiert le changement de la longueur maximale de la trame Ethernet IEEE 802.3 (1518 octets étendus à 1522 octets). Les ordinateurs et les commutateurs doivent être mis à jour pour GMRP, IGMP est toujours requis sur l'ordinateur. (voir Multicast).

**802.1 -** Norme IEEE traitant des architectures (802.1a), des ponts et du spanning tree (802.1d) et du System Load Protocol (802.c) - High Level Interface

**802.10 -** Norme IEEE définissant les Méthodes d'accès entre les couches MAC et LLC (niveau 2) ainsi que pour la couche application (niveau 7) pour les données confidentielles. Sécurité des réseaux.

Ce standard a été proposé par la compagnie Cisco Systems en 1995. Cisco a proposé d'utiliser le standard 802.10, qui avait été établi originellement pour spécifier un début de solutions sécuritaires dans les réseaux locaux comme norme pour les VLANs. Cisco a essayé de "détourner "l'entête de trame optionnelle 802.10 pour l'utiliser comme identificateur de VLAN au lieu de la laisser utile aux spécifications de sécurité pour lesquelles elle était prévue originellement. Le comité de l'IEEE s'est opposé rigoureusement au fait que Cisco s'attribue la norme et qu'il existe un standard utilisé pour définir deux concepts différents. De plus, cette solution, basée sur un entête pouvant contenir des champs de longueurs variables, ne permettait pas une implémentation facile sur des ASICs ce qui en limitait les performances.

**802.11 -** Ensemble de spécifications de réseaux sans fil développées par le groupe LAN/MAN de l'IEEE.

Normes IEEE définissant un réseau local sans fil. Un réseau local 802.11 est basé sur une architecture cellulaire (subdivisé en cellules), et où chaque cellule (appelée Basic Service Set ou BSS dans la nomenclature 802.11), est contrôlée par une station de base (appelée Access Point ou AP, Point d'Accès en français).

Même si un réseau local sans fil peut être formé par une cellule unique, avec un seul Point d'Accès, (et comme décrit plus loin, il peut même fonctionner sans Point d'Accès), la plupart des installations seront formées de plusieurs cellules, où les Points d'Accès sont interconnectés par une sorte de backbone (appelé Distribution System ou DS, Système de Distribution en français), typiquement Ethernet, et dans certains cas, lui-même sans fil.

L'ensemble du réseau local sans fil interconnecté, incluant les différentes cellules, leurs Points d'Accès respectifs et le Système de Distribution, est vu par les couches supérieures du modèle OSI comme un unique réseau 802, et est appelé dans le standard Extented Service Set (ESS).

**802.11a -** Norme IEEE définissant un réseau local sans fil qui utilise la bande des 5GHz, doté de 8 canaux de transmission (en France) - Taux de transfert jusqu'à 54Mbps. Autorise les architectures Infrastructure uniquement. Supporte l'encryptage WEP. Il existe des solutions bi bandes intégrant le 802.11b & a.

Opérant dans la bande des 5 à 5.8 GHz, la norme 802.11a met l'accent sur l'utilisation de la technologie OFDM au niveau physique pour atteindre des débits de 54 Mbps. OFDM est également la technologie préconisée par la norme HiperLAN/2. La norme prévoit grâce à cette technologie une meilleure immunité aux interférences.

OFDM (Orthogonal Frequency Division Multiplexing) divise les canaux de 20 MHz en 52 sous-canaux de 0,3125 MHz (sur 64 sous-canaux possibles) pour obtenir au choix des débits de 6, 9, 12, 18, 24, 36, 48 ou 54 Mbps. Seuls les débits de 6, 12 et 24 Mbps doivent être impérativement implémentés sur tous les produits.

**802.11b -** Norme IEEE définissant un réseau local sans fil qui utilise la bande des 2.4GHz, doté de 14 canaux de transmission. Taux de transfert jusqu'à 11 Mbps. Autorise les architectures Ad-Hoc et Infrastructure. Permet les connexions inter bâtiments. Supporte l'encryptage WEP Solutions certifiées Wifi pour garantir la compatibilité des produits 802.11b.

Normalisée en septembre 1999, la norme 802.11b ou 802.11HR (High Rate) n'est modifiée par rapport à la norme 802.11 qu'au niveau de la couche physique. Seule la technologie DSSS dans la bande 2,4 GHz est gardée, permettant des débits de 11 Mbps et des portées de 300 mètres. Bien sûr, les débits chutent avec l'augmentation de la distance entre les éléments.

Un organisme, la WECA, s'est donné la mission de certifier l'interopérabilité des produits avec la norme 802.11b afin d'aider son implantation au niveau du marché.

La bande des 2,4 GHz, ou bande ISM (Industriel, Scientifique et Médical), est exploitée par d'autres équipements, dont les fours micro-ondes, les téléphones sans fil et les puces Bluetooth.

**802.11c -** Complément de la couche MAC améliorant les fonctions "pont", reversé au groupe de travail 802.11d.

**802.11d -** Adaptation des couches physiques pour conformité aux exigences de certains pays particulièrement strictes (essentiellement la France et le Japon).

**802.11e -** Complément de la couche MAC apportant une qualité de service aux réseaux 802.1Aa, b et g. Cette norme permet notamment la technologie VoWi-Fi.

En définissant des mécanismes de Qos sur le réseau WLAN, 802.11e permettra aussi l'utilisation et le transport de la vidéo sur WLAN. Premier mécanisme de 802.11e : Mise en place de 8 catégories de trafic et du multiplexage temporel (TDMA). 802.11e permettra aussi de réduire les collisions (les pertes de données) au sein de chaque catégorie de trafic. Les catégories de trafic seront traitées en fonction de leur niveau de priorité.

**802.11f -** Standard qui définit des fonctions de "roaming" et permettant de dialoguer avec d'autres points d'accès type 802.11 a, b ou g.

Document normatif décrivant l'interopérabilité inter constructeurs au niveau de l'enregistrement d'un point d'accès (AP) au sein d'un réseau, ainsi que les échanges d'information entre AP lors d'un saut de cellule (roaming).

**802.11g -** Norme IEEE définissant un réseau local sans fil qui utilise la bande des 2.4GHz, doté de 14 canaux de transmission. Taux de transfert jusqu'à 54Mbps. Permet les connexions inter bâtiments. Autorise les architectures Ad-Hoc et Infrastructure. Adaptation d'OFDM aux réseaux 802.11b, mode turbo apportant également les mécanismes de code de protection par redondance (PBCC). Supporte l'encryptage WEP.

**802.11h -** Amélioration de la couche MAC visant à rendre compatible les équipements 802.1 la avec les infrastructures Hiperlan2. 802.11h s'occupe notamment de l'assignation automatique de fréquence de l'AP et du contrôle automatique de la puissance d'émission visant à éliminer les interférences entre points d'accès (à ne pas confondre avec un asservissement de la puissance d'émission de l'AP en fonction de la force du signal du client, tel que c'est le cas pour le MMAC Hiswan japonais). Travail commun entre l'IEEE et l'Etsi.

**802.11HR -** Norme IEEE définissant un réseau local sans fil. Le standard IEEE 802.11HR est un système de transmission des données conçu pour assurer une liaison indépendante de l'emplacement des périphériques informatiques qui composent le réseau et utilisant les ondes radio plutôt qu'une infrastructure câblée. Dans l'entreprise, les LAN sans fil sont généralement implémentés comme le lien final entre le réseau câblé existant et un groupe d'ordinateurs clients, offrant aux utilisateurs de ces machines un accès sans fil à l'ensemble des ressources et des services du réseau de l'entreprise, sur un ou plusieurs bâtiments.

**802.11i -** Norme IEEE définissant une amélioration du niveau MAC destinée à renforcer la sécurité des transmissions, et se substituant au protocole de cryptage WEP (Wireless Equivalent Privacy) et WPA. La norme 802.11i permettra de s'assurer qu'un terminal vocal ne peut pénétrer le réseau WLAN sauf autorisation explicite. Standard de l'IEEE, cette norme comble les lacunes du WPA1 en remplaçant le chiffrement RC-4 par du chiffrement AES (Advanced Encryption Standard). Aussi dénommée WPA2, la norme reprend les spécifications du WPA1 : Mécanismes d'authentification IEEE 802.1x et schéma de distribution de clés dynamiques TKIP (Temporal Key Integrity Protocol).

L'AES dans 802.11i peut être utilisé selon plusieurs modes, le CCMP (Counter Mode with CBC-MAC Protocol) étant celui retenu. Le Counter Mode est l'algorithme chargé du secret des données, alors que le Cipher Block Chaining Message Authentification Code (CBC-MAC) permet de contrôler l'intégrité et l'authentification des données. L'AES dans sa version IEEE 802.11i propose des clefs de 128, 192 et 256 bits.

Sur le plan de l'authentification, le protocole 802.11i prévoit deux modes :

- Un mode dit personnel sans serveur d'authentification,
- Un mode entreprise, qui, à la manière de WPA, implémente le protocole 802.1x entre le client, le point d'accès et le serveur d'authentification.

Le protocole 802.11i ne spécifie pas le type de serveur utilisé. Le 802.1x utilise la méthode EAP (Extensible Authentification Protocol) pour transporter les messages d'authentification vers le serveur.

EAP pouvant être implémenté suivant différentes variantes (EAP-TLS, EAP-LEAP, EAP-TTLS, etc.), le client et le serveur doivent convenir d'une méthode commune. Le point d'accès n'intervient pas pendant cette phase: il attend simplement la réponse du serveur pour savoir s'il autorise le client à entrer sur le réseau.

Durant les dernières étapes de cet échange, le client et le serveur se mettent d'accord sur une clé PMK (Pairwise Master Key), puis le serveur la transmet au point d'accès en lui indiquant également qu'il peut accepter la station. Ces clés PMK permettent de générer des clés temporaires utilisées pour les opérations de chiffrement et d'intégrité et regroupées sous l'appellation de PTK (Pairwise Transient Key). Elle servent durant toute la durée de l'échange et sont recalculées tous les 10000 paquets.

**802.11k -** Amélioration de la couche MAC destinée à optimiser l'allocation des ressources du réseau sans fil selon la qualité de chaque liaison. Chaque station terminale délivrera un bilan de sa connexion aux points d'accès en échange duquel ces derniers redistribueront les ressources adéquates pour garantir le débit et la disponibilité de la liaison.

**802.11n -** Norme IEEE définissant les spécifications Wifi haut débit. Cette norme met en œuvre la technologie MiMo pour augmenter les débits et garantir une meilleure performance de transmission (100 à 450 Mbit/seconde). Ce standard apporte des changements à la fois au niveau de la couche Physique et de la couche MAC.

Considéré par certains comme annonciatrice de la fin de l'Ethernet filaire, la norne 802.11n va évoluer dans ses composants, dans la gestion de la partie radio (antennes notamment), du contrôle réseau, de la sécurité, de la gestion de l'alimentation. Ses améliorations vont contribuer à l'érosion du marché de l'Ethernet commuté.

Si l'on considère que plus de 200 millions de chipsets 802.11 ont été vendus en 2006, il est évident que les utilisateurs vont créer le besoin d'un réseau Ethernet sans fil constant et fiable, avec une capacité et des débits très importants.

Il n'est plus d'ordinateur portable livré sans sa connexion wifi, et la très grande majorité des téléphones évolués font aussi appel à la technologie 802.11 pour écouler une partie du trafic data sans écrouler le réseau de l'opérateur.

**802.11r -** Amélioration de la couche MAC destinée à optimiser le roaming (saut de cellule) dans les réseaux sans fil. Approuvée par l'Institut des Ingénieurs électroniques et électriques pour la VoIP.

Lors d'un appel en VoIP passé sous la norme IEEE 802.11 (qui fut instaurée pour simplifier l'accès à une connexion propre) en déplacement, la machine (le terminal ou le téléphone) recherche alors systématiquement ce type de réseau.

Depuis 2005, le travail réalisé sur le Wi-Fi "r" vise à simplifier le roaming, sans qu'il n'y ait de déconnexion entre deux bornes, le 802.11 ayant été conçu pour ne gérer qu'un seul point d'accès. La reconnexion engendrait une perte de l'appel.

Pour une zone de couverture plus importante, il faut multiplier les bornes et ainsi passer par plusieurs ré-association.

Ce nouveau protocole simplifie largement l'utilisation de la VoIP dans le cadre de l'entreprise, en évitant au maximum les coupures, et en limitant la reconnexion qui est de l'ordre de 100 ms pour le 802.11 à 50 ms pour le 802.11r.

**802.11s -** Norme IEEE définissant les spécifications du WLAN Mesh (pas encore standardisé en décembre 2005). Deux principaux groupes se sont formés :

- SeeMesh, dont fait partie Cisco Systems.
- Wi-Mesh Alliance soutenu par Nortel et Philips.

Dans les architectures Mesh, seuls certains points d'accès sont connectés au réseau filaire, par contre tous les points d'accès sont connectés entre eux de façon à former une dorsale (backbone) hertzienne.

**802.12 -** Norme IEEE définissant les spécifications des réseaux locaux 100 Mbps avec DPMA (Demand-Priority Access Method) - Voir 100BaseVG.

**802.14 -** Norme IEEE définissant les réseaux sur les câbles télévision CATV - CATV (Câble TV)

**802.15 -** Réseaux locaux d'une couverture de 10 m et d'un débit de 500 Mbit/s à 1 Gbit/s. Les débits offerts par cette technologie progressent d'année en année grâce à un spectre radio quatre-vingts fois plus large (de 3,1 à 10,6 GHz) que celui du standard 802.11b. Voir UWB

**802.15.1 -** Spécification IEEE aussi dénommée Bluetooth. Voir Bluetooth. Norme IEEE définissant le standard Bluetooth 1.x permettant d'obtenir un débit de 1 Mbit/sec

**802.15.2** - Spécification IEEE aussi dénommée Bluetooth. Voir Bluetooth. Norme IEEE définissant des recommandations pour l'utilisation de la bande de fréquence 2.4 GHz (fréquence utilisée également par le WiFi)

**802.15.3 -** Spécification IEEE aussi dénommée Bluetooth 2. Voir Bluetooth 2. Norme IEEE définissant un standard en cours de développement visant à proposer du haut débit (20 Mbit/s) avec la technologie Bluetooth

**802.15.4 -**Spécification IEEE définissant un standard pour des applications Bluetooth à bas débit.

**802.16 -** Aussi appelé WiMax - Worldwide Interoperability for Microwave Access - Standard de l'IEEE utilisé pour développer de nouveaux réseaux métropolitains sans fil (WMAN). Le WiMax offrira des débits jusqu'à 70 Mbits/seconde sur une portée de 50 kms (transport voix et vidéo). Utilisé dans le raccordement du client final au réseau haut débit sur les derniers kilomètres, il est une alternative à l'ADSL et au câble. Il permet aussi de relier les Hot spots Wifi 802.11 à Internet. WiMax utilise les bandes de fréquence 3,4 GHz et 5,8 Ghz.

**802.16a -** Spécification issue du 802.16, le 802.16a utilise une technologie de modulation de type OFDM. Concentré entre 2 et 11 GHz, le réseau sans-fil porte sur 50 kms avec un très large spectre d'utilisation (égal à 3,8 bit /Hz) qui autorise un débit pouvant aller jusqu'à 280 Mbits / seconde pour les stations qui se connectent. Cette spécification décrit les processus logiciels et physique à mettre en œuvre.

**802.16d -** Spécification issue du 802.16, ce standard supporte des formes de nomadisme limitées.

**802.16e -** Spécification issue du 802.16, le 802.16e reprend les attributs de la spécification 802.16 complétés de la spécification 802.16a, en y apportant les fonctionnalités de "roaming".

**802.17 -** ou RPR, Resilient Packet Ring - Ce standard est orienté cœur de réseau. Il apporte aux réseaux métropolitains optiques Ethernet une capacité de restauration de liens rapides (type Sonet/SDH) et résout en partie les problèmes de congestion.

**802.1d -** IEEE 802.1d - Standard qui définit le Spanning Tree.

**802.1p -** Norme IEEE traitant la gestion du flux et des priorités sur Ethernet. Pour améliorer les performances des commutateurs, la norme 802.1p introduit des classes de service permettant d'échanger du trafic prioritaire en cas de congestion des équipements. Ainsi, le flux prioritaire à la possibilité de passer par des files d'attente plus rapides que le flux considéré comme de priorité normale (ou "best-effort "). Ainsi, huit niveaux de priorité ont été définis par la norme 802.1p.

Bien que la norme définisse huit niveaux de priorité, le nombre de files d'attente n'est pas défini et peut varier entre 1 et 7. Mais attention, s'il n'y a qu'une seule file d'attente, il ne peut pas y avoir de gestion de priorité car le flux sera traité en FIFO (First In First Out). Le choix est donc laissé libre au constructeur mais ne figure pas toujours dans les caractéristiques commerciales. Ainsi, à l'intérieur d'un pont ou d'un commutateur qui possède suffisamment de files d'attentes, les trames en attente en sortie d'un port en file d'attente de priorité N ne seront pas écoulées tant que les files d'attente de priorité supérieure (au moins N+1) sont vides. La configuration des classes de priorité peut se faire de manière centralisée par l'administrateur.

**802.1Q -** Norme IEEE traitant les Réseaux locaux virtuels pontés - VLAN Tagging (marquage) - Standard qui définit la manière d'inscrire une étiquette dans une trame Ethernet de manière à reconnaître l'appartenance de celle-ci à un réseau local virtuel au niveau du port d'un commutateur.

Le comité 802.1Qa spécifié un standard pour le Frame Tagging qui permettrait le dialogue entre des équipements VLANs de divers constructeurs. Cette norme est basée sur un marquage explicite et est construite sur les normes 802.1D (Spanning Tree) et le 802.1p. Il s'agit de rajouter l'identificateur VLAN (VLAN Tag) sur 4 octets dans la trame Ethernet entre l'adresse source et le champ type/longueur pour identifier les différents VLANs.

La norme 802.1Q prévoit un maximum de 4096 VLANs et utilise la technique du marquage de trames (Frame Tagging) comme moyen de communication. Le marquage des trames permet d'une part de savoir à quelle VLAN appartient une trame et permet, grâce au protocole 802.1p, d'ajouter un niveau de priorité cette trame. De plus, ce standard définit 3 façons différentes d'interconnecter des équipements VLAN:

- Le Trunk Link: Tous les matériels connectés à un "trunk link", y compris les stations, doivent être compatibles VLAN. Toutes les trames sur le "trunk link" ont un entête spécifique et utilisent le "frame tagging ".
- L'Access Link (lien d'accès) : Un "access link" connecte un matériel non-compatible VLAN à un switch compatible VLAN. Toutes les trames sur "l'access-link" doivent être implicitement taggées (c'est-à-dire non-taggées). Le matériel non-compatible VLAN peut-être un ou plusieurs segments LAN composés de stations non-compatibles VLAN.
- Le Hybrid Link (lien hybride) : Il s'agit d'une combinaison des deux liaisons précédentes. C'est-à-dire un segment où sont connectés à la fois des périphériques compatibles VLAN et non-compatibles VLAN. Ce sont des liens où peuvent transiter à la fois des trames taggées et des trames non taggées. Toutefois, les trames pour un VLAN spécifique doivent être ou taggées, ou non taggées.

**802.1v -** Norme IEEE traitant de la normalisation des VLANs de niveau 3. La norme 802.1v s'intitule "Classification des VLAN par protocoles et par ports" et est une extension du protocole 802.1D. Cette norme permet une cohabitation des VLANs de niveau 3 entre les différents constructeurs, elle est utilisée avec des trames utilisant le marquage explicite et implicite.

**802.1w -** IEEE 802.1w - Standard qui définit le Rapid Spanning Tree.

**802.1x -** Sous-section du groupe de travail 802.11i visant à l'intégration du protocole EAP (authentification) dans les trames Ethernet (indépendamment de tout protocole PPP, contrairement aux accès RAS conventionnels). 802.1x permet l'usage d'un serveur d'authentification de type Radius. Standard de sécurisation des réseaux sans fil par authentification d'un hôte.

**802.2 -** Norme IEEE traitant des spécifications de la sous-couche LLC du niveau 2 du modèle OSI (802.2c, f et h) - LLC Logical Link Control.

**802.3 -** Norme IEEE définissant un réseau local ayant une topologie en bus (voir Ethernet) - Ethernet CSMA/CD.

**802.3ac -** IEEE 802.3ac - Standard qui définit le "VLAN Tagging" (marquage de la trame pour une appartenance à un VLAN donné.

**802.3ad -** IEEE 802.3ad - Standard qui définit l'agrégation de liens. Ce standard porte le nom de "port trunking" dans les notices des équipements.

**802.3af -** Norme IEEE définissant le Power Over Ethernet - PoE - a pour principe de faire circuler le courant électrique dans un câble Ethernet. Son objectif est de réduire les coûts de déploiement de certaines infrastructures telles que les réseaux Wi-Fi et de téléphonie IP.

En assurant l'alimentation électrique et le transfert des données sur un seul et unique câble, le PoE élimine les frais liés à l'installation de câbles et de prises électriques. Pour raccorder un appareil, tel qu'une borne Wi-Fi, un téléphone IP ou une caméra IP de vidéo-surveillance, il suffira de disposer d'une prise réseau. D'où également une plus grande liberté d'installation.

Le PoE est utilisé sur des câbles de catégorie 3 et 5 (ou plus) avec des débits de 10 ou 100 Mbit/s. Pour faire circuler le courant sur ces câbles de catégorie 5 (quatre paires de cuivre), deux solutions existent : exploiter soit les deux paires libres non utilisées pour les données (les brins de cuivre 4,5 et 7,8), soit les brins de cuivre employés pour le transport des données (1,2 et 3,6), à une fréquence différente de celle en usage pour les données.

Pour les câbles de catégorie 3 composés de deux paires de cuivre, données et électricité vont cocirculer.

Pour mettre en place un réseau avec PoE, les équipements terminaux (téléphones IP, bornes Wi-Fi, etc.) doivent accepter la norme et les équipements émetteurs. Ces derniers sont soit des commutateurs délivrant le PoE sur leur port Ethernet, soit des injecteurs de courant (appelés midspans) placés entre le commutateur et l'équipement terminal.

Avant de délivrer le courant, l'émetteur (PSE pour Power Sourcing Equipment) va vérifier qu'un terminal (appelé PD pour Powered Device) PoE est bien connecté et en état de marche

D'après le standard 802.3af, tous les PD doivent être capables d'être alimentés par les deux types d'alimentations, sur paires 1,2 et 3,6 ou 4,5 et 7,8. Pour vérifier l'état du PD, le PSE va détecter la signature d'une résistance électrique spécifique, intégrée dans tous les PSE supportant le PoE. Cette phase de détection dure moins de 500 ms. Ensuite, le PSE va déterminer la puissance maximale que le PD va accepter. Cette phase dure de 50 à 75 ms. L'alimentation électrique peut alors commencer. Quant à la déconnexion de l'équipement terminai, elle va s'effectuer de manière sécurisée, et en moins de 300 ms. Le 802.3af a pour limite de distance celle de l'Ethernet. Ainsi, les PSE doivent être éloignés de 100 mètres maximum de la source d'émission.

Le voltage est de 48 volts, tandis que la puissance est de 15,4 watts maximum (au niveau du PSE, soit 12,95 w au niveau du récepteur).

**802.3ah -** Ethernet in the First Mile - Permet d'accroître la présence d'Ethernet sur la boucle locale. Ce standard prévoit le support de plusieurs types de medias et de liaisons point à point sur paire cuivre, liaisons optiques point à point ou multipoint. Ce standard spécifie aussi les mécanismes d'exploitation, d'administration et de maintenance pour les réseaux d'accès Ethernet.

**802.3u -** Norme IEEE définissant un réseau local ayant une topologie en bus (topologie logique) mais représentée en étoile, également appelée FAST ETHERNET. Spécifications du Fast Ethernet, Couche MII (Media Independant Interface), 100bTX, 100bT4 …

**802.3x -** Norme IEEE définissant le Signal intercommuteurs émis pour arrêter le trafic lorsque la mémoire est saturée - Full Duplex et contrôle de flux.

**802.3z -** Norme IEEE définissant les spécifications du Gigabit Ethernet - Ethernet 1000bT.

**802.4 -** Norme IEEE définissant un réseau local ayant une topologie en bus à jeton.

**802.5 -** Norme IEEE définissant un réseau local ayant une topologie de type anneau. (Voir Token Ring).

**802.6 -** Norme IEEE définissant les spécifications des réseaux métropolitains - Réseaux MAN DQDB.

**802.7 -** Norme IEEE définissant le Groupe de travail BBTAG (Broadband Technical Avisory Group). Norme Slotted Ring - Réseaux Large Bande.

**802.8 -** Norme IEEE définissant le Groupe de travail FOTAG (Fiber Optics Technical Advisory Group) Réseaux fibres optique

**802.9 -** Norme IEEE définissant les IS LAN (Integrated Services LAN) Ethernet Isochrone & IsoEnet - Réseaux voix/données.

# A

**AAA -** Authentication, Authorization, and Accounting - Eléments de sécurité généralement utilisés pour offrir un accès sécurisé aux ressources :

- Accounting (Gestion) : processus permettant d'identifier l'auteur ou la cause d'une action spécifique, tel que le pistage des connexions d'un utilisateur et la journalisation des utilisateurs du système.
- Authentication (Authentification) : validation de l'identité d'un utilisateur ou d'un système (hôte, serveur, commutateur ou routeur).
- Authorization (Autorisation) : moyen permettant d'accorder l'accès à un réseau à un utilisateur, un groupe d'utilisateurs, un système ou un programme.

**AAL-1 -** ATM Adaptation Layer de type 1 - Fonction permettant d'adapter à la structure des cellules les informations des applications qui nécessitent des débits constants (voix, par exemple).

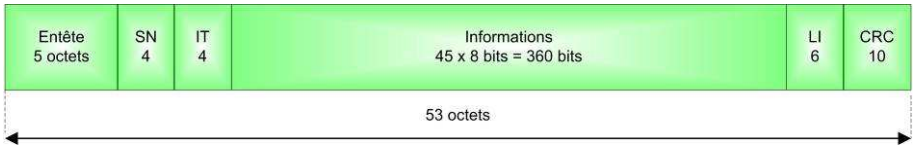
L'objectif de l'AAL type 1 est le support d'une transmission continue à débit constant. Certaines applications ont actuellement besoins de services de transmission à débit constant. Ce type de service peut être utilisé pour remplacer les lignes louées.


Les champs relatifs à l'AAL type 1 occupent un octet de la charge utile, laissant 47 octets disponibles pour l'information. Ils incluent un numéro de séquence (SN, Sequence Number), aussi appelé SC (Sequence Counter), permettant de détecter les cellules manquantes ou insérées, ainsi qu'un champ de vérification (SNP, Sequence Number Protection), aussi appelé CRC, pour la détection d'erreurs multiples et la correction d'erreurs simples portant sur le numéro de séquence.

Le SNP (CRC) est calculé sur les premiers 4 bits suivant le polynôme x3+x+1. Une fois le SNP calculé, le bit de parité est calculé sur les 7 premiers bits et placé dans le huitième.

**AAL-2 -** ATM Adaptation Layer de type 2 - Adaptation des informations à débit variable qui nécessitent toutefois une relation stricte entre horloges d'extrémité (vidéo...).

L'objectif de l'AAL type 2 est de même nature que l'AAL type 1. Cependant, le besoin de ce type d'adaptation n'apparaît pas clairement et l'ITU-T ne l'a pas standardisé.




Les champs correspondant à ces fonctions sont différents afin de s'adapter à la transmission d'unités de données de longueur variables. Ils occupent trois octets, laissant 45 octets pour l'information utile. On y trouve un numéro de séquence sur 4 bits (modulo 8), une information (IT) décrivant le type de cellule, le nombre significatif d'octets dans le cas d'une cellule partiellement remplie (LI), ainsi qu'un code CRC sur 10 bits qui permet la détection des erreurs dans la charge utile de la cellule, ainsi qu'une correction d'erreur simple.

**AAL-3/4 -** ATM Adaptation Layer de type 3/4 - Adaptation pour transmission de données, mode connecté ou non.

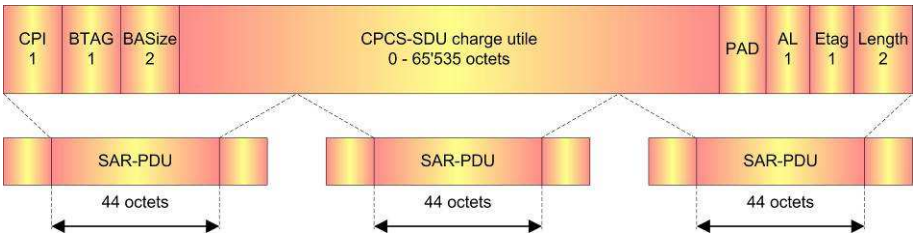
L'AAL type 3/4 est le résultat des efforts de standardisation de deux AAL. L'AAL type 3 qui avait pour objectif de fournir un service d'encapsulation pour les protocoles orientés connexion tel que X.25 et l'AAL type 4 qui avait pour objectif de fournir un service pour les protocoles orientés sans connexion tel qu'IP.

Dans la pratique, l'encapsulation est pratiquement identique pour les deux cas et les deux AAL ont été combinées. Finalement, l'industrie des transmissions de données est arrivée à la conclusion que l'AAL type 3/4 n'est pas adaptée au transport des données d'ordinateur à ordinateur, ce qui a conduit au développement de l'AAL type 5.

Les fonctions d'adaptation type 3 et 4 étant très similaires, leur sous-couche SAR est commune ainsi qu'une partie de la sous-couche de convergence appelée CPCS (Common Part Convergence Sublayer). Les fonctions supportées par la CPCS sont les suivantes :

- Délimitation de la trame CPCS-SDU
- Détection des erreurs
- Information du récepteur sur l'espace mémoire nécessaire pour recevoir la CPCS-SDU (tampon)
- Envoi d'un message d'abandon

Les fonctions CPCS permettent de supporter aussi bien un service de classe D qu'un service de classe C.

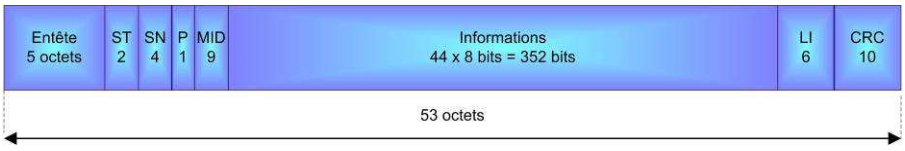



Les champs significatifs du CPCS sont :

- Champ d'identification pour partie commune (CPI, Common Part Indicator) qui donne des indications pour l'interprétation des champs suivants.
- Des indicateurs de début et de fin de la CPCS-SDU (Btag, Etag), qui permettent d'éviter la concaténation de deux CPCS-SDU résultant de la perte des cellules transportant la fin du premier datagramme et le début du suivant.
- Un indicateur initial de la taille de la CPCS-SDU (BASize) qui permet au récepteur d'attribuer une mémoire tampon de taille suffisante pour son stockage.
- Un bourrage (AL, Alignement) pour aligner la CPCS-SDU sur une frontière de 32 bits.

Un indicateur final de la taille de la CPCS-SDU (Length) qui donne la longueur exacte des données utiles.

La sous-couche SAR, en plus d'assurer la segmentation et le réassemblage de la CPCS-SDU, préserve l'intégrité de la charge utile de la cellule appelée SAR-PDU. Les champs permettant cette gestion occupent 4 octets dans la cellule, réduisant la charge utile à 44 octets.




Ces champs comportent :

- Un indicateur de type de segment (ST, Segment Type). Début, milieu et fin de message ou message composé d'un seul segment.
- Un numéro de séquence (SN, Sequence Number) modulo 16 pour détecter les cellules manquantes ou insérées.
- Un indicateur de priorité (P, Priority) permettant aux SAR-PDU de haute priorité d'être transmises avant celles de basse priorité.
- Un indicateur de multiplexage, permettant d'identifier des cellules appartenant à des messages différents multiplexés dans le même canal virtuel (MID, Multiplexing IDentifier).
- Un indicateur donnant le nombre d'octets utiles dans le champ information (LI, Length Indicator)
- Un code CRC sur 10 bits identique à celui utilisé avec la fonction AAL type 2

Il a été défini quelques services au dessus de l'AAL 3/4 dont les plus notables sont IEEE 802.6 (DQDB) et le Switched Multimegabit Data Service (SMDS). Les comités de normalisation SMDS et IEEE 802.6 envisagent tous les deux de changer leurs spécifications pour utiliser l'AAL type 5.

**AAL-5 -** ATM Adaptation Layer de type 5 - Pour transmission de données en mode connecté.

La fonction d'adaptation type 5 est désignée au transport de message en mode non assuré. Afin de répondre immédiatement à la demande, le comité ANSI T1S1.5 à décidé de travailler à une rapide standardisation appelée SEAL (Simple and Efficient AAL). Cette rapide standardisation est la base de l'AAL type 5.


L'AAL type 5 est caractérisée par un algorithme beaucoup plus simple que l'AAL type 3 et 4. Il est relativement simple à implémenter sur les éléments électroniques (Chips). C'est la raison pour laquelle cette fonction est apparue la première.

Les champs nécessaires sont les suivants :

- Un indicateur d'adaptation de charge (PAD) afin de permettre au CS-PDU d'être un multiple de 48 octets,
- Un indicateur de contrôle (CTRL),
- Un indicateur de longueur utile de la charge (LI, Length Indicator),
- Un code CRC-32 sur 4 octets pour la détection des erreurs.

**Abélien -** Un groupe est dit abélien s'il satisfait les propriétés mathématiques suivantes : Associative, Identité (existence de l'élément neutre), Inverse, Interne et Commutatif.

**Aberration chromatique -** Défaut optique qui se traduit sur l'image par des franges colorées visibles autour des zones de fort contraste.

**Absorption -** Atténuation d'une onde radio due à la dissipation de son énergie, convertie sous une autre forme, généralement en chaleur.

En FTTH, c'est une des composantes de l'atténuation linéique d'une fibre. Phénomène de diminution de l'intensité lumineuse dans le coeur de la fibre plus ou moins important selon la longueur d'onde utilisée, dû à la présence d'impuretés ou d'ions OH- ( traces d'humidité ).

**AC -** Autorité de Certification - Appelée aussi PSC, Prestataire de Services de Certification - Organisme chargé de délivrer les certificats numériques qui garantiront l'identité des utilisateurs au cours des échanges de clés publiques et privées.

**AC3 -** Dolby digital - Système de codage/décodage pour le son, qui utilise six canaux séparés dans un seul flux.

**Accès de base -** Désigne le raccordement élémentaire au RNIS (Numéris), procurant deux canaux à 64 Kbps (canaux B) et un canal de signalisation à 16 Kbps (canal D). L'interface de ce raccordement est définie par la norme S0 du CCITT. En anglais BRI pour Basic Rate Interface.

**Accès Hertzien -** Liaison assurée par voie radioélectrique entre un terminal de télécommunication et un commutateur du réseau d'infrastructure et par extension, ensemble de telles liaisons.

On peut distinguer, selon la nature du terminal :

- l'accès hertzien fixe (terminal en un point fixe déterminé)
- l'accès hertzien mobile (terminal mobile)
- l'accès hertzien nomade ou itinérant (terminable transportable)

**Accès Mobile à Internet -** Service d'accès à l'internet par l'intermédiaire d'un réseau de radiocommunication avec les mobiles. Cet accès nécessite un protocole spécifique dérivé des protocoles usuels de l'internet. Un de ces protocoles spécifiques est appelé WAP, sigle de l'expression anglaise "Wireless Application Protocol". Un autre de ces protocoles est dénommé I-Mode.

**Accès multiple -** Multiple Access - Technique permettant à plusieurs équipements d'accéder à une ressource commune partagée :

- Selon une technique de répartition dans le temps (AMRT ou TDMA: time division ...)
- Selon une technique de répartition en fréquences (AMRF ou FDMA: frequency division ...)
- Par détection de porteuse (CSMA/CD)

**Accès primaire -** Interface S2 du RNIS (Numéris) procurant trente canaux B à 64 Kbps et un canal D de signalisation à 64 Kbps en Europe (plus un canal de synchronisation). En anglais PRI pour Primary Rate Interface. Aux états unis, un accès primaire comporte seulement 23 canaux à 64 kbits (plus 2 canaux : 1 signalisation, l'autre synchronisation) pour une liaison d'une capacité totale de 1544 Kbits/seconde.

**ACD -** Automatic Call Distributor - Distributeur automatique d'appel. Equipement permettant d'affecter sur un autocommutateur des appels téléphoniques entrants ou sortants sur différentes lignes selon un plan programmé. Utilisé par les services émettant ou recevant de grandes quantités d'appels (compagnies de taxi, réservation, services après-vente...). L'ACD peut être intégré à l'autocommutateur ou séparé. L'ACD gère le flux et la disponibilité des équipes d'opérateurs dans le cadre d'opérations de vente et service par correspondance.

**ACF -** Advanced Communication Function - Logiciel de contrôle des communications IBM dans une architecture SNA.

**Acheminement -** Synonyme de routage. Détermination des chemins de données à travers les nœuds d'un réseau. Détermination de la route (ou chemin) à suivre pour la transmission d'un message dans un réseau ou l'établissement d'un appel.

Ne pas confondre Acheminement et Routage.

**ACL -** Access Control List - Liste de contrôle d'accès - Liste (des personnes, des protocoles, des fonctions, …) ayant le droit ou l'interdiction d'accéder à une ressource (un fichier, un réseau ...), et parfois à quelles conditions.

**ACL -** Affichage à Cristaux Liquides - Traduction de l'anglais LCD = Liquide Crystal Display. Ces afficheurs à la faible consommation énergétique sont utilisés pour visualiser l'état de "service" de multiples équipements.

**Acquittement -** Accusé de réception positif dans une procédure de transmission.

**ACR -** Atténuation Crosstalk Ratio - Valeur qui définit le rapport Signal/bruit. Affaiblissement ou Atténuation d'amplitude d'un signal qui se propage le long d'un câble. L'atténuation se mesure en dB (0 dB = pas d'atténuation) par unité de longueur. L'atténuation (ou affaiblissement) augmente en fonction de la longueur d'un câble et de la fréquence du signal.

**ACS -** Advanced Access Content System - Système de gestion des droits numériques basé sur une norme de cryptage avec des clefs de 128 bits et utilisé par les lecteurs HD-DVD et Blu-Ray.

**Acte -** Approval Committe for Telecommunications Equipment - Organisme réglementaire en cours de mise en place dans le cadre de la Communauté européenne. Selon de nouvelles directives européennes en préparation, il émettra des CTR (Common Technical Regulations), normes à la fois techniques et commerciales pour l'accès à des réseaux, s'appliquant de manière "obligatoire" aux pays de la CEE.

Comité présidé par la Commission européenne chargé de l'application de la directive relative aux équipements terminaux (98/13/CE) à travers l'élaboration des normes techniques communes pour l'accès aux réseaux (CTR).

**Activation -** Processus d'enregistrement d'un client pour l'attribution d'un numéro de téléphone, l'établissement d'un compte de facturation, la mise en service d'une carte SIM et d'un terminal.

**ActiveX -** Réponse de Microsoft à JavaScript - Un contrôle ActiveX est une application enrichissant une page internet de fonctions complexes exécutables seulement sur un micro fonctionnant avec Windows.

**Adaptateur -** Carte apportant à un ordinateur des fonctions de communication en réseau. Egalement appelé carte d'interface réseau ou coupleur.

**Adaptateur de ligne -** Dispositif assurant la mise en conformité des informations émises par l'émetteur aux caractéristiques de la ligne de transmission et réciproquement.

**ADMD -** ADministrative Management Domain - Ensemble du domaine, au sens informatique du terme, géré par une autorité publique dans le cadre de la norme de messagerie électronique X400.

**Administration de réseaux -** Technique de contrôle et de gestion d'un réseau, permettant d'avoir une vue plus ou moins synthétique du fonctionnement complet d'un réseau. L'objectif peut aller de la centralisation d'alarmes à la gestion des données d'exploitation, de performances, de changements de configuration jusqu'à des données de planification à long terme. L'administration de réseau est un outil qui doit assurer l'exploitation du réseau (intervention en cas de panne, configuration de secours et surveillance), mesurer les performances et superviser les changements d'architecture et de coûts. La plupart des administrations de réseaux sont dédiées aux fournisseurs de produits réseaux locaux, elles sont néanmoins basées sur deux standards qui se dégagent à l'heure actuelle :

- SNMP -Simple Network Management Protocol - Apparu aux Etats Unis en 1988 sur les réseaux Ethernet sous le protocole TCP/IP - son rôle est de collecter et d'échanger les données entre les éléments et agents du réseau et des consoles de supervision. Ce protocole permet d'alimenter une base de données de type MIB (Management Information Base), base où sont définis les paramètres des éléments à gérer (trafic et table de routage). Ce protocole est maintenant généralisé à l'ensemble des supports physiques (Ethernet, Token Ring et Transfix) et est utilisé ou supporté par la plupart des constructeurs (Cisco, Digital, Wellfleet, IBM ...),
- CMIP - Common Management Information Protocol - Définit un ensemble de services communs situés dans la couche Application qui fournit les moyens d'établir et de libérer une association entre deux "system management" et divers outils les autorisant à échanger leurs données administratives.

**ADN -** Acide DésoxyriboNucléique - Ca n'a rien à faire ici mais j'aime bien cette définition ☺

**ADPCM -** Adaptive Pulse Code Modulation - Voir MICDA.

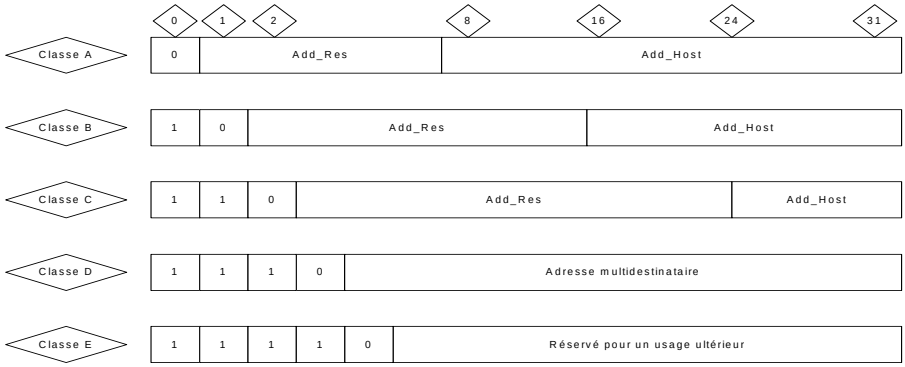
**Adresse -** Address - En informatique : ensemble de bits ou de caractères qui indique la destination d'une communication ou d'une donnée (trame, paquet, message...) En télécommunications : ensemble des chiffres qui, en un point d'un réseau de télécommunication, détermine l'extrémité demandée.

**Adresse MAC -** Adresse Medium Access Control - Adresse unique sur 6 octets (48 bits) qui identifie une carte réseau. Cette adresse unique est représentée en notation hexadicimale. Chaque coupleur de réseau installé dans un ordinateur possède une adresse unique au monde. Elle est gravée en dur dans la carte. Elle peut être considérée comme l'équivalent du numéro de téléphone d'une personne. Certaines technologies de réseau incluaient la numérotation sur un octet de la carte (système Arcnet de Novell), ces technologies ne sont plus d'actualité.

Adresse matérielle affectée à la carte d'interface réseau Ethernet au moment de sa fabrication. Il s'agit d'un numéro unique de 48 bits (soit 248 -1 adresses possibles).

**Adresse TCP IP V4 -** Adresse sur 32 bits comportant 5 classes :

Seules les 3 premières sont utilisées pour constituer un plan d'adressage, selon le format ci-après:




En notation décimale, les plages d'adresses IP possibles pour chacune des classes d'adresses sont les suivantes (certaines valeurs n'apparaissent pas car elles sont réservées à des usages particuliers):

| Classe | Adresses les + basses | Adresse les + hautes |
|---|---|---|
| Classe A ➔ | 0.1.0.0 | 126.0.0.0 |
| Classe B ➔ | 128.0.0.0 | 191.255.0.0 |
| Classe C ➔ | 192.0.1.0 | 223.255.255.0 |
| Classe D ➔ | 224.0.0.0 | 239.255.255.255 |
| Classe E ➔ | 240.0.0.0 | 247.255.255.255 |

Adresse de rebouclage = 127.0.0.1 (adresse de classe A) Cette adresse est réservée à ce que l'on appelle un rebouclage (loopback Interne).

**ADSL -** Asymmetric Digital Subscriber Line ou réseau de raccordement numérique asymétrique - l'ADSL fait partie des technologies xDSL qui permettent d'améliorer les performances des réseaux d'accès et en particulier de la ligne d'abonné du réseau téléphonique classique, constituée de fils de cuivre. Grâce à l'utilisation de deux modems, l'un placé chez l'abonné, l'autre sur la ligne d'abonné, devant le répartiteur principal, il permet d'améliorer considérablement le débit du réseau et d'obtenir des transmissions 70 fois plus rapides qu'avec un modem analogique classique. Le principe de l'ADSL consiste à réserver une partie de la bande passante au transport de la voix, une autre au transport des données circulant en direction du cœur de réseau (données montantes) et une troisième, plus importante au transport des données circulant vers l'abonné (données descendantes). Pour la restitution correcte de la voix, des filtres situés à chaque extrémité de la ligne éliminent les parties du signal inutiles. La technologie ADSL est particulièrement bien adaptée aux liaisons de boucle locale puisque le débit qu'elle permet diminue avec la longueur de la ligne. En raison de son faible coût, elle constitue une solution intéressante pour bénéficier d'un accès rapide à Internet.


La technologie ADSL permet de transformer une ligne téléphonique ordinaire existante en ligne de transmission de données numériques à

haut débit en utilisant la partie haute de ces fréquences. Les principes de base d'ADSL ont été définis dès la fin des années soixante dix au Cnet, mais cette technologie n'a vraiment été utilisée qu'au début des années 90. En pratique ADSL numérise la partie terminale de la ligne téléphonique et donne accès à un flux de données à haut débit tout en laissant disponible la ligne téléphonique. Lorsqu'on téléphone, la voix utilise à peine 10 % de la bande de fréquence disponible dans les fils de cuivre des lignes téléphoniques.

L'ADSL exploite les 90 % restants pour transporter les données à grande vitesse. Elle utilise les bandes supra vocales d'une ligne téléphonique de type analogique. Pour que la ligne téléphonique soit le support de la technologie ADSL, il faut utiliser un modem ADSL, seul équipement permettant de transformer la ligne téléphonique existante en ligne de transmission numérique à haut débit. Un modem standard peut continuer à fonctionner à côté pour un télécopieur, un téléphone ou un Minitel.

Par multiplexage la liaison téléphonique entre l'abonné et le central de l'opérateur est divisée en trois canaux

• un canal destiné au transport des données en provenance d'Internet. Les données circulent à une vitesse maximale théorique de 8 Mbit/s

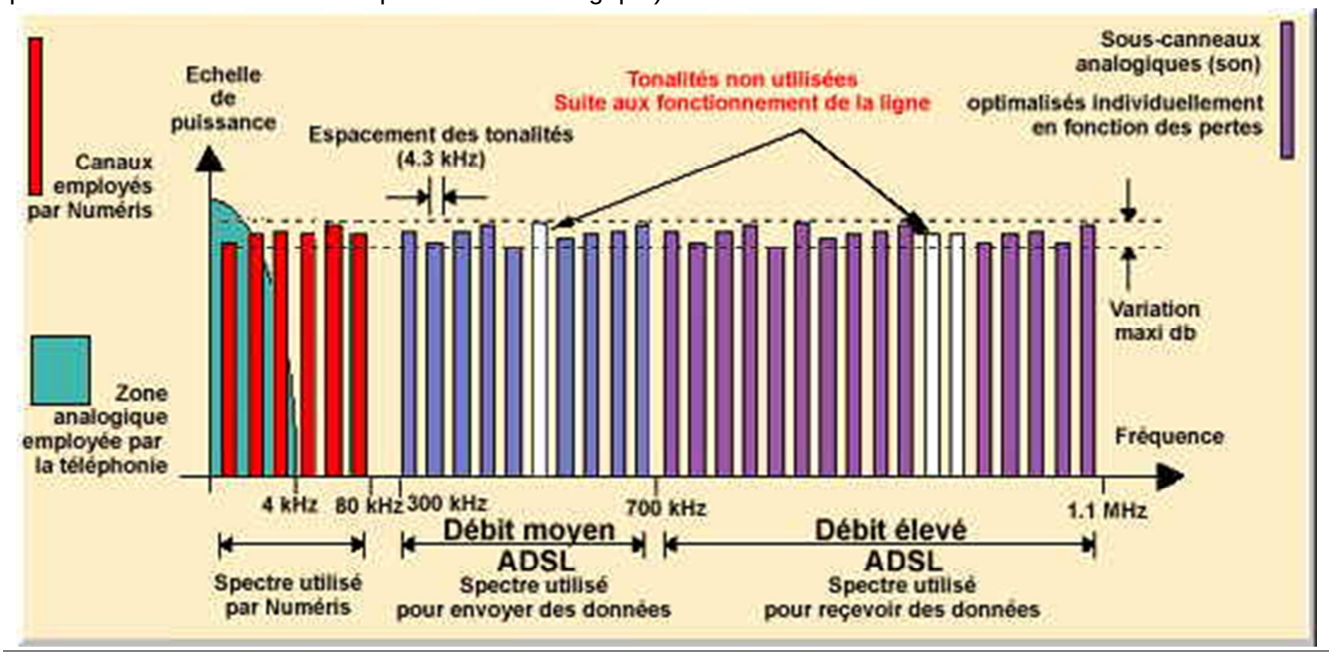
• un canal bidirectionnel entre l'abonné et Internet sur lequel la vitesse est limitée à 800 Kbit/s

• un troisième canal plus petit qui est réservé à la voix.

Pour créer ces canaux, des modifications sont apportées aux extrémités des lignes téléphoniques. Des filtres, posés chez l'abonné, permettent de séparer les données de la voix. Côté central téléphonique, sont installés des multiplexeurs DSLAM (DSL Access Multiplexer) qui aiguillent les données vers de gros serveurs BAS (Broadcast Access Server).

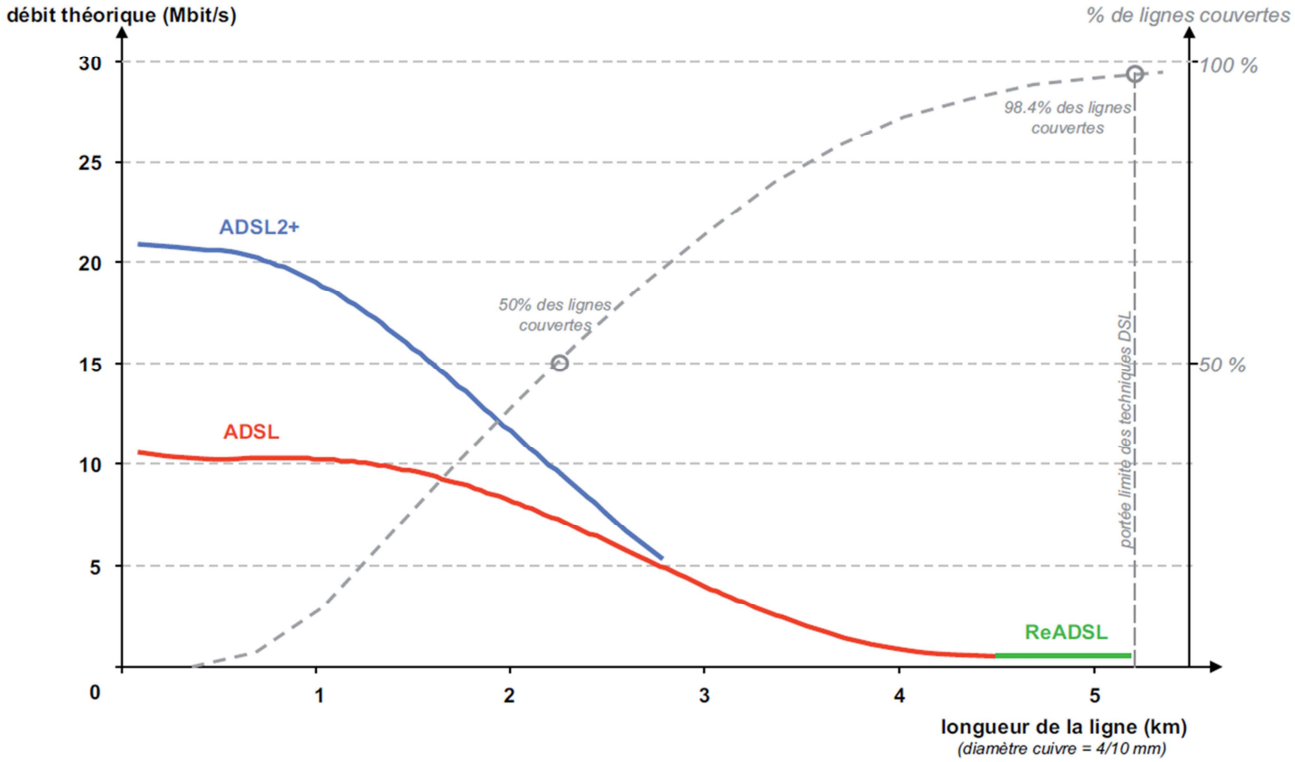
SDSL, version à débit symétrique (Symmetric Digital Subscriber Line ou réseau de raccordement numérique à débit symétrique), s'adressera en priorité aux entreprises. Les débits varient de 192 Kbits/sec. à 2,3 Mbits/sec. La distance entre le central et le boîtier SDSL pourra atteindre 7 km alors que l'ADSL est limité à 4,5 km.

L'ADSL utilise une bande de fréquence comprise entre 20 kHz et 1,1 MHz sur la paire de cuivre, libérant la bande 0-4 kHz de la voix analogique. Le SDSL est appliqué dès 0 kHz et au-delà de 1,1 MHz (une seconde paire dont donc être raccordée pour la voix analogique).



**ADSL 2+ -** Variante de l'ADSL utilisant un spectre de fréquence deux fois plus élevé (jusqu'à une fréquence de 2,2 MHz, contre 1,1 MHz pour l'ADSL), permettant de doubler la bande passante pour une ligne. Le signal s'atténue rapidement, en fonction de la longueur de la ligne et de sa qualité. Le débit initial de 25 Mbit/seconde chute à 3Mbit/seconde pour une distance de 2300 mètres.

Là où l'ADSL poussait jusqu'à 8 Mbits/s en voie descendante, l'ADSL 2+ est ainsi capable d'afficher une bande passante de 25 Mbits/s. En voie montante, on passe de 1 Mbit/s au maximum à 2 Mbits/s. En théorie.




Connue sous le nom d'ADSL 2+, la norme G.992.5 a été adoptée par l'ITU en janvier 2003. Comme tous les procédés xDSL, le débit s'affaiblit en proportion de la distance parcourue. Reste que, à deux kilomètres du central (cas de la majorité des foyers des grandes villes), le débit est encore d'environ 5 Mbits/s. Et de 2 Mbits/s à quatre kilomètres, ce qui permet d'élargir la cible potentielle des raccordables au haut débit. En outre,l'ADSL 2+ est plus résistant aux perturbations extérieures que son prédécesseur. En termes de débit ascendant, la différence est plus faible : 1,2 Mbit/s contre 1 Mbit/s.

**AES -** Advanced Encryption Standard - Système (Algorithme) de cryptage ou de chiffrement approuvé par le gouvernement américain en mai 2002 pour remplacer DES et à terme 3DES. Ce système répond aux besoins des sociétés dont l'information à protéger est particulièrement sensible. Certains systèmes proposent sur les réseaux ce mode de cryptage encore plus sécurisé qui répond aux besoins des sociétés dont l'information à protéger est particulièrement sensible.

**AFA -** Association des Fournisseurs d'Accès à Internet.

**Affaiblissement -** Terme général utilisé pour indiquer la perte de puissance d'un point à un autre, un affaiblissement s'exprime en dB par unité de longueur. Attention, l'échelle utilisée est logarithmique, une augmentation de 3 dB correspond au double de la valeur précédente.

On utilise aussi le terme pour caractériser une perte d'amplitude du signal à travers les lignes et les équipements de transmission.

C'est un terme quantitatif qualifiant l'affaiblissement d'une ligne selon divers facteurs comme la longueur de la ligne, la section du cable utilisé (4/10e ou 6/10e), la qualité de cablage, les réflexions, etc...

En Optique, c'est un phénomène physique par lequel la puissance des signaux propagés sur un support diminue. Lors de la propagation d'un signal sur fibre optique, la distance parcourue, les soudures, les connecteurs ou les irrégularités placées sur le parcours de la lumière sont, par exemple, des facteurs d'affaiblissement du signal.

Dans une fibre optique on constate que toute l'énergie lumineuse entrante n'est pas récupérée en sortie. Il y a des phénomènes de dispersion, causes de perte atténuation).

Maitriser les phénomènes d'affaiblissement permet de dimensionner :

- Le réseau (longueur, points de flexibilité, typologie, architecture…)
- Les équipements actifs (puissance d'émission, longueurs d'ondes…)
- Les équipements passifs (type de coupleur…)

Inversement, le signal transmis dans une fibre optique DOIT être atténué sans quoi le récepteur risque d'être « saturé ». Au même titre que l'œil humain ne doit pas regarder le soleil, le récepteur d'une liaison optique doit recevoir un signal dont l'intensité est « compatible ».

Toute transmission de signal est soumise à un phénomène d'affaiblissement .

Les termes « Perte », « Affaiblissement » et « atténuation » peuvent être communément utilisés pour caractériser une liaison.

Les pertes ou affaiblissements ou encore atténuation caractérisent un phénomène.

L'atténuation peut être recherchée pour éviter la saturation d'un récepteur.

L'affaiblissement « α » est la différence de puissance du signal lumineux entre deux points (connecteurs, épissures, défauts, longueur de fibre ...).

L'affaiblissement qui s'exprime en dB est calculée selon l'équation :

$$\alpha = 10 \log^{10} (P \text{ entrée } ( \text{ ou } P1 ) / P \text{ sortie } ( P0 )).$$

**Affaiblissement de Réflexion -** Return-loss - En FTTH - Partie de l'énergie lumineuse réfléchie vers la source lors du passage d'un dioptre (Réflexions de Fresnel). Suivant la nature de l'émetteur on peut assister à une dégradation du signal émis.

**Affaiblissement Linéique -** En FTTH - Affaiblissement d'une fibre ramené à une unité de longueur. L'affaiblissement linéique s'exprime en dB/km.

**Affaiblissement Spectral -** En FTTH - Affaiblissement d'une fibre dépendant de la longueur d'onde utilisée. Exemple: 3 dB/km à 850 nm & 1 dB/km à 1300 nm pour la même fibre.

**AFNIC -** Association Française pour le Nommage et la Coopération - Association à but non lucratif, créée en décembre 1997 par la volonté conjointe de l'INRIA et de l'état français, représenté par les ministères chargés des télécommunications, de l'industrie et de la recherche.

L'AFNIC a repris les activités du NIC-France / INRIA le 1er janvier 1998 pour mieux associer tous les acteurs d'Internet, publics ou privés, à son action et avoir une souplesse de gestion qu'un établissement de recherche ne permettait pas.

Les missions de l'AFNIC sont :

- L'établissement d'un plan de dénomination ou nommage de la zone ".fr ", conformément à la loi française,
- La mise en oeuvre du plan de nommage et la diffusion des informations sur le nommage,
- L'exploitation de serveurs de noms d'accès à l'Internet pour la zone ".fr ",
- Le transfert, au plan national et international, des connaissances et du savoir-faire acquis.

L'AFNIC est le lieu d'enregistrement des noms de domaine de la zone .fr, et dans ce cadre, ses seuls interlocuteurs sont les fournisseurs d'accès Internet (FAI) qui en sont membres. Il en découle donc que tout individu ou toute organisation souhaitant déposer un nom de domaine dans la zone .fr doit impérativement s'adresser à un fournisseur d'accès Internet (FAI) membre de l'AFNIC. Une fois choisi, le fournisseur d'accès aidera à déterminer le nom de domaine de façon à être en conformité avec la charte de nommage. Il transmettra à l'AFNIC les documents nécessaires pour l'enregistrement du nom de domaine : responsable administratif, responsable technique et délégué de la zone, ainsi que leurs coordonnées complètes.

**AFNOR -** Association Française de NORmalisation - Institution française responsable de la normalisation, elle est membre de l'ISO (International Standard Organisation). Fondée en 1926, L'AFNOR est une association loi 1901 reconnue d'utilité publique et regroupant environ 5500 membres. Branche française du CEN (Comité européen de normalisation), elle représente la France à l'ISO (Organisation internationale de normalisation). Ses ressources proviennent pour 30% environ de subventions, pour 10% des cotisations de ses membres et pour 60% de ses propres activités (publications, ...). L'AFNOR a le monopole de la normalisation en France.

**AFTEL -** Association Française de TELématique.

**AFUTT -** Association Française des Utilisateurs du Téléphone et des Télécommunications.

**Agence Nationale des Fréquences (ANFR) -** Agence qui a pour mission de gérer le spectre hertzien, de répartir les fréquences entre différents organismes et administrations affectataires (l'Autorité, le CSA, le ministère de la défense etc.), de traiter les brouillages et de conduire les négociations internationales sur les fréquences.

Assure la planification, la gestion, le contrôle de l'utilisation, y compris privative, du domaine public des fréquences radioélectriques. Elle coordonne l'implantation sur le territoire national des stations radioélectriques de toutes natures.

**Agent -** Ressource, généralement logicielle, qui rend un service à distance.

**Agent (snmp) -** Programme installé au sein des équipements connectés au réseau. L'agent échange des informations de gestion de réseaux avec le Manager, au travers de messages appelés PDU (Protocol Data Unit). Il répond aussi aux requêtes (Get) que lui envoie le Manager et peut alerter ce dernier (Trap) d'un événement ponctuel afférant à l'équipement sur lequel il se trouve.

**Agent de transfert de message -** Message Transfer Agent - MTA - Entité qui selon la norme de messagerie X400 assure l'acheminement des messages.

**Agent utilisateur -** User Agent - UA - Entité qui selon la norme de messagerie X 400, assure les fonctions d'interface, de transfert et de stockage des messages destinés à (ou émanant de) l'utilisateur.

**Agora -** Espace dont la fréquentation importante par le public justifie la mise à disposition de services radioélectriques temporaires ou permanents.

**AIFF -** Audio Interchange File Format - Format de fichier vidéo ou Audio Interchange Format File - Format de fichier son d'origine Apple.

**Algorithme -** Suite d'opérations appliquées systématiquement à des données. On utilise un algorithme pour trier des données, les encoder, les crypter.

**Algorithme bayesien -** (anti-spam) - Algorithme fonctionnel qui n'essaye pas de comprendre le message ou son contenu, mais qui effectue des statistiques pures sur des "jetons". Le texte est en fait discrétisé en jetons. Le théorème de Bayes donne une table de probabilités associées à chacun de ces tokens. C'est en se basant sur les jetons les plus lourds qu'est calculée la probabilité qu'un mail soit du spam ou non. Il permet de faire de l'analyse comportementale sur les habitudes de l'utilisateur. Trop lié au profil de lecture de l'utilisateur, il est par conséquent moins efficace au niveau d'une passerelle. Egalement sensible aux méthodes de destruction "virales" de la base de connaissance locale que pourraient "inventer" les spammeurs.

**Algorithme neuronal -** (anti-spam) - Il a été créé pour diminuer, voire éviter la "fausse positive". C'est un apprentissage automatique du "nouveau spam". On l'utilise dans des offres sous forme de services, car ce sont les seules qui possèdent des bases de taille pour recueillir l'ensemble des mails et effectuer le travail nécessaire dessus. Tout comme les systèmes anti viraux, il faut mettre à jour la passerelle régulièrement avec des méthodes constamment perfectionnées. Les mises à jour fréquentes alourdissent le fonctionnement, et une lenteur d'exécution générale est souvent constatée.

**Alias -** Entrée qui pointe vers une autre entrée. Utilisé dans les services de messagerie électronique, les alias permettent de rediriger un flux de messages adressé à destination de cet alias vers l'entrée "camouflée".

**Alimentation en Energie -** Les sources d'alimentation en énergie des matériels réseaux doivent respecter notamment les contraintes suivantes, et devront être conformes aux spécifications de la norme NF-C-15100 (règles d'installations électriques à basse tension) sans que la liste ci-dessous supplante le strict respect à minima des exigences règlementaires (dont en particulier la norme NF-C-15100) :

- Alimentation dont la source est un onduleur avec secours batteries pour les matériels dont le fonctionnement est nécessaire pour ne pas perdre une information et/ou son stockage permettant de la récupérer.
- On admet que les matériels du type écrans, imprimantes, console système et autres (à définir) puissent être alimentés par des alimentations de type Eclairage / Prise de courant (dont la source n'est pas un onduleur avec secours batteries) dès lors que ce matériel n'est pas nécessaire pour ne pas perdre une information et/ou son stockage permettant de la récupérer (même si la récupération d'informations stockées nécessite la remise sous tension de matériels de ce type).
- Le régime de neutre entre les différents circuits de distribution électrique de chaque site sera relevé par le fournisseur qui s'engage à respecter ce régime de neutre, quel qu'il soit, sur chaque site.

- L'autonomie minimale des batteries de secours de l'onduleur choisi doit être égale à l'autonomie des batteries de l'onduleur utilisé comme source d'alimentation des calculateurs ou des salles informatiques.
- L'installation électrique devra être équipée d'un "by-pass" réseau, par opération manuelle.
- Le raccordement des armoires et matériels aux dispositifs de Mise à la Terre existants dans le local après contrôle ce celle-ci.
- Les protections électriques (disjoncteurs, fusibles) utilisées et/ou fournies pour les matériels seront dimensionnées selon des justifications techniques décrites dans un document d'étude établi et diffusé par le constructeur, accompagné des calibres et des courbes de déclenchement de ces protections, avec démonstrations des sélectivités de ces protections. Ces justifications doivent être basées, entre autres, sur des mesures réelles des courants transitoires (de mise sous tension) et des courants nominaux des matériels alimentés.

**Alphabet -** Tableau de correspondance entre un ensemble conventionnel de caractères et les signaux ou séquence de symboles qui représentent ces caractères.

**Alphamosaïque -** Alphamosaic - Mode de représentation d'une image à l'aide de carrés élémentaires juxtaposés à l'intérieur d'un rectangle, chaque carré contenant soit un caractère alphabétique, soit un caractère semi-graphique.

La norme française de vidéotex, Antiope, est une norme alphamosaïque : chaque caractère alphabétique ou mosaïque est inscrit dans une matrice de 8 colonnes sur 10 lignes.

**Alphanumérique -** Désigne un code comportant l'ensemble des lettres de l'alphabet, les chiffres et un certain nombre de symboles de ponctuation.

**Alphapage -** Service de radiomessagerie - Un récepteur portable muni d'un écran à cristaux liquides permettait à des personnes en déplacement de recevoir des messages courts (sonores ou alphanumériques) de 40 à 80 caractères envoyés à partir d'un poste téléphonique ou d'un Minitel.

**Alternat -** half-duplex - Se dit d'une liaison bidirectionnelle où les deux interlocuteurs empruntent chacun à leur tour le canal de transmission. Transmission des informations entre deux points alternativement dans un sens puis dans l'autre. Voir simplex. Attention : on emploie parfois, à tort, le terme semi-duplex.

**ALU -** Arithmetic Logic Unit - Unité arithmétique et logique.

**AM -** Application Management - Equivalent de "T.M.A." - Service consistant pour une S.S.I.I. à prendre en charge la responsabilité complète de la gestion d'une ou plusieurs applications du système d'information de son client.

**AME -** Partie centrale d'un conducteur dans le cadre d'un câble ou d'une fibre optique. Monobrin (fil unique) ou multibrins.

**AMPS -** Advanced Mobile Phone Service (AMPS). Norme (et technologie) de transmission analogique mobile mise en place dans les années1980 aux Etats-Unis et au Canada. L'AMPS fonctionne à 800 MHz.

**AMR -** Adaptive Multi-Rate - Codec de voix utilisé dans les téléphones mobiles de troisième génération (3G). Ce codec offre huit taux différents de transmission allant de 12.2 kbps à 4.74 kbps, et qui peuvent être variés d'une manière dynamique toutes les 20 msec.

Spécifications :

- Full Rate Speech Processing Functions - Introduit les fonctions de codage de la parole plein débit et les Spécifications qui le définissent au sein de la série 06.
- Half Rate Speech Processing Functions - Introduit les fonctions de codage de la parole demi-débit et les Spécifications qui le définissent au sein de la série 06.
- Half-rate speech: ANSI-C code for GSM half-rate speech codec - Contient (sur une disquette formattée pour un PC) le code source en C simulant le codeur de parole demi-débit.
- Half Rate Speech: Test Sequence for GSM Half Rate Speech Codec - Contient (sur 2 disquettes formattées pour un PC) des séquences de test permettant de vérifier le bon fonctionnement d'un codeur de parole GSM demi-débit.
- Half Rate Speech; Performance Characterization of the GSM Half Rate speech codec - Donne les tests de caractérisation et de vérification effectués pendant les phases de sélection et d'optimisation du codeur de parole demi-débit, ainsi que leurs résultats.
- Full-rate speech transcoding - Spécifie au bit près l'algorithme de conversion de la parole entre un format PCM de loi uniforme avec des échantillons de 13 bits et le codage plein débit constitué de blocs de 260 bits toutes les 20 ms.
- Substitution and Muting of Lost Frames for Full Rate Speech Channels - Spécifie la façon dont les portions manquantes du flux de parole codé à 13 kbit/s doivent être regénérées.
- Comfort Noise Aspects for Full Rate Speech Traffic Channels - Spécifie la façon dont le bruit de fond doit être évalué et les informations correspondantes transmises afin de permettre sa regénération en l'absence de parole plein débit.
- Half Rate Speech Transcoding - Spécifie au bit près l'algorithme de conversion de la parole entre un format

PCM de loi uniforme avec des échantillons de 13 bits et le codage demi débit constitué de blocs de 112 bits toutes les 20 ms.

- Half rate speech; Substitution and muting of lost frames for half rate speech traffic channels - Spécifie la façon dont les portions manquantes du flux de parole codé à 5.6 kbit/s doivent être regénérées.
- Comfort Noise Aspects for Half Rate Speech Traffic Channels - Spécifie la façon dont le bruit de fond doit être évalué et les informations correspondantes transmises afin de permettre sa regénération en l'absence de parole demi débit.
- Discontinuous Transmission (DTX) for Full Rate Speech Traffic Channels - Spécifie comment réduire la quantité d'informations à transmettre lorsqu'aucun signal de parole utile n'a a être transmis par la station mobile ou le réseau (pour le codage plein débit).
- Voice Activity Detection (VAD) - Spécifie (au bit près) l'algorithme utilisé pour détecter la présence de parole à la sortie du codeur de parole plein débit, dans le but de mettre en oeuvre les mécanismes de transmission discontinue décrits dans la spécification 06.31.
- Discontinuous Transmission (DTX) for Half Rate Speech Traffic Channels - Spécifie comment réduire la quantité d'informations à transmettre lorsqu'aucun signal de parole utile n'a a être transmis par la station mobile ou le réseau (pour le codage demi débit).
- Voice Activity Detection (VAD) for Half Rate Speech Traffic Channels - Spécifie (au bit près) l'algorithme utilisé pour détecter la présence de parole à la sortie du codeur de parole demi débit, dans le but de mettre en oeuvre les mécanismes de transmission discontinue décrits dans la spécification 06.41.
- GSM Enhanced full rate speech processing functions: General description - Introduit les fonctions de codage de la parole plein débit amélioré et les Spécifications qui le définissent au sein de la série 06.6x et 06.8x.
- ANSI-C code for the GSM Enhanced full rate speech codec - Contient (sur une disquette formattée pour un PC) le code source en C simulant le codeur de parole plein-débit amélioré.
- Test sequences for the GSM Enhanced Full Rate (EFR) - Contient (sur des disquettes formattées pour un PC) des séquences de test permettant de vérifier le bon fonctionnement d'un codeur de parole GSM plein débit amélioré.
- Performance characterisation of the GSM EFR Speech Codec - Donne les tests de caractérisation et de vérification effectués pendant les phases de sélection et d'optimisation du codeur de parole plein débit amélioré, ainsi que leurs résultats.
- Enhanced full rate speech transcoding - Spécifie au bit près l'algorithme de conversion de la parole entre un format PCM de loi uniforme avec des échantillons de 13 bits et le codage plein débit amélioré constitué de blocs de 244 bits toutes les 20 ms.
- Substitution and muting of lost frames for encanced full rate speech traffic channels - Spécifie la façon dont les portions manquantes du flux de parole codé avec le codage de parole plein débit amélioré doivent être regénérées.
- Comfort noise aspects for Enhanced Full Rate (EFR) speech traffic channels - Spécifie la façon dont le bruit de fond doit être évalué et les informations correspondantes transmises afin de permettre sa regénération en l'absence de parole en codage plein débit amélioré.
- AMR speech Codec; General description - Introduit les fonctions de codage adaptatif multi-débit (AMR) de la parole et les Spécifications qui le définissent au sein de la série 06.
- AMR speech Codec; C-source code - Contient le code source en C simulant le codeur de parole adaptatif multi-débit.
- AMR speech Codec; Test sequences - Liste les séquences de test permettant de vérifier le bon fonctionnement du codeur de parole adaptatif à débit variable.
- Performance Characterization of the GSM Adaptive Multi-Rate (AMR) speech codec - Donne les tests de caractérisation et de vérification effectués pendant les phases de sélection et d'optimisation du codeur de parole adaptatif à débit variable, ainsi que leurs résultats.
- Adaptive Multi-Rate (AMR) speech codec; Study phase report - Résume les résultats de l'étude de faisabilité technique d'un codeur de parole multi-débits, donne les avantages d'une telle technique et indique les contraintes imposées pour son développement.
- Minimum performance requirements for noise suppresser application to the Adaptive Multi-Rate (AMR) speech encoder - Recommande des performances minimales pour les algorithmes de suppression de bruit utilisés avec le codeur de parole multi-débits AMR, et dont le but est de favoriser le signal de parole relativement au bruit ambiant à l'entrée du codeur de parole.
- Results of the AMR noise suppression selection phase - Donne les données de performance de plusieurs algorithmes de suppression de bruit ambiant proposés en tant qu'exemples pour utilisation avec le codeur de parole multi-débit AMR. Liste les résultats des tests expérimentaux faits avec différents types de bruits de fond ainsi que des évaluations de complexité et de temps de traitement.
- Discontinuous Transmission (DTX) for encanced full rate speech traffic channels - Spécifie comment réduire la quantité d'informations à transmettre lorsqu'aucun signal de parole utile n'a a être transmis par la station mobile ou le réseau (pour le codage plein débit amélioré).
- Voice Activity Detection (VAD) for encanced full rate speech traffic channels - Spécifie (au bit près)

l'algorithme utilisé pour détecter la présence de parole à la sortie du codeur de parole plein débit amélioré, dans le but de mettre en oeuvre les mécanismes de transmission discontinue décrits dans la spécification 06.81.

- Subjective tests on the interoperability of the HR/FR/EFR speech codecs; single, tandem and tandem free operation - Donne les résultats de tests subjectifs d'écoute visant à évaluer la qualité résultant de différentes combinaisons utilisant les codeurs de parole GSM.
- AMR speech Codec; Transcoding Functions - Spécifie au bit près l'algorithme de conversion de la parole entre un format PCM de loi uniforme avec des échantillons de 13 bits et le codage de parole adaptatif multi-débit (AMR) dans ses différents modes allant de 4.75 à 12.2 kbit/s.
- AMR speech Codec; Error concealment of lost frames - Spécifie la façon dont les portions manquantes du flux de parole codé dans l'un des modes du codage adaptatif multi-débit (AMR) doivent être regénérées.
- AMR speech Codec; comfort noise for AMR Speech Traffic Channels - Spécifie la façon dont le bruit de fond doit être évalué et les informations correspondantes transmises afin de permettre sa regénération en l'absence de parole lorsque celle-ci est codée dans l'un des modes du codage adaptatif multi-débit (AMR).
- AMR speech Codec; Source Controlled Rate operation - Spécifie comment réduire la quantité d'informations à transmettre lorsqu'aucun signal de parole utile n'a a être transmis par la station mobile ou le réseau (pour le codage adaptatif multi-débit AMR).
- AMR Speech Codec; Voice Activity Detector for AMR Speech Traffic Channels - Spécifie (au bit près) l'algorithme utilisé pour détecter la présence de parole à la sortie du codeur de parole adaptatif multi-débit (AMR), dans le but de mettre en oeuvre les mécanismes de transmission discontinue décrits dans la spécification GSM 06.93.

**AMRC -** L'Accès Multiple à Répartition de Code (AMRC) est l'une des nombreuses méthodes de transmission numérique mobile dans laquelle les signaux sont codés à l'aide d'une séquence pseudo aléatoire (qui correspond à une voie de communication différente) qui est connue également du récepteur et qu'il peut utiliser pour décoder le signal reçu. L'AMRC est l'une des multiples techniques "à large spectre". Elle offre des améliorations par rapport à la transmission analogique en termes de réduction des appels interrompus, de préservation de l'alimentation des batteries, de fiabilité de transmission et de meilleures options de services.

Le principe de cette méthode d'accès est l'allocation de canal par durée et non par paquet, ceci en utilisant un code identifiant chacune des stations du système de communication. En effet, les stations peuvent alors utiliser la totalité de la bande passante, le code qui leur est affecté permet de dissocier les données qu'elles envoient de celles des autres stations. Pour illustrer cette méthode, prenons l'exemple d'une foule de personnes qui sont en conversation. Si nous écoutons de façon générale les conversations, il ne se dégage de la foule qu'un bruit incompréhensible. En revanche, si l'on se focalise sur une discussion entre deux personnes de la foule, il est possible de comprendre la conversation. Le principe de focaliser son attention sur une chose donnée correspond, dans le cas de l'AMRC, à l'affectation d'un code identifiant chaque station émettrice. En effet, toutes les stations vont émettre sur le même canal en même temps, avec la même fréquence, mais chacune de ces stations pourra reconnaître les données qui lui sont destinées grâce au code d'identification approprié.

**AMRF -** Accès Multiple à Répartition de Fréquences - FDMA - Technique de multiplexage en fréquence employée notamment pour la radiotéléphonie analogique où chaque terminal dispose d'une portion des fréquences d'un canal de transmission. Technique permettant à plusieurs équipements d'accéder à une ressource commune partagée selon une technique de répartition en fréquences.

L'AMRF est la technique d'accès multiple la plus couramment utilisée dans les systèmes de télécommunication par satellite. Chaque station terrienne a sa propre fréquence et les ressources du satellite sont utilisées en commun. Ce système est actuellement utilisé pour les liaisons internationales. L'ennui est que, comme de nombreux signaux traversent simultanément le répéteur du satellite, l'intermodulation entre ces signaux, due à la non-linéarité du répéteur, donne naissance à un bruit de brouillage. Pour réduire les effets de cette intermodulation, on doit réduire considérablement le niveau de l'amplificateur de puissance par rapport à son point de saturation. Cette réduction est ce qu'on appelle, en anglais, le"back-off ". De plus, on doit limiter avec précision la puissance d'émission de chaque station terrienne.

**AMRT -** Accès Multiple à Répartition dans le Temps - TDMA - L'une des nombreuses méthodes de transmission numérique mobile qui augmente le rendement du réseau en autorisant un plus grand nombre de transmissions simultanées. Les réseaux qui utilisent l'AMRT affectent 6 voies temporelles à chaque canal de fréquence. Les appareils utilisant le réseau mobile envoient des rafales d'informations qui sont réassemblées côté réception.

Technique de multiplexage temporel attribuant à chaque voie bas débit une fraction du temps total de transmission. Notamment utilisé pour les liaisons satellites et la radiotéléphonie, cette technologie permet à plusieurs équipements d'accéder à une ressource commune partagée selon une technique de répartition dans le temps.

L'AMRT (en communication spaciale) est une technique d'accès multiple numérique dans laquelle les diverses émissions des terminaux terriens peuvent être reçues par le satellite dans des créneaux de temps séparés, sans chevauchement, dans lesquels les informations sont mises en mémoire. Ceci rend impossible la formation de produits d'intermodulation dans un répéteur non linéaire, comme c'est le cas avec l'AMRF. Chaque terminal au sol doit pouvoir déterminer l'heure du système à satellite et sa distance, afin que les signaux qu'il émet soient cadencés de manière à arriver au satellite dans les créneaux de temps appropriés. Aucune intermodulation ne peut résulter d'une non-linéarité instantanée puisqu'un seul signal arrive au répéteur du satellite à un instant donné. Il est à noter que les débits binaires des salves transmises sont en général beaucoup plus élevés que ceux des trains de bits continus à l'entrée du terminal au sol.

**Analogique -** Désigne un signal présentant des variations continues et pouvant prendre des valeurs quelconques entre certaines limites. Les sons, la voix, les couleurs, tels que les perçoivent nos sens, sont des entités analogiques. En télécommunications et en informatique, ce terme est souvent opposé à numérique, qualificatif d'un signal ne pouvant prendre qu'un nombre limité de valeurs discontinues (deux si le signal est binaire).

Représentation d'une information par un signal à évolution continue (par exemple sinusoïdal).

**Analyse de risque -** Processus comprenant l'identification des risques en matière de sécurité, leur impact et l'identification des zones nécessitant une protection.

**Analyseur -** Appareil de contrôle et de mesure du signal ou des informations échangées sur un canal de transmission. On trouvera de nombreux types d'analyseurs. On utilise souvent en télécommunications des analyseurs de protocoles qui contrôlent non seulement le signal, mais aussi la structuration des informations sur le canal.

**ANF -** Agence Nationale des Fréquences - Définie par la loi de réglementation des télécommunications le 26 juillet 1996, l'ANFR a commencé ses travaux le 1er janvier 1997. Son rôle est de planifier et de répartir le spectre des fréquences radioélectriques, d'organiser les procédures pour une bonne cohabitation des utilisateurs et de contrôler l'utilisation des fréquences et le respect des règles.

**Angle d'acceptance - Voir** Ouverture Numérique.

**Angle critique -** (en technologie optique) Angle d'incidence de la lumière dans une fibre sous lequel la réflexion totale est possible. Dans ce cas, la lumière est guidée par la fibre.

**ANI -** Automatic Number Identification - Identification automatique du numéro appelant.

**Anneau -** Ring - Topologie de réseau en boucle fermé. Voir topologies et Anneau à Jeton

**Anneau à jeton -** L'anneau à jeton est d'origine IBM. Celui-ci est normalisé pour deux débits compatibles de 4 ou de 16 Mbit/s.

Son fonctionnement est simple : un jeton de trois octets circule en permanence de station en station. Une station qui veut émettre bascule l'un de ces octets en position"occupée" et émet son ou ses paquets immédiatement à la suite (en fonction d'un taux d'occupation maximal et de règles éventuelles de priorité). L'ensemble est transmis tel quel de station en station jusqu'à la station destinataire qui, reconnaissant son adresse dans l'en-tête, lit son message et remet le jeton à l'état "libre" ; au bout d'un tour d'anneau, la station émettrice voit ainsi repasser son jeton libre et sait que le message a été reçu. Le temps maximal du tour d'anneau est déterminé et le remplissage de l'anneau peut ainsi être optimal avec un mécanisme de priorité évolué. Une station chargée de la gestion surveille la régularité des passages du jeton et les priorités. En cas de défaillance de sa part, une autre prend sa place. Lorsqu'une station se déconnecte de l'anneau, celui-ci est automatiquement refermé par un mécanisme situé au point de connexions des stations.

Les stations sont insérées en coupure sur l'anneau. Un message émis parcourt tout l'anneau pour revenir à son point de départ afin d'être absorbé par l'émetteur initial. Les ruptures d'anneau sont traitées par la présence de "concentrateurs" de raccordement (MAU). Ces derniers donnent une topologie physique en arbre, capable de court-circuiter une station en panne.

**Annuaire** - Selon la norme définie par l'UIT-T, un annuaire est une collection de systèmes d'informations ouverts qui coopèrent pour maintenir une base de données d'informations, ces dernières étant relatives à des objets du monde réel.

Base de données spécialisée, qui enregistre des informations ordonnées et typées sur les objets. L'annuaire recueille les informations concernant un ensemble d'objets, arrangés dans un ordre bien défini, et les rend accessibles aux utilisateurs autorisés.

Les objets généralement concernés sont bien souvent ceux qui ont un rôle au niveau de la communication, comme des personnes, des organisations, des applications, des fichiers stockés, des terminaux et des équipements. Ces informations comprennent les noms et adresses de différentes sortes, ainsi que les capacités de ces objets. L'annuaire peut être comparé à un support de publication. Les objets l'utilisent pour fournir leurs coordonnées à ceux qui désirent communiquer avec eux.

Un annuaire peut être distribué ou centralisé. Si l'annuaire est centralisé, il n'y a qu'un seul serveur d'annuaire qui fournit l'accès à l'annuaire. S'il est distribué, il y a plusieurs serveurs qui permettent d'accéder au même annuaire.

Différents protocoles d'annuaires : (liste non exhaustive)

DAP : Directory Access Protocol - Destiné à véhiculer des informations à l'extérieur de l'annuaire.

DOP : Directory Operational binding management Protocol - Utilisé pour faire communiquer les DSA entre eux, il permet d'ouvrir une connexion entre deux DSA.

DSP : Directory System Protocol - Permet de transporter les requêtes initialement acheminées par le protocole

DISP : Directory Information Shadowing Protocol - Protocole utilisé pour la réplication d'annuaire.

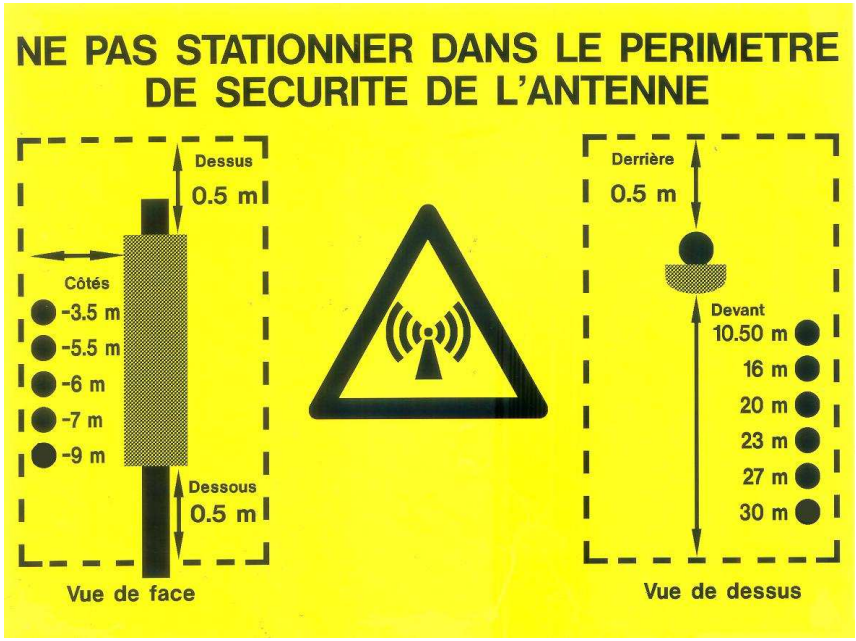
**ANSI -** American National Standards Institute - Consortium de l'industrie américaine chargé de développer des normes commerciales et de communication. On lui doit notamment la conversion de numérotation des caractères Ascii.

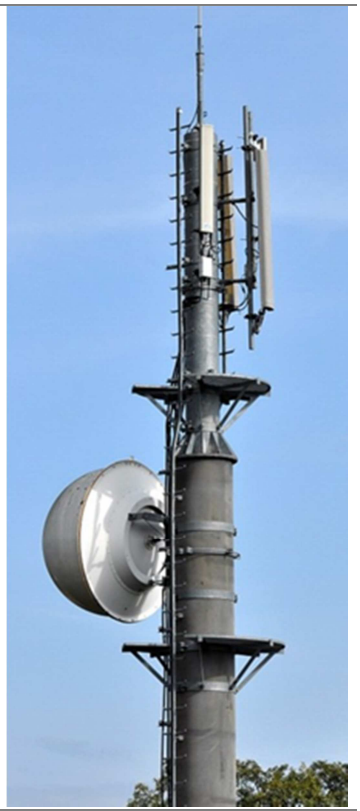
Organisme chargé de coordonner l'activité de normalisation aux Etats-Unis d'Amérique.

C'est l'organisme qui développe et publie des standards pour les USA. L'ANSI a publié des standards pour la compression de la voix, pour les réseaux.

**Antenne -** Voir aussi Station de base. Dispositif passif ou actif permettant d'émetre et/ou de recevoir des signaux véhiculés par les ondes.

Dans le cadre de la téléphonie mobile (GSM et UMTS), les antennes des sites relais sont soumises à des règles strictes limitant les expositions des intervenants à proximité.



**Anticipation -** Technique consistant à émettre des données par blocs ou trames sans attendre l'acquittement (signal de bonne réception) entre chaque bloc ou trame. Employée notamment dans la procédure synchrone HDLC.

**Antiope -** Service de vidéotex utilisé en diffusion, notamment par TDF sur des canaux de télévision hertzienne.

**Anycast -** Mode de transmission de trames depuis un seul poste vers un ou plusieurs postes d'un même groupe utilisant le routeur le plus proche.

**API -** Application Programminq Interface - Interfaces pour langages de programmation, matérialisées par des primitives, permettant à une application d'accéder à des programmes système pour, par exemple, communiquer ou extraire des données.
Éléments utilisés par les programmeurs, grâce auxquels l'application développée peut faire directement appel aux ressources du système d'exploitation ou d'une application tierce.

**APNF -** Association de la Portabilité des Numéros Fixes.

**Appel -** Processus consistant à émettre des signaux d'adresse en vue d'établir une liaison entre les stations de données.

**Appel en instance -** Call waiting service - Complément de service qui permet de signaler à un abonné, déjà en communication avec un correspondant, qu'un second interlocuteur cherche à le joindre.

**Applet -** Sous programme chargé d'exécuter une application en rapport avec le concept OLE (Object linking and embedding).

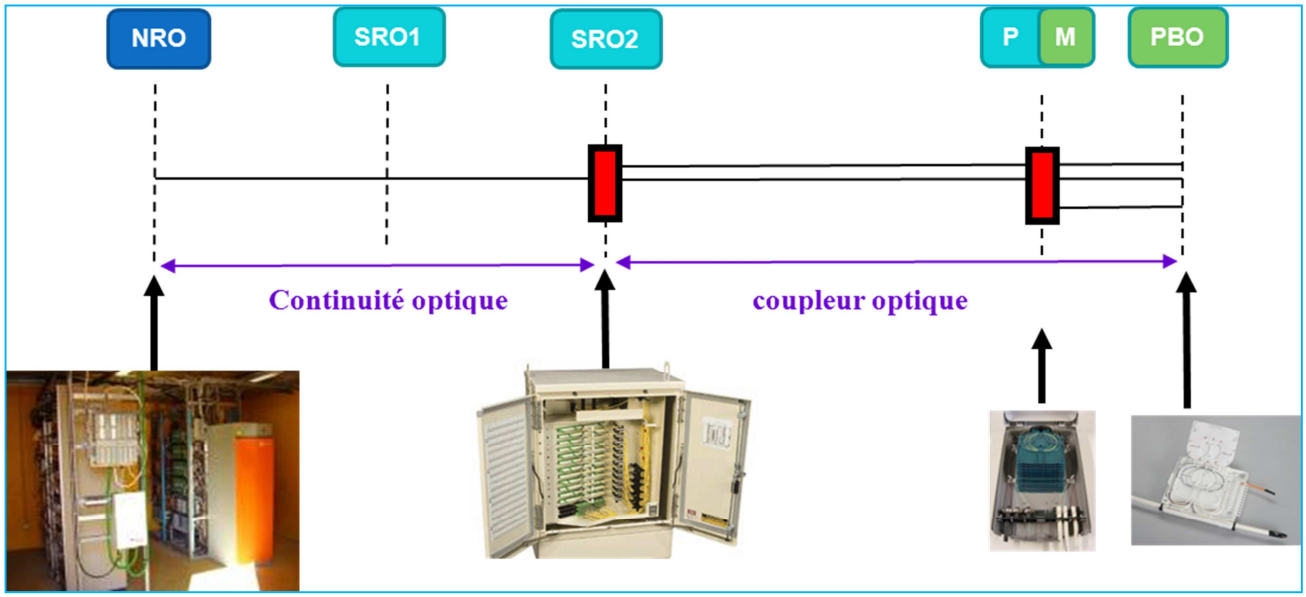
**AppleTalk -** Architecture de réseau local développée par Apple, permettant à des Macintosh ou à des PC d'échanger des données et de partager des ressources matérielles et logicielles (serveurs de fichiers, périphériques...). Réseau informatique pour la connexion d'ordinateurs Macintosh et d'autres périphériques telles que les imprimantes LaserWriter. Topologie en Bus.

**Application -** Niveau 7 du modèle OSI

**APPN -** Advanced Peer to Peer Networking - Architecture mise en œuvre par IBM pour faire communiquer ses systèmes, initialement de petite et moyenne taille (AS/400, PS/2), dans le cadre de l'architecture SNA. La particularité d'APPN est de permettre la constitution de réseaux non hiérarchisés.

**Arbre PON -** Architecture réseau optique point-à-multipoints dont le « tronc » serait le câble en fibre optique qui débute au NRO et dont les feuilles sont les fibres optiques reliées aux logements des usagers.

- Des coupleurs sont placés aux points de séparation entre le tronc et les feuilles.
- Les points de séparation sont aussi appelés point de flexibilité.
- Les coupleurs sont passifs dans le cadres des arbres GPON.




**ARCEP -** l'Autorité de Régulation des Communications Electroniques et des Postes - Suite à la promulgation de la loi sur la régulation des activités postales le 20 mai 2005, l'ART est devenue l'ARCEP.

**Architecture -** Cadre général fixant les règles de communication (codes, protocoles, interfaces) entre les divers constituants d'un réseau.

**Architecture mono-fibre -** En FTTH, désigne une architecture mono-fibre sur la partie terminale du réseau en fibre optique qui est caractérisée par une fibre unique qui relie le point de mutualisation à la prise terminale optique.

**Architecture multi-fibres -** En FTTH, désigne une architecture multi-fibres sur la partie terminale du réseau en fibre optique qui est caractérisée par plusieurs fibres qui relient le point de mutualisation à la prise terminale optique.

**Architecture Omnidirectionnelle / Directionnelle (point à point) - Réseaux sans fil / Réseau radio -** Dans les réseaux utilisant une technoligie sans fil, il existe deux grandes familles d'architecture : Omnidirectionnelle et directionnelle.

Dans le cas d'une architecture omnidirectionnelle, il n'y a qu'un seul point d'accès au réseau pour plusieurs terminaux. Ce type de liaison est très utilisé pour relier plusieurs terminaux au réseau de l'entreprise. Le support utilisé est les ondes radios car celles-ci se propagent dans l'espace en se souciant assez peu des obstacles qu'il peut y avoir entre le point d'accès et le terminal. On peut faire une analogie avec les réseaux filaires classiques en comparant le point d'accès du réseaux sans fils à un HUB et les ondes radios au câble reliant les stations à ce HUB. La distance entre le point d'accès et les stations varie en fonction de la topologie des lieux. En effet, selon la structure des murs qui sont plus ou moins opaques pour ce type d'ondes, les perturbations dues à des moteurs d'ascenseur par exemple peuvent diminuer la distance maximale entre le point d'accès et le terminal. De plus, cette distance ou portée varie en fonction de la puissance et de la qualité des équipements, que ce soit au niveau du point d'accès ou du terminal mobile. La notion de cellule est la zone située autour d'un point d'accès dans laquelle un terminal peut se connecter à ce point d'accès. Le rayon d'une cellule est souvent compris entre 50 et 300 mètres.

Dans le cas d'une architecture point à point, la liaison se fait uniquement entre deux points d'accès. Cela équivaut à un câble qui serait installé entre deux points. Ce type de liaison est le plus souvent réalisé à l'aide de point d'accès spécifiques (laser en vue directe, radio dite à faisceau hertzien (FH),…). Cette liaison permet de très hauts débits mais est limitée en ce qui concerne les directions de diffusion du signal.

**Argentique -** Nom donné à la photographie "traditionnelle" qui utilisait des films aux sels d'argent.

**Armoire de Répartition -** Armoire de brassage pour panneaux 19" dans les salles informatique. Les armoires de répartition, lorsqu'elles sont en extérieur, sont aussi appelées armoire de rue.

**ARP -** Address Resolution Protocol - Associe une adresse IP à une adresse MAC (interface dans les réseaux locaux). C'est une portion du protocole TCP/IP qui associe une adresse IP à l'adresse physique Ethernet de l'ordinateur ou périphérique réseau. II existe aussi RARP qui fonctionne à l'envers.

Chaque machine connectée au réseau possède un numéro d'identification de 48 bits. Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte en usine. Toutefois la communication sur Internet ne se fait pas directement à partir de ce numéro (car il faudrait modifier l'adressage des ordinateurs à chaque fois que l'on change une carte réseau) mais à partir d'une adresse dite logique attribuée par un organisme: l'adresse IP.

Ainsi, pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.

Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance. Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête sur le réseau. L'ensemble des machines du réseau vont comparer cette adresse logique à la leur. Si l'une d'entre-elles s'identifie à cette adresse, la machine va répondre à ARP qui va stocker le couple d'adresses dans la table de correspondance et la communication va alors pouvoir avoir lieu.

Les adresses IP sont attribuées indépendamment des adresses matérielles des machines. Pour envoyer un datagramme dans l'internet, le logiciel réseau doit convertir l'adresse IP en une adresse physique qui est utilisée pour transmettre la trame. Si l'adresse physique est un entier court, elle peut être facilement modifiée pour lui faire correspondre l'adresse machine IP. Sinon, la traduction doit être effectuée dynamiquement.

C'est le protocole ARP qui effectue cette traduction en s'appuyant sur le réseau physique. ARP permet aux machines de résoudre les adresses sans utiliser de table statique. Une machine utilise ARP pour déterminer l'adresse physique destinataire en diffusant (broadcast), sur le sous réseau, une requête ARP qui contient l'adresse IP à traduire. La machine possédant l'adresse IP concernée répond en renvoyant son adresse physique. Pour redre ARP plus performant, chaque machine tient à jour, en mémoire, une table des adresses résolues et réduit ainsi le nombre d'émissions en mode broadcast.

Spécifications

La structure d'une trame ARP est définie ci-dessous :

- Champs
  - Type Hardware : spécifie le type de l'interface hardware
  - Type de protocole : spécifie le type du protocole de haut niveau émis par l'expéditeur
  - Hlen : longueur de l'adresse hardware
  - Plen : longueur de l'adresse de haut niveau
  - Opération : type de l'opération effectuée : Requête ARP Réponse ARP Requête RARP Réponse RARP Requête RARP dynamique Réponse RARP dynamique Erreur RARP dynamique Requête InARP Réponse InARP
  - Adresse hardware de l'expéditeur : explicite
  - Adresse protocole de l'expéditeur : explicite
  - Adresse hardware du destinataire : explicite
  - Adresse protocole du destinataire : explicite

**Arpanet -** historiquement le premier réseau expérimental de commutation par paquets, destiné à la recherche militaire américaine.

**Arrobe ou Arrobase - @ -** Caractère fréquemment employé dans les adresses du courrier électronique pour séparer le nom identifiant l'utilisateur de celui du gestionnaire de la messagerie.

Le linguiste Berthold Louis Ullman date son apparition au VIe siècle où des moines copistes l'ont utilisé comme raccourci du mot latin ad qui a des significations variées qui vont de "à" à "auprès de" en passant par "vers".

Le mot arobase serait, quant à lui, la déformation de a rond bas (de casse), c'est à dire a minuscule entouré d'un rond. Mais il y a confusion avec une unité de mesure espagnole l'arroba (25 livres espagnoles, soit 11,502 kg) dont le nom français est arrobe. Cette mesure espagnole viendrait elle même de l'arabe ar-roub (le quart).

Quoi qu'il en soit, le nom français préconisé par la Délégation Générale à la Langue Française pour ce caractère est le terme arrobe. Le monde universitaire et informatique à l'origine de son expansion mondiale parle plus volontiers d'arobase, terme qui, en français, semble le plus employé.

On a aussi vu utiliser le même signe @ dans le commerce pour indiquer "à" dans le prix par unité d'un produit. Même si l'époque est moins clairement connue pour cet usage, cela explique sans doute la présence du signe sur les claviers de machines à écrire dès le dix-neuvième siècle, puis sur ceux des ordinateurs du vingtième siècle.

**ART -** Autorité de Régulation des Télécommunications (France) - Autorité indépendante (créée par la loi de réglementation des télécommunications de 1996) chargée de favoriser une concurrence durable dans les télécommunications, au service des intérêts des consommateurs. Elle statue notamment sur les interconnexions et les licences, l'économie et la concurrence, la technique et la technologie. Organisme officiel chargé de la régulation du marché des télécoms et de l'institution du cadre juridique régissant ce marché. Voir ARCEP

**Artefact -** Pixels indésirables consécutifs à des défauts d'enregistrement d'une image numérique.

**Artère de Transmission -** Transmission Line - Support sur lequel sont routés les circuits. Les câbles métalliques ou à fibres optiques, les faisceaux hertziens et les liaisons radioélectriques sont des exemples d'artères de transmission.

**ASAP -** Acronyme de l'expression anglaise "As Soon As Possible", repris par SAP pour désigner une méthodologie. Méthodologie permettant d'accompagner l'implantation et le déploiement de SAP dans une société utilisatrice.

**ASCII -** American Standard Code for Information Interchange - Principal code utilisé dans l'informatique pour les données alphabétiques. Il utilise 7 bits par lettre et comporte 128 combinaisons. Normalisé sous le nom de CCITT n° 5, il a fait l'objet d'une extension à 8 bits permettant notamment d'élargir le code pour prendre en compte les accents et caractères spéciaux. On parle souvent d'ASCII étendu.

Ce code définit la représentation d'un jeu de caractères comprenant les 26 lettres minuscules et majuscules, les chiffres de 0 à 9, les signes de ponctuation, des caractères spéciaux et des caractères de commande.

**ASFI -** Accès Sans Fil à Internet - Moyen d'accès radioélectrique de haut débit à un réseau de télécommunication de type internet, généralement composé d'une station de base d'un réseau d'accès sans fil à l'internet. Traduction en français du "hot spot"… par le gouvernement français.

**ASIC -** Application Specified Integrated Circuit - Circuit intégré spécifique dédié à une fonction ou une application. Il existe des ASICs dédiés pour le décodage de la musique, pour le traitement (pré ou post traitement) de la vidéo ou le calcul de session encodées de type HTTPS.

**ASN1 -** Abstract Syntax Notation 1 - Langage de spécifications permettant de décrire des protocoles de façons complète et non ambiguë. Il a été normalisé dans le cadre de l'ISO et du CCITT.

**ASP -** Application Service Provider - Prestataire qui offre à plusieurs clients la possibilité d'utiliser la même application informatique à travers un réseau de télécommunication afin d'en répartir le coût.

**Asservi -** Mode de transmission ou la direction du dialogue est dirigée par une station principale ou station maître.

**Asynchrone -** Désigne un mode de transmission dans lequel l'émetteur et le récepteur ne se sont pas synchronisés au préalable -chaque mot ou caractère possède sa propre synchronisation, le plus souvent grâce à des bits délimitant le début et la fin d'un mot (start-stop). On parle souvent de mode "caractère". Le rythme de transmission est assuré par la superposition dans chaque mot des bits d'information et d'un signal d'horloge. Ce mode s'oppose au mode synchrone (plus efficace mais plus contraignant en termes de mobilisation des ressources de calcul), mode synchrone où la transmission est réalisée par un accord "préalable" de l'émetteur et du récepteur sur un rythme d'horloge constant.

**ATLAS 400 -** Service public de messagerie et d'échange de documents informatisés proposé par Transpac selon les normes X400. Disponible sur abonnement, il permet l'interconnexion de messageries privées ou la connexion d'abonnés individuels.

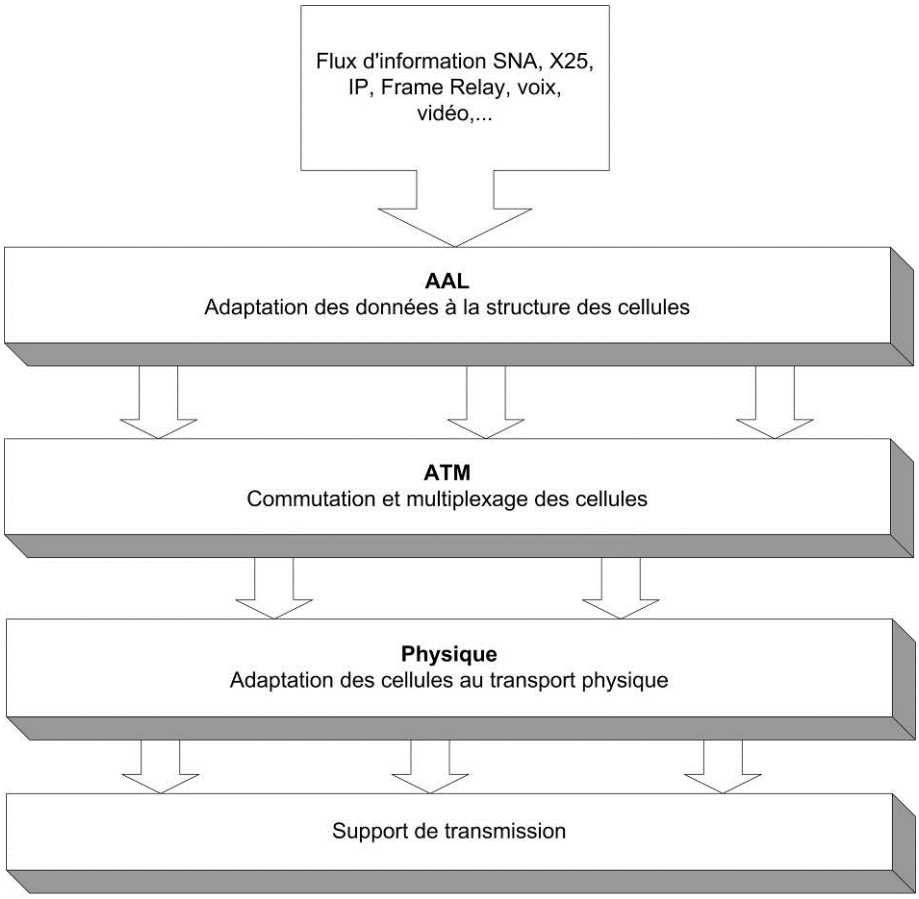
**ATM -** Né dans les années 80, l'ATM (Asynchronous Transfer Mode, ou mode de transfert asynchrone), revendique le rôle de protocole réconciliateur de toutes les contraintes liées au transport des données multimédias sur des réseaux à très hauts débits (jusqu'à 622 Mbits/s, bien au delà des 2 Mbits/s du réseau Transpac avec X25, ou des 34 Mbits/s des services à relais de trames (Frame Relay)). C'est une variante des technologies par paquets (X25, Frame Relay) mais qui possède l'avantage de fonctionner selon un découpage des données en cellules de taille réduite et fixe.

Le découpage des données en cellules courtes (48 octets de charge utile et 5 octets pour l'entête), associé au principe de fonctionnement par émulation de circuit virtuel (qui garantit l'acheminement de bout en bout de l'information), rend l'ATM capable, en natif, de véhiculer le trafic des applications ne souffrant aucun aléa de transmission (voix et vidéo, notamment). De plus, le fait que l'entête des cellules de l'ATM soit allégé des mécanismes de contrôle simplifie la tâche de commutation des commutateurs dits "brasseurs" ATM, d'autant que ceux ci commutent les cellules à très hauts débits (de 150 Mbits/s à 622 Mbits/s).

L'ATM est une technique de commutation, de multiplexage, de transmission de données multimédias (voix, données, images), et multi débit. L'ATM fonctionne en mode connecté (les données ne sont acheminées dans le réseau qu'après l'établissement d'un chemin virtuel à travers celui ci). Principal intérêt: l'ordre de séquence d'émission des cellules est respecté. L'ATM met en a œuvre des circuits virtuels permanents (comme le fait le Frame Relay), pour des connexions de longue durée, mais son point fort est d'offrir aussi des circuits virtuels commutés pour des besoins à la demande de communication.

Dans le modèle architectural de fonctionnement à 3 couches de l'ATM (voir schéma), la commutation de cellules s'intercale entre les fonctions de transmission proprement dite et les fonctions d'encapsulation de la couche AAL (ATM Adaptation layer) qui adaptent les flux d'informations de toutes origines (données, voix, vidéo) à la structure des cellules ATM.

Le relais de cellules, appellation courante de l'ATM par analogie au relais de trames, met aussi en œuvre la technique de multiplexage statistique (modification dynamique et en permanence des voies de transmission à emprunter selon l'activité réelle des terminaux). Les cellules sont ainsi générées à la demande. en fonction du débit de la source. D'où, le caractère asynchrone de l'ATM par opposition à la commutation et au multiplexage de circuits (transfert synchrone). Avantage du multiplexage statistique de l'ATM: l'allocation dynamique de la bande passante, très utile pour l'interconnexion de réseaux locaux.




**La commutation de cellules s'insère entre les fonctions de transmission et celles qui adaptent les différents flux à la taille des cellules : fonctions AAL-1, AAI-2, AAL-3/4 et AAL-5**

Les principes fondamentaux de ATM sont :

- L'absence de contrôle de flux a l'intérieur du réseau à partir du moment ou la communication est établie,
- L'absence de contrôle d'erreur (la transmission sur fibre optique, qui est le support pour lequel ATM a été initialement développé, présente une bonne qualité de transmission) et la détection et la reprise d'erreur diminuent le débit utile,
- Un mode orienté connexion pour faciliter la réservation des ressources et assurer le séquencement des PDU (Packet Data Unit),
- L'absence de contrôle de perte au niveau du réseau car les ressources suffisantes ont été allouées aux connexions lors de leurs établissements,
- Une unité de transfert que l'on appellera cellule, de taille réduite pour faciliter l'allocation mémoire dans les commutateurs et permettre un meilleur entrelacement des flux et une commutation rapide,
- Un en-tête de cellule de taille limitée et aux fonctions réduites pour assurer une commutation rapide.
- La priorisation des flux divisée en 2 modes : La priorité spatiale : certaines cellules ont une probabilité de perte plus élevé (cas de congestion, il y a élimination des cellules de faible priorité), La priorité temporelle : certaines cellules peuvent rester dans le réseau plus longtemps que d'autres lorsque la durée de vie des cellules est limitée, elle permet d'augmenter les performance temps réel du réseau.

La fourniture de ces priorités est réalisée de deux manières : Explicitement, en définissant un champ dans l'en-tête pour identifier la priorité (bit CLP), ou implicitement, en affectant à l'établissement une priorité à chaque connexion virtuelle, négociée par signalisation.

**ATSC -** Advanced Television Systems Commitee - Norme de diffusion de télévision par voie terrestre. Déployée aux Etats-Unis, au Canada et en Corée du Sud. Cette norme ne permet pas la réception en situation de mobilité (pas de réception mobile).

**Attaque -** Aussi appelé Intrusion - Les attaques peuvent être classées sous deux types : les attaques internes et les attaques externes. Parmi ces deux types, on distingue les attaques intentionnelles et les attaques accidentelles. Une attaque se caractérise aussi sous divers aspects, elle est passive si le but est de prendre connaissance de l'information sans l'altérer, actives si en plus de prendre connaissance de l'information le but est aussi de modifier l'information (altération, modification…). La notion de coût est aussi importante pour caractériser une attaque, selon 2 axes : le coût pour casser l'algorithme par rapport à la valeur de l'information cryptée ou encore le coût (en temps) pour casser l'algorithme par rapport à la durée de vie de l'information cryptée.

Les techniques d'attaques peuvents être classifiées sous différentes formes :

- Attaque exhaustive ou force brute - L'attaque exhaustive est une attaque dite à force brute, c'est-à-dire que l'on va essayer toutes les clés possibles l'une après l'autre jusqu'à l'obtention de la bonne. Il faut noter que cette attaque peut aussi bien aboutir dans l'heure que ne jamais aboutir. C'est une attaque complètement aléatoire. Cette méthode a l'avantage d'être générique et parallélisable (on peut distribuer le calcul sur de nombreuses machines). Statistiquement, il faudra essayer la moitié des clés avant de trouver la bonne.
- Attaque par dictionnaires - Elle consiste à tester toutes les clés possibles parmi un dictionnaire de clés.
- Attaque à texte clair connu - Soit le cryptanalyste a accès aux textes chiffrés de plusieurs messages et aux textes en clair correspondants contenu. Soit, il est en mesure d'en deviner le contenu par extrapolation de bloques de messages chiffrés en émettant des hypothèses. La tâche est de retrouver la ou les clés utilisées pour chiffrer ces messages ou un algorithme en mesure de déchiffrer n'importe quel nouveau message chiffré avec la même clé.
- Attaque à texte chiffré choisi - Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes chiffrés lui sont fournis. Par exemple, le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique, sa tâche est de retrouver la clé.
- Attaque à texte chiffré - Elle consiste en une attaque aveugle, le cryptanalyste n'as pas connaissance du type d'information contenu dans le message. En pratique, il est toujours possible de deviner le contenu du message par le fait que chaque message début toujours d'une manière plus ou moins commune, donc prévisible. De plus, il est possible de déterminer dans le message chiffré des bloques de mots communs qui vont servir de base à l'attaque.Le cryptanalyste dispose donc du texte chiffré de plusieurs messages, tous ayant été chiffré avec le même algorithme. La tâche du cryptanalyste consiste à retrouver le texte en clair du plus grand nombre de messages possible ou mieux encore de trouver la ou les clés qui ont été utilisé pour chiffrer les messages ce qui permettrait de déchiffrer de déchiffrer d'autres messages chiffrés avec ces mêmes clés.

Attaque cyclique ou à timing - C'est une méthode toute récente qui consiste à déterminer le moment exact où l'opération d'exponentiation modulaire a lieu.

Une attaque se fait toujours en deux phases distinctes :

Scan - Cette première phase d'une attaque consiste pour l'attaquant à obtenir le maximum de renseignements sur le réseau informatique qu'il prend pour cible. Il va essayer de savoir à quel type de système d'exploitation il est confronté, les protocoles utilisés, les ports TCP laissés ouverts… Cette phase est sans aucun doute celle qui va nécessiter le plus de temps, l'attaquant devant collecter les informations sans attirer l'attention de l'administrateur système.

Exploit - Des qu'il a le maximum d'informations sur le réseau cible, l'attaquant va lancer son attaque. Il va tout d'abord pénétrer le réseau, puis dans un second temps, effectuer les actions délictueuses.

Objectifs ➔ méthodes d'attaques :

Déni de service ➔ Abus de droits, action physique, Intrusion,

Altération ➔ Injection de code, action physique, Intrusion,

Renseignement ➔ Abus de droits, Ecoute, Injection de code, Intrusion,

Utilisation de ressources ➔ Abus de droits, Intrusion.

Les objectifs :

- Le déni de service - Correspond à la perturbation d'un échange par le réseau, d'un service ou d'un accès à un service. On parle de déni de service lorsque l'attaquant empêche le système de fonctionner normalement.
- L'altération - Correspond à la modification ou la destruction de données, notamment des données de configurations.

- Les renseignements - L'objectif est d'obtenir des informations sur le système, sur un utilisateur ou encore sur un projet dans le but de nuire à l'entreprise.
- L'utilisation de ressources - L'objectif est d'utiliser les ressources de façon clandestine sur le système informatique.

Les méthodes d'attaques :

- L'intrusion - Correspond à l'exploitation des vulnérabilités du système. L'attaquant exploite les erreurs de configurations et les bugs du système pour exécuter des commandes non autorisées. L'intrusion apparaît comme méthode quel que soit l'objectif de l'attaque.
- L'abus de droits légitimes - Utilisation abusive des fonctionnalités d'un système. L'attaquant peut diffuser des logiciels sur des comptes anonymes, ou encore envoyer trop de requêtes à un serveur dans le but de le saturer.
- L'action physique - L'action physique sous-entend la dégradation volontaire d'un matériel, la destruction, l'altération d'un composant. L'attaquant débranchera un appareil, détruira un câble, …
- L'usurpation d'identité - L'attaquant utilise une fausse identité pour tromper soit le système soit un utilisateur. L'exemple le plus fréquent est l'" IP spoofing ", c'est à dire que l'attaquant va changer d'adresse IP pour tromper le système ou encore l'attaquant se fait passer pour l'administrateur réseau pour obtenir diverses informations, comme les mots de passe.
- L'injection de code - Correspond à installer et exécuter un module clandestin sur le système. Les exemples les plus fréquemment rencontrés sont les virus, les bombes, les vers, etc.
- L'écoute - Ecoute de façon passive et clandestine ce qui passe sur le réseau pour récupérer des informations, à l'aide de sondes ou d'analyseurs de réseau.

**Atténuation -** voir affaiblissement

**Attestation de conformité -** Les équipements terminaux destinés à être connectés à un réseau de télécommunications (postes téléphoniques, télécopieurs, modems etc.) ainsi que les émetteurs radioélectriques (télécommandes, postes CB etc.) doivent être conformes à des normes de qualité et de sécurité avant leur mise sur le marché. La loi prévoit des procédures d'évaluation dont l'aboutissement est la délivrance par l'Autorité d'une attestation de conformité. Les appareils conformes sont signalés par une étiquette spécifique.

**Attribution de fréquences -** Décision de l'Autorité de Régulation des Télécommunications autorisant un opérateur à utiliser une ou plusieurs fréquences selon certaines conditions sur une station ou une zone géographique définie. (Ceci n'est valable qu'en France bien sûr !)

**AUA -** Architecture Unifiée d'Applications - System Application Architecture - SAA - Ensemble de règles définies par IBM pour permettre une cohérence globale des applications entre tous les systèmes IBM (PC/PS, AS 400 et Systèmes 370). Elle vise une interface unique de programmation, un support commun de communication, une interface utilisateur commune et à terme une portabilité générale des applications d'un système à l'autre.

**AUC -** AUthentication Center - Réseau Mobile - Le centre d'authentification garde en mémoire pour chaque abonné une clé secrète qui sert à prouver son identité lors d'une demande de service ou pour chiffrer les communications. Un AUC est associé à un HLR, il peut même être intégré mais du point de vue matériel il ne fait pas partie du même sous-système.

**Audioconférence -** Mise en relation phonique, avec la qualité hi-fi, de deux groupes de personnes (de trois à six participants) réunies autour d'un terminal d'audioconférence. Il y a des possibilités d'audioconférence multipoints mettant en relation plusieurs groupes avec un dispositif adapté.

Téléconférence dans laquelle les participants sont reliés par des circuits téléphoniques qui permettent la transmission de la parole et éventuellement d'autres signaux tels que ceux de vidéo, de télécopie ou de téléécriture.

**Audiotel -** Service de France Télécom généralement accessible en composant un numéro commençant par "08 36" qui permet aux utilisateurs d'accéder à des informations, à des jeux, etc., généralement par l'intermédiaire d'un serveur vocal, c'est-à-dire un serveur informatique qui oriente l'appelant grâce à des messages préenregistrés.

Marque déposée par France Télécom désignant des numéros à revenus partagés pour lesquels France Télécom reverse une partie des revenus aux entreprises qui les utilisent. Les numéros Audiotel ne sont pas pour le moment ouverts à la concurrence.

**Audiotex -** Système de communication vocal utilisant la voix numérisée.

**Audit -** L'audit est un processus méthodique, indépendant et documenté permettant de recueillir des informations objectives pour déterminer dans quelle mesure les exigences satisfont aux référentiels du domaine concerné, permettant d'assurer que les activités et résultats relatifs à la qualité satisfont aux dispositions préétablies. Il peut porter sur un réseau, un système, un produit ou un processus. Un audit peut aussi porter sur la vérification de la légalité et de la conformité de l'utilisation des moyens. L'audit a pour objet de déterminer si, et dans quelle mesure, les activités et les procédures organisationnelles sont conformes aux normes et critères prédéfinis.

**AUI -** Attachement Unit Interface - Interface se présentant sous la forme d'une prise 15 broches destinée à recevoir la connexion réseau.

**AUP -** Acceptable Use Policy - Règles d'Usage Acceptable - Ensemble de règles qui décrit les conditions d'usage qui sont considérées comme "acceptables" par un Fournisseur d'Accès Internet. Ces règles sont communiquées par le FAI à ses clients lors de leur inscription. Dans la grande majorité des cas, elles excluent tout comportement abusif. Leur rédaction est entièrement laissée à l'appréciation du FAI.

**Authentification -** Vérification de l'identité d'un utilisateur ou d'un équipement.

**AUTIPAC -** Association des utilisateurs de Transpac.

**Autocommutateur -** Système permettant la sélection automatique et temporaire d'une liaison entre deux points d'un réseau. On distingue les autocommutateurs publics, pour les liaisons des réseaux publics, notamment le téléphone, et les autocommutateurs privés d'entreprise, souvent appelés PABX (Private Automatic Branch Exchange), qui assurent la même fonction pour les circuits de l'entreprise.

**Autocommutateur multiservice -** Autocommutateur privé fournissant des fonctions enrichies, telles que la messagerie vocale ou écrite, l'annuaire d'entreprise, la connexion à des réseaux de données, en plus des fonctions téléphoniques de base. Appelé aussi PABX.

**Autocommutateur Privé -** Private Automatic Branch eXchange - PABX - Autocommutateur appartenant à une entreprise et généralement relié aux réseaux publics de télécommunication.

**Autofocus (AF) -** Système de mise au point automatique à une ou plusieurs zones. Ce système est utilisé en prise de vue pour améliorer automatiquement l'image en procédant automatiquement à la mise au point en tenant compte de la distance du sujet principal.

**Autorité de certification -** CA - Entité de confiance chargée de signer les certificats numériques et d'attester de l'identité d'autres utilisateurs autorisés.

**AVI -** Audio Vidéo Interleaved, format de fichier vidéo.

**Avis -** Document normatif publié par le CCITT (Comité Consultatif International Télégraphique et Téléphonique) concernant les télécommunications. On distingue par exemple les avis en V, pour les interfaces de réseaux analogiques, et les avis en X pour les réseaux de données.

**AWG -** American Wire Gauge - Unité qui définit les sections standard des brins conducteurs.

**AXFR -** (voir DNS) - Le transfert de zone total est le mécanisme qui permet la mise à jour de l'information dans l'architecture distribuée du DNS. Elle permet aux serveurs secondaires de tenir à jour leur version de la zone pour assurer la cohérence de l'information dans le domaine.

Chaque fichier zone possède un compteur de rafraîchissement, celui-ci permet de régler la fréquence à laquelle les serveurs secondaires contactent un serveur primaire pour vérifier si leur version du fichier zone est à jour. Cette vérification se fait à l'aide d'un numéro de série dans l'enregistrement de la zone, qui est incrémenté à chaque modification du fichier. Si le numéro de série ne correspond pas, le serveur secondaire met en route le mécanisme de transfert de zone pour récupérer la nouvelle version du fichier zone.

Il est important de bien paramétrer la valeur du rafraîchissement de la zone : une valeur trop petite entraînera une augmentation de trafic sur le réseau, les serveurs secondaires interrogeront trop souvent le serveur primaire et risquent même de le ralentir dans son travail. Mais à l'inverse, une valeur trop importante remet en cause toute la cohérence du domaine, les informations modifiées ne seront pas mises à jour tout de suite dans les serveurs secondaires, ils fourniront alors des données erronées aux resolvers. Pour résoudre ce problème on peut utiliser la méthode de notification ponctuelle de modification de zone.

Lorsque le serveur secondaire détecte une version plus récente du fichier zone, il établit une connexion TCP avec le serveur primaire et télécharge la nouvelle version du fichier. Cette procédure ne doit pas entraver le bon fonctionnement des serveurs, qui doivent toujours fournir leurs services en même temps que le transfert s'effectue. Le serveur primaire doit être capable d'établir plusieurs sessions TCP avec différents serveurs secondaires, et doit conserver la connexion ouverte jusqu'à la fin du transfert signalée par le serveur secondaire.

# B

**Backbone -** Littéralement épine dorsale - Artère principale et fédératrice du réseau. Désigne l'épine dorsale d'un réseau de télécommunications. Les réseaux backbone des opérateurs sont des artères à très haut débit de transmission, qui relient les principaux nœuds du réseau et sur lesquels des liaisons de plus faible capacité de transmission sont raccordées. On distingue les réseaux backbone nationaux, régionaux ou mondiaux lorsque ces artères couvrent le territoire d'un pays, d'un groupe de pays (backbones européens) ou l'ensemble de la planète.

**Backhauling -** Littéralement : Acheminement des marchandises. Le backhauling est un mode de collecte des flux jusqu'à un point de service. On pourrait expliquer le concept en le comparant à une collecte de trafic vers une destination donnée, l'inverse exact du point à multipoint. Le backhauling désignerai un réseau bâti sur une notion de "multipoint" vers "point", le "multipoint" pouvant être fixe ou mobile, et la liaison pouvant être filaire (cuivre ou optique) ou radio (GSM, UMTS, Wifi, WiMax).

Par exemple, on peut traduire le concept en disant qu'il correspond au raccordement d'un point d'accès (Wifi, GSM, ...) au réseau Internet, ou encore désignant la concentration de trafic IP multipoint vers un équipement (point-multipoint). Ce terme se rencontre généralement dans le cas des architectures de type WiMax (trafic des bornes vers les concentrateurs), ADSL (abonnés vers les DSLAM), en 3G/UMTS/HSDPA pour qualifier les accès Internet,….

Certaines traductions abordent aussi la notion de "voie de retour", et comme le terme est utilisé aussi bien en réseau "terrien" que satellitaire, le concept de voie de retour se transpose bien aussi.

En fait, ce terme issu du transport de marchandises a plusieurs usages dans le monde des réseaux et des télécommunications :

- Dans la communication par satellite, le terme de backhauling est utilisé pour désigner l'opération qui consiste à concentrer des données en un point, point à partir duquel il peut être rediffusé sur un réseau. Par exemple, la collecte de reportages vidéos en un point via une liaison satellitaire (backhauling - en principe de multipoint vers point) permet ensuite de les redistribuer en diffusion point vers multipoint (multicast). Il s'agit de transmettre des données vers un point depuis lequel elles peuvent être uploadées (envoyées) à un satellite.
- Certains fabricants d'équipement de commutation emploient le terme de backhauling pour désigner la collecte des données à destination du backbone. A la nuance près que le point de destination de la collecte correspond très souvent à un service (ex : accès Internet). En technologie de réseau sans fil, il s'agit de transmettre la voix et le trafic de données depuis un site cellulaire vers un switch, c'est-à-dire depuis un site distant vers un site central.
- D'après certaines lectures, le backhauling consiste en l'envoi de données à destination d'une route ou d'un service au moindre coût. Ce type de notion induit de facto un système de routage dynamique particulier tenant compte des coûts d'acheminement.
- Le terme de Backhauling peut parfois être employé pour désigner l'utilisation d'un canal dans une communication bidirectionnelle.

En étant un peu synthétique, il s'agit donc de transporter/réinjecter/transmettre des données depuis un réseau "périphérique" vers son réseau maître ou référent. Typiquement, il s'agit de transmettre des données (quelles qu'elles soient) d'un réseau d'entreprise de type LAN vers la backbone de l'entreprise national. Dans le monde du mobile, il va plutôt s'agir de transmettre des données d'une BTS vers un MSC.

Les RFC de référence sur le concept :

- rfc3807 - V5.2-User Adaptation Layer (V5UA) - This document defines a mechanism for the backhauling of V5.2 messages over IP using the Stream Control Transmission Protocol (SCTP). This protocol may be used between a Signaling Gateway (SG) and a Media Gateway controller (MGC). It is assumed that the SG receives V5.2 signaling over a standard V5.2 interface.
- rfc4129 - This document defines a mechanism for backhauling Digital Private Network Signaling System 1 (DPNSS 1) and Digital Access Signaling System 2 (DASS 2) messages over IP by extending the ISDN User Adaptation (IUA) Layer Protocol defined in RFC 3057. DPNSS 1, specified in ND1301:2001/03 (formerly BTNR 188), is used to interconnect Private Branch Exchanges (PBX) in a private network. DASS 2, specified in BTNR 190, is used to connect PBXs to the PSTN. This document aims to become an Appendix to IUA and to be the base for a DPNSS 1/DASS 2 User Adaptation (DUA) implementation.

**BAL -** Abréviation de Boite aux Lettres - Ce terme est utilisé dans tous les systèmes de messagerie électronique et désigne l'espace de stockage dans lequel sont stockés les messages destinés à une adresse (une personne, un groupe, une entité…).

**Balance des Blancs -** Terme utilisé en photo comme en vidéo. Opération qui consiste à régler l'appareil pour adapter l'appareil de prise de vue pour modifier la colorimétrie en l'adaptant à l'éclairage afin d'éviter une dominante colorée.

**Balun -** Adaptateur d'impédance permettant de raccorder un câble à paires torsadées (Balanced) à un câble coaxial (UNbalanced).

**Bande -** En communication mobile, la bande fait référence à une fréquence ou à une plage de fréquences contiguës. Voir également Fréquence de fonctionnement.

Gamme de fréquences continues entre deux limites.

**Bande de base (transmission en) -** Transmission de signaux numériques ou analogiques sous leur forme originale, sans modulation. Transmission d'un signal de données dans sa bande de fréquence d'origine sans qu'il subisse de modulation. Mode de transmission où les informations à transmettre ne subissent pas de modification de rythme entre l'émetteur et le canal de transmission, et où la modulation occupe la totalité de la bande passante.

**Bande de fréquences -** Frequency Band - Ensemble continu des fréquences comprises entre deux fréquences spécifiées. La bande de fréquences transmise par le téléphone est : 300 - 3400 Hz.

Tableau des bandes de fréquence :

| Bandes de fréquences / ULF, VLF, LF, MF, HF, VHF, UHF, SHF, EHF | | |
|---|---|---|
| Numéro de la bande | Symbole | Gamme de fréquences (limite inférieure exclue, limite supérieure incluse) |
| 3 | ULF | 300-3 000 Hz |
| 4 | VLF | 3-30 kHz |
| 5 | LF | 30-300 kHz |
| 6 | MF | 300-3000 kHz |
| 7 | HF | 3-30 MHz |
| 8 | VHF | 30-300 MHz |
| 9 | UHF | 300-3 000 MHz |
| 10 | SHF | 3-30 GHz |
| 11 | EHF | 30-300 GHz |

**Bande Latérale Unique (BLU) -** Une onde porteuse est modulée en amplitude à 2 valeurs. Les deux bandes latérales transmettent la même information, on peut donc supprimer une bande sans pour autant perdre de l'information.

Système d'émission radio sans sous-porteuse, celle-ci étant restituée à la réception par l'oscillateur local du récepteur. La BLU autotrise une meilleure portée tout en restant moins sensible aux parasites atmosphériques pour une consomation moindre, au détriment de la qualité sonore.

**Bande passante -** (en téléphonie mobile) - La largeur (ou capacité) d'une voie de communication. La bande passante analogique se mesure en Hertz (Hz) ou cycles par seconde. La bande passante numérique correspond à la quantité ou au volume de données pouvant être envoyées par une voie de communication sans distorsion ; elle se mesure en bits par seconde. Ne pas confondre bande passante et "bande," par exemple quand on indique qu'un téléphone mobile fonctionne sur la bande 900 MHz. La bande passante est l'espace occupé sur cette bande. L'importance relative de la bande passante en téléphonie mobile réside dans le fait que la taille d'une voie ou bande passante, a des répercussions sur la vitesse de transmission. Un nombre important de données passant dans une voie étroite met plus longtemps à arriver à destination que dans une voie plus large.

Ainsi, les lignes téléphoniques analogiques traditionnelles ont une bande passante de 3100 hertz, car elles peuvent transmettre des signaux de fréquence supérieure à 300 hertz et inférieure à 3 400 hertz.

**Bande passante -** Désigne la capacité de transmission d'une liaison de transmission. Elle détermine la quantité d'informations (en bits/s) qui peut être transmise simultanément. C'est aussi la différence entre les fréquences les plus hautes et les plus basses disponibles pour les signaux du réseau. Ce terme est également utilisé pour décrire le débit évalué d'un média de transmission ou d'un protocole donné.

Dans le jargon des réseaux, la quantité de données que peut transporter un câble est déterminée par sa largeur de bande passante. En d'autres termes, par le nombre ou la taille des canaux électroniques disponibles sur la connexion réseau, qui est en général fonction du type de câble utilisé.

Tout ceci fonctionne comme les signaux radio. Les données électroniques se déplacent par vagues et plus la fréquence des vagues est élevée, plus le signal est de bonne qualité. Toutefois, les ondes haute fréquence parcourent des distances beaucoup moins grandes que les signaux basse fréquence. C'est pourquoi le son d'une radio grandes ondes est facile à capter mais de bien moindre qualité que celui d'une radio modulation de fréquence qui utilise des longueurs d'ondes plus courtes.

Le problème pour les ingénieurs réseaux est donc de faire en sorte que la connexion entre deux ordinateurs possède une capacité électronique - ou largeur de bande passante - suffisante pour recevoir la quantité de données qu'elle devra transporter. Si la largeur de bande passante est insuffisante, la connexion sera lente ou la transmission sera irrégulière et des données peuvent être perdues.

Chaque facteur qui complique la nature du signal à transporter s'ajoute aux paramètres auxquels doit répondre la largeur de bande. Les fichiers générés par le bureau d'étude, par exemple, seront très volumineux. Si les plans doivent être envoyés sur une machine, il faut aussi envoyer les données dont la machine aura besoin pour les interpréter.

La technologie réseau présente donc des avantages intrinsèques, mais il reste encore quelques problèmes à résoudre. Comme souvent, la solution est venue de l'industrie de la défense sous la forme d'Internet.

La bande passante d'une fibre optique est définie comme étant la fréquence maximum de transmission en Mhz pour laquelle le signal transmis subit un affaiblissement de 3dB. Plus la bande est large plus la capacité à supporter des transmissions hauts débits sera importante. Elle s'exprime en Mhz.km voire en Ghz.km. Elle dépend de la longueur d'onde de transmission, des paramètres physiques de la fibre ( diamètre de coeur, matériaux... ).

**BAS -** Broadband Access Server - Serveur d'accès large bande. Equipement dont la fonction est de gérer le transport de données en mode ATM dans le cadre des offres d'accès à Internet par ADSL. Sur le réseau de France Télécom, chaque BAS regroupe le trafic ATM issu d'une dizaine de DSLAM. Un BAS gère donc le trafic de l'ensemble des lignes ADSL situées dans les zones couvertes par les DSLAM qui lui sont connectés. La zone ainsi couverte par un BAS est appelée "plaque" par France Télécom. Il est établi un circuit ATM "montant" et un circuit ATM "descendant" entre chaque client connecté et le BAS auquel il est raccordé.

**Base de temps -** Structure de nature chronologique, basée sur des événements périodique.

**BASIC -** Beginnner's All-purpose Symbolic Instruction Code - Conçu en 1963 par deux professeurs de mathématiques du Darmouth College, le concept original était de développer un langage complet mais accessible à tous. Principale évolution : Le Visual Basic.

**Batterie -** (Téléphonie mobile) - Source d'alimentation d'un téléphone mobile. Les batteries utilisées dans les téléphones mobiles et appareils de communication sont des batteries rechargeables du type nickel cadmium, à hydrure métallique de nickel et au lithium. Voir également Li-Ion, NiCd, NiMH.

**Baud -** Unité de rapidité de modulation par seconde (du nom de l'ingénieur français Emile Baudot, inventeur du code télégraphique). Si le signal n'est constitué que de deux valeurs (signal binaire, 1 ou 0), le baud est équivalent au bit par seconde. Le baud, qui mesure la vitesse de modulation (sur une liaison analogique) et non un débit au sens strict, tend à disparaître au profit du "bit par seconde" devenu la principale unité officielle en télécommunications numériques.

**BC -** Committed Burst Size - Voir Frame Relay et Relais de Trame - Désigne le flot maximum de données (en bits) que le réseau autorise à transférer, dans des conditions normales, pendant un intervalle de temps T.

**BCAST -** Protocole de la famille Novell Netware. BCAST sert à diffuser les annonces du réseau informant l'utilisateur qu'il a bien reçu un message.

**BCS -** Bull Cabling System - Système de câblage préconisé par Bull. Le BCS référence des câbles et connecteurs à 9 contacts, en 120 Ohms, avec du câble MNC8 ou équivalent. Voir Câblage et Pré Câblage.

**Be -** Excess Burst Size - Voir Frame Relay et Relais de Trame - Le terme Be désigne le maximum de données durant la période T que l'utilisateur peut excéder audessus de Bc.

**BECN -** Backward Explicit Congestion Notification - Bit situé dans l'entête de la trame Frame Relay et initialisé par un nœud en l'état de congestion dans le réseau, l'objectif est de prévenir le destinataire que les trames qu'il va émettre se heurteront à des problèmes de congestion.

Il s'agit d'un bit positionné par le réseau Relais de Trames pour indiquer à un DTE (ETTD) que la procédure permettant d'éviter une congestion est initialisée.

**BGan -** Broadband Global Area Network - Solution de type service compatible 3G basée sur des satellites Inmarsat 4, offrant des circuits voix numérisés et des accès IP Duplex au débit maximal de 432 kbit/seconde. A noter que la commutation des circuits voix est réalisée "inboard (à bord du satellite)"

**BGCF -** Break out Gateway Control Function - Cette passerelle contrôle la compatibilité des équipements et renvoie les appareils non compatibles vers des passerelles spécifiques, permettant d'assurer la conversion entre le flux voix RTP et la téléphonie standard. Voir IMS.

**BGP4 -** Border Gateway Protocol - Protocole de routage de type PATH-vecteur [RFC 1771 - IPv4, 03/95 & RFC 2545 - IPv6, 03/99]. Chaque entité est identifiée par un numéro d'AS. La granularité du routage est le Système Autonome (AS). Le support de la session BGP est TCP (port 179). Les sessions BGP sont établies entre "borders routers", c'est un protocole point à point entre routeurs de bord d'AS, symétrique, et enfin un annonceur BGP n'est pas forcément un routeur.

Il existe 2 grandes familles de protocoles de routage :

- Les protocoles intérieurs (IGP)
  - Distance-vecteur : RIP, IGRP
  - État des liens : OSPF, IS-IS
  - Taille <100 routeurs, 1 autorité d'administration
  - Échange de routes, granularité = routeur
- Les protocoles extérieurs (EGP)
  - EGP, BGP, IDRP
  - Taille = Internet, coopération d'entités indépendantes
  - Échange d'informations de routage, granularité = AS

Rappel sommaire sur les types de protocoles de routage :

- distance vecteur : la distance est le nombre de routeurs pour joindre une destination, chaque routeur ne connaît que son voisinage et propage les routes qu'il connaît à ses voisins (ex. RIP).
- états des liens : chaque routeur connaît la topologie et l'état de l'ensemble des liens du réseau, puis en déduit les chemins optimaux. À chaque interaction les routeurs s'envoie toute leur table de routage (ex. OSPF).

Le protocole BGP peut être considéré comme à mi-chemin entre les deux types de protocoles précédents. En effet, l'échange de chemins d'AS permet à chaque routeur de reconstruire une grande partie de la topologie du réseau, ce qui est caractéristique des protocoles de type "état des liens", mais deux routeurs voisins n'échangent que les routes qu'ils connaissent, ce qui est caractéristique d'un protocole de type "distance-vecteur".

Règles de base pour les AS multi connectés en BGP :

- Les routeurs de bord d'un même AS échangent leurs informations de routage en I-BGP
- Les connexions en I-BGP forment un maillage complet sur les routeurs de bord d'un AS.
- Ce sont les IGP internes à l'AS qui assurent et maintiennent la connectivité entre les routeurs de bord qui échangent des informations de routage en I-BGP
- Le numéro d'AS est un numéro officiel (si connexions vers 2 AS différents)

Attention, dans un même AS, c'est bien l'IGP (ou le routage statique) qui est responsable de la connectivité interne de l'AS. Si un routeur de bord ne peut pas atteindre une route de son AS (qui lui a été annoncée par un voisin interne par exemple), il ne la propagera pas à ses voisins BGP (externes ou internes).

Détails sur un processus BGP :

Automate à 6 états, qui réagit sur 13 événements, Il interagit avec les autres processus BGP par échange de 4 types de messages :

- OPEN - 1er message envoyé après l'ouverture de la session TCP, il informe son voisin de sa version de BGP, son numéro d'AS, d'un numéro identifiant le processus BGP, propose une valeur de temps de maintien de la session (valeur suggérée : 90 secondes si 0 : maintien sans limite de durée, met le processus en attente d'un KEEPALIVE. En cas de démarrage simultané de deux sessions BGP par deux voisins, il faut choisir de ne conserver que l'une des deux connexions. Pour cela on ne conserve que celle ouverte par le processus de numéro identifiant le plus petit. Pour déterminer ce numéro identifiant, l'implémentation de Cisco choisit par défaut le plus petit numéro IP des interfaces connues.
- KEEPALIVE - Confirme un OPEN, réarme le minuteur contrôlant le temps de maintien de la session si temps de maintien non égal à 0, est réémis toutes les 30 secondes (suggéré). C'est un message de taille minimum (19 octets). En cas d'absence de modification de leur table de routage, les routeurs ne s'échangent plus que des messages KEEPALIVE toutes les 30 secondes, ce qui génère un trafic limité à environ 5bits/s au niveau BGP. L'implémentation BGP de Cisco porte par défaut à 60 secondes l'intervalle entre 2 messages KEEPALIVE.
- NOTIFICATION - Le message NOTIFICATION est envoyé au moindre incident lors du déroulement du processus BGP. Le message ferme la session BGP, fournit un code et un sous code

renseignants sur l'erreur, ferme aussi la session TCP, annule toutes les routes apprises par BGP. Le fait de supprimer lors de son arrivée toutes les routes apprises par BGP peut provoquer des instabilités de routage injustifiées (un incident ne veut pas forcément dire que toutes les routes apprises précédemment sont devenues fausses). Le message est émis sur incidents lorsqu'il n'y a pas de KEEPALIVE pendant 90s (<hold time>), lorsqu'un message incorrect arrive, s'il y a détection d'un problème dans le processus BGP,… Dans son implémentation de BGP, Cisco donne la possibilité de supprimer cette fonctionnalité, en conservant telle quelle la table de routage en cas de réception d'un message NOTIFICATION.

- UPDATE - C'est le message principal du protocole. Il sert à échanger les informations de routage (routes à éliminer (éventuellement), ensemble des attributs de la route, ensemble des réseaux accessibles (NLRI - chaque réseau est défini par (préfixe, longueur)), le message est envoyé uniquement si changement, il active le processus BGP avec modification des RIB (Update, politique de routage, conf.) et génère l'émission d'un message UPDATE vers les autres voisins. Lors du paramétrage d'un processus BGP il faut aussi faire un choix entre synchroniser ou pas les annonces (update) de l'IGP et les annonces BGP.

La taille des messages de 19 à 4096 octets, ils peuvent être éventuellement sécurisés par MD5. Les messages étant de longueur variable, ils sont marqués dans le flot d'octets du canal TCP par une séquence spéciale de trois octets qui repère leur début.

- La liste complète des événements pouvant arriver est la suivante :

1 : Démarrage BGP
2 : Fin BGP
3 : Session TCP ouverte
4 : Session TCP fermée
5 : Ouverture session TCP échouée
6 : Erreur fatale dans session TCP
7 : Minuteur ConnectRetry expiré
8 : Minuteur Hold Time expiré
9 : Minuteur KeepAlive expiré
10 : Réception d'un message OPEN
11 : Réception d'un message KEEPALIVE
12 : Réception d'un message UPDATE
13 : Réception d'un message NOTIFICATION

Les RFC et BGP4 :

- RFC1657 Définition of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4). S. Willis, J. Burruss, and J. Chu. 06/1995.(DS)
- RFC1771 A Border Gateway Protocol 4 (BGP-4). Y. Rekhter, T. Li. 03/1995. (DS)
- RFC1772 Application of the Border Gateway Protocol in the Internet. Y Rekhter, P. Gross. 03/1995. (DS)
- RFC1773 Experience with the BGP-4 protocol. P. Traina. 03/1995. (INFO)
- RFC1774 BGP-4 Protocol Analysis. P. Traina, Editor. 03/1995. (INFO)
- RFC1966 BGP Route Reflection An alternative to full mesh IBGP. T. Bates & R. Chandrasekeran. 06/1996. (EXP)
- RFC1997 BGP Communities Attribute. R. Chandra, P. Traina & T. Li. 06/1996. (PS)
- RFC1998 An Application of the BGP Community Attribute in Multi-home Routing. E. Chen & T. Bates. 06/1996. (INFO)
- RFC2042 Registering New BGP Attribute Types. B. Manning. 01/1997. (INFO)
- RFC2385 Protection of BGP Sessions via the TCP MD5 Signature Option. A. Heffernan. 08/1998. (PS)
- RFC2439 BGP Route Flap Damping. C.Villamizar, R.Chandra, R.Govindan. 1/1998. (PS)
- RFC2457 Definitions of Managed Objects for Extended Border Node. B. Clouston, . Moore. 11/1998. (PS)
- RFC2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing. P. Marques, F. Dupont. 03/1999. (PS)
- RFC2547 BGP/MPLS VPNs. E. Rosen, Y. Rekhter. 03/1999. (Status: INFO)
- RFC2796 BGP Route Reflection - An Alternative to Full Mesh IBGP. T. Bates, R. Chandra, E. Chen. 04/2000. (Updates RFC1966) (PS)
- RFC2842 Capabilities Advertisement with BGP-4. R. Chandra, J. Scudder. 06/2000. (PS)
- RFC2858 Multiprotocol Extensions for BGP-4. T. Bates, Y. Rekhter, R. Chandra, D. Katz. 06/2000. (PS)
- RFC2918 Route Refresh Capability for BGP-4. E. Chen, 09/2000. (PS)

- RFC3065 Autonomous System Confederations for BGP. P. Traina, D. McPherson, J. Scudder. 02/2001. (PS)

Bref historique de l'évolution du protocole BGP (voir RFC1773) :

- BGP-1 : RFC1105, juin 1989
- BGP-2 : RFC1163, juin 1990

La hiérarchisation des AS est supprimée (notion de liens inter-AS haut/bas/horizontaux), introduction des attributs de routes, beaucoup de changements dans les formats des messages.

- BGP-3 : RFC1267, octobre 1991

Détection et gestion des collisions d'ouvertures de sessions BGP, introduction d'un identifiant de routeur, le NEXT_HOP peut être situé dans un autre AS que celui du routeur qui fait l'annonce.

- BGP-4 : RFC1771, mars 1995

Ajout des adresses CIDR, introduction des ensembles d'AS (non ordonnés) dans les AS_PATH, et ajout des attributs de route MED (remplace INTER-AS METRIC), LOCAL-PRFERENCE, AGGREGATOR.

- BGP-4+ : RFC2283, février 1998 et RFC2545, mars 1999

Extensions multi protocoles (dont IPv6), Routage multicast

**Bi-Bande -** Téléphone mobile pouvant fonctionner sur deux bandes de fréquence comme la bande numérique 900 MHz et la bande GSM numérique 1800 MHz, par exemple. Les téléphones bi-bandes peuvent être utilisés en Europe, Afrique et Asie. Voir également Tri-bande.

En Wi-Fi, qualifie un équipement gérant les deux bandes de fréquence correspondant aux technologies a et b/g.

**Bidirectionnel (ou Duplex) -** Mode de transmission permettant le transfert d'informations dans les deux sens sur un même canal. Il peut être simultané (on parle souvent alors de "full duplex") ou non simultané. Dans ce dernier cas, les informations sont transmises alternativement dans un sens et dans l'autre (on dit aussi "half-duplex" ou "alternat").

**Bilan de liaison -** Calcul dont la finalité est de déterminer la qualité d'une liaison. Toute transmission de signal est soumise à un phénomène d'affaiblissement .

**Bilan optique -** En FTTH - Dans une transmission par fibre optique, on constate que toute l'énergie lumineuse entrante n'est pas récupérée en sortie. Il y a des phénomènes de dispersion, causes de perte (ou atténuation).

Le bilan de liaison optique est un calcul dont la finalité est de déterminer la qualité attendue ou mesurée de la liaison. Le bilan optique doit toujours tenir compte de la longueur d'onde dans laquelle le bilan est effectué ou estimé. In fine, la longueur d'onde à une incidence sur le bilan (voir tableaux ci-après).

Un bilan de liaison optique peut être estimé (calcul global sur la base d'éléments constituant le réseau) et / ou mesuré (avec un réflectomètre ou un photomètre).

Le bilan optique est la mesure de l'affaiblissement total entre deux points d'un réseau optique (en décibels).

Le bilan optique peut conduire à dimensionner :

- Le réseau (longueur, points de flexibilité, typologie, architecture…)
- Les équipements actifs (puissance d'émission, longueurs d'ondes…)
- Les équipements passifs (type de coupleur…)

Inversement, le signal transmis dans la fibre optique DOIT être atténué sans quoi le récepteur risque d'être « saturé ». Au même titre que l'œil humain ne doit pas regarder le soleil, le récepteur d'une liaison optique doit recevoir un signal dont l'intensité est « caractéristique».

Principales valeurs d'affaiblissement dans une liaison optique :

Les coupleurs (ou splitters)

| | 1x4 | 1x8 | 1x16 | 1x32 | 1x64 |
|---|---|---|---|---|---|
| Longueur d'onde | 1260 nm à 1360 nm et 1460 nm à 1650 nm | | | | |
| Perte d'insertion | 7,5 dB | 10,8 dB | 14,5 dB | 18,2 dB | 20,4 dB |

Les composants du réseau :

| | Connecteur SC/APC | Epissure fusion | Epissure mécanique | Prise (2 connecteurs + corps de traversée) | Liaisons Affaiblissement (en dB / km) | |
|---|---|---|---|---|---|---|
| Longueur d'onde | de 1260 nm à 1360 nm et de 1460 nm à 1650 nm | | | | 1310 nm | 1550 nm |
| Atténuation | 0,5 dB | 0,15 dB | 0,3 dB | 1,5 dB | 0,4 | 0,3 |

**Binaire -** Système fonctionnant en tout ou rien : zéro ou un.

**BISDN -** Broadband ISDN - RNIS large bande.

**Bit -** Abréviation pour "élément binaire" (Binary Digit) - Unité élémentaire d'information, en général utilisée pour coder une information. Elle s'exprime sous deux formes le 0 ou le 1, le langage des circuits électroniques (ouvert/fermé). Toute information (texte image ou son) peut-être exprimée par un bit.

En général, dans un ordinateur, dans une unité de stockage ou dans une chaîne de traitement numérique, les données sont représentées dans un code binaire, sous la forme de 1 ou de 0 appelés bits. Ces bits, pour faciliter la lecture, sont la plupart du temps regroupés en octets ou groupes de 8 bits, ou encore en mots. Un mot, qui sera en général la plus petite entité "adressable" dans un équipement informatique, peut regrouper 1,2 4 ou n octets. Les mots sont stockés dans des mémoires ou des registres. Mémoires et registres ne se distinguent que par le temps pendant lequel est conservée la donnée : un registre est une mémoire temporaire, le temps d'un calcul par exemple ; une mémoire peut être décrite comme un ensemble de nombreux registres où les informations sont conservées pendant des temps plus longs. Une donnée est représentée comme une succession d'état "haut" ou "bas", de "1" ou de "0" auxquels correspondent à un moment donné des niveaux de tension électrique dans un circuit de l'ordinateur.

**Bit par seconde (ou bps) -** Mesure du débit d'information sur une ligne de transmission de données.

**Bitmap -** Écran pour lesquels à chaque pixel correspond, dans la mémoire d'écran, une zone de mémoire directement accessible. Un programme peut ainsi changer la couleur d'un pixel en modifiant sa définition directement dans la mémoire d'écran.

**BitTorrent -** Système d'échange de fichiers adapté aux gros fichiers en mode P2P. BitTorrent n'est pas exploitée uniquement pour échanger des fichiers multimédias. Des éditeurs s'en servent pour diffuser leurs logiciels.

BitTorrent a été conçu pour le partage de fichiers volumineux, de type images ISO. Le fichier à distribuer n'est pas sur un serveur central (sauf lors de sa création), il est découpé en morceaux répliqués et répartis sur les PC de plusieurs utilisateurs. Il n'est pas nécessaire d'ouvrir un serveur dédié avec une bande passante importante.

Le logiciel client BitTorrent ne dispose pas de moteur de recherche, l'utilisateur doit savoir ce qu'il veut télécharger. Dans un premier temps, il télécharge, sur un site web un «torrent» : un fichier de description de très petite taille contenant les informations nécessaires au téléchargement et lisible par le client BitTorrent.

Ce torrent indique le nom du fichier, sa taille, le nombre de morceaux qui le composent et surtout le «tracker». Il s'agit d'un programme permettant d'identifier les adresses des personnes qui téléchargent le fichier recherché, ou qui ont terminé leur téléchargement mais laissent le fichier disponible dans son intégralité (les «seedem»). Conséquence, plus le fichier est téléchargé à un instant T, plus le nombre de machines recensées par les trackers est élevé, et par conséquent le téléchargement est rapide.

L'utilisateur récupère, dans n'importe quel ordre, les morceaux de fichiers disponibles. Pendant le téléchargement, le logiciel client vérifie à intervalles réguliers la liste des machines disponibles sur le réseau, ainsi que les morceaux de fichiers qu'elles détiennent. Inversement, l'utilisateur précise quelles parties il possède. Plusieurs morceaux du fichier peuvent être téléchargés simultanément. Le client vérifie leur intégrité. BitTorrent se veut plus équitable que d'autres systèmes P2P. Ainsi, le logiciel client envoie les morceaux du fichier en priorité aux PC depuis lesquels il a récupéré le plus de données. Les parties les moins répandues sont envoyées en premier.

**BLC -** Boucle Locale en Cuivre, par opposition à la Boucle Locale Radio. Ces expressions sont désormais remplacées par celles de "réseau d'accès (numérique) filaire ou radio "(Access Network), de façon à éviter la confusion avec les nouvelles architectures de réseau en anneau qui sont maintenant proposées pour la distribution optique.

**Blindage -** Couverture protectrice d'un câble qui élimine les interférences électromagnétiques et radioélectriques.

**Bloc -** Groupe de bits ou de caractères manipulés comme un tout cohérent. Il correspond souvent à une caractéristique physique d'un terminal (par exemple, le nombre de caractères affichés sur un écran d'ordinateur) ou à une entité logique à laquelle s'applique un système de détection ou de correction d'erreurs.

**Bloc numérique -** Un bloc numérique correspond au regroupement de plusieurs communications sur un même support physique de transmission, grâce à une technique appelée multiplexage. Dans la norme de transmission PDH (Plesiochronous Digital Hierarchy), traditionnellement utilisée sur les réseaux de télécommunications, les communications peuvent être regroupées en blocs primaires numériques ou BPN (30 communications), puis en blocs secondaires numériques ou BSN (120 communications), puis en blocs tertiaires numériques (480 communications), puis en blocs quaternaires numériques (1920 communications). Chaque bloc numérique correspond à un débit ou à une capacité, exprimée en bits par seconde, le bit désignant l'élément binaire numérique de base (qui peut prendre deux valeurs : 1 ou 0). Ainsi le BPN correspond à un débit de 2Mbit/s. Dans le cadre de l'interconnexion, la tarification peut être établie en fonction de la capacité de transmission, exprimée en BPN.

**Blog -** Le terme Blog provient de la contraction des mots Web Log (carnet de bord web en anglais). C'est un espace réservé et personnel mis à disposition par un hébergeur qui permet de publier facilement des actualités ("Articles", "Notes", "Billets" ou "Posts" dans la langue des blogueurs) sur un sujet, de les illustrer de façon multimédia (dessins, photos, vidéos, sons…) et de recueillir les commentaires des visiteurs sur ses articles. Les articles sont consultables dans l'ordre chronologique inverse (du plus récent au plus ancien). Un blog est consultable en permanence par tous les internautes de la planète. A la différence d'un site Internet personnel, le blog est plus simple et interactif. Le blog est un moyen de communication de plus en plus répandu.

**Blooming -** Expression utilisée pour désigner l'éblouissement des cellules d'un capteur numérique en cas de forte luminosité.

**BLR -** Boucle Locale Radio - Elle consiste à établir un réseau de boucle locale en substituant aux fils de cuivre qui équipent aujourd'hui les réseaux une technologie radio offrant l'avantage d'une plus grande souplesse pour le déploiement des infrastructures. Elle permet de raccorder le client final au réseau d'un opérateur de télécommunications en utilisant la transmission hertzienne ou radio. Cette technologie constitue une alternative au réseau filaire et offre de hauts débits. En France, les licences d'exploitation ont été attribuées en août 2000.

La Boucle Locale est définie comme étant le moyen de transmission entre l'abonné et le central téléphonique local. La Boucle Locale Radio s'applique à toutes les techniques ou applications par lesquelles la connexion est partiellement ou entièrement réalisée par des moyens et/ou technologies radios ➔ Utilisation des technologies Radio pour raccorder les abonnés au Réseau Téléphonique Public Commuté en lieu et place de la aire de câble cuivre traditionnelle.

L'exploitation commerciale de la BLR se fait dans deux bandes distinctes, la bande 3,5 GHz et la bande 26 GHz. Les caractéristiques physiques différentes des gammes de fréquences 3,5 GHz et 26 GHz sont complémentaires : les fréquences en 26 GHz peuvent être utilisées pour desservir les zones plus denses ou les clients aux besoins en débits plus élevés ; tandis que la portée plus grande des systèmes en 3,5 GHz peut être exploitée afin de couvrir des zones géographiques plus étendues dont la densité en trafic est moins importante. Les solutions utilisées sont normalisées ou propriétaires, les technologies sont analogiques ou numériques.

La BLR se présente sous 3 modèles :

- Isolé (Point à Point) : Permet de raccorder un site à un réseau existant. On trouvera ce modèle dans la conception de nouveau site ou dans le rattachement d'une ville nouvelle à un réseau existant. Le faisceau radio, souvent directionnel, permet des débits d'information importants sur des distances supérieures à 15 kilomètres. Les systèmes point à point n'ont pas été spécifiquement conçus pour des applications de Boucle Locale Radio : leur champ d'application initial est plutôt l'établissement du réseau d'infrastructures (faisceaux hertziens). Ils peuvent toutefois être également utilisés en application "boucle locale radio" pour desservir des habitats ruraux isolés. France Télécom par exemple exploite des systèmes en bandes VHF et UHF développés spécifiquement pour la desserte de certains abonnés ruraux.
- En étoile (Point à Multiploint) : Plutôt destiné à un milieu urbain ou sub urbain, ce modèle est avant tout destiné, de part sa conception, à des débits assez faibles (autour de 2 Mbits seconde) et sur des distances relativement courtes compte tenu de la faible directivité des faisceaux (antenne omnidirectionnelle). Les systèmes point-multipoints peuvent être schématiquement présentés comme des systèmes cellulaires où tout terminal dans la zone de couverture peut avoir accès au réseau. Toutefois, le système ne possédant pas les fonctionnalités permettant de gérer les mouvements du terminal, celui-ci doit rester fixe. Ces systèmes n'ont pas vocation à offrir une couverture continue. En général, le terminal de l'abonné est relié par voie filaire jusqu'à une antenne placée en extérieur, sur le toit des habitations ou de locaux techniques par exemple. L'équipement de l'abonné peut être aussi branché directement dans un coffret avec antenne.
- Arborescent = C'est une combinaison des modèles ci-dessus. Des faisceaux directifs à haut débit permettent de raccorder des sites omnidirectionnels pour un rattachement à plus bas débit. Ce modèle convient assez bien à une implantation de service dans les zones rurales ou à faible densité d'habitants.

**Bluesnarfing -** Attaque dirigée vers un appareil Bluetooth sans que rien ne s'affiche à l'écran. Certains terminaux contiennent des failles de sécurité qui rendent possible ce genre d'attaque. En général, cela nécessite pour le "pirate" des moyens particuliers (un ordinateur, un émetteur récepteur Bluetooth, les logiciels adéquats.

**Bluetooth -** Technologie permettant de faire communiquer entre eux, sans câble et dans un rayon de couverture radio limité, différents objets mobiles (ordinateur portable, téléphone mobile…). La technologie Bluetooth est le fruit des efforts conjugués des principales sociétés des secteurs de l'informatique et des télécommunications, regroupées en un groupe d'intérêt (SIG) Bluetooth.

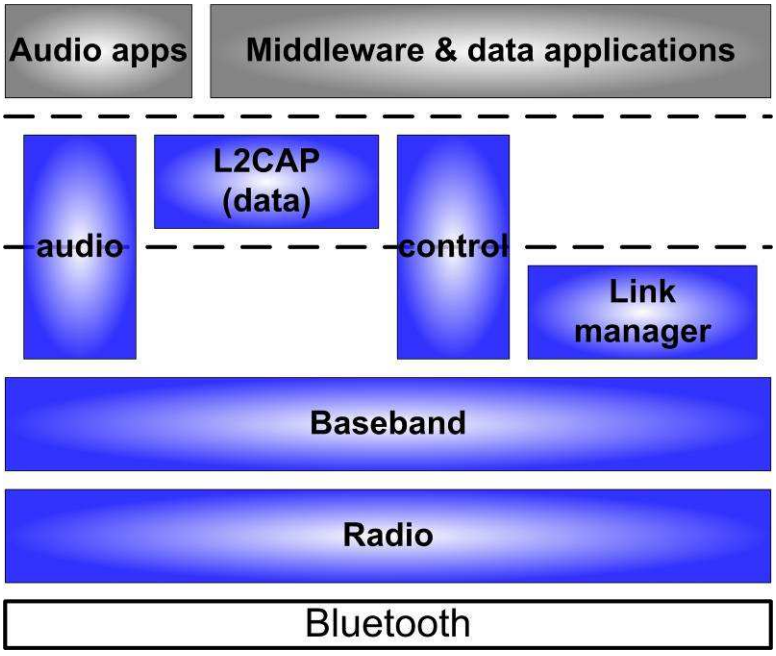
La communication Radio Bluetooth fonctionne selon le principe de la modulation de fréquence : l'onde

porteuse est modulée en fonction des données qu'elle transporte. La modulation employée est de type GFSK - Gaussian Frequency Shift Keying - un élément binaire se traduit par une déviation de fréquence. Bluetooth bénéficie de divers algorithmes de correction d'erreur pour lutter contre les pertes de données. Au niveau physique, Bluetooth utilise la technologie par saut de fréquence (FHSS) pour minimiser au maximum les interférences sur 79 canaux dans la bande 2,402 à 2,480 GHz. Le réseau est basé sur un système maître/esclave, et le maître décide des sauts de fréquence de façon pseudo-aléatoire, 1600 fois par seconde. La norme 1.0A définie en juillet 1999 prévoyait un débit brut de 1 Mbps (soit 720 kbps). Nul doute que ce débit sera amené à augmenter par la suite, même si la version 1.1, approuvée en mars 2001, ne le prévoit pas encore.

L´envoi des informations s´effectue par paquets, comme lors des communications par IP. Ces paquets sont encadrés de blocs de données de contrôle identifiant notamment l´appareil auquel sont destinées les informations. Ces données de contrôle permettent de plus la mise en réseau des appareils équipés de la puce.

Le contrôle des données effectué sur les paquets émis permet également d´adapter le débit au type d´informations circulant en fonction des appareils connectés.

Architecture du protocole :




Baseband layer - Cette couche permet de définir trois types de liens :

- Les liaisons SCO (Synchronous Connection-Oriented) pour l'audio (ou audio et données),
- Les liaisons ACL (Asynchronous Connectionless) pour les données. Dans le cas où les débits montants et descendants ne sont pas égaux, les liaisons ACL peuvent être asymétriques.
- Les liaisons de base : pour toute la gestion des connexions au sein du piconet

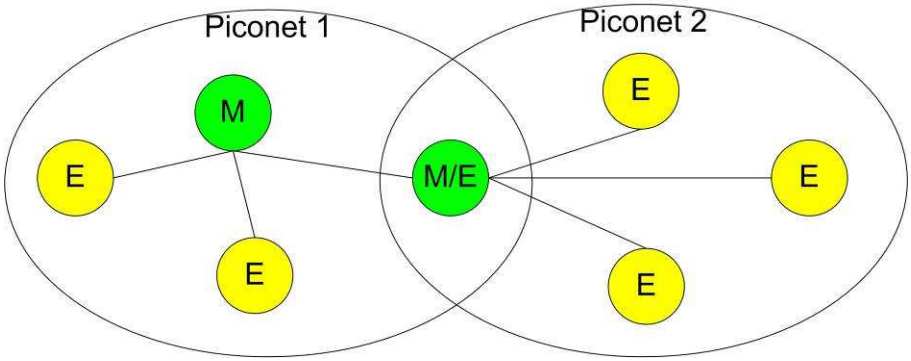
Les paquets ont alors la forme suivante :


Le code d'accès permet la synchronisation des composants Bluetooth.

L'entête stocke le numéro de paquet, l'adresse source et destination, le type de paquet, le CRC…

Link manager protocol - Ce protocole est responsable de la supervision des différentes connexions, de l'authentification des appareils, et du chiffrement. Il gère également les mises en veille des différents appareils.

Link Layer Control & Adaptation (L2CAP) - Cette couche permet l'adaptation des protocoles supérieurs (comme TCP/IP) au réseau Bluetooth : elle supporte la segmentation et le réassemblage, et le multiplexage de protocole.




Les machines d'un réseau Bluetooth se rassemblent en sous-réseaux appelés piconets. Dans ce piconet, une des machines joue le rôle de maître, et gère à ce titre l'horloge et les sauts de fréquence. Chaque maître peut accueillir jusqu'à 7 esclaves actifs, soit 8 appareils actifs maximum par piconet.

Plusieurs piconets adjacents constituent un scatternet et peuvent interagir. Une machine peut ainsi être esclave d'un piconet et maître d'un autre. Chaque piconet dispose d'un débit de 1 Mbps. 10 scatternets peuvent ainsi interagir, soit 72 appareils maximum (8 x 10 - 8 appareils).

On peut distinguer trois types de liaisons :

- Les liaisons synchrones à débit élevé,
- Les liaisons asynchrones,
- Les canaux voix/données.

Les liaisons synchrones :

Les connexions synchrones possèdent un débit bidirectionnel de 432 Kb/s. Les données transitent avec la même rapidité de l´esclave vers le maître que dans le sens inverse. Ce type de liaison s´avère particulièrement adapté lorsque deux appareils ont le même besoin de puissance de communication. Typiquement, c´est le lien qui sera privilégié dans la cadre d´une interconnexions de plusieurs ordinateurs en picoréseau, quand plusieurs utilisateurs souhaitent accéder aux données de chacun. Une machine maître peut supporter jusqu´à 3 liaisons du type synchrone avec ses esclaves.

Le flux de données étant continu, il n´y a jamais de rupture du débit. Cela n´empêche pas en revanche les possibles pertes d´informations dues à une erreur de décodage de l´information envoyée. Un paquet signifiant l´erreur est alors envoyé à l´émetteur qui ré adresse l´information. Aussi pratique que ce soit lors des échanges de données entre deux machines, ce contrôle d´erreur et les pertes d´informations momentanées potentielles rendent impossible l´utilisation de ce type de liaison avec des appareils dont le but serait de faire transiter des sons tels que la voix, comme avec les téléphones, ou encore avec le casque présenté par Ericsson au Comdex.

Les liaisons asynchrones :

Le mode asynchrone privilégie un débit élevé dans une direction: 721 kb/s dans un sens, contre seulement 57,6 kb/s dans l´autre. La direction peut être fixée temporairement par l´utilisateur ou par l´application et implique la définition d´un maître et d´un esclave entre les périphériques communicants. C´est la solution qui sera retenue en principe dans le cadre d´un accès à Internet via Bluetooth si les téléchargements sont plus fréquents que les uploads. De même, cette solution sera également celle préférée pour les imprimantes. Il est en effet inutile de réserver une large bande aux communications de l´imprimante vers le poste de travail. En revanche, les communications asynchrones peuvent présenter des discontinuités. Elles ne sont donc pas adaptées à la transmission de parole, de vidéo (même si le débit actuel, limité à 1 Mbits/s ne permet pas d´envisager de toute façon de solution plein écran), ou de musique.

Les canaux voix/données :

Enfin, Bluetooth propose trois canaux dits "vocaux" synchrones. Bidirectionnels, ils possèdent un débit de 64 Kb/s. Plus clairement, le débit de 64 Kb/s est assuré simultanément en envoi et en réception et s´avère donc particulièrement adapté à la transmission de la voix ou de tout fichier numérique devant être reconstitué en temps réel : communication téléphonique, MP3, etc.

Le groupe de travail IEEE 802.15.1 travaille actuellement sur la normalisation de Bluetooth.

Sur le plan de la sécurité, des systèmes sont bien sûr en place : authentification et chiffrement jusqu'à 128 bits.

Le standard Bluetooth définit en effet 3 classes d'émetteurs proposant des portées différentes en fonction de leur puissance d'émission :

| Classe | Puissance (affaiblissement) | Portée |
|---|---|---|
| I | 100 mW (20 dBm) | 100 mètres |
| II | 2,5 mW (4 dBm) | 15-20 mètres |
| III | 1 mW (0 dBm) | 10 mètres |

Le standard Bluetooth définit un certain nombre de profils d'application permettant de définir le type de services offerts par un périphérique Bluetooth. Chaque périphériques peut ainsi supporter plusieurs profils de type :

- Advanced Audio Distribution Profile (A2DP) : profil de distribution audio avancée
- Audio Video Remote Control Profile (AVRCP) : profil de télécommande multimédia
- Basic Imaging Profile (BIP) : profil d'infographie basique
- Basic Printing Profile (BPP) : profil d'impression basique
- Cordless Telephony Profile (CTP) : profil de téléphonie sans fil
- Dial-up Networking Profile (DUNP) : profil d'accès réseau à distance
- Fax Profile (FAX) : profil de télécopieur
- File Transfer Profile (FTP) : profil de transfert de fichiers
- Generic Access Profile (GAP) : profil d'acc&egave;s générique
- Generic Object Exchange Profile (GOEP) : profil d'échange d'objets
- Hardcopy Cable Replacement Profile (HCRP) : profil de remplacement de copie lourde
- Hands-Free Profile (HFP) : profil mains libres
- Human Interface Device Profile (HID) : profil d'interface homme-machine
- Headset Profile (HSP) : profil d'oreillette
- Intercom Profile (IP) : profil d'intercom (talkie-walkie)
- LAN Access Profile (LAP) : profil d'accès au réseau
- Object Push Profile (OPP) : profil d'envoi de fichiers
- Personal Area Networking Profile (PAN) : profil de réseau personnel
- SIM Access Profile (SAP) : profil d'accès à un carte SIM
- Service Discovery Application Profile (SDAP) : profil de découverte d'applications
- Synchronization Profile (SP) : profil de synchronisation avec un gestionnaire d'informations personnelles (appelé PIM pour Personal Information Manager).
- Serial Port Profile (SPP) : profil de port série

**Bluetooth 2 -** Aussi appelé 802.15.3 - Standard qui prévoit le triplement du débit de la spécification 1.2 (1Mbit/seconde théorique, 721 kbit/seconde effectif) dans la même bande de fréquence (2,4GHz).

La mise en œuvre du protocole EDR (Enhanced Data Rate) qui agit au niveau de la modulation radio sans compromettre la compatibilité ascendante, associé à un niveau d'erreur plus faible, permettent cet accroissement de la bande passante.

**Blu-Ray -** Format d'enregistrement sur support numérique de 12 cms de diamètre, utilisant un faisceau laser de couleur bleue (le CD utilise une couleur plutôt rouge). Ce support, dans ce format, permet de stocker 25 Go de données par couche (dounc 50 Go de données en double couche.

**BNC -** Connecteur pour câble coaxial.

**BOC -** Bell Operating Company - Société américaine de télécommunications issue du démantèlement d'AT&T (en 1984) et exploitant les réseaux de ses 22 anciennes filiales locales. Les BOC sont au nombre de 7 : Ameritech, Bell Atlantic, Bell South, Nynex, Pacific Telesis, Southwestern Bell et US West. Leur activité ne se limite plus aux Etats-Unis et touche les autres continents.

**Bogue -** Défaut de conception ou de réalisation se manifestant par des anomalies de fonctionnement.

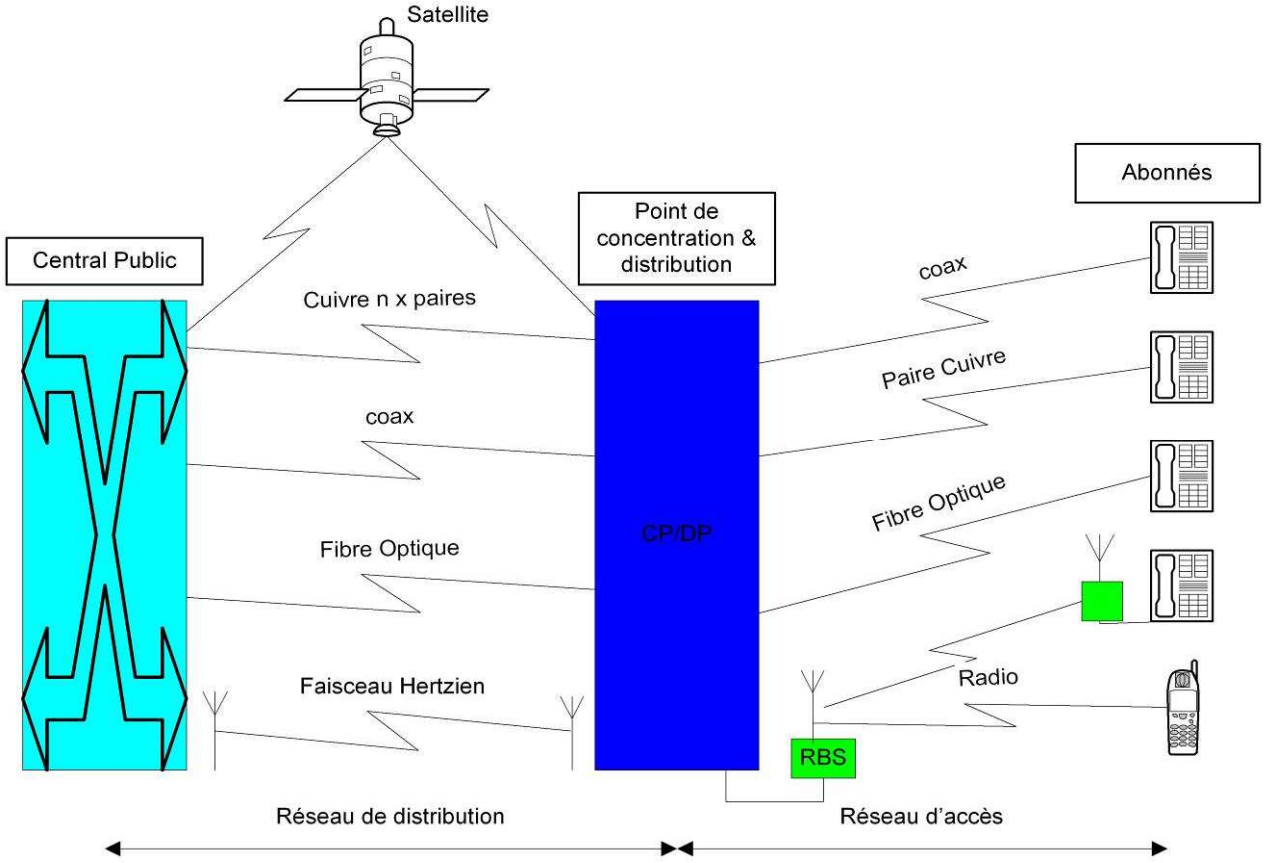
**Bookmark -** en français « marque-page », est employé de façon similaire aux marques-pages utilisés avec les livres pour retrouver la page à laquelle la lecture avait été interrompue. Appelé aussi « favori », ou signet, le marque-page électronique des navigateurs internet permet à son utilisateur de mettre en mémoire une adresse web afin de pouvoir y revenir ultérieurement.

**Boucle Locale -** Appelé aussi dernier kilomètre, c'est la portion de ligne téléphonique qui relie l'abonné à son central téléphonique.

La Boucle Locale est définie comme étant le moyen de raccordement entre l'abonné et le central téléphonique local ou encore la partie terminale du réseau de télécommunications donnant accès à l'abonné. Ce peut être aussi une solution radio ou filaire pour transmettre à une échelle locale (quartier, ville, région) des données à différents réseaux secondaires raccordés sur la "boucle", ensemble des liens filaires ou radioélectriques existant entre le poste de l'abonné et le commutateur d'abonnés auquel il est rattaché.

La boucle locale constitue un enjeu important pour les opérateurs et un marché croissant pour les industriels.

La boucle locale peut utiliser les supports suivants : Paire cuivre, Fibre Optique, Câble coaxial, Radio…




Représentation schématique de la boucle locale

**Box -** Une box (de l'anglais signifiant littéralement « boîte ») est, selon un terme générique utilisé en France, un décodeur ou adaptateur sous forme de boitier qu'un fournisseur d'accès à Internet fournit à ses abonnés au haut débit (par ADSL ou câble) pour bénéficier du « triple-play », d'un bouquet de services annexes à l'accès à Internet (téléphonie IP et télévision IP en HD de plus en plus souvent), et de fonctionnalités supplémentaires à un modem classique (routeur, Wi-Fi, gestion du CPL, partage de connexion).

En France, le premier FAI à en proposer une a été l'opérateur Free. Devant le succès rencontré par la « Freebox », l'ensemble des opérateurs a proposé un concept similaire.

**BPAM -** Business Process and Applications Management - Service consistant pour une S.S.I.I. à prendre en charge la responsabilité complète de la gestion d'une partie du système d'information de son client.

**BPM -** Business Process Management - Modélisation des processus métier - Consiste à modéliser le fonctionnement de l'entreprise à partir de diagrammes de flux et à recenser l'ensemble des intervenants - humains ou applicatifs - qui participent à un processus. Chaque action est associée à un processus et répertoriée dans un référentiel.

**BPO -** Business Process Outsourcing - Souvent raccourci en "Outsourcing" - Externalisation d'une des fonctions de l'entreprise

**Bps -** Voir Bit par seconde.

**BR -** Bureau des Radiocommunications de l'UIT.

**Bracketting -** Méthode consistant à prendre plusieurs fois la même vue avec des paramètres d'exposion différents. Cette technique est utilisée entre autre pour la mise au point de la balance des blancs, mais surtout pour apprécier la mise au point ou la profondeur de champ.

**BRAN -** Broadband Radio Access Network - Réseau d'accès radio large bande - Projet mené par l'Etsi (European Telecommunications Standards Institute) visant à développer de nouveaux standards de réseaux qui fourniront des accès radio à large bande. L'un des standards soutenus au sein du projet BRAN est HiperLAN/2.

**Brassage -** Action d'interconnecter, par des cordons adaptés, les liens arrivant sur les panneaux de brassage dans une armoire ou un coffret.

**Brasser -** Modification par le biais d'un branchement de l'affectation d'une liaison d'un réseau munie d'un connecteur sur un panneau de connecteurs relié à un autre réseau.

**Brasseur Optique -** Les brasseurs optiques ont trois fonctions : la commutation de fibres (commutation spatiale pure), la commutation et la conversion de longueurs d'onde.

Ces fonctions de brasseur optique sont encore trop souvent assurées par du matériel électrique; le temps de conversion des signaux électrique en signaux optiques et inversement est important. Une meilleure exploitation de la fibre et de DWDM passe donc par la mise en place de réseaux tout optique dotés de brasseurs optiques performants.

**BRI -** Basic Rate Interface - Accès de base du RNIS, composé de 2 canaux B (soit 128 kbps), et un canal D à 16 kbps pour la signalisation.

**Bribe -** Partie temporelle du signal représentant un symbole, émise avec des caractéristiques distinctes de celles des autres parties du même signal, selon une loi déterminée. Dans la modulation à spectre étalé à séquence directe, une bribe correspond à un élément de la suite superposée au signal à transmettre. Dans la modulation à spectre étalé à sauts de fréquence, une bribe correspond à l'intervalle de temps pendant lequel le signal reste sur une des fréquences porteuses.

**Broadband -** Désigne un système qui permet une vitesse de transmission supérieure à 2 Mbit/s.

**Broadcast -** Diffusion - Configuration dans laquelle un équipement transmet simultanément en direction de plusieurs équipements.

**Browser -** Application pour rechercher des informations sur des ressources en environnement Internet (WWW, FTP...)

Le terme « Browser » vient du verbe « to browse » qui veut dire « feuilleter un livre », il s'agit d'un logiciel de navigation qui permet de se déplacer d'un serveur à un autre et, à l'intérieur d'un serveur donné, d'accéder aux différentes ressources documentaires.

Les principaux browsers du marché sont Internet Explorer (Microsoft), Netscape Navigator (Netscape), FireFox, Opera,…. Les Québécois disent volontiers fureteur ou butineur.

Le terme navigateur que l'on utilise en français vient de Netscape Navigator.

**Bruit -** Noise - Ensemble des composantes aléatoires et non significatives d'un signal introduites par des perturbations soit internes (composants électroniques), soit externes (champs magnétiques, radiations naturelles).

Phénomène apparemment aléatoire de même nature qu'un phénomène déterministe tel qu'un signal en télécommunication.

Généralement, un bruit peut être considéré comme un signal non désiré accompagnant un signal désiré.

Le bruit numérique n'a rien de sonore, il s'agit de la détérioration d'un signal électronique amplifié.

En photo numérique, le bruit se traduit par des pixels indésirables qui donnent un aspect granuleux à l'image.

**BSC -** Base Station Controler - Contrôleur de Station de Base - Multiplexeur transmettant l'appel au commutateur sur le réseau filaire. Voir aussi Contrôleur de station de base.

Le contrôleur de station reçoit diverses mesures de la BTS. Il est en charge de les analyser pour gérer la ressource radio, commander l'allocation des canaux, contrôler les puissances d'émission du mobile et prendre la décision du handover. Il réalise de plus la concentration des circuits vers le MSC.

Du point de vue des stratégies de déploiement, les opinions des divers constructeurs d'infrastructure divergent. Certains préfèrent des BSC de faible capacité, leur nombre étant plus grand la distance BTS-MSC est plus faible, d'autres le contraire. Seule une étude économique globale permet d'adopter la stratégie de déploiement la plus adaptée.

**BSC -** Binary Synchronous Communications - Protocole de liaison de données synchrone introduit par IBM. Procédure de transmission synchrone de blocs de 8 bits dans un environnement IBM. Tend à laisser la place au SDLC.

**BSI -** British Standards Institute - Organisme britannique de normalisation membre de l'ISO (International Standard Organisation), équivalent de l'Afnor française.

**BtoB -** Business to business - S'écrit également "B2B" - Relations client ↔ fournisseur entre deux entreprises.

**BtoC -** Business to Customer - S'écrit également "B2C" - Relations client ↔ fournisseur entre une entreprise et son client final.

**BTS -** Base Terminal Station - Station de base - Station radio relayant l'appel vers un contrôleur de station de base. Voir aussi Station de base.

Une BTS est un ensemble de TRX qui sont des émetteurs-récepteurs. La fonction principale d'une BTS est d'assurer la transmission radio en effectuant des opérations telles que la modulation, la démodulation, l'égalisation, le codage correcteur d'erreurs.

La BTS est en charge de la gestion de la couche physique : multiplexage TDMA, saut de fréquence et chiffrement. Elle réalise tout un ensemble de mesures vérifiant le bon déroulement de la communication. Ses mesures ne sont pas exploitées directement par la BTS mais sont transmises au BSC de rattachement.

La BTS gère la couche liaison de données pour les échanges de signalisation entre les MS et l'infrastructure GSM, ainsi que la liaison de données avec la BSC pour assurer la fiabilité du dialogue. Ces liaisons s'appellent LAP D.

La capacité d'une BTS est définie par le nombre de TRX qu'elle contient. Le maximum étant de 16 porteuses, la moyenne en zone urbaine est généralement de 2 à 4 TRX voir une unique porteuse en zone rurale. Chaque porteuse permet 7 connexions en simultanées.

Il existe différent type de BTS :

- Les BTS rayonnantes sont situées sur des points hauts. Comme leur nom l'indique, elles émettent dans toutes les directions. La limitation des ressources radio leur interdit l'usage en zone urbaine car elles occupent toute la bande passante sur un large périmètre d'environ 20 km de rayon.
- Les BTS ciblées sont utilisées dans des zones plus denses que les rayonnantes. Leur angle d'émission très précis permettent de réutiliser le canal dans une cellule proche.
- Les micro-BTS sont celles utilisées en zone urbaine. Leur champ d'action est très faible, elles sont donc très nombreuses dans des grandes villes comme Paris. Leur petite taille leur permet de se fondre dans le paysage. Leur coût est plus faible que celui d'une BTS normale.

**BTU -** British Thermal Unit - Unité Thermique Anglaise - Cette unité de mesure est souvent utilisée les fabricants de matériel de climatisation ou par les "thermiciens".

Il s'agit d'une mesure anglaise qu'il faut convertir en système métrique si nécessaire.

Tableau de correspondance :

| | Horse power | Kilogramme force mètre/seconde | Joule/sec = Watt | Kilowatt | Kilocalorie | British thermal unit par second |
|---|---|---|---|---|---|---|
| 1 hp | 1 hp | 76,04 kgf m/s | 745,7w | 0,7457 kw | 0,1782 kcal/s | 0,7073 btu/s |
| 1 kgf m/s | 13,15. 10-3 hp | 1 kgf m/s | 9,807w | 9,807. 10-3 kw | 2,344. 10-3 kcal/s | 9,296. 10-3 btu/s |
| 1 j/s = 1 w | 1,341. 10-3 hp | 0,102 kgf m/s | 1w | 10-3 kw | 239. 10-6 kcal/s | 948,4. 10-6 btu/s |
| 1 kw | 1,341 hp | 102 kgf m/s | 1 000w | 1 kw | 0,239 kcal/s | 0,9484 btu/s |
| 1 kcal/s | 5,614 hp | 426,9 kgf m/s | 4 187w | 4,187 kw | 1 kcal/s | 3,968 btu/s |
| 1 btu/s | 1,415 hp | 107,6 kgf m/s | 1 055w | 1,055 kw | 0,252 kcal/s | 1 btu/s |

**Buffer -** Unité de stockage temporaire utilisée pour compenser une différence de débit et de flux de données entre deux équipement.

**Bus -** Ensemble physique de canaux de transmission capables de délivrer simultanément la même information à plusieurs entités. Très utilisée en informatique, par exemple pour relier les différents éléments d'un ordinateur (mémoire, cartes de contrôle des périphériques), cette notion très générale concerne surtout, en transmissions de données, les réseaux locaux. C'est notamment la topologie utilisée par les réseaux de type Ethernet, ou dans le domaine industriel le réseau MAP (Manufacturing Automation Protocol) dit "bus à jeton" (Token bus).

Support de transmission non bouclé qui permet d'assurer les transferts d'information entre différentes stations.

Principe de transmission des données par paquets codés sur un même câble (ETHERNET).

**Bus PCI -** Norme définissant l'emboîtement physique des éléments, signaux électriques échangés et structure du dialogue entre les périphériques qui composent un ordinateur personnel. Le bus PCI (Peripheral Component Interconnect) est un intermédiaire entre le jeu de composants et les périphériques d'entrée/sorties. Il est constitué de pistes parallèles tracées sur la carte mère qui relient électriquement tous les circuits et les cartes branchés sur le bus. Son débit (133 Mo par seconde pour le Bus PCI à 32 bits) est partagé par tous les périphériques reliés au BUS.

**Bus PCI Express -** Evolution du Bus PCI, dont la partie "bus" a été remplacée par un commutateur. Le débit n'est plus partagé entre les périphériques, l'architecture évolue d'un mode parallèle à un mode série. Avec PCI Express, ce sont des liaisons série rapides qui relient les périphériques deux à deux. Chaque lien série élémentaire fonctionne à 2,5 Gbit/seconde (250 Mo / seconde) et ne consomme que 0,8 V. Rien n'empêche de faire fonctionner plusieurs liens série en parallèle pour un même périphérique, ce qui accroît le débit. On parle alors de PCI Express Nx (où N exprime la quantité de liens série utilisés par le périphérique).La norme PCI Express actuelle va jusqu'à 32x. En 16x, le débit atteint 4 Go / seconde.

**Bus PCI-X -** Bus d'extension 64 bits, évolution du bus PCI 64 bits avec une fréquence de fonctionnement de 100 ou 133 MHz.

**Byte -** Correspond généralement au français octet, groupe de 8 bits représentant un caractère de données.

# C

**C4ISR -** Command, Control, Communication, Computer, Information, Surveillance and Reconnaissance.

**CAA -** Commutateur à Autonomie d'Acheminement ou commutateur d'abonnés - Commutateur du réseau téléphonique de France Télécom auquel sont raccordés les abonnés. Le réseau de France Télécom étant organisé de façon hiérarchique, le CAA correspond au niveau le plus bas dans la hiérarchie des commutateurs qui équipent le réseau. On distingue ainsi deux catégories de commutateurs :

Les commutateurs d'abonnés (ou CAA) sont les plus bas dans la hiérarchie. Les abonnés y sont reliés par l'intermédiaire d'une Unité de Raccordement d'Abonné (URA).

Les commutateurs de transit (CT) correspondent au niveau le plus élevé.

**Câblage croisé -** Schéma de câblage qui permet à deux DTE ou à deux DCE de communiquer entre eux. Les conducteurs se connectent à un numéro de broche différent à chaque extrémité du câble.

De façon générique, on constatera qu'une paire émission est croisée avec la paire réception cas d'un câblage croisé en Ethernet = On envoie ainsi l'émission vers la réception. Ce même principe est conservé dans les autres liaisons.

**Cablage et Precablage -** Le câblage représente l'un des supports de transmission de l'information. L'information transportée peut être de différente forme. Il existe en effet différentes données susceptibles d'être transmises, et ce avec des contraintes de temps, de qualité, de sécurité, de transport, de vitesse, qui sont propres. Dans le cas d'un câblage de bâtiment, le câble devra servir de support de transmission à la voix (le téléphone), aux données numériques variées que l'informatique a multipliées (accès au RNIS, liaison de type terminal asynchrone, réseau locaux, contrôle d'accès, ...).

La transmission est basée sur le principe de la propagation des ondes :

- Ondes électriques se déplaçant dans des lignes bifilaires (câbles),
- Ondes électromagnétiques se propageant en milieu aérien (faisceau hertzien),
- Ondes lumineuses se déplaçant en milieu aérien ou dans des fibres optiques.

Chaque support de transmission doit répondre à des caractéristiques précises permettant sa mise en œuvre dans un contexte donné, ses caractéristiques sont les suivantes :

- Largeur de bande et bande passante,
- Débit d'information binaire,
- Atténuation caractéristique,
- Impédance,
- Rapport signal/bruit,

Remarque : Chacune des caractéristiques d'un support d'information a (ou peut avoir) une incidence sur une autre caractéristique. Par exemple, le débit d'information est lié à la largeur de bande et bande passante, le rapport signal/bruit varie constamment dans le temps puisque le bruit n'est pas uniforme, le bruit étant un phénomène aléatoire, néanmoins mesurable, auquel sont soumis les supports (le bruit est l'ensemble des perturbations qui affectent la transmission)...

Le rapport signal/bruit est mesuré en décibel sur un intervalle de temps, une moyenne étant établie.

Enfin il est judicieux de rappeler ici que si la transmission peut être affectée par des rayonnements électromagnétiques ou d'autres origines, l'augmentation de la fréquence de transmission ou l'augmentation du débit d'informations transportées peut induire un phénomène inverse, le support de transmission devenant alors élément perturbateur en place d'élément perturbé.

Un câblage structuré permettra de mieux contrôler et gérer les communications dans l'entreprise. Au départ, un pré câblage est un investissement important, aussi son étude et son dimensionnement devront être réalisé de façon extrêmement précise. Seul un bon dimensionnement permettra de rentabiliser un pré câblage, par sa souplesse d'évolution.

Afin d'apporter souplesse, évolutivité tant organisationnelle que technologique, un pré câblage doit être :

- Systématique,
- Banalisé,

Correctement dimensionné (nombre de prises par poste de travail, densité de prises au mètre carré, ...),

- Adaptable à tout type de matériel,
- Aisément reconfigurable.

Le point d'accès standard est un fait un ensemble de prises nécessaires à un poste de travail de type bureau.

Il peut être constitué de la façon suivante :

- Au moins 2 prises murales dites "basses tension" par opposition aux prises d'alimentation électrique (ces prises étant destinées à connecter le téléphone et le poste informatique),
- Au moins 1 prise de courant aux normes Européennes 240 Volts,
- Au moins 1 prise de courant aux normes Européennes dotée d'un détrompeur (cette prise étant au

mieux ondulée, au pire régulée, et exclusivement destinée à l'alimentation des équipements informatiques sauf imprimantes).

L'E.I.A. (Electronics Industries Association) a développé un standard de câblage d'immeubles et de bureau. Dans ce document sont spécifiés :

- Le type de câbles.
- Les distances entre armoires de brassage.
- Les distances entre les armoires de brassages et les prises situées dans les zones de travail.

Les câbles proposés comme supports de transmission sont le câble quatre paires torsadées 100 Ohms, non écranté (ISDN), le câble deux paires torsadées 150 Ohms, écrantés (IEEE 802.5), le câble coaxial 50 Ohms (IEEE 802.3), la fibre optique 62,5/125 µm.

D'autres organismes officiels, tels l'I.S.O. (International Standard Organisation), le C.C.I.T.T. (Comité Consultatif International des Téléphones et Télégraphes), le C.E.N.E.L.E.C. (Comité Européen de Normalisation ELECtrotechnique) produisent des normes régulièrement.

L'objectif d'une norme est, dans le domaine qui nous occupe, de permettre ou d'améliorer l'interopérabilité des équipements en vue de créer un système performant basé sur un modèle donné. La multiplicité de ces normes amène l'utilisateur final à un dilemme:

Que faire ou comment faire pour sélectionner le type de pré câblage idéal ?

La réponse à cette question n'est pas dans l'une ou l'autre des normes. Les normes sont des guides, imposent des valeurs minimales et/ou maximales de mise en service, des règles de conduite. C'est en s'appuyant sur ses normes que des constructeurs ont pu développer des offres sur mesure de pré câblage d'immeuble et de campus.

Les utilisateurs souhaitant un câble polyvalent, les différentes normes ne les ont pas pleinement satisfaits. En effet, divers paramètres ne sont pas pris en compte quant au choix des composants d'un système de câblage : le coût, l'environnement, les contraintes utilisateurs, la fiabilité, la capacité d'évolutivité, ... De plus, seule une parfaite connaissance de toutes les normes relatives à la construction, aux rayonnements, au câblage, aux offres constructeurs, aux infrastructures permettrait aux utilisateurs de réaliser un choix pertinent, eux seuls étant au fait des besoins d'évolutivité de leur entreprise.

Des contraintes d'installations existent, par exemple :

- Les contraintes de sécurité électrique (isolation, mise à la terre, ...),
- Les contraintes liées à la protection contre les rayonnements parasites électromagnétiques ou autre,
- Les contraintes de protection liées à l'environnement climatique,
- Les risques d'effets perturbateurs liés à la nature du support,
- Les contraintes mécaniques de pose (limite de courbure, tension maximale des câbles, chemins de câblage spécifiques, ...)

Pour toutes ces raisons, le pré câblage ou le câblage restent un exercice particulier où l'assistance d'un spécialiste et de son outillage seront gage d'un résultat moins approximatif.

Les normes de câblage cuivre :

| *Catégorie* | *Année* | *Bande passante* | *Type de câble* | *Applications* |
|---|---|---|---|---|
| Catégorie 5 | 1995 | 100 MHz | UTP, FTP, SFTP, STP | Ethernet 10 et 100 Mbits, ATM 155 Mbits/seconde |
| Catégorie 5e | 1999 | 100 MHz | UTP, FTP, SFTP, STP | Gigabit Ethernet (sur 4 paires) |
| Catégorie 6 | 2002 | 250 MHz | UTP, FTP, SFTP, STP | Gigabit Ethernet (sur 4 paires), ATM 1 Gbit/sec. |
| Catégorie 7* | 2002 | 600 MHz | STP (blindage paire par paire) | Gigabit Ethernet (sur 2 paires), ATM 1 Gbit/sec et 10 Gigabits Ethernet sur 4 paires. (Les connecteurs ne sont pas encore normalisés) |

- La norme ISO11801 impose un câble blindé paire par paire pour la catégorie 7. Le comité américain EIA-TIA n'a, pour cette raison, pas accepté la catégorie 7, étant défenseur d'un câblage non écranté (UTP).

Règles d'ingénierie :

La norme TIA/EIA-569 stipule que chaque étage d'un bâtiment doit avoir au moins un Local Technique appelé Local Technique d'Etage (LTE), qu'un Local Technique supplémentaire doit être installé tous les 1.000 m2 si la surface de l'étage desservi est supérieure à 1.000 m2 et/ou la distance du câblage horizontale est supérieure à 90 m (longueur maximale des câbles en paires torsadées). Un Local Technique ne doit pas concentrer plus de 100 à 350 câbles de distribution (conseillé).

Un local technique doit être suffisamment grand pour pouvoir loger tous les équipements et le câblage nécessaires au réseau, doit être prévu pour la croissance future du réseau. Sur la base d'un poste de travail pour 10 m2, la zone desserte couverte par le local technique donne les dimensions de local technique de : 3.0m x 3.4m pour 1 000m², 3.0m x 2.4m pour 800 m² et de 3.0m x 2.2m pour 500m².

Pour respecter les contraintes d'environnement, l'emplacement et l'aménagement du local technique doit être conforme à des règles concernant les matériaux des murs, du sol et des plafonds. Exemples : pour contrôler la présence de poussières et protéger les équipements contre l'électricité statique ; le sol doit être recouvert de carrelage ou de tout autre type de surface de finition équivalent. Pour contrôler la température et l'humidité, par exemple pour préserver les câbles en paires torsadées ; la température doit rester voisine de 21° et l'humidité doit rester comprise entre 30 et 50%. Il faut aussi veiller à l'emplacement des appareils d'éclairage et leur type pour éviter la présence d'interférences externes (l'installation d'appareils d'éclairage fluorescent est à éviter).

Un système de câblage doit être homogène. L'hétérogénéité, bien que possible, génère très (trop ?) souvant des "rupture de continuité (section des câbles différents, classe d'équiement différentes,…) Les chaînes de liaison (câbles, connectique, cordons de brassage et de station) doivent être réalisées avec des composants garantis par un seul constructeur.

Un précâblage (ou câblage) est organisé en étoiles autour de sous répartiteurs (ou locaux de brassage). Les étoiles sont composées d'un ensemble de câbles 4 paires reliant les postes de travail au sous répartiteur. Cette partie du câblage est appelée distribution horizontale. La longueur d'une branche de cette étoile ne doit pas dépasser 90 mètres. Les locaux de brassage sont raccordés entre eux par des câbles de forte capacité appelés rocades, qui peuvent être réalisés avec des câbles en cuivre ou des câbles optiques. Cette partie du câblage s'appelle distribution verticale. Ces étoiles et ces rocades permettent, à l'aide de moyens de brassage et de concentration (commutateurs, concentrateurs et cordons de brassage) de raccorder n'importe quel ordinateur à n'importe quel serveur et de configurer les différents réseaux quel que soit leur topologie.

Quel type de câble ? Paires torsadées ou fibre optique ?

- Arguments pour la paire torsadée :

- Câbles et connecteurs beaucoup moins cher, la fibre coûtant 60% plus cher que de la paire torsadée SFTP $5^E$.
- Equipements d'interconnexion moins chers.
- Des ports pour la fibre coûtent environ 2 fois plus chers (avec en plus une densité de ports deux fois moins élevée).

- Arguments pour la fibre optique

- Permet de s'affranchir des contraintes de distance très fortes pour la paire torsadée.
- Insensible aux perturbations électromagnétiques.

En conclusion : Paires torsadées pour la distribution horizontale plutôt que la distribution verticale (backbone) et Fibre optique pour la distribution verticale (backbone).

Les principales caractéristiques et paramètres d'un système de câblage :

- Bande passante - Détermine le débit maximale de transmission
- Affaiblissement linéïque - Fixe la longueur maximale des câbles
- Réflexion ou affaiblissement de désadaptation (Return Loss), rapport de puissance entre le signal transmis et le signal réfléchi - Du à des irrégularités d' impédance (sur un fil ou entre fils d'une paire)
- Paradiaphonie - Near End and Cross Talk (NEXT). Niveau de bruit induit en entrée sur une paire voisine par une autre paire
- Télédiaphonie - Far End and Cross Talk (FEXT). Niveau de bruit induit en sortie sur une paire voisine par une autre paire
- Ecart de délai de propagation - Skew Delay. Ecart de délai de propagation sur les différentes paires
- ELFEXT (Equal level FEXT) ou Attenuation Cross Talk Ratio (ACR)
- Power Sum Near and Crosstalk (PSNEXT). Paradiaphonie cumulée qui mesure la quantité de signal engendrée par toutes les paires sur une autre.

Les normes à respecter ou faire respecter :

Les techniques et les produits dédiés au précâblage proposés par les constructeurs sont désormais polyvalents et indépendants du système constructeur. Cela permet de réunir une offre plus vaste pour réaliser des systèmes pré-câblés dits "ouverts "dont l'environnement normatif (ISO/IEC 11801, EN, EIA/TIA) est l'assurance de critères de fonctionnement. L'ISO 11801 définit, depuis juillet 1994, l'installation complète en pré-câblage système : composants, câbles et liens. Elle reprend les catégories 3, 4 et 5 de l'ETA/TIA mais avec des valeurs d'affaiblissement et de paradiaphonie différentes. Elle définit aussi le rapport signal bruit (RSB) pour les liens ainsi que les classes d'applications. La seconde édition prend en compte les besions et spécificités actuels

Les normes :

ISO/CEI 11 801- 2nd édition Norme Internationale. (liaison classe E)

| | |
|---|---|
| EN 50173 - 2nd édition | Norme européenne. (liaison classe E) |
| EIA/TIA-568B.2-1 | Norme américaine. (catégorie 6) |
| NFC 15 100 | Installation électrique basse tension. |
| NFC 15 900 | Compatibilité entre les courants forts et faibles. |
| EN 50167 | Norme européenne relative aux câbles de capillarité. |
| EN 50168 | Norme européenne relative aux câbles de rocade. |
| EN 50169 | Norme européenne relative aux cordons. |
| EN 50173 | Norme européenne relative au pré-câblage. |
| EN 50174 | Norme européenne sur les règles d'installation. |
| IEC 60332-1, NF C 32070 2.1 | Propagation de la flamme. |
| IEC 61034, NF C 32073 | Densité des fumée. |
| IEC 60754, NF C 32074 | Toxicité des fumées. |
| NF C 32-062 LS0H | (low smoke, zero halogène) |
| IEEE 802.3an | Réseau à 10 gigabit sur paires torsadées |

La norme ISO/IEC 11801 :

L'architecture définie est l'étoile, à trois niveaux :

- Répartiteur général : câblage en étoile entre les bâtiments.
- Répartiteur principal : câblage en étoile entre les étages.
- Sous-répartiteur d'étages : câblage en étoile entre les points utilisateurs.

Le support :

- Le support défini est la paire symétrique et la fibre optique.

Les connecteurs :

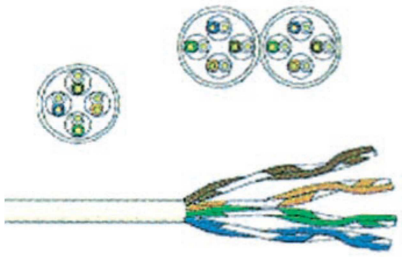
- Les composants définis sont les prises RJ 45 et les connecteurs ST et SC.

Les liaisons :

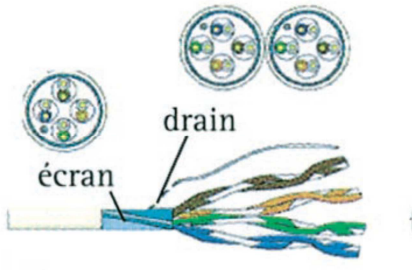
- Les liaisons définies sont les classes A, B, C, D, E et F basées sur les composants définis.

La famille des câbles à paires torsadées se subdivise en quatre groupes , selon leur constitution :

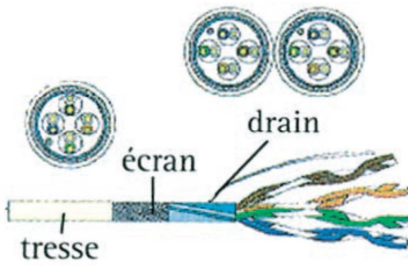
- les câbles UTP, non blindés et d'impédance de 100 Ohms,



- les câbles FTP, écrantés et d'impédance de 120 Ohms, 100 Ohms




- les câbles SFTP, blindés et d'impédance de 100 Ohms, S-FTP.




Précautions de câblage :

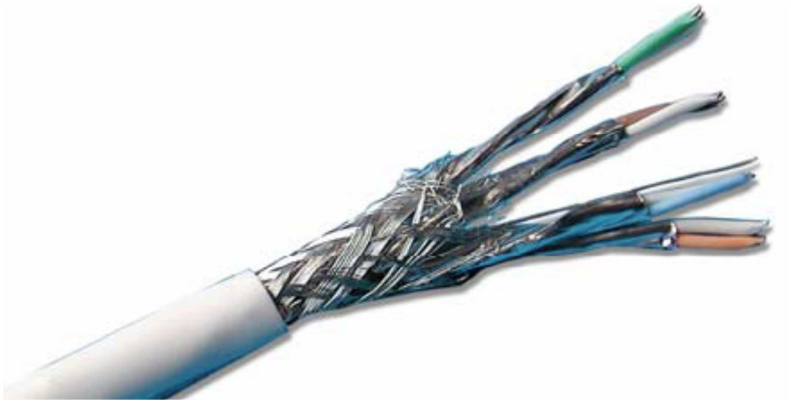
Pour assurer une bonne liaison, des précautions de câblage sont à respecter :

- Rayon de courbure du câble

- Détorsadage des paires : 13 mm maxi en cat. 5
- Dégainage du câble réduit au maximum (30 à 60 mm typique)
- Pour un câble écranté, l'écran devra être conservé le plus près possible du point de connexion
- Raccordement des écrans à la masse à chaque extrémité du câble, à 360° si possible.

Description des câbles :

Un câble destiné à un précâblage est constitué d'un seul conducteur (généralement en cuivre) qui est caractérisé par une "jauge" (diamètre du fil de cuivre utilisé pour l'âme du conducteur), ce qui le différencie d'un cordon de brassage qui est généralement constitué de plusieurs fils souples.



Câble catégorie 7

Les câbles doivent présenter une impédance de 100 Ohms (ou 120 ou 150 Ohms). Il sont réalisés en paires de conducteurs cuivre jauge AWG 23 (pour de la catégorie 6 ou 7) (0,57mm) écrantées (pour de la catégorie 6 ou 7) ou non individuellement, et peuvent comporter un blindage général constitué par un feuillard ou une tresse métallique (pour de la catégorie 6 ou 7).

Ils sont pourvus en standard d'une gaine extérieure en matériau sans halogène (LSZH : Low Smoke Zéro Halogen) conformément aux normes internationales IEC 60332-1 concernant la non propagation du feu, IEC 60754-1&2 concernant la toxicité et l'acidité des fumées et IEC 61034-2 concernant la densité des fumées.

Code couleur ISO :

paire 1 : blanc-bleu / bleu

paire 2 : blanc-orange / orange

paire 3 : blanc-vert / vert

paire 4 : blanc-marron / marron

| Prise RJ45 | Câbles UTP & FTP 100 Ohms | | Câbles L120 | Câbles Type Bull A2 |
|---|---|---|---|---|
| N° Contact | EIA 568A Standard | EIA 568B AT&T 258A | COREL/RNIS | BCS |
| 1 | **Vert / Blanc** | **Orange / Blanc** | **Gris** | **Bleu** |
| 2 | **Vert** | **Orange** | **Blanc** | **Incolore** |
| 3 | **Orange / Blanc** | **Vert / Blanc** | **Rose** | **Blanc** |
| 4 | **Bleu** | **Bleu** | **Orange** | **Jaune** |
| 5 | **Bleu / Blanc** | **Bleu / Blanc** | **Jaune** | **Orange** |
| 6 | **Orange** | **Vert** | **Bleu** | **Gris** |
| 7 | **Marron / Blanc** | **Marron / Blanc** | **Violet** | **Marron** |
| 8 | **Marron** | **Marron** | **Marron** | **Violet** |

Les tests sur un câblage / Système de câblage / la recette:

La certification du câblage sera constituée par mesures au niveau de chaque prise et attestera de la conformité de l'installation aux normes retenues dans le cahier des charges. Le testeur employé sera le testeur Wirescope ou équivalent.

La recette comprend un cahier de recette rassemblant le synoptique du câblage avec repérage, le tableau de mesures (avec notice explicative de valeur des tests) , lesplans d'implantation (avec plan de base).

Les principaux tests attendus :

- Numérotation de la prise, conforme à identification du cahier des charges.
- Contrôle de continuité,
- Mesure de la longueur,
- Mesure de l'affaiblissement,
- Mesure de la paradiaphonie,
- Mesure de la paradiaphonie cumulée
- Mesure de l'ELFEXT et du PS ELFEXT,

- Mesure de l'ACR,
- Mesure du temps de propagation et du skew,
- Mesure du Return Loss,

Les tests doivent indiquer les valeurs minimales et maximales attendues pour chaque type de test.

En cas de multiples points de coupures, ne seront retenues que les tests "bout en bout", prenant en compte l'ensemble des points de coupures nécessaires à l'établissement de la communication.

Diagnostiquer des problèmes sur un câblage :

Sur un plan de câblage :

- Mauvais appariement entre le connecteur et le conducteur,
- Défectuosité d'une prise ou d'une fiche,
- Un ou plusieurs cassés.

Problèmes de longueur de câble :

- Mauvaise NVP.
- Câble trop long.
- Une terminaison appariée fonctionne mal.
- Dommages sur l'isolant du câble affectant les paires longues.
- Rupture ou court-circuit dans une paire.
- Capacité élevée dans une paire.

Problèmes de résistance :

- Types de câble mal appariés.
- Mauvaise connexion du bloc de serrage.
- Mauvaises connexions de terminaison RJ-45.
- Une paire de fils présente un écoulement (jamais fait).
- Dommage sur le câble.
- Câble court-circuité.

Problèmes de NEXT et ELFEXT :

- Mauvais étalonnage du câble installé ou du cordon de test.
- Câble défectueux ou de mauvaise qualité, trop de connecteurs.
- Mauvaise qualité de l'installation aux points de connexion.
- Une trop grande quantité d'isolant a été enlevé sur la terminaison des fils.
- Une paire de fil a été trop détorsadée à la terminaison.
- Paires dépairées.
- Mauvaise qualité des connecteurs ou connecteurs avec une capacité nominale de mauvaise catégorie.
- Alignement retardé (ELFEXT).

Problèmes d'atténuation :

- Mauvaise qualité des points de terminaison d'un connecteur.
- Câble trop long.
- Adaptateur de test inadapté ou défectueux.
- Mauvais choix de câble.

Problèmes de Return Loss :

- Câble coupé, court-circuité ou endommagé.
- Caractéristiques inappropriées du câble installé, de certains segments de câble ou du cordon de test.
- Dommages/usure du câble ou de certains connecteurs.
- Mauvaise qualité du serrage.
- Épissure faite en usine dans le câble.

Diagnostiquer des problèmes d'impédance

- Câble trop comprimé, étiré ou trop plié.
- Connecteurs défectueux.
- Dommages sur l'isolation du connecteur.
- Boucles de terre créées entre le blindage du câble (si utilisé) et le dispositif de mise à la terre de l'équipement (dans un câble RS-232 vers un ordinateur ou une alimentation auxiliaire).
- Mauvais choix de câbles ou de cordons de liaison.
- Humidité dans le câble.

Diagnostiquer des problèmes de délai et skew

- Le câble utilise différents matériaux pour isoler les quatre paires de fils.

- Une paire comporte une coupure ou un court-circuit.
- Câble trop long.
- Problème avec l'installation du câble.

Diagnostiquer des problèmes de capacité

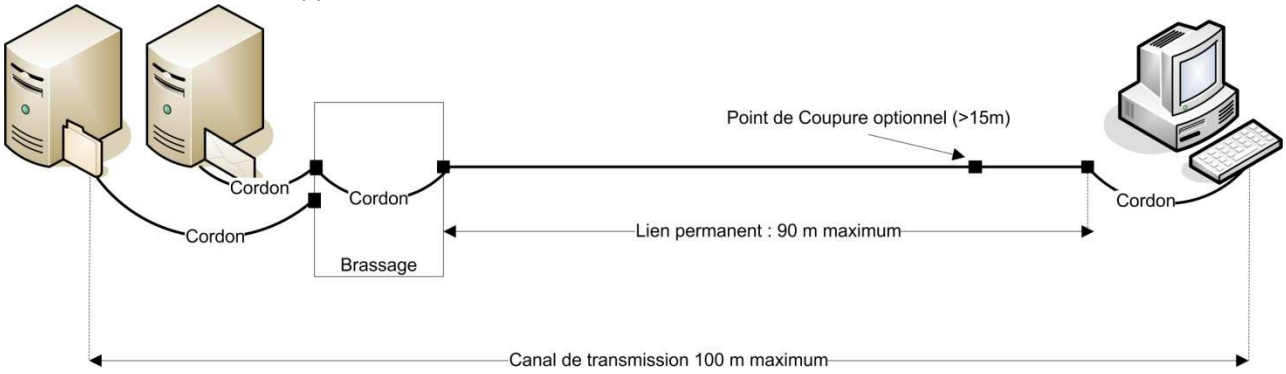
- Câble trop comprimé, étiré ou trop plié.
- Connecteurs défectueux.
- Dommages sur l'isolation du connecteur.
- Boucles de terre créées entre le blindage du câble (si utilisé) et le dispositif de mise à la terre de l'équipement (dans un câble RS-232 vers un ordinateur ou une alimentation auxiliaire).
- Mauvais choix de câbles ou de cordons de test.
- Humidité dans le câble.
- Mauvaises connexions sur les bagues de serrage et les plaques murales

Diagnostiquer des problèmes d'ACR et Powersum ACR

- Voir la résolution des problèmes de NEXT, ELFEXT et atténuation

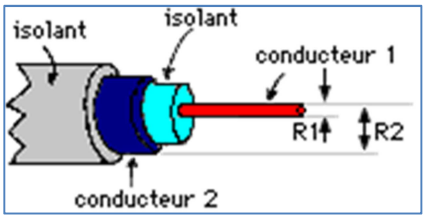
Définition du lien :

Le schéma ci-dessous rappelle la définition du lien conformément à la norme ISO 11801 :




**Câble Coaxial -** Câble à structure concentrique comprenant un conducteur central entouré d'un diélectrique, d'une tresse assurant le blindage et d'une gaine isolante. Le conducteur central est un fil monobrin ou un fil multibrins. Le blindage est formé d'une tresse en fils ou d'une feuille métallique.

Le câble coaxial constitue une amélioration de la paire torsadée. Ce support constitué de 2 conducteurs à symétrie cylindrique de même axe, l'un central de rayon R1, l'autre périphérique de rayon R2, séparés par un isolant.




Avantages : coût relativement faible, immunité plus importante au bruit, débit plus important que la paire torsadée

Inconvénients : affaiblissement relativement rapide, installation à soigner.

Utilisation : réseaux de vidéosurveillance, réseaux de vidéo-distribution.

Débit : quelques dizaines Mbits/s jusqu'à 100 Mbits/s sur une distance courte (< 1000 m)

**Câble de Rocade -** Building Backbone Cable. Câble assurant la connexion entre le répartiteur du bâtiment et le répartiteur d'accès.

**Câble Horizontal -** Câble assurant la connexion entre le répartiteur d'accès et le point de distribution (câble capillaire)

**Câble Multiconducteur -** Câble composé de plusieurs conducteurs.

**Câble Multipaires -** Câble composé de plusieurs paires torsadées.

**Câbles en Fibre Optique -** Voir aussi Fibre Optique - Câble composé d'une ou plusieurs fibres optiques assurant la transmission des signaux d'ondes lumineuses par un phénomène de réflexion interne.

Une fibre est composée :

- D'un coeur : milieu diélectrique intérieur ne conduisant pas le courant électrique, mais conducteur de lumière (silice, plastique ou composite),
- D'une gaine : entoure le coeur d'un milieu d'indice de réfraction plus faible
- D'un revêtement : entoure le coeur et la gaine de couches concentriques en plastique pour fournir une protection mécanique

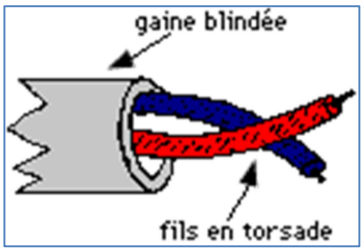
- Souple pour les câbles dit d'intérieur (distribution verticale)
- Rigide pour les câbles d' extérieur (rocade) : le revêtement peut alors être métallique

Terminologie :

- Alupe : Barrière d'étanchéité transversale en forme d'anneau en aluminium soudé ou contre collé à la gaine extérieure, empêchant toute pénétration de liquide dans le câble.
- Armure :Elément, métallique ou non, du câble, qui constitue, à la fois une protection mécanique du câble et une protection contre les rongeurs (retardement de l'attaque).
- Câble assemblé : Câble optique posé et fixé muni de connecteurs à ses extrémités.
- Câble à jonc rainuré : Câble à structure lâche dans lequel les fibres optiques sont logées dans des rainures pratiquées sur un jonc cylindrique. On peut obtenir de gros câbles en assemblant plusieurs joncs sous une enveloppe appropriée.
- Câble mixte : Câble intégrant des fibres optiques et des conducteurs métalliques.
- Câble multifibre : Câble optique contenant au moins deux fibres optiques qui transmettent chacune des signaux indépendants.
- Câble optique : Ensemble comportant une ou plusieurs fibres optiques ou un ou plusieurs faisceaux de fibres sous une enveloppe commune de façon à les protéger contre les contraintes mécaniques et les agents extérieurs tout en conservant la qualité de transmission des fibres.
- Câble optique autoporteur : Structure de câble comportant des fibres optiques et un dispositif permettant sa pose en aérien, sans traction sur les fibres.
- Câble préconnectorisé : Câble dont toutes les fibres à chaque extrémité sont munies de dispositifs (connecteurs, épissures mécaniques...) permettant le raccordement direct sur un composant passif ou actif.
- Câble à rubans : Câble optique dans lequel les fibres optiques sont disposées en ruban parallèle pour former des rubans. On peut obtenir de gros câbles en empilant plusieurs rubans sous une enveloppe appropriée. Un câble à rubans peut être un câble à structure serrée ou un câble à structure lâche.
- Câble à structure lâche : Câble optique dans lequel chaque fibre optique sous revêtement primaire est logée dans un tube ou une alvéole avec un certain jeu.
- Câble à structure serrée : Câble optique dont les fibres optiques sous revêtement secondaire ne sont pas libres de se mouvoir mais sont maintenues en position.
- Câble à tubes : Câble à structure lâche dans lequel les fibres optiques sont logées dans un ou plusieurs tubes.
- Câble zéro halogène : Câble qui au cours d'une combustion ne propage pas de gaz toxique.
- Cordon optique : C'est une certaine longueur de câble optique à une ou à deux fibres équipées des connecteurs d'extrémité.
- Facteur de remplissage : Rapport de l'aire totale des zones de coeur dans une section droite d'un faisceau de fibres à l'aire totale de la section du faisceau habituellement à l'intérieur de la ferrule, y compris les gaines et les interstices.
- Protection anti-rongeurs Gaine de protection permettant de retarder l'attaque des rongeurs sur les câbles à fibres optiques, sans la supprimer. Ces gaines sont métalliques, à base de fibres synthétiques, ou encore à base de fibres de verres tressées.
- Rayon de courbure : Le rayon de courbure est le rayon minimal de la courbe que peut faire une fibre ou un câble sans qu'il y ait dommage pour la fibre.
- Résistance à l'écrasement : Définit la charge radiale que peut supporter de façon temporaire ou permanente un câble à fibres optiques sans modifier ses caractéristiques mécaniques et optiques.
- Rubans gonflants : Remplissage du câble à fibres optiques entre les faisceaux et la gaine à fibre de verre.
- Température admissible : Gamme de température dans laquelle un câble à fibres optiques voit ses performances nominales conservées. On distingue la température admissible en installation et la température admissible en service.
- Traction maximum admissible : La traction maximum admissible est la force exprimée en Newton (N) avec laquelle on peut "tirer" sur le câble à fibres optiques sans y créer de déformation irréversible et en lui conservant toutes ses propriétés nominales. On définit également une traction maximum admissible avec boucle de tirage.

**Câbles en paires torsadée -** Un câblage en paire torsadée est constituée de deux conducteurs (minimum) en cuivre torsadés ensemble autour d'un même axe. Un câble en paires torsadées peut comporter une ou paires (quatre le plus souvent) torsadées également ensemble. Le but de cet arrangement en torsade (avec un pas précis) est de limiter les interférences entre fils.

Le signal transmis correspond à la tension entre les deux fils. La paire peut se présenter emprisonnée dans une gaine blindée augmentant l'immunité contre les perturbations électromagnétiques




Avantages : coût très bas et facilité d'installation.

Inconvénients : affaiblissement rapide, sensibilité aux bruits, faible largeur de bande, faible débit.

Utilisation : réseaux locaux, raccordements téléphoniques .

Débit : quelques Mbits/s jusqu'à 1 Gbits/s sur une distance très courte (< 100 m)

Un câble en cuivre est d'abord caractérisé par son diamètre ou American Wire Gauge (AWG) qui est l'inverse du diamètre en "inch" (22 AWG = 0.63mm, 24 AWG = 0.5mm (le plus courant), 26 AWG = 0.4mm), son impédance : valeur caractéristique de tout milieu traversée par un onde (100 ohms, 120 ohms (le plus courant en France), 150 ohms).

Systèmes de protection :

- Ecrantage : consiste à entourer toutes les paires d'un même câble d'une tresse métallique ou d'une feuille très fine d'aluminium
- Blindage : consiste à entourer indépendamment chaque paire d'une tresse métallique ou d'une feuille très fine d'aluminium

Catégories de câbles :

- Paires sans protection (UTP : Unshielded Twisted Paired) - Les plus utilisées aux Etats-Unis.
- Paires écrantées (FTP : Foiled Twisted Paired) - Les plus utilisées dans la Communauté Européenne
- Paires blindées (STP : Shielded Twisted Paired)
- Paires écrantées et blindées (SFTP) - les moins utilisées car difficile à manier (courbure difficile des câbles)

**Cablo Opérateur -** Opérateur de services utilisant le réseau câblé.

**CAD -** Connectique auto dénudante. Connectique très largement utilisée dans les mise en œuvre de câblage téléphonique traditionnel. La connexion se réalise par retrait automatique d'isolant lors de l'insertion.

**CAI -** Common Air Interface - Standard d'interface permettant à des téléphones portables de communiquer par radio avec une station fixe (borne). Voir norme CT2.

**Call back -** Procédure de rappel qui fonctionne de la manière suivante : l'utilisateur compose un numéro d'appel dans le pays qui opère le "call back", sans qu'une communication soit établie, donc sans facturation. Un automate le rappelle et le met en communication avec une ligne internationale. L'utilisateur compose alors le numéro de son correspondant. La facturation de la communication est effectuée au tarif de l'opérateur étranger choisi. Ce système permet donc de bénéficier du tarif du pays appelé.

**Canal -** Channel - En théorie de la communication, partie d'un système de communication qui assure la transmission de l'information entre une source et un destinataire.

**Canal B -** Liaison numérique terminale à 64 Kbps sur le Réseau numérique à intégration de services (RNIS). Un Accès de base du RNIS comporte 2 canaux B utilisables par un terminal RNIS quelconque (téléphone, télécopieur, terminal informatique). Un Accès RNIS dit primaire comporte 30 canaux B utilisables indépendamment les uns des autres.

**Canal D -** Canal de signalisation utilisé sur le Réseau numérique à intégration de services (RNIS). Il sert à transmettre différentes informations de "service", indépendamment de la communication principale : demande de connexion, identité de l'appelant, établissement de l'appel, fin de l'appel... Sa capacité est de 16 Kbps pour l'Accès de base S0 du RNIS et de 64 Kbps pour l'Accès primaire S2.

**Canal de transmission -** Par canal de transmission on entend tout phénomène physique identifié et délimité sur le support physique et capable de véhiculer un signal : fil de cuivre, atmosphère (pour les transmissions hertziennes ou autrement dit ondes radio) ou fibre de verre (fibre optique). Le signal est transporté sous la forme d'une onde ou d'une oscillation faisant varier une caractéristique physique du support : différence de potentiel électrique le plus souvent, onde radio électrique ou intensité lumineuse dans le cas de la fibre optique.

Généralement, le signal se présente sous la forme d'une ondulation de base régulière, baptisée porteuse, à laquelle on fait subir des déformations qui distingueront les éléments du message. Cette déformation est appelée modulation. On peut jouer sur l'amplitude des oscillations (on parlera alors de modulation d'amplitude), sur leur fréquence (modulation de fréquence) ou encore sur le déphasage de la périodicité

d'oscillation (modulation de phase). Un canal de transmission est caractérisé par sa bande passante, c'est à dire la gamme de fréquences que laisse passer sans déformation ce canal, en fonction de ses caractéristiques physiques et de l'environnement susceptible de le perturber, particulièrement en provoquant des modulations parasites ou bruit. Cette BP exprimée en Hertz est la différence entre la plus haute fréquence (dite fréquence de coupure) et la plus basse fréquence que laisse passer le support. Intuitivement on comprend que plus la bande passante est large, plus on pourra transmettre pendant un temps donné un grand nombre de modulations (déformations du signal). Dans la réalité, les choses sont plus compliquées, du fait que le signal se dégrade relativement à la distance (atténuation) et que cette dégradation n'est pas la même pour toutes les fréquences.

Cependant, il existe des lois bien définies, permettant de connaître le nombre de modulations par seconde qu'accepte de transmettre un canal en fonction de sa BP. Ce nombre est exprimé en Bauds.

Si le codage est binaire, donc si l'on utilise que deux états du signal transmis (0 et 1 ou haut et bas), cette rapidité de modulation sera égale au débit. On exprime ce débit en bit/sec. parfois en octet/sec. (1 octet = 8 bits).

Dans la pratique, les ingénieurs ont développé des types de codage à plus de 2 états qui, permettent d'obtenir des débits plus élevés pour une même BP.

**Canal Sémaphore -** Common Channel Signalling - Moyen de transmission utilisé pour transporter des messages de signalisation indépendamment des voies de trafic. Voir par exemple CCITT n°7.

**CAP -** Carrierless Amplitude Modulation - Technique de modulation dérivée du MAO (QAM, en anglais) - Aujourd'hui utilisée pour la DSL, cette technique de codage est apparue pour augmenter la distance maximale de transmission nécessaire à l'introduction du réseau RNIS. Dans le cas d'une ligne téléphonique, elle permet de séparer les canaux réservés à la réception de ceux de l'émission.

**Capacité de transmission -** Débit maximal d'un canal, exprimé en bits par seconde.

**Capacité Linéique -** C'est la capacité entre deux éléments sur une longueur donnée. Unité µF/km.

**CAPEX -** Capital Expenditures - Expression anglophone définissant les investissements coprporels et incorporels. Ce sont généralement des investissements amortissables et qui sont pris en compte dans la valorisation des actifs.

**CAPI -** Common Application Programming Interface - Interface de programmation ISDN non propriétaire. La version 2.0 requiert une interface CAPI pour la fonction de passerelle du central téléphonique IP.

**Capteur -** En photo numérique, le capteur désigne un élément sensible à la lumière qui convertit l'énergie lumineuseen signal électrique. Le capteur se présente sous la forme d'une petite plaque recouverte de cellules photoélectriques.

**CAPWAP -** Control And Provisionning of Wireless Access Points - Protocole développé par IETP afin de permettre aux réseaux WLAN multiconstructeurs de fonctionner. Ce projet était une réponse à IWAPP, protocole propriétaire de Cisco, originellement développé par Airespace.

**Carder -** Celui qui pirate les codes de carte bancaire pour détourner de l'argent. Il est souvent méprisé par les authentiques hackers.

**Carillon -** Tonalité ou ensemble de tonalités constituant un signal sonore qui caractérise une opération ou un évènement.
Les carillons sont utilisés en particulier pour compléter les informations fournies par l'écran d'un ordinateur ou donner des informations particulières à l'utilisateur d'un service téléphonique.

**Carrier -** Terme anglais désignant les opérateurs télécoms ou "transporteurs", tous privés, aux Etats-Unis.

**Carte SIM -** Subscriber Identity Mobile - Carte à puce présente dans les téléphones mobiles, reliant le client au réseau de son opérateur. Contient les informations permettant l'identification et l'habilitation de l'abonné.

La carte SIM contient des dossiers, des fichiers ainsi qu'un système de droits qui limite leur accès.

Une carte SIM est articulée autour d'un processeur et contient trois types de mémoire :

- La ROM qui contient le système d'exploitation ainsi que les algorithmes de chiffrement et d'authentification,
- L'EPROM qui contient les données liées aux applications spécifiques. Elle permet de garder en mémoire les données même si le terminal est éteint.
- La RAM qui contient aussi des données liées aux applications spécifiques.

Le système de fichier est dépendant du fabricant de carte, elle suit néanmoins toujours une organisation normalisée.

La racine est constituée par le fichier maître (MF) qui contient soit des fichiers élémentaires (EF) ou bien des fichiers dédiés (DF). Les DF sont en fait des dossiers qui peuvent contenir soit des EF soit d'autres DF.

Chaque fichier est protégé par un niveau d'accès, il est donc possible de le protéger soit en lecture soit en écriture. Il existe cinq niveaux d'accès:

- ALW : la donnée est toujours accessible.
- CHV1 : elle est protégée par le code CHV1.

- CHV2 : donnée protégée par le code CHV2.
- ADM : modifiable uniquement par l'opérateur.
- NEV : la donnée est inaccessible.

Contenu de la carte SIM :

- Les données obligatoires du dossier GSM :
  - Informations administratives.
  - Numéro de la phase GSM utilisée (1, 2, 2+).
  - IMSI.
  - Classe de contrôle d'accès (limitation au PLMN d'origine, ou autorisation d'en utiliser un autre dans le cas de roaming international).
  - Période de recherche du PLMN nominal (dans le cas de roaming international).
  - Table des services SIM.
  - Information de localisation.
  - Liste des fréquences radio à utiliser.
  - Liste des quatre derniers réseaux utilisés.
  - Clé de chiffrement Kc et numéro de cette clé.
  - Langue.
- Les données de sécurité :
  - CHV1.
  - Indicateur d'activation/désactivation du CHV1.
  - La clé de déblocage du CHV1.
  - Compteurs d'erreur du CHV1 et de la clé de déblocage.
  - Clé d'authentification Ki.
- Données facultatives liées à la configuration :
  - Sélecteur de PLMN par ordre décroissant de préférence.
  - Type de SMS accepté.
  - Nom de l'opérateur.
  - Derniers appels entrants ou sortants.
  - Numéros abrégés.
  - MSISDN : non utilisé par le terminal.

Paramètres de sécurité :

Une carte SIM contient les informations nécessaires au chiffrement et à l'authentification ainsi que deux codes de sécurité supplémentaires spécifiques au GSM, les codes CHV1 et CHV2.

- CHV1 est un code à quatre chiffres utilisé pour identifier l'abonné sur le terminal. Connu sous le nom de code PIN durant la phase 1 du GSM, le CHV1 est initialisé par l'opérateur lors de l'abonnement. Le client peut ensuite le modifier à tout moment sans intervention de l'opérateur. Il est de plus possible de désactiver cette fonction directement depuis l'équipement terminal.
- Le code CHV2 permet de contrôler des suppléments de personnalisation. Ce code dénommé PIN2 durant la phase 1 peut être utilisé par l'opérateur, il possède les même caractéristiques que le CHV1 à l'exception de la désactivation qui ne peut être effectuée.

Pour empêcher un cassage du code par la force brute, une carte SIM se bloque au bout d'un certain nombre d'essais infructueux (généralement trois). Une fois bloquée toute manipulation du terminal est impossible avant le déblocage de la carte. Les clefs de déblocage sont connues comme code PUK mais sont aussi dénommées Unblocking CHV. C'est une clé à huit chiffres, qui peut lui aussi se bloquer après dix essais. Si l'utilisateur bloque cette clé la carte SIM devient alors inutilisable.

**CASE -** Common Application Services Elements - Englobait, au niveau 7 (Application) du modèle OSI de l'ISO, des ensembles de protocoles utilisables par des applications de services normalisées. A été redéfini par l'ISO sous le nom d'ACSE (Application Common Service Elements).

**Cassette -** *Terme utilisé dans le contexte de l'installation ou l'utilisation de fibre optique -*

Elément constitutif d'un boîtier permettant d'accueillir un nombre défini de raccords de fibres, avec possibilité de love. Une cassette peut abriter des fibres en attente, des fibres soudées, des fibres épissurées.

**Catalogue d'interconnexion -** Offre technique et tarifaire d'interconnexion que les opérateurs désignés chaque année comme puissants par l'Autorité, en vertu de l'article L. 36-7 du code des postes et télécommunications, sont tenus de publier annuellement, afin que les autres opérateurs puissent établir leurs propres offres commerciales et tarifaires. Le catalogue prévoit également les conditions dans lesquelles s'effectue l'interconnexion physique avec les opérateurs.

**Catégorie 3, 4, 5, 6, 6a, 7 -** Spécification des caractéristiques d'un système de câblage. Par exemple la catégorie 5 doit tenir une fréquence jusqu'à 100 Mhz, la transmission des données et de la voix jusqu'à 100 Mbps (IEEE 802.5 16 mbps et ANSI X 3T9.5 100 mbps TPDDI).

Classification d'un composant à partir de ses caractéristiques d'atténuation et de paradiaphonie.

**CATI -** Computer Assisted Telephone Interview - Système permettant de recueillir les données en direct durant l'entretien téléphonique sans avoir recours au papier.

**CATV -** Cable Antenna TV - Abréviation utilisée aux Etats-Unis pour désigner la télévision par câble et, par extension, des dispositifs qui en sont dérivés. Exemple : le câble CATV, désignant le câble coaxial de petit diamètre utilisé en télévision.

**CBAC -** Context-Based Access Control - Fonction intégrée au logiciel IOS de Cisco offrant le filtrage avancé de session de paquets pour tout le trafic routable. En configurant des ACL, il est possible d'autoriser ou de refuser le traitement ou le transfert du trafic.

**CBC -** Cipher Block Chaining mode - Mode opératoire de l'algorithme D.E.S où chaque bloc de texte chiffré yi opère une action sur les blocs de texte clair suivants xi+1 avant qu'il ne soit chiffré.

**CBDS -** Connexionless Broadband Data Service - Service d'interconnexion de réseaux locaux défini par l'ETSI d'après le service SMDS de Bellcore (voir SMDS).

**CBR -** Constant Bit Rate - Débit Constant - Catégorie de trafic utilisée pour le transport d'information numériques comme la vidéo ou la voix, qui peut être représenté par un flux continu de bits. Le trafic CBR nécessite une bande passante et un niveau de service garanti. Aussi appelé service de classe A.

**CCD -** Coupled Charge Device - Désique l'une des technologies utilisées pour réaliser les capteurs d'appareils photo, de caméscopes et descanners. (voir CMOS).

**CCE -** Cryptosystème à Courbes Elliptiques - Système cryptographique dont les calculs permettant le chiffrement sont effectués sur une courbe elliptique. Les opérations arithmétiques modulaires sont remplacées par des opérations de courbes elliptiques : une multiplication est remplacée par une addition, une exponentiation modulaire par une succession d'additions.

**CCETT -** Centre Commun d'Etudes de Télédiffusion et Télécommunications - Organisme français de recherche et développement, implanté à Rennes, dépendant à la fois de TDF (Télévision et télédiffusion de France) et du Cnet (Centre national d'études des télécommunications). Sa compétence est principalement orientée vers les systèmes de communication de l'image.

**CCIR** - Comité Consultatif International des Radiocommunications - Branche de l'UIT qui traitait des problèmes techniques de radiocommunications. Il est maintenant remplacé, pour l'essentiel, par l'UIT-R. Le CCIR était situé à Genève.

**CCITT - Comité Consultatif International Télégraphique et Téléphonique -** Organe permanent de l'Union Internationale des Télécommunications (UIT), institution spécialisée des Nations Unies compétente dans le domaine des télécommunications. Le CCITT regroupe les administrations des pays membres de l'UIT et les exploitations privées reconnues.

Comité consultatif international télégraphique et téléphonique - Depuis 1993, cet organisme est devenu le secteur de la normalisation de l'Union Internationale des Télécommunications (UIT).

Dépendant de l'Union internationale des télécommunications (UIT), siégeant à Genève. Il délivre des "avis" qui fixent les principales normes techniques dans le domaine des télécommunications, en particulier les avis en V (exemple V23, V24) pour l'utilisation des lignes analogiques ou en X (exemple X25) pour réseaux de données. La liste et le contenu officiel de ces avis sont mis à jour tous les quatre ans.

**CCITT n° 7 -** Système de signalisation par canal sémaphore du CCITT. Le CCITT n°7 utilise un langage à messages.

**CCR - France -** Commission Consultative des Radiocommunications et CCRST (Commission Consultative des Réseaux et Services de Télécommunications) - Commissions consultatives placées par la loi de réglementation des télécommunications du 26 juillet 1996 auprès du ministre chargé des télécommunications et du président de l'Autorité.

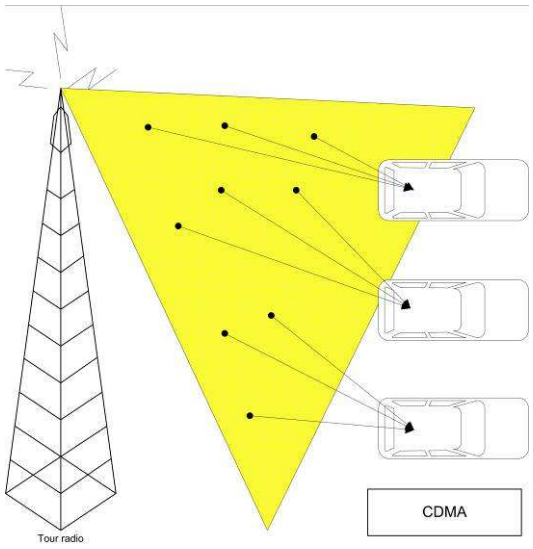
**CD -** Compact Disc. Disque faisant 12 centimètres de diamètre, 1,2 millimètre d'épaisseur, constitué de polycarbonate recouvert d'une couche d'aluminium, le tout étant vernis et permettant de stocker de 650 Mo à 700 Mo de données pour les formats "normalisés". Il fut normalisé en 1985 dans le Yellow Book, puis utilisé massivement pour stocker du son, et enfin pour enregistrer des données informatiques de toutes sortes (CD-ROM).

**CDFS -** CD-Rom File System - Désigne le système de fichiers permettant à un ordinateur de lire les données des CD-Rom. Ce système de fichiers permet de retrouver facilement des fichiers classés dans des répertoires hiérarchisés. Le système le plus couramment utilisé par les PC répond à la norme ISO 9660 (version internationale d'un standard établi par le High Sierra Group). Les spécifications originelles de ce standard, compatibles MS-DOS, n'autorisaient pas les noms de fichiers de plus de 8 caractères + extension de 3 caractères. Ces limitations ont été repoussées avec les "Joliet Extensions".

**CD-I -** Compact Disc Interactif - Disque compact conçu par Philips et Sony constituant une extension multimédia du CD-ROM, puisqu'il est capable de contenir des données, du son, des images graphiques et de la vidéo.

**CDM -** Code Division Multiplexing - Voir multiplexage par répartition en code.

**CDMA -** Code Division Multiple Access - Voir UMTS - Technologie de transmission hertzienne développée aux Etats-Unis dans laquelle un code numérique par utilisateur permet l'exploitation du spectre total des fréquences. Système de multiplexage d'informations utilisé en Radio communication. Technique de modulation à étalement de spectre. Le débit est augmenté en insérant un code ou séquence d'étalement entre plusieurs symboles.




Ci-dessus la représentation schématique du CDMA dans le spectre radio.

**CDMA 2000 -** Evolution 3G du CDMA (IS 95) - Désigné également comme CDMA MC (Multi Carrier)

**CDMA 2000 1x -** Première version du CDMA 2000 exploitant des canaux de 1,25 MHz duplex et proposant des débits moyens entre 40 et 70 kbit/s - Système voix et données.

**CDN -** Content Delivery Network - Réseau de livraison de contenu - L'objet d'un CDN est d'accélérer la diffusion du contenu d'un site web en rapprochant au plus près le contenu de l'internaute au moyen d'un réseau de serveurs de cache. Outre l'accélération de la diffusion, l'utilisation d'un CDN permet de gérer les pics de trafic tout en diminuant les besoins en bande passante. Il permet ainsi un lissage des coûts dû à la bande passante. Il s'adresse donc à tous les sites web bénéficiant d'une certaine audience.

**CD-Photo -** Disque compact conçu par Kodak et servant de support de stockage de photos.

**CD-R -** Compact Disk - Recordable - CD que l'on peut graver (une seul fois) avec un graveur de CD. Une fois gravé, le CD devient un CD-ROM normal, utilisable par n'importe quel lecteur de CD-ROM.

**CD-ROM -** Compact Disc-Read Only Memory - Support de stockage non réinscriptible sur lequel sont enregistrés des fichiers informatiques, des séquences sonores, voire même des séquences vidéo. Les informations sont enregistrées sous forme numérique.

**CD-RW -** Compact Disc Rewriting - Format de disques compact sur lesquels on peut écrire, effacer et réécrire (contrairement au CD-R).

**CD-TV -** Commodore Dynamic Total Vision - Système qui s'appuie sur trois technologies, l'informatique (un micro-ordinateur Amiga), le CD-ROM et la télévision. Il permet d'utiliser des programmes interactifs à partir du clavier d'une télécommande.

**CD-V -** Compact Disc-Video - Support optique numérique et analogique. Image en analogique, son en numérique.

**CD-WORM -** Compact Disc-Write Once Read Many - Disque compact que les utilisateurs ne peuvent enregistrer qu'une seule fois.

**CEI -** Commission Electrotechnique Internationale - IEC International Electrotechnical Commission - Organisme composé des Comités électrotechniques nationaux de plus de quarante pays. Elle forme avec l'ISO un comité technique commun (joint technical committee) ISO/IEC/JTC 1 pour traiter des problèmes relatifs à l'informatique et aux télécommunications pour l'informatique.

**Cellulaire -** En communication mobile, le terme cellulaire fait essentiellement référence à la structure du réseau de transmission mobile, qui se compose de cellules, ou sites de transmission. Cellulaire est aussi le nom du système de téléphonie mobile développé initialement par Bell Laboratories et qui utilise un équipement radio analogique basse puissance pour la transmission interne aux cellules. L'expression "téléphone cellulaire" est utilisée indifféremment en référence aux appareils mobiles. Dans l'industrie de la téléphonie mobile, cellulaire fait aussi référence aux produits et services non SCP.

Désigne un mode d'organisation des systèmes de radiotéléphonie dans lequel un plan d'attribution de fréquences élémentaires est appliqué à une zone géographique baptisée cellule, ce qui permet de réutiliser une même fréquence pourvu que ce ne soit pas dans la cellule voisine.

**Cellule -** Cell - En radio communications, désigne une zone élémentaire d'un réseau radio cellulaire à laquelle on affecte un ensemble de fréquences non réutilisables dans les zones contiguës. Zone géographique de couverture des signaux d'une station de base (site comportant un émetteur/récepteur radio et un équipement de communication réseau). Les réseaux de transmission mobile se composent de plusieurs cellules hexagonales qui se chevauchent afin d'utiliser efficacement le spectre radio. Egalement à la base de l'expression "téléphone cellulaire".

En mode ATM, mini-paquet normalisé, comportant 48 octets de données et 5 octets d'adresse. Les commutateurs ATM brassent des cellules.

**CEM -** Compatibilité électromagnétique - Caractéristiques de perturbation et d'immunité aux phénomènes électromagnétiques de rayonnements et de conduction sur les fils d'alimentation et de signaux. La Compatibilité ÉlectroMagnétique est définie par les normes EN 55022 (émission) et EN 50082-1 (immunité).

**CEN -** Comité Européen de Normalisation - Organisme de normalisation officiel dans la Communauté Economique européenne.

**CENELEC -** Comité Européen de Normalisation ELECtrotechnique - Joue un rôle similaire au CEN dans le domaine de l'électrotechnique. Le CEN et le Cenelec harmonisent leurs décisions au sein d'une structure commune, le CEN-Cenelec.

Le Comité européen de normalisation électromagnétique, basé à Bruxelles, est une association regroupant les organismes nationaux de normalisation de dix-huit pays européens dans le domaine de l'électrotechnique. Le CENELEC, qui a pour correspondant en France l'UTE (l'Union Technique de l'Electricité) et le CEI, est chargé de l'élaboration des normes européennes.

**Central dégroupé -** Central téléphonique desservi par le réseau de collecte d'un opérateur téléphonique alternatif et où son DSLAM est hébergé. Il peut ainsi proposer ses services à tous les abonnés dont la ligne est raccordée à ce central et situés à moins de 5 km.

**Central téléphonique -** Désigne l'entité qui, dans un réseau téléphonique, assure les fonctions de commutation mettant en relation les abonnés entre eux. Le central peut désigner un équipement privé pour assurer la commutation au sein d'une entreprise. Dans ce cas, on parle plus souvent aujourd'hui de PABX (Private Automatic Branch Exchange) ou, mieux, d'autocommutateur d'entreprise. On tend donc à réserver l'expression "central téléphonique" aux autocommutateurs publics, ceux de France Télécom par exemple.

**Centre d'appel -** Call Center - Ensemble d'agents utilisant des moyens de télécommunication et d'informatique pour assurer les contacts d'une entreprise avec sa clientèle.

Les agents des centres d'appels peuvent, par exemple, répondre à des demandes de renseignements, traiter des commandes ou des réservations, assurer un service après-vente, effectuer des campagnes de prospection ou de sondage.

Un centre d'appels comprend généralement un dispositif de répartition des appels vers les différents agents. Aux Etats Unis ce dispositif, appelé "automatic call distributor (ACD)" est souvent utilisé pour désigner le centre d'appels lui-même.

**Centre de commutation radio mobile -** MSC - Mobile service Switching Centre - Equipement assurant toutes les fonctions de traitement d'appels pour les mobiles et assurant l'interface entre le système radio et le réseau téléphonique fixe (RTCP).

**Centre de transit -** Transit Exchange - Commutateur connectant des circuits (ou jonctions) entre commutateurs, mais ne desservant pas directement les abonnés. La vocation principale des centres de transit est d'écouler du trafic interurbain à moyenne ou grande distance. On distingue, en France, les centres de transit principaux (CTP) et les centres de transit secondaire (CTS).

**Centrex -** Central Exchange - Service de commutation privée fourni par un exploitant public à partir de ses ressources générales de commutation. Il évite ainsi à une entreprise de posséder son propre autocommutateur.

Service permettant à une ou plusieurs entreprises d'utiliser un autocommutateur public en disposant de tous les compléments de service normalement disponibles sur les PABX.

**CEPT -** Conférence Européenne des Postes et Télécommunications - Organisme de coopération réglementaire et de travaux techniques (en matière de fréquences, notamment) qui regroupe la presque totalité des Etats du continent européen.

Conférence européenne des postes et télécommunications - Organisme regroupant les administrations des 26 pays du continent européen. Il agit auprès du CCITT pour appuyer les recommandations européennes.

**CERN -** Laboratoire de physique nucléaire établi à Genève à l'origine de la création du WWW (World wide web).

**CERT -** Computer Emergency Response Team - Fondé par le DARPA à Fort Lee en réponse à l'incident du vers Morris en 1988,a été créé pour centraliser les efforts de réponse à des incidents informatique de grande ampleur qui comme en 1988. Le groupe est aujourd'hui basé à l'Université Carnegie Mellon à Pittsburgh sous le nom de CERT Coordination Center.

**Certificat -** Message signé numériquement au moyen d'une clé privée d'une tierce partie de confiance (voir autorité de certification) et indiquant qu'une clé publique spécifique appartient à une personne ou à un système possédant un nom et un ensemble d'attributs précis.

**Certificat numérique -** Document électronique certifiant l'identité de l'émetteur ou du récepteur dans le cadre d'un échange électronique.

Il comporte des renseignements comme la version du certificat, le numéro de série, l'identité de l'autorité de certification, l'identité du serveur source, la date d'expiration, et l'algorithme utilisé.

Il existe différents types de certificats numériques :

- Les certificats serveur identifiant un serveur marchand, et permettant d'effectuer des sessions de communication chiffrée. De tels types de certificat sont liés à une URL.
- Les certificats personnels identifiant une personne physique, qui peut être un consommateur ou un collaborateur d'une entreprise. Ces certificats peuvent être stockés sur un ordinateur ou sur des cartes à puce.
- Les certificats IPSEC identifiant un équipement réseau comme un routeur ou un firewall. Ces certificats sont mis en place pour la création d'un VPN par exemple.

**CFB -** Cipher FeedBack mode - Mode opératoire de l'algorithme D.E.S où on commence avec y0 (un bloc initial de 64 bits), et l'on produit la clé zi en chiffrant le bloc de texte chiffré précédent, soit zi = ek (yi-1) avec i ≥ 1.

**CFONB -** Comité Français d'Organisation et de Normalisation Bancaires - Comité actif en particulier dans le domaine des Echanges de données informatisé (EDI) et des normes bancaires Etebac.

**CFRAC -** Continued fraction Method - Méthode de factorisation de fraction en continue.

**CFT -** Cross File Transfer - Logiciel de gestion et de transfert de fichiers développé par la société Crédintrans disponible sur les principaux ordinateurs du marché en France. Il est surtout utilisé dans le domaine bancaire.

**CGMP -** Cisco Group Management Protocol - Utilise les adresses Multicast de la couche standard MAC pour limiter le trafic Multicast, transparent pour les ordinateurs, CGMP programme dynamiquement les commutateurs en fonction des messages IGMP, il économise les ressources (bande passante du réseau, charge CPU) et offre les performances de la commutation de niveau 2. CGMP est destiné aux communications inter équipements du LAN, RGMP est destiné aux routeurs connectés à un commutateur. (voir Multicast).

**Chambre -** Regard de dimensions importantes permettant l'accès sur un réseau enterré. Les fourreaux et les câbles passent par la chambre. Les câbles sont interconnectés dans des boites de jonction, elles-mêmes installées dans les chambres. Elles sont fermées par un ou plusieurs tampons en fonte.

**Champs -** Ils peuvent être électriques ou magnétiques. Les premiers sont produits par des variations de tension (plus elle est élevée, plus le champ résultant est intense) même si le courant ne passe pas.

Les champs magnétiques n'apparaissent que si le courant circule dans la ligne. L'intensité du champ magnétique variera selon la consommation d'électricité (ampérage) alors que celle du champ électrique reste constante. On peut se protéger des champs électriques grâce à des écrans métalliques. Les champs électriques générés par les lignes à haute tension peuvent être atténués par les murs des bâtiments ou par des arbres. Si ces lignes sont enterrées, elles ne produisent pratiquement aucun champ en surface. En revanche, on ne se protège pas des champs magnétiques par des arbres ou des murs, et ils ne sont pas réduits par l'enfouissement.

Quand ils sont agricoles, les champs représentent une parcelle de terrain d'une surface extrêmement variable ☺

**Changement d'opérateur - Churn -** Action d'un client final consistant à changer d'opérateur. Le taux de « churn » définit la perte et le renouvellement des abonnés, les actions de désabonnement.

**CHAP -** Challenge Handshake Authentication Protocol - RFC 1994 - Protocole d'authentification permettant d'empêcher les accès non autorisés. Le protocole CHAP authentifie et identifie l'entité distante. Le routeur ou le serveur d'accès détermine ensuite si l'utilisateur peut être autorisé à accéder au réseau. Il s'agit d'une authentification mutuelle basique s'appuyant sur un échange challenge/réponse.

Les étapes de l'échange (challenge/réponse) sont les suivantes :

- un nombre aléatoire de 16 bits est envoyé au client par le serveur d'authentification, ainsi qu'un compteur incrémenté à chaque envoi,
- la machine distante"hache " ce nombre, le compteur ainsi que sa clé secrète (le mot de passe) avec l'agorithme de hachage MD5 et le renvoie sur le réseau;
- le serveur d'authentification compare le résultat transmis par la machine distante avec le calcul effectué localement avec la clé secrète associée à l'utilisateur.

Si les deux résultats sont égaux, alors l'identification réussit, sinon elle échoue.

Le protocole CHAP améliore le protocole PAP dans la mesure où le mot de passe n'est plus transmis en clair sur le réseau.

**CHAPS -** Clearing House Automated Payment System - Système de télé compensation interbancaire britannique.

**Charge -** Résistance permettant de conserver une impédance du câble et une intensité du signal correctes. On utilise également les termes de bouchon et de terminator.

**Charte Informatique (Une) -** Une charte informatique est un bon moyen pour sensibiliser les utilisateurs à un usage raisonné de l'outil informatique.

Un canevas pour les chartes (ce que doit contenir une charte, d'après la CNIL (Commission Nationale Informatique et Liberté) - Recommandations 2002 :

- Statut de la charte,
- Rappels légaux - Diffamation, pornographie, propriété intellectuelle,
- Sécurité et confidentialité,
- Courrier électronique - Droit d'accès au web mail, sauvegarde des messages, utilisation privée, modes de contrôles de l'usage,
- Internet - Connexion par modem, devoir de réserve, participation aux forums et aux chats, usage privé, téléchargements, accès au FTP,
- Outils de surveillance, d'administration et de sauvegarde - fonctionnement des proxys, politique de filtrage, gestion des sauvegardes sur les postes et les serveurs, périodicité, fichiers concernés.

**Chat -** Espace de discussion permettant à plusieurs personnes ayant des centres d'intérêts communs de discuter en ligne.

**Chiffrement -** Méthode de codage consistant à rendre des données indéchiffrables pour tout autre utilisateur que le destinataire du message, permettant de garantir la totale confidentialité de l'information véhiculée.

**Chiffrement de Hill -** Procédé cryptographique qui consiste à transformer m caractères d'un bloc de texte clair en m carctères dun bloc de texte chiffré par des combinaisons linéaires.

**Chiffrement de Vigenère -** Procédé cryptographique qui traite m caractères alphabétiques à la fois. Chaque bloc de texte clair est équivalent à m caractères alphabétiques.

**Chiffrement en chaîne -** Procédé cryptographique qui engendre une séquence de clés dont chaque élément de la séquence est utilisé pour chiffrer un bloc particulier constituant le texte en clair.

**Chiffrement par blocs -** Procédé cryptographique dont les éléments du texte clair sont chiffrés de la même manière à partir d'une seule clé K.

**Chiffrement par décalage -** Procédé cryptographique basé sur l'arithmétique modulaire (algorithme de la division euclidienne).

**Chiffrement par permutation -** Procédé cryptographique qui conserve les mêmes caractères du texte clair mais en les réordonnant.

**Chiffrement par substitution -** Procédé cryptographique qui consiste à remplacer chaque caractère du texte clair par un autre dans le texte chiffré.

**Chiffrement quantique -** la cryptographie quantique a pour objet de résoudre un grand défi de la cryptographie : l'échange d'une clé de chiffrement sur un réseau public.

D'apparence simple, le problème est pourtant complexe : comment permettre à deux personnes qui ne partagent rien de s'accorder sur une clé secrète en ne communiquant qu'au travers d'un réseau public?

Là où les solutions classiques, tel l'algorithme Diffie-Hellman, reposent sur des principes mathématiques, la cryptographie quantique exploite, elle, un principe physique : le comportement imprévisible de la lumière sur une fibre optique. Les solutions de cryptographie quantique actuelles fonctionnent donc sur une fibre optique. Elles imposent que les deux correspondants disposent d'un second canal de communication. Pour transmettre sa clé, l'émetteur envoie une série de photons sur la fibre optique. Chacun peut être polarisé (aligné) selon quatre angles différents. La polarisation de chaque photon est décidée par l'émetteur, qui la garde secrète. Chaque photon correspond à un bit d'information et prendra à l'arrivée la valeur 0 ou 1 selon sa polarisation d'origine. À l'autre bout de la ligne, le destinataire dispose d'un filtre polarisant, qui peut être réglé sur deux axes seulement, vertical ou oblique. Le destinataire choisit au hasard un des deux réglages pour chaque photon qu'il reçoit. Seuls seront reçus ceux étant clans le même sens à l'émission et à la réception. les autres photons étant perdus. D'autre part, si un filtre réglé verticalement laisse bien passer les photons polarisés à la verticale (0") et bloque ceux polarisés à l'horizontale (90"), il est en revanche impossible de prévoir son comportement face aux photons polarisés sur un axe oblique (45 ou 135°). Certains passeront, d'autres pas. C'est cette incertitude quantique, documentée en 1927 par le physicien Werner Karl Heisenberg, qui garantit l'inviolabilité de la communication.

À l'issue de la transmission, les deux partenaires font le point sur les photons émis (avec quelle polarisation) et reçus (avec quel réglage de filtre). Il est alors possible d'évaluer statistiquement le taux d'erreurs du destinataire dans la réception des photons (entre ses propres mauvais choix d'alignement et l'imprécision quantique naturelle). Un intrus sur la ligne viendra totalement bouleverser ce modèle statistique, et il sera facilement détecté. Si aucun intrus n'a été détecté, les photons reçus, associés à leur bit d'information. constituent la clé qui permettra le chiffrement de n'importe quel document avec n'importe quel algorithme.

**Chiffrer -** Discipline qui englobe tous principes, moyens et méthodes destinées à la transformation de données afin de cacher leur contenu, d'empêcher leur modification et leur utilisation frauduleuse. (ISO 8732)

Le chiffre définit les méthodes de chiffrement et déchiffrement.

Les verbes "crypter" et "encrypter", de même que les substantifs "cryptage" et "encryptage" sont des anglicismes.

**CHILL -** CCITT High Level Language - Langage conçu par le CCITT pour la programmation des commutateurs téléphoniques. Outre CHILL, les constructeurs de commutateurs téléphoniques utilisent également le langage Ada.

**Churn -** Changement d'opérateur - Action d'un client final consistant à changer d'opérateur commercial.

**CICS -** Customer Information Control System - Moniteur système transactionnel d'IBM.

**CIFS -** Common Internet File System - Protocole de Microsoft qui définit un standard d'accès à des fichiers distants, basé sur SMB (Server Message Block).

**Cigref -** Club Informatique des GRandes Entreprises Françaises.

**CIIBA -** Comité Interministériel pour l'Informatique et la Bureautique dans l'Administration - Organisme rattaché au Premier ministre et chargé d'harmoniser les systèmes d'information des différentes administrations, notamment pour favoriser l'Echange de données informatisé (EDI) entre ces administrations ou avec les entreprises.

**CIR -** Commited Information Rate - Débit minimum garanti qui définit le volume moyen d'informations que le réseau s'engage à transporter jusqu'au destinataire pendant un intervalle de temps T.

Customer Information Rate - Débit autorise et garanti par un opérateur sur son réseau pour une liaison sur un intervalle de temps.

**Circuit -** Canal de communication bidirectionnel établi de manière temporaire ou permanente, directe ou passant par des intermédiaires, entre deux entités terminales d'un réseau.

**Circuit virtuel -** Voie de communication logique, entre deux entités, n'empruntant pas un chemin physique fixé une fois pour toutes, mais un ensemble de ressources "possibles" dont l'affectation peut être temporaire (on parle alors de Circuit virtuel commuté ou CVC) ou permanent (Circuit virtuel permanent). Un circuit virtuel est identifié par les en-têtes des messages ou paquets qui l'empruntent. Le réseau de transmission de données par paquets Transpac fonctionne selon ce mode.

En commutation par paquets, possibilité offerte par le réseau de faire un transfert de données entre deux extrémités en garantissant leur réception dans l'ordre d'émission, comme si ce transfert utilisait un circuit.

Circuit utilisé par une technologie niveau 2 orientée connexion comme ATM ou Frame Relay, requerrant la maintenance d'information d'état dans les commutateurs niveau 2.

Circuit virtuel commuté (CVC) : circuit virtuel établi et libéré à l'initiative d'un des correspondants.

Circuit virtuel permanent (CVP): circuit virtuel établi d'une manière permanente entre deux extrémités.

**Circuits de données -** Ensemble de deux voies de transmission de données pour assurer une transmission dans les deux sens.

**CITICS -** Comité Interprofessionnel des Technologies de l'Information, de la Communication et des Services. Le CITICS a pour objet de permettre à l'ensemble des acteurs concernés par les technologies de l'information, de la communication et des services d'agir en commun aussi bien au plan national qu'européen.

**Classe -** (voir câblage et pré câbalge) - Définition des caractéristiques d'une installation, d'un lien (classe A, B, C, D, E, F). Dépend de la catégorie des composants utilisés et de leur mise en oeuvre.

**Classe de services -** Désigne à l'intérieur d'une couche du modèle OSI différentes options selon la qualité et la fiabilité désirées.

**Classes de Débit -** La plage des débits possibles est évidemment très large et dépend des supports utilisés, des méthodes de codage et de l'électronique de transmission associée. En informatique, le débit d'un canal pourra aller de 50 caractères/sec. (télétype) à plusieurs centaines de millions d'octets/sec (par exemple pour relier les mémoires des gros ordinateurs). Sur les réseaux publics, la plage des débits s'étend de 50 caractères/sec. pour le réseau télex à plusieurs centaines de millions de bits/sec.

**Classificateur de paquets -** Fonction du contrôle de trafic qui sélectionne une classe de service pour chaque paquet, en accord avec l'état de réservation de ressource fourni par RSVP.

**CLE -** Concentrateur Local d'Entreprise - Equipement commercialisé par Transpac pour regrouper et commuter des Accès de façon à réduire le nombre des liaisons directes au réseau Transpac.

**Clé cryptographique -** Code numérique servant au cryptage, au décryptage et à la signature d'informations.

**Clé de session -** Algorithme de cryptage symétrique (même clé pour le cryptage et le décryptage). La clé de session est un algorithme qui ne sert qu'une seule fois. Elle est elle même envoyée, cryptée avec un cryptage fort (asymétrique en général).

**Clé privée -** Code numérique utilisé pour décrypter les données et vérifier les signatures numériques. Cette clé doit demeurer secrète et ne doit être connue que de son propriétaire.

**Clé publique -** Code numérique utilisé pour décrypter les données et vérifier les signatures numériques. Cette clé peut être diffusée librement.

**Clé publique et clé privée -** Algorithmes de cryptage utilisés par les systèmes de cryptage asymétrique (clés différentes pour le cryptage et le décryptage). Un utilisateur diffuse largement sa clé publique, mais lui seul conserve sa clé privée. Pour crypter un message, il utilise la clé publique du destinataire, qui décryptera avec sa clé privée. Pour signer son message, il utilise sa clé privée, et le destinataire le décryptera avec sa clé publique.

**Client -** Dans les réseaux de données, se dit d'un ordinateur ou d'un équipement qui utilise des ressources partagées par des serveurs.

**Client-Serveur -** Cadre général fixant les règles de communication (code, protocoles, interface,) entre les divers constituants d'un réseau. Modèle conceptuel d'informatisation consistant à répartir les traitements entre un poste de travail intelligent (de type micro-ordinateur) et un serveur.

**Cluster -** Terme anglo-saxon équivalent approximatif du français "grappe", il désigne la concentration de plusieurs ressources ou terminaux distincts en un même ensemble homogène.

**CMIS/CMIP -** Common Management Information Services/Common Management Information Protocol - Protocoles élaborés dans le cadre de l'ISO (International Standard Organisation) pour servir de cadre à la gestion et à l'administration de réseaux. Ils reposent sur le principe d'une base de données contenant les informations utiles à l'administration de réseaux.

**CMOS -** Complementary Metal Oxyde Semi-conductor - Désique l'une des technologies utilisées pour réaliser les capteurs d'appareils photo, de caméscopes et descanners. (voir CCD).

**CNES -** Centre National d'Etudes Spatiales.

**CNET -** Centre National d'Etudes de Télécommunications - Organisme de recherche appartenant à France Télécom, il gère en particulier tous ses dossiers techniques (mise au point des architectures, spécifications, rédactions d'appel d'offres, recettes, gestion du réseau, réception des achats, tests...) liés aux infrastructures publiques de télécommunication.

Le CNET est implanté en région parisienne (Issy les Moulineaux et Bagneux), à Lannion, à Grenoble, à Rennes (en commun avec TDF) et à Caen (en commun avec La Poste), à Belfort et à Sophia-Antipolis.

**CNIL -** Commission nationale informatique et libertés - Autorité indépendante composée de parlementaires, de représentants de trois grands corps de l'Etat et de personnalités qualifiées. Elle veille au respect des principes énoncés dans la loi du 6 janvier 1978 relative à l'informatique et aux libertés.

Cette Commission instituée en France par la Loi n° 78-17 du 6 janvier 1978 (dite loi « Informatique et Libertés ») est une des armes les plus puissantes mises en place dans un pays occidental par l'intermédiaire du corps législatif pour défendre le citoyen dans son interaction de plus en plus quotidienne avec l'informatique.

Autorité administrative indépendante (son statut est proche de celui du Conseil Supérieur de l'Audiovisuel (CSA), de la Commission des Opérations de Bourse (COB), ou encore de la Commission d'Accès aux Documents Administratifs (CADA)), elle a six missions principales :

- Recenser les fichiers
- Contrôler et vérifier sur place
- Réglementer
- Garantir le droit d'accès
- Instruire les plaintes
- Informer le public et les entreprises

**Coaxial -** Qualifie un câble dans lequel l'un des deux conducteurs est central, pendant que l'autre sous forme de tresse métallique, entoure concentriquement le premier, empêché d'entrer en contact avec lui par une gaine isolante, le tout enfermé dans une gaine externe qui peut elle aussi être blindée. Aujourd'hui remplacé par la paire torsadée blindée (STP).

Le câble coaxial est encore largement utilisé pour raccorder les antennes des systèmes Radio (Wi-Fi, GSM, GPRS, UMTS, TV,…)

**Codage -** Ensemble de règles définissant une correspondance biunivoque entre des informations et leur représentation par des caractères, des symboles ou des éléments de signal.

La difficulté de restituer à l'arrivée l'information telle qu'elle a été envoyée tient aux contraintes que font peser sur la transmission l'effet de filtrage exercé par la bande passante, la difficulté de réduire la composante continue du signal en présence d'équipements isolants, et la nécessaire synchronisation des horloges. Toutes ces raisons font qu'il est nécessaire de modifier, c'est à dire, de coder le signal à transmettre.

Il existe trois types de codage pour "coder" l'information en ligne, autrement dit, pour préparer l'information à sa transmission. Il y a les codages qui fonctionnent en binaire, tels le codage dit "NRZ" (Non Retour à zéro),

ou le codage Manchester, ou encore le Manchester différentiel. Viennent ensuite les codages dits "bipolaire à haute densité", connus sous leur acronyme anglais HDB (High Density Bipolar), enfin, des codages qui fonctionnent par substitution de groupes binaires.

Le premier objectif derrière toute opération de codage est de diminuer la composante continue du signal. Sur ce point, le codage NRZ, le plus simple de tous, se révèle peu performant. En effet, le principe sur lequel il repose (qui est de classer l'information en deux camps, les valeurs positives "1" d'un côté et négatives "0" de l'autre), ne permet pas d'obtenir une composante continue nulle (les deux sommes ne s'annulant pas forcément). De plus, avec ce codage, les transitions se font trop rares surtout lorsque la transmission dure longtemps (longue suite de "0" et de "1").

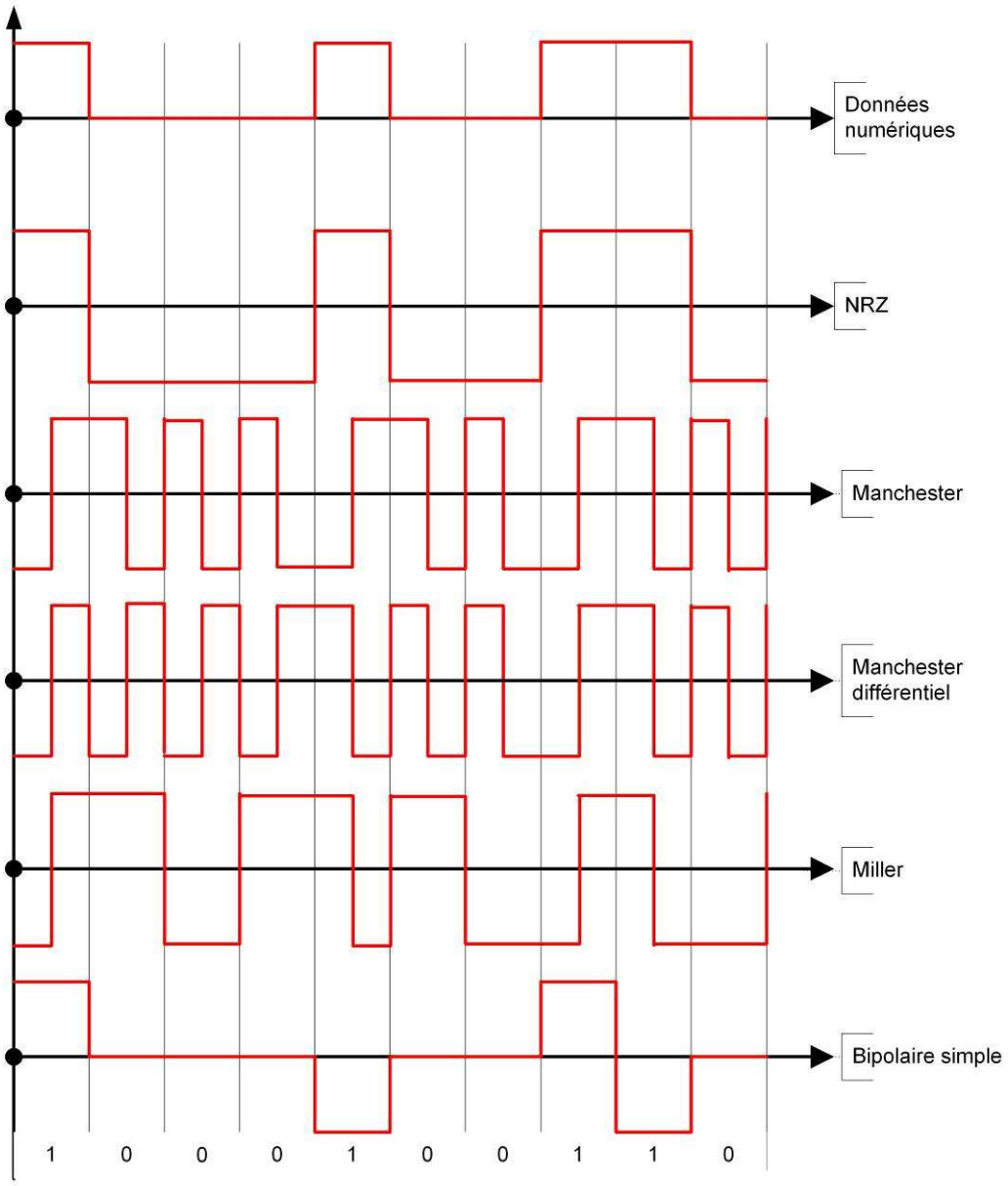
Le codage Manchester, utilisé dans les réseaux de type Ethernet à 10 Mbits/s, tente de remédier aux lacunes du NRZ en présentant une transition au milieu de chaque temps "bit". La transition est croissante pour 1, décroissante pour 0. Mais le sens des transitions imposé par ce type de codage pose problème en cas d'inversion des fils de liaison. Le codage Manchester différentiel, retenu dans les environnements réseaux de type Token Ring, permet de coder chaque transition, au milieu du temps alloué à chaque bit, par rapport à la précédente: si le bit à coder vaut 0, la transition est de même sens que la précédente; si le bit est à 1, on inverse le sens de la transition par rapport à celui de la précédente. Ce codage résout la plupart des problèmes posés, mais son spectre est cependant relativement large.

Avec les codages bipolaires, on obtient une réduction significative du spectre en ne codant qu'un type de bit (par exemple, les "1 ") et en alternant leur polarité (c'est à dire que le premier bit à "1 "est par exemple positif, le second négatif, le troisième positif, etc.) pour éliminer la composante continue du signal. Toutefois, lors de longues séquences de "0", ou de "1 ", il n'y a pas de transition.

Les codes HDBn (Haute Densité Binaire d'ordre n) sont des codes bipolaires complexes dans lesquels, pour éviter de longues séquences sans transition (suite de "0"), si le bit de rang n+1 est à zéro, on le remplace par un bit particulier en violation de la règle d'alternance des signes.

Pour respecter la bipolarité, ces bits sont alternativement inversés. De ce fait, ils peuvent ne plus être en opposition par rapport au dernier bit à 1. Dans ce cas, pour éviter la confusion, on introduit un bit supplémentaire. HDB3 est utilisé dans les liaisons spécialisées numériques Transfix. Enfin, d'autres codages, plus complexes, utilisant les techniques de modulation, sont mis en œuvre dans les réseaux à haut débit. Ils optimisent l'utilisation de la bande passante et améliorent la résistance aux erreurs.

Le principe est le suivant: on substitue à une combinaison binaire de n bits une autre combinaison généralement de n+ l bits ou n+2 bits. Ces codes résolvent facilement les problèmes de composante continue et de largeur de spectre. Les combinaisons binaires sont choisies de telle manière qu'au moins une transition est assurée pendant un intervalle de temps t dépendant essentiellement de la stabilité de l'horloge de réception. Le réseau FDDI (Fiber Distributed Data Interface) utilise un code de cette catégorie, le 4B5B, où une séquence de 4 bits est remplacée par une combinaison de 5 bits.




Les principaux codes

**Code -** Pour qu'il y ait communication, autrement dit échange d'informations, il faut que le signal ait un sens que le récepteur puisse interpréter en le rapportant à un système de signification stable. Ce système de référence définit un code qui devra être commun à l'émetteur et au récepteur, soit naturellement soit par convention préalable.

Un code pourra se définir par sa précision et son extension (*le nombre de récepteurs ou d'émetteurs potentiels se référant à un même code*). Les codes les plus précis et les plus universels sont les codes numériques, c'est à dire reposant sur l'arithmétique. Ils ont surtout la propriété de permettre des combinaisons en systèmes parfaitement définis : par exemple le code décimal (*à dix éléments de base*) ou hexadécimal, ou encore binaire, le plus simple puisqu'il n'a que deux éléments (0 *et 1*). Autre avantage des codes numériques : ils peuvent se convertir les uns les autres par des lois précises de transcodage. Le code binaire fait de 0 et de 1 est particulièrement intéressant puisqu'il s'adapte parfaitement à l'électronique numérique : un 1 pouvant se définir par un passage du courant électrique et un 0 par un courant bloqué.

Le code binaire est en dernier ressort le plus universel des codes dans les équipements électroniques de transmission ou de stockage. Mais à moins d'un entraînement acharné, il n'est pas compris intuitivement par le cerveau humain. Entre les codes compris par l'homme (*langues parlées, signes visuels, images, écriture* ...) et le code binaire, il faudra opérer des conversions successives. Le microphone, le clavier, la caméra en entrée ou le tube cathodique (*écran TV, vidéo*), l'imprimante, le haut-parleur, en sortie, sont des convertisseurs de codes.

Les deux principaux codes sont:

Le code ASCII originellement à 7 bits et 128 combinaisons, aujourd'hui doublé d'une version à 8 bits et 256 combinaisons qui permet de coder les chiffres, les lettres en majuscules et minuscules, plus des caractères spéciaux de commande et les accents nationaux. Normalisé sous le nom de CCITTn°5, il est de très loin le plus employé dans les transmissions de données.

Le code EBCDIC à 8 bits et 256 combinaisons, d'origine informatique IBM. L'EBCDIC continue d'être utilisé dans le stockage et le traitement des données, nettement moins dans leur transmission, bien qu'il demeure en vigueur pour les principaux terminaux d'IBM et plusieurs de ses concurrents.

**Code correcteur d'erreurs -** Code autocorrecteur - Error-correcting code - Code qui permet, outre la détection, la correction automatique de certaines fautes détectées.

**Code Redondant -** Redundant Code - Code utilisant plus de symboles qu'il n'est nécessaire pour représenter des informations. La redondance est généralement utilisée pour la détection et la correction éventuelle des erreurs.

**CODEC -** Abréviation de Codeur-Décodeur. Equipement ou composant électronique permettant de transformer un signal analogique (par exemple, un son ou une image) en train de données numériques et inversement.

**Cœur -** (en câblage et pré câblage) Partie centrale d'une fibre optique dans laquelle est transmise l'information.

**Cœur de réseau -** Backbone - Le cœur de réseau, également appelé réseau général, correspond à l'ensemble des supports de transmission et de commutation d'un réseau. Voir Backbone. Par extension ou habitude, le cœur de réseau peut aussi désigner un seul et même équipement qui aura la charge, la capacité et la fonction d'assurer la concentration, la commutation, le filtrage et le routage d'un réseau d'entreprise.

Dans l'organisation d'un réseau on distingue 2 parties :

- La boucle locale ou réseau d'accès, qui correspond à la ligne d'abonné,
- Le cœur de réseau, également appelé Core Network, qui correspond à l'ensemble des supports de transmission et de commutation à partir du commutateur d'abonné.

**Cogecom -** Compagnie holding portant les participations détenues par France Télécom dans des sociétés extérieures.

**Collapsed backbone -** Dans la technique du collapsed backbone ou artère rapide, le commutateur tient le rôle de l'épine dorsale du réseau local. Le backbone reporté sur le fond de panier du mutateur, qui "multiplexe" les connexions au réseau local.

**Collecte pour le compte de tiers -** Service qui, dans le cadre de l'interconnexion, permet à un opérateur de réseau de collecter du trafic depuis le réseau de l'opérateur historique pour le compte d'un autre opérateur qui n'exploite pas d'infrastructure sur la zone géographique concernée. Ce service est notamment utilisé par les opérateurs de service téléphonique, titulaires d'une licence L. 34-1, qui souhaitent pouvoir fournir leur service sur un territoire étendu sans pour autant déployer un réseau.

**Collision -** (sur Ethernet) - Une collision se produit lorsque deux ordinateurs tentent d'émettre des données au même moment et provoquent un conflit. Les émissions sont alors interrompues, et les ordinateurs émettent à nouveau après un temps d'attente aléatoire.

**Colocalisation -** Dans le cadre du catalogue d'interconnexion de France Télécom, l'interconnexion physique peut être réalisée par trois techniques distinctes :

- La colocalisation : l'opérateur installe ses équipements dans les locaux de France Télécom
- La liaison de raccordement : France Télécom installe ses équipements dans les locaux de l'opérateur.
- L'interconnexion en ligne, intermédiaire entre ces deux modes de raccordement : le point de connexion se situe sur le domaine public, par exemple.

**Colonne montante -** Conduit d'un immeuble permettant de desservir les étages et pouvant regrouper les réseaux d'eau, de gaz, d'électricité ou de communications électroniques.

Par extension, partie du câblage d'un immeuble comprise entre le pied d'immeuble et les différents points de branchement dans les étages.

Un immeuble peut et doit contenir contenir plusieurs colonnes montantes.

*Attention au strict respect des usages dans les colonnes montante. Toujours veiller à n'utiliser que la colonne désignée à l'usage. Ainsi on ne passe jamais l'électricité par la colonne de gaz.*

**Commerce Electronique -** L'European Information Technology Observation (EITO, 1997) a défini le commerce électronique en ces termes : "Le commerce électronique est l'activité qui mène à un échange de valeurs par le biais des réseaux de télécommunications. "

Aussi le business électronique peut être défini comme l'utilisation de tout ou partie des technologies d'Internet pour transformer le fonctionnement des activités principales de la chaîne de valeurs de l'entreprise en vue d'en dégager une valeur économique supérieure directe ou indirecte.

Ces définitions englobent tous les processus consistant à promouvoir ses biens et services sur un canal électronique. Cela va de la présentation de la société, de son catalogue (produits, caractéristiques, disponibilité, etc.) en passant par la mise à disposition de contenus éditoriaux relatifs à l'entreprise, la prise de commande automatique, le paiement en ligne et même parfois la livraison d'un produit en ligne. Bref, le commerce électronique couvre tous les moyens permettant à la société d'améliorer son activité quotidienne ; il donne la possibilité à l'entreprise de communiquer sur sa marque, de vendre ses produits et services et d'établir un contact direct avec son environnement commercial par le réseau. A cela, on ajoute une précision sur le type de clientèle à atteindre.

On parle de Business to Consumer (B to C) lorsque l'entreprise vend des produits ou services aux particuliers. Il s'agit de Business to Business (B to B) dès lors que les échanges sont réalisés entre personnes morales (sociétés, distributeurs, grossistes, détaillants, etc.). Le site d'Amazon.com est un très bon exemple de société virtuelle pour le commerce B to C. Le commerce Business to Administration (B to A) couvre toutes les transactions entre les compagnies et les organisations gouvernementales. Le commerce Consumer to Administration (C to A) commence à peine à se développer, les développements possibles concernent les transactions électroniques de paiements de sécurité sociale ou des paiements d'impôts.

Le tableau ci-dessous représente le type d'échange que l'entreprise peut être amenée à réaliser et les fonctions concernées en interne.

| Type de commerce électronique | Fonctions concernées au sein de l'entreprise | Exemple de fonctionnalités |
|---|---|---|
| Site comercial B-to-C | Marketing et force de vente | Vente de produits avec paiement sur Internet et expédition |
| Extranet client B-to-B | Marketing, achats, gestion de stocks, ventes | Consultation de l'encours client |
| Extranet distributeurs B-to-B | Gestion des stocks et logistique | Consultation de disponibilité des produits. |
| EDI B-to-B | Gestion de stocks, logistique, achats, comptabilité | Liaison EDI par Internet entre deux sociétés |
| Site C-to-C | Site intermédiaire au service de la communication entre particuliers | Ventes aux enchères de particuliers à particuliers. |

**Communication -** Une communication est d'abord un échange de signaux entre un émetteur et un récepteur. Pour l'homme les principaux signaux échangeables (essentiellement sonores et lumineux) sont de nature analogique, c'est à dire qu'ils se présentent comme des variations de grandeurs physiques (ou modulations) pouvant prendre n'importe quelle valeur de façon continue entre deux instants. Un signal sonore est une modulation des vibrations sinusoïdales des couches d'air. Un signal lumineux est une variation des oscillations des ondes lumineuses. L'air ou les ondes lumineuses ou encore les ondes radio constituent les supports (ou médias) du signal. Les principales propriétés d'un signal sont la fréquence (nombre d'oscillations par seconde exprimé en Hertz) et l'amplitude (taille des oscillations). Bien entendu un média ou support, en fonction de ses caractéristiques physiques ne pourra pas supporter n'importe quelle oscillation. Il sera caractérisé, entre autres, par sa bande passante (BP), c'est à dire l'ensemble des fréquences qu'il pourra propager.

**Communication Conférence -** Conference Calling - Complément de service permettant d'établir une communication simultanément avec plusieurs correspondants qui tous participent à la conférence. On connaît en France deux modes de communication conférence : la conférence rendez-vous, dans laquelle les correspondants appellent un numéro convenu (commercialisé par France Télécom sous le nom de Réunion téléphone) et la conférence additive, dans laquelle des appels peuvent être ajoutés par le directeur de conférence (la conversation à trois est une forme de conférence additive).

**Commutateur - Commutation -** Switch - Dispositif permettant d'établir ou de faire cesser des connexions (circuits) temporaires entre plusieurs points quelconques d'un réseau. Ces connexions peuvent être physiques (commutation de circuits) ou logiques (commutation temporelle ou circuits virtuels).

Le concept de "commutateur" a été inventé par Kalpana. Les commutateurs Kalpana transmettent un paquet à un segment récepteur aussitôt que son adresse a été analysée. Ils n'attendent pas que le paquet entier soit arrivé au commutateur. L'avantage de la vitesse a cependant un revers : les commutateurs Kalpana retransmettent également des paquets pour lesquels la détection de collision se produit seulement après la réception de l'adresse ou pour lesquels le contrôle CRC détecte une erreur à la fin du paquet. Etant donné que la norme IEEE pour ponts proscrit la transmission de trames ayant de telles erreurs, Kalpana ne pouvait nommer ce produit un "pont" et choisit dès lors l'expression "commutateur". Kalpana connut un grand succès marketing avec ce produit, ce qui amena d'autres fabricants à désigner leurs ponts ainsi ou encore "ponts commutateurs" (bridging switches) .

Il existe plusieurs types de commutateurs dédiés à des fonctions ou des protocoles précis : Commutateurs voix (assurant de la commutation de circuit), commutateur ATM (assurant la commutation de cellules), commutateur Frame Relay (assurant la commutation et le relayage de trame), commutateur Ethernet (assurant la commutation de trames Ethernet) etc. etc.

Principes de base des commutateurs LAN :

Dans un réseau local, le commutateur vient prendre la place d'un concentrateur (hub) classique. Il est capable de fournir des connexions de 10 Mbits/s, 100 Mbits/s, 1 Gbits/s voire aujourd'hui de 10 Gbit/s par port sans que cette bande passante ne soit partagée. Il est possible d'allouer des débits importants à des groupes de travail, des serveurs ou des stations de CAO. Mais afin d'atteindre de tels débits, les commutateurs doivent transmettre les paquets à des vitesses élevées. Pour que cela fonctionne il y a en fait deux techniques. La première est dite de packet-by-packet. Dans ce cas, le commutateur lit entièrement chaque trame avant de décider de sa destination. Le commutateur peut ainsi effectuer différents traitements (contrôle d'erreurs, filtrage des adresses MAC et protocole, adaptation au milieu hétérogène, fragmentation...). Ce procédé permet donc de réduire les erreurs, mais il en découle une augmentation du temps de latence. Par contre, la seconde technique dite flow-based lit uniquement le début de l'en-tête de la trame de données afin d'identifier l'adresse de destination avant de commuter la trame vers le port voulu. L'avantage de cette technique est sa rapidité d'exécution. En effet le temps de latence est réduit au minimum. Par contre, il n'y a pas de protection contre les trames endommagées. Et cette technologie ne s'applique pas aux réseaux hétérogènes. Les commutateurs permettent de découper le réseau en plusieurs sous-réseaux.

Commutation de niveau 3 paquet par paquet :

Haut niveau d'intégration avec les produits de routage existants, du fait de l'utilisation de protocoles standard.

Sont capables d'évoluer en même temps que les protocoles de routage.

Fort temps de latence du fait de l'examen de chacun des paquets entrants.

Peut être mis en place dans un modèle distribué avec plusieurs autres types de routeurs.

Commutation de niveau 3 flow-based :

Faible interopérabilité avec les routeurs traditionnels du fait de l'utilisation d'une technique de routage propriétaire.

Evolution limitée à la technique propriétaire choisie.

Très peu de temps de latence du fait que seul le premier paquet est examiné.

Ne peut pas évoluer avec des matériels différents. Peuvent donc devenir un goulet d'étranglement dans le réseau.

Le filtrage au niveau réseau (niveau 3) permet de mieux gérer le trafic de son réseau. Mais on peut encore aller plus loin, ou plus haut si l'on se réfère au modèle OSI. Certains commutateurs sont déjà capables aujourd'hui de filtrer le trafic au niveau 4. En clair, ils peuvent analyser le trafic en fonction du type d'application utilisée. Ils peuvent ainsi faire la différence entre du trafic HTTP ou mail. Un commutateur de niveau 7, quant à lui, est capable de filtrer le trafic en fonction de l'application qui est utilisée ou en fonction de l'utilisateur. Ainsi, il sera possible pour l'entreprise de mettre en place une politique cohérente d'utilisation de son réseau. Ce point est particulièrement utile dans le cas d'Internet lorsque l'on souhaite pouvoir en contrôler l'utilisation, soit pour ne pas saturer la bande passante soit pour s'assurer qu'aucun employé ne l'utilise à mauvais escient.

II s'agit donc de l'intégration au sein d'un commutateur de fonctions de filtrage que l'on réalise normalement avec un logiciel proxy ou un firewall (Firewall-1 de Checkpoint, par exemple). Ces commutateurs de niveau 7 permettent en outre d'analyser finement le trafic réseau et de contrôler les accès réseaux. II est ainsi possible d'assigner des priorités à certaines applications ou à certains utilisateurs.

Plusieurs types de commutation sont possibles pour les commutateurs, avec chacun leurs avantages et leurs inconvénients. Les deux plus courants sont le mode Store & Forward et le mode Cut Through.

Un commutateur en mode Store & Forward stocke l'intégralité de la trame et l'analyse avant de la retransmettre. Ce mode de fonctionnement correspond à la norme IEEE 802.1D qui stipule qu'un pont, et donc un commutateur, se doit d'implémenter une couche MAC complète sur chacun de ses ports. Suite à l'analyse des trames de niveau 2, le mode de fonctionnement Cut Through est apparu. Celui-ci se base sur les informations nécessaires à la commutation situées en début de trame, et effectue la commutation de la trame dès que les premiers octets de celle-ci ont été reçus.

Le mode Store & Forward :

Un commutateur qui fonctionne en Store & Forward stocke l'intégralité de la trame reçue avant d'effectuer la commutation et re-transmettre la trame selon le principe suivant :

1. Une trame parvient sur un des ports du commutateur.
2. Stockage de la trame dans la mémoire interne de celui-ci.
3. Analyse de la trame : FCS calculé, longueur vérifiée, adresse de destination extraite.
4. Commutation de la trame vers le bon port.

L'un grand avantage de ce mode de fonctionnement est de permettre de commuter des trames entre des débits différents (de 100 Mb/s à 10Mb/s par exemple) . De plus, il permet d'effectuer l'intégralité des vérifications de la couche MAC. Enfin, le stockage complet de la trame permet la pose de filtres sur différents champs de la trame si on le souhaite.

L'inconvénient principal de ce mode de fonctionnement est la lenteur du processus de commutation puisque le temps de traitement dépend de la longueur totale de la trame.

Le mode Cut Through :

Ce mode de fonctionnement est aussi appelé "On The Fly ".Il permet d'accélérer le processus de commutation par rapport au mode Store & Forward en effectuant la commutation dès que la réception du champ destination, selon le principe suivant :

1. Arrivée d'une trame sur un port du commutateur.
2. Lecture des premiers octets de la trame jusqu'au champ destination.
3. Analyse de l'adresse destination.
4. Commutation de la trame vers le bon port.

De part son fonctionnement, l'avantage principal du Cut Through est la grande vitesse du processus de commutation, ne dépendant pas de l'analyse complète de la trame. Ainsi, le point faible du mode store & forward devient le point fort du Cut Through.

La vitesse du processus de commutation se fait au détriment du traitement d'erreur de la couche MAC. La trame n'étant pas stockée par le commutateur, aucune analyse (CRC, intégrité, …) n'est possible. De plus, le mode Cut Through ne permet pas une bonne gestion des collisions. En effet, si une collision apparaît, la trame n'ayant pas été stockée par le commutateur ne peut être réémise par celui-ci.

Enfin, ce mode de fonctionnement ne permet pas une commutation avec changement de débit.

Il existe aussi d'autres modes de fonctionnement des commutateurs, en général dérivé des deux modes précédents :

- Le mode Adaptive :

Ce mode de fonctionnement permet au commutateur de s'adapter en temps réel aux performances de commutation, en imposant les modes Store & Forward et cut Through en fonction des résultats de commutation obtenus :

Démarrage du commutateur en mode Cut Through. Cela permet une grande vitesse de commutation.

Si le taux d'erreur est trop grand (collision, trames erronées, …), le commutateur passe en mode Store & Forward, plus sécurisé.

Lorsque le taux d'erreur est redevenu convenable, le commutateur repasse en mode Cut Through

Ce type de fonctionnement permet au commutateur d'obtenir un bon niveau de performance général.

- Le mode Fragment-free :

Ce mode de fonctionnement est une variante du mode Cut Through, qui ajoute à ce dernier un traitement d'erreur simplifié sur la trame à commuter :

1. Arrivée d'une trame sur un port du commutateur.
2. Lecture et analyse des 64 premiers octets de la trame. Cela permet de vérifier que celle-ci possède un champ de données cohérent et n'est donc pas un fragment erroné de trame.
3. Commutation de la trame vers le bon port.

Ce mode de fonctionnement permet au commutateur d'obtenir de bonnes performances de commutation, avec une vitesse de commutation rapide, et un niveau de correction d'erreurs supérieur au mode Cut Through.

**Commutateur à Autonomie d'Acheminement -** CAA - Commutateur téléphonique capable d'analyser les signaux de numérotation qu'il reçoit et de choisir un circuit sortant pour acheminer un appel vers sa destination.

**Commutateur de Données -** Data Switching exchange, Data Switch - Nœud d'un réseau de données capable de transférer des données d'une ligne d'entrée vers une ligne de sortie par commutation de circuits ou par paquets.

**Commutation -** Mode d'acheminement de messages par lequel les unités d'informations sont relayées par des équipements sur un réseau en suivant une règle (ou table) entre la source et la destination.

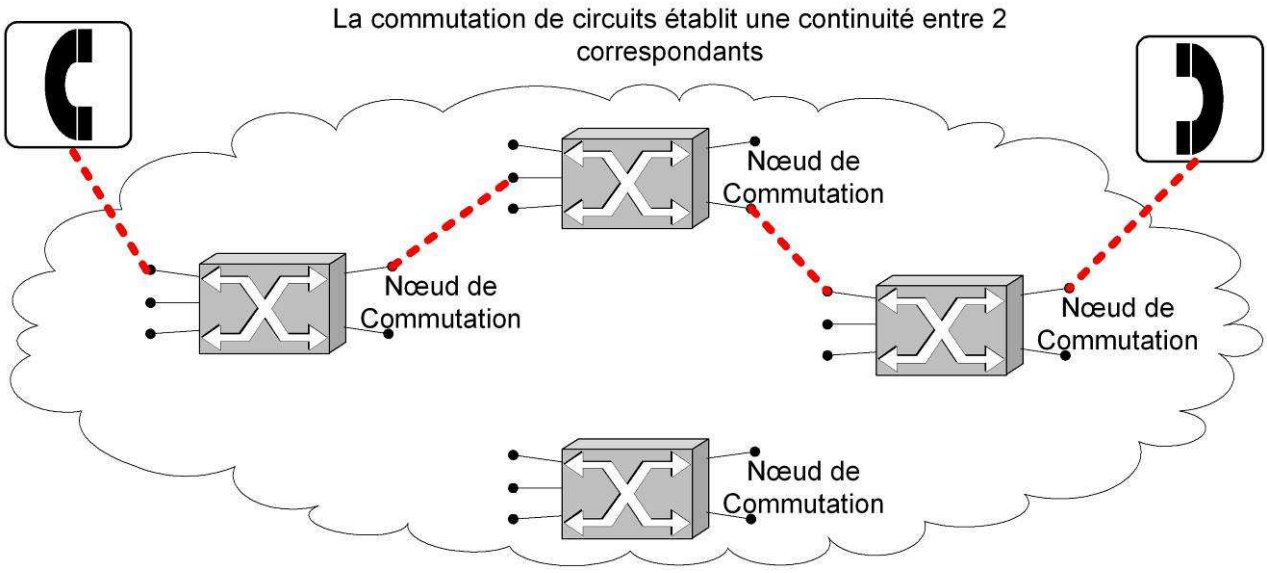
**Commutation de circuit -** Processus qui relie deux ou plusieurs utilisateurs et permet leur utilisation exclusive d'un circuit de données pendant la durée de la communication.

Mise en relation pendant une durée déterminée de deux utilisateurs au moyen d'un lien physique.

Technique permettant d'allouer des voies de communication qui disposent de ressource de multiplexage et de commutation qui leur sont propres durant toute la durée de la commutation.

Dans les réseaux à commutation de circuits, il n'y a pas de stockage intermédiaire des données. Les abonnés monopolisent toute la ressource durant la connexion. La régulation de trafic est faite à la connexion; s'il n'y a plus de ressource disponible, la connexion est simplement refusée. Les nœuds du réseau sont de simples relais de commutation. Dans ces conditions, la facturation est généralement fonction du temps (temps d'occupation des ressources) et de la distance (quantité de ressource utilisée).

La numérisation du réseau a conduit non plus à mettre des circuits en relation mais des intervalles de temps, à travers un réseau de multiplexeurs temporels (TDM, Time Division Multiplexing). Bien que plus complexe, cette technique s'assimile à la commutation de circuits.




sur un réseau de télécommunications, la fonction de commutation assure l'aiguillage du trafic en établissant des connexions temporaires entre deux ou plusieurs points du réseau. Cette opération s'effectue dans des équipements placés à différents endroits du réseau et appelés commutateurs. Ainsi, dans sa structure de base, un réseau de télécommunications est composé de supports de transmission connectés entre eux par des commutateurs. Les modes "paquet" ou "circuit" sont deux techniques de commutation utilisées par les réseaux de télécommunications. La première est par exemple utilisée par les réseaux Internet (IP), la seconde par les réseaux téléphoniques classiques (RTC).

**Commutation de messages -** Technique d'acheminement de messages sans établissement au préalable d'une connexion de bout en bout entre l'émetteur et le récepteur.

La notion de réseaux à commutation de messages correspond plus à un type de service qu'à une technique réellement utilisée pour réaliser des réseaux. Dans la commutation de messages, aucun chemin physique n'est établi entre les deux systèmes. Un message peut être envoyé même en l'absence de son destinataire. Chaque bloc d'information (baptisé message) constitue une entité de transfert (fichier, écran de terminal...) acheminée individuellement par le réseau. Le message est mémorisé par chaque nœud, avant d'être retransmis au nœud suivant. Dans le cas où le destinataire n'est pas connecté, le nœud final mémorise le message, celui-ci sera délivré lors de sa prochaine connexion.

Le concept de réseaux à commutation de messages est utilisé dans les Télex modernes et les systèmes de messagerie publique comme Atlas 400, même si ce type d'application utilise comme réseau support un réseau à commutation de paquets (type Transpac).

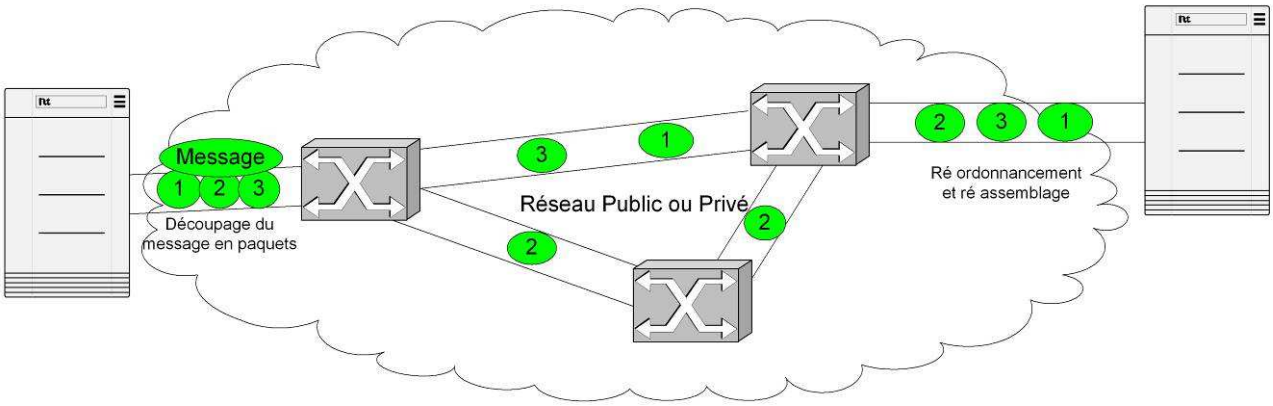
**Commutation de paquets -** La technique de commutation de messages introduit en outre le découpage de chaque message en paquets comportant les adresses nécessaires à leur routage. Les paquets qui arrivent sur un nœud du réseau se présentent dans une file d'attente avant d'être retransmis, après analyse des adresses, sur la voie de transmission appropriée. Les messages sont reconstitués à l'arrivée.

Technique permettant des communications en n'affectant les ressources nécessaires au multiplexage et à la commutation qu'en fonction de leur besoin. La technique consiste à transporter un paquet d'information d'une entrée vers une sortie dans un commutateur.

L'usage des réseaux à commutation de paquets s'est généralisé au milieu des années soixante dix avec la norme X25. Dans un réseau à commutation de paquets, les messages sont découpés en fragments (paquets). Les paquets sont envoyés, dans le réseau, indépendamment les uns des autres, le séquencement n'est pas obligatoirement garanti. Le destinataire doit réassembler les paquets pour reconstituer le message. En principe, il n'y a pas de connexion préétablie, les unités de données sont commutées vers telle ou telle destination en fonction d'une indication d'acheminement, baptisée "en-tête", contenue dans le paquet. Les paquets de différentes sources étant multiplexés sur un même circuit, ce mode de commutation optimise l'utilisation des ressources. Cette utilisation est banalisée et non attribuée à une communication particulière comme dans la commutation de circuits.

Cette technique est parfaitement adaptée au transfert de données (réseaux privés ou publics tel Transpac, Internet ...). Les flux informatiques sont sporadiques, et dans ces conditions, le débit théorique admissible dans le réseau peut être nettement supérieur au débit réel que peut acheminer le réseau (effet statistique). Compte tenu de ces éléments, la facturation, sur le réseau public, se fait généralement au volume.

La commutation de paquets découpe le message en fragments (paquets) acheminés indépendamment les uns des autres par le réseau.




**Commutation électronique -** Commutation basée sur l'emploi de semi-conducteurs (transistors, circuits intégrés) et d'éléments à mémoires. Seule la commutation temporelle mérite pleinement le qualificatif électronique. La commutation à commande électronique et à réseau de connexion spatial, faisant appel à des points de connexion à contacts métalliques, n'est que semi-électronique.

**Commutation spatiale -** Technique de commutation où un chemin physique est établi soit par manœuvre de contact (commutation électromécanique), soit par circuits électroniques (commutation électronique). S'oppose à la commutation temporelle.

**Commutation temporelle -** Technique de commutation où les liaisons ne sont pas physiquement permanentes, mais reconstituées par l'alliance du multiplexage (utilisation d'un même support physique pour plusieurs communications tour à tour) et de mémoires intermédiaires stockant temporairement des éléments du message.

Commutation utilisant les principes de la modulation par impulsions et codage (MIC). Aucune liaison durable n'est établie entre deux lignes reliées à travers l'autocommutateur, mais plusieurs communications se partagent, à intervalles de temps réguliers, un trajet à travers cet autocommutateur.

**Compatibilité Fonctionnelle -** Aptitude d'un équipement terminal à fonctionner avec d'autres équipements terminaux permettant d'accéder à un même service de télécommunication, soit dans le même réseau, soit dans des réseaux différents interconnectés ou interconnectables.

**Complément de Service -** Supplementary Service, User Facility - Prestation qui complète ou modifie un service de télécommunication (service support ou téléservice). L'appel en instance, la conférence à trois, le renvoi temporaire et la facturation détaillée sont des exemples de compléments de service.

**Compression -** Ensemble de techniques permettant de diminuer la quantité d'information à transmettre pour réduire le temps des échanges. Grâce à diverses méthodes mathématiques, la compression tire souvent partie de la redondance naturelle d'un message (répétitions...) soit de ses éléments non significatifs (par exemple, inutilité des blancs sur un document). Procédé permettant de réduire le volume (en bits) ou le débit (en bit/s) des données numérisées (parole, images, textes, ...).

Attention : le verbe correspondant est "comprimer". Compresser n'existe pas en français.

**Compromission -** Dans le domaine de la sécurité informatique, ce terme signifie l'attaque d'un réseau par la violation de la politique de sécurité.

**COMSAT -** Communications Satellite Corporation - Société privée américaine de communications par satellite représentant officiellement les USA dans l'organisation internationale Intelsat.

**COMSIS -** Commission des Sites et Servitudes.

**Concentrateur -** Equipement permettant le regroupement de plusieurs canaux de transmission faiblement utilisés de façon à les additionner pour mieux utiliser un canal rapide. L'opération inverse s'appelle la diffusion. Si le même équipement assure les deux fonctions, on parlera de concentrateur-diffuseur.

**Concentrateur de Données -** Data Concentrator - Équipement qui permet à un support de transmission de desservir plus d'ETTD qu'il ne dispose de voies de transmission.

**Concentrateur VPN -** Plate-forme matérielle permettant la mise en place de connexions réseaux privées bout en bout via une infrastructure réseau publique et offrant un accès distant ou une connectivité site à site.

**Cône d'acceptance -** (en optique) - Voir Ouverture Numérique.

**Conférence téléphonique -** La conférence téléphonique permet de faire participer à la conversation trois ou plusieurs personnes simultanément. Le nombre exact de personnes pouvant participer à une conférence téléphonique dépend du modèle d'appareil téléphonique. Il faut également que cette fonction soit activée par l'opérateur réseau.

**Confidentialité -** Rendre un message inintelligible par un tiers non autorisé.

**Confidentialité des données -** Moyen permettant de garantir que seules les entités autorisées peuvent voir les paquets de données dans un format intelligible. Processus de protection des données d'un réseau contre l'espionnage ou l'altération. Dans certains cas, la séparation des données à l'aide de technologies de tunnellisation, telles que GRE (Generic Routing Encapsulation) ou le L2TP (Layer 2 Tunneling Protocol), offre une confidentialité des données efficace. Toutefois, il est parfois nécessaire d'augmenter la confidentialité à l'aide de technologies de cryptage numérique et de protocoles tels que Ipsec, en particulier lors de la mise en œuvre de VPN.

**Congestion -** La congestion est statistiquement inévitable sur un réseau. Elle est la résultante de l'augmentation des délais d'acheminement. Si la taille des files d'attente augmente dans les commutateurs, les blocs ne sont pas acheminés dans les délais et sont donc retransmis, ce qui augmente encore le trafic.

Pour prévenir la congestion, il faut mettre en place un contrôle d'admission (ne pas admettre dans le réseau plus de trafic que celui-ci ne peut supporter) et un contrôle de flux (asservir le débit de la source aux capacités de traitement du noeud).

**Connecteur N -** Connecteur coaxial utilisé dans les réseaux IEEE 802.3 10Base5. Il permet de raccorder les charges, les répéteurs, etc.

**Connecteur optique-** Elément servant à établir une liaison par branchement entre deux fibres optiques. Il en existe de plusieurs types et de plusieurs tailles.

**Connexion -** Procédure permettant à un utilisateur de se mettre en relation avec un système informatique et, si nécessaire, de se faire reconnaître de celui-ci.

On peut définir aussi une connexion comme étnt une relation logique entre deux entités.

**Conservation de son numéro -** Possibilité offerte à un usager de conserver le même numéro d'appel en cas de déplacement géographique, de changement du service souscrit ou de changement d'opérateur.

**Contention -** Mode d'utilisation d'une voie de communication lorsque deux ou plusieurs équipements peuvent décider d'émettre à n'importe quel moment. Ce mode suppose une technique de résolution des conflits possibles.

**Continuité d'utilisation -** Aptitude d'un service, une fois obtenu par un usager, à continuer d'être fourni pendant la durée voulue dans des conditions données.

**Contrat de service -** Contrat qui décrit les services fournis par un opérateur mobile et le coût de ces services. Il précise généralement le montant du forfait mensuel (et le nombre de minutes comprises dans le forfait), ainsi que le prix de la minute en cas de dépassement du forfait.

**Contrôle d'erreur -** Le signal électrique peut subir des perturbations (distorsion, présence de bruit), notamment lors du transport des données sur longue distance. Le contrôle de la validité des données est nécessaire pour certaines applications (professionnelles, bancaires, industrielles, confidentielles, relatives à la sécurité, ...). Il existe des mécanismes permettant de garantir un certain niveau d'intégrité des données, c'est-à-dire de fournir au destinataire une assurance que les données reçues sont bien similaires aux données émises. La protection contre les erreurs peut se faire de deux façons :

- soit en fiabilisant le support de transmission, c'est-à-dire en se basant sur une protection physique. Une liaison conventionnelle a généralement un taux d'erreur compris entre 10-5 et 10-7.
- soit en mettant en place des mécanismes logiques de détection et de correction des erreurs.

La plupart des systèmes de contrôle d'erreur au niveau logique sont basés sur un ajout d'information (on parle de "redondance") permettant de vérifier la validité des données. On appelle somme de contrôle cette information supplémentaire.

**Contrôle d'accès -** Limitation du flux de données des ressources d'un système uniquement vers les personnes, programmes, processus autorisés ou vers d'autres systèmes du réseau. Les ensembles de règles de contrôle d'accès des routeurs Cisco sont appelés listes de contrôle d'accès ou ACL.

**Contrôle d'admission -** En X25, on réserve les ressources nécessaires lors de la mise en place du circuit, mais ceci est incompatible avec un trafic en rafale. Pour garantir la QoS, une connexion ne doit être acceptée que si le réseau est apte à la satisfaire. Les demandes de connexion seront donc accompagnées par des informations comme le débit moyen et le débit de pointe nécessaire.

**Contrôle de flux -** Mécanisme d'asservissement de l'émetteur sur les capacités de réception du destinataire.

Un contrôle des flux est un processus de contrôle de la cadence des unités d'information.

En mode connecté, le contrôle de flux se fait par fenêtre glissante. La fenêtre est le nombre de blocs que la source peut émettre sans avoir reçu d'acquittement. Plus la fenêtre est importante, plus l'émission peut-être continue mais le contrôle de la source est faible. Etant donné la rapidité du passage des informations sur un réseau haut débit, il ne peut y avoir de contrôle de flux par fenêtre glissante. Celui-ci est assuré par les couches supérieures.

**Contrôle de la sécurité -** Procédure de sécurisation du réseau au moyen de tests réguliers et de SPA (Security Posture Assessments).

**Contrôle de parité** (ou d'imparité) - Technique de détection d'erreur dans laquelle un bit (1 ou 0) est ajouté à chaque caractère pour que le nombre de bits total soit toujours pair (ou impair).

Le contrôle de parité (VRC - Vertical Redundancy Check ou Vertical Redundancy Checking) est un des systèmes de contrôle les plus simples. Il consiste à ajouter un bit supplémentaire, appelé bit de parité à un certain nombre de bits de données appelé mot de code (généralement 7 bits, pour former un octet avec le bit de parité) dont la valeur (0 ou 1) est telle que le nombre total de bits à 1 soit pair.

En clair, le contrôle de parité consiste à ajouter un 1 si le nombre de bits du mot de code est impair, 0 dans le cas contraire.

**Contrôle de parité croisé -** Le contrôle de parité croisé aussi appelé contrôle de redondance longitudinale ou Longitudinal Redundancy Check - LRC, consiste non pas à contrôler l'intégrité des données d'un caractère, mais à contrôler l'intégrité des bits de parité d'un bloc de caractères.

**Contrôle de trafic -** L'ensemble du dispositif mis en œuvre dans un routeur ou un ordinateur qui fournit la qualité de service demandée par les flots de données.

**Contrôle d'erreurs -** Mécanisme qui assure une détection des erreurs de transmission et, éventuellement, une correction de celles-ci par retransmission.

**Contrôleur de communications -** Equipement qui prend en charge la gestion des communications dans un réseau.

**Contrôleur de grappe -** Equipement qui prend en charge la gestion de plusieurs terminaux et le transfert des données entre ces terminaux et un contrôleur de communications local ou distant.

**Contrôleur de station de base -** (BSC - Base Station Controller) - Equipement commandant une ou plusieurs BTS et responsable de toutes les fonctions liées à la transmission radio.

**Convention d'interconnexion -** Contrat de droit privé négocié et signé entre deux opérateurs pour déterminer au cas par cas les conditions de l'interconnexion entre eux. Lorsqu'une convention est signée avec un opérateur puissant, elle s'inspire le plus souvent de l'offre inscrite dans le catalogue d'interconnexion de cet opérateur. Dans le cas contraire, elle détermine les conditions de l'interconnexion sans référence à un catalogue.

**Convergence -** Ce terme est utilisé pour désigner plusieurs phénomènes distincts :

- Tendance qu'ont les industries de l'informatique, des télécommunications et des médias à se rapprocher, grâce aux technologies numériques qui permettent de convertir la voix, le texte, les données et les images fixes et mobiles en messages codés qui peuvent être mélangés, transmis, stockés, gérés sans erreur, en grande quantité et pratiquement sans délais à travers des réseaux fixes ou mobiles.
- La convergence entre les secteurs de l'audiovisuel et des télécommunications ; il s'agit de la possibilité, offerte par les progrès de la technologie, d'utiliser des supports différents (réseaux câblés, hertziens terrestres ou satellitaires, terminaux informatiques ou télévision ) pour transporter et traiter toutes sortes d'informations et de services, qu'il s'agisse du son, de l'image ou des données informatiques ; issue d'un bouleversement technologique (la numérisation de l'information), cette convergence a également des implications économiques et réglementaires.
- La convergence fixe / mobile, qui consiste en un rapprochement des technologies utilisées et des services proposés par le téléphone fixe et le téléphone mobile. Les perspectives ouvertes par cette convergence pourraient conduire les opérateurs à proposer à l'ensemble des utilisateurs les mêmes services quels que soient la technologie et les réseaux utilisés.

**Conversion Analogique-numérique -** Analog to Digital Conversion - Opération qui permet de convertir un signal analogique en un signal numérique représentant les mêmes informations. Un signal analogique téléphonique (bande de fréquences 300-3400 Hz) peut être converti en un signal numérique de débit 64 kbit/s.

La transformation d'un signal analogique en signal numérique est appelée numérisation. La numérisation comporte deux activités parallèles : l'échantillonnage (sampling) et la quantification. L'échantillonnage consiste à prélever périodiquement des échantillons d'un signal analogique. La quantification consiste à affecter une valeur numérique à chaque échantillon prélevé.

La qualité du signal numérique dépendra de deux facteurs:

- la fréquence d'échantillonnage (appelé taux d'échantillonnage): plus celle-ci est grande (c'est-à-dire que les échantillons sont relevés à de petits intervalles de temps) plus le signal numérique sera fidèle à l'original
- le nombre de bits sur lequel on code les valeurs (la résolution): il s'agit en fait du nombre de valeurs différentes qu'un échantillon peut prendre. Plus celui-ci est grand, meilleure est la qualité

Ainsi, grâce à la numérisation on peut garantir la qualité d'un signal, ou bien la réduire volontairement pour diminuer le coût de stockage, diminuer le cout de la numérisation, diminuer les temps de traitement, tenir compte du nombre de valeurs nécessaires selon l'application et tenir compte des limitations matérielles.

**Cookie (Magic Cookie) -** Certains sites Web enregistrent sur votre disque dur des informations à votre sujet (par exemple, la date de votre dernière connexion). On appelle ces informations cookies.

**COPS -** Common Open Policy Service Protocol - Protocole léger bâti sur le modèle maître/esclave. Il communique avec un annuaire LDPA pour récupérer en temps réel les données. Assure le dialogue entre un serveur qui centralise les règles et les équipements du réseau. Permet de gérer plus facilement les paramètres de Qos.

**CORBA -** Common Object Request Broker Architecture - Standard de l'OMG définissant l'architecture logicielle nécessaire pour permettre à des parties de programmes (objets) de communiquer avec d'autres, issues d'environnements différents. Modèle d'architecture Client/Serveur distribué orienté objet. Ce modèle a été spécifié pour la première fois par l'OMG (Object Managment Group) en 1989, la première version de CORBA étant apparue en 1992.

CORBA repose sur un modèle orienté objet Client/Serveur d'abstraction et de coopération entre applications réparties. Chaque application peut exporter certaines fonctionnalités, appelées aussi Services, sous la forme d'objet CORBA : c'est la composante d'abstraction (structuration) du modèle. Les interactions entre les applications sont alors matérialisées par des invocations à distance des méthodes des objets : c'est la partie coopération du système.

CORBA est une spécification normative basée sur les cinq grands domaines constituant les systèmes objets distribués :

- Un langage de description des objets, appelé IDL (Interface Definition Language) et une infrastructure de distribution d'objet, appelé ORB (Object Request Broker).
- Une description des services communs nécessaires à tous les objets applicatifs. Ces spécifications, appelées CORBA Services, couvrent entre autres des services de nommages, de persistance, d'annuaire, de cycles de vie des objets… Ces services, tous décrits dans l'IDL, sont nécessaires dans les systèmes distribués, car ils permettent d'isoler les clients et les serveurs des détails d'implémentation dus à leur localisation et à leur état d'activation.
- Une description des services nécessaires aux applications et non plus seulement aux objets. Ces spécifications sont appelées CORBAFacilities et permettent d'offrir des services de plus haut niveau comme l'interface utilisateur, l'administration des systèmes et réseaux… Le but des CORBA Facilities est de définir des objets préfabriqués pour les applications récurrentes de l'entreprise, comme la conception de documents, l'administration des systèmes informatiques…
- Un ensemble de descriptions de services spécialisés par domaines d'activité, tels que les télécommunications, la santé, la finance… Sous le nom de Domain Services, ces spécifications visent à offrir une description standard des objets et des services communs à une activité donnée.
- Une spécification normative d'interopérabilité entre ORB. Cette spécification, permettant la communication entre différents ORB, est devenu nécessaire devant le nombre d'implémentations, souvent incompatibles entre elles, de CORBA.

Le Bus CORBA est l'entité qui permet l'acheminement des requêtes de l'application cliente vers l'objet invoqué. Ainsi, par son intermédiaire, les objets vont pouvoir dialoguer entre eux, sans se soucier des problèmes d'hétérogénéité. Le bus CORBA présente les caractéristiques suivantes :

- Une liaison avec "tous "les langages de programmation grâce à l'IDL.
- La transparence des invocations : les requêtes aux objets semblent toujours être locales, le bus CORBA se chargeant de les acheminer en utilisant le canal de communication le plus approprié.
- L'invocation statique et dynamique : ces deux mécanismes complémentaires permettent de soumettre les requêtes aux objets. En statiques, les invocations sont contrôlées à la compilation. En dynamique, les invocations doivent être contrôlées à l'exécution.
- Un système auto-descriptif : les interfaces sont connues du bus et sont aussi accessibles par les programmes par l'intermédiaire du référentiel d'interface.
- L'activation automatique et transparente des objets : les objets sont en mémoire uniquement s'ils sont utilisés par des applications clientes.
- L'interopérabilité entre bus : à partir de la norme CORBA 2.0, un protocole générique de transport des requêtes (GIOP pour General Inter-ORB Protocol) a été défini, permettant l'interconnexion de bus CORBA provenant de fournisseurs distincts. L'une des implémentations de GIOP est IIOP (Internet Inter-ORB Protocol) ; elle fonctionne au-dessus de TCP/IP.

**Cordon -** Câble comportant des connecteurs à ses extrémités.

**COREL -** Câble Ouvert pour Réseaux d'Entreprise Locaux - Standard de câblage utilisé en France et défini par France Télécom.

**Correcteur d'exposition -** Terme utilisé en photographie numérique pour désigner un dispositif permettant de décaler le réglage fourni par le dispositif de mesure automatique dans le sens de la sur exposition ou dans le sens de la sous exposition. Ce dispositif est utilisé dans le cas où le dispositif de mesure automatique n'arrive pas à fournir seul la bone exposition lors de prises de vue particulières (fort constraste, contre jour, etc…).

**COS -** Corporation for Open Systems - Organisme regroupant les principaux constructeurs informatiques américains pour promouvoir les normes de l'ISO (International Standard Organisation).

**COSINE -** Cooperation for Open Systems Interconnection Networking in Europe - Projet européen dans le cadre du programme Eurêka visant une infrastructure de communication avancée à l'échelle de l'Europe pour la recherche scientifique et industrielle.

**Couche physique -** Couche inférieure de l'architecture d'interconnexion de systèmes ouverts. S'occupe des niveaux de tension, du câblage, de la vitesse et des signaux utilisés entre les matériels.

**Couplage -** En optique **-** Opération consistant à récupérer un maximum de l'énergie lumineuse en sortie d'une fibre ou d'un composant d'émission dans une autre fibre ou dans un composant de réception.

**Couplage Téléinformatique -** Association de l'installation téléphonique d'une entreprise à tout ou partie de ses installations informatiques.

**Coupleur acoustique -** Modem permettant d'utiliser le microphone et le haut-parleur d'un téléphone pour transmettre et recevoir des données.

**Coupleur Optique - Splitter -** Equipement passif utilisé dans la technologie PON. Dans le sens descendant (réseau vers abonnés), le coupleur réplique le signal optique en provenance d'une fibre vers un nombre défini de fibres (on parle alors de coupleur 1 vers 8, 1 vers 4 etc.). Dans le sens montant, il combine les signaux optiques en provenance des abonnés.

On peut comparer un coupleur à un prisme qui diffuse les longueurs d'onde vers différentes sorties.

| | 1x4 | 1x8 | 1x16 | 1x32 | 1x64 |
|---|---|---|---|---|---|
| Longueur d'onde | 1260 nm à 1360 nm et 1460 nm à 1650 nm | | | | |
| Perte d'insertion | 7,5 dB | 10,8 dB | 14,5 dB | 18,2 dB | 20,4 dB seulement Nexans |

**Courrier Electronique -** Service permettant aux utilisateurs habilités la saisie, la consultation différée et la transmission, sur des ordinateurs connectés en réseau, de documents informatisés ou messages électroniques.

**Courtier de messages -** Message broker - Dans une couche middleware, intermédiaire orchestrant le flux des messages entre applications. Il fournit des services tels que la transformation de données.

**Coûts moyens incrémentaux de long terme -** Aux termes de la loi, les tarifs d'interconnexion doivent être établis en fonction des coûts correspondants de l'opérateur qui fournit la prestation d'interconnexion. Pour déterminer ces coûts, deux méthodes génériques peuvent être employées : la première consiste à prendre en compte les coûts historiques du réseau de l'opérateur ; la seconde consiste à évaluer le coût de la construction d'un nouveau réseau aux prix actuels et futurs, moins élevés que le coût historique en raison du progrès technique. La méthode des coûts moyens incrémentaux de long terme a pour objet de concilier ces deux démarches en se fondant sur la comparaison de deux évaluations :

Une approche partant de la comptabilité de l'opérateur,

Un modèle technico-économique de construction et d'exploitation de réseau.

Cette conciliation doit permettre une meilleure compréhension des mécanismes de formation des coûts de réseau et de leur lien avec les différents services d'interconnexion.

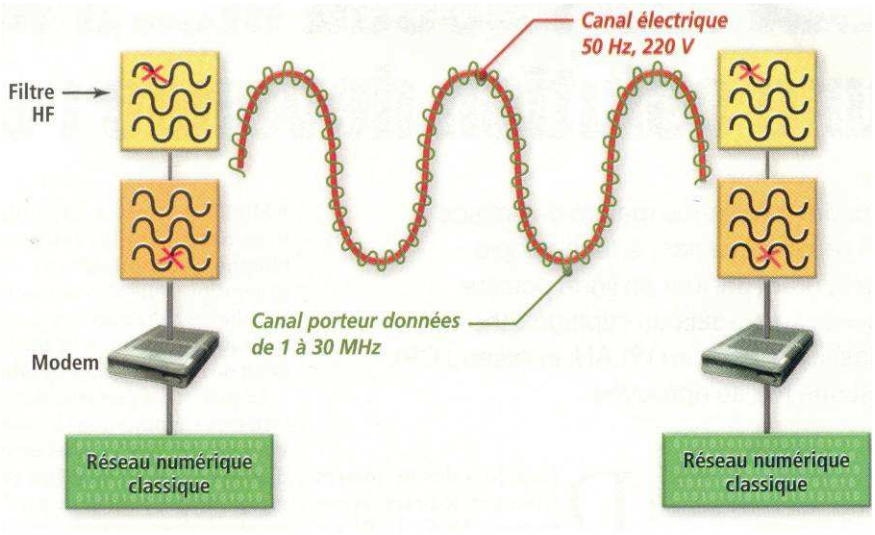
**Couverture -** Zone géographique de couverture du réseau mobile. Correspond à la zone de service cellulaire proposée par votre opérateur réseau.

**CPE -** Customer Premices Equipement - Terme désignant les équipements terminaux de réseaux situés dans les limites de propriété d'un utilisateur.

**CPF -** Commission de Planification des Fréquences.

**CPL -** Courant Porteur en ligne - Pour véhiculer son signal, le courant porteur en ligne utilise, dans le fil électrique, une bande de fréquence entre 4 MHz et 20 MHz. A l'intérieur de cette bande, la technologie PowerPacket, reconnue par le standard HomePlug, transporte les paquets de données, en utilisant la même modulation que le sans-fil 802.11g, dite OFDM.

Mais dans un fil électrique, l'impédance (ou force de résistance) varie souvent, notamment en fonction des appareils qui tirent sur le courant. Or, un changement d'impédance peut bloquer la fréquence utilisée par le signal ; c'est donc le rôle de PowerPacket de changer de fréquence, à la volée, pour en trouver une libre. La technologie est suffisamment au point pour tenir le coup, même si de nombreux appareils sont branchés. Enfin, un mécanisme de correction d'erreur, dit CSMA, vérifie qu'aucun paquet de données ne s'est perdu en route.




Principes de base du CPL

Le support du réseau électrique n'a pas été étudié pour transporter des signaux Haute fréquence, il faut donc prendre en compte les contraintes de ce support pour assurer une bonne transmission des signaux HF sans pour autant perturber les appareils environnants, ni les fréquences de la bande 1-30 Mhz par rayonnement, certaines fréquences de cette bande étant réservées à l'armée ou bien aux radio amateurs. Tout ceci doit enfin être étudié pour donner un débit suffisant à l'utilisateur en bout de ligne.

Le problème consiste à limiter la puissance de fonctionnement des courants porteurs tout en assurant un débit suffisant, et limiter les effets du bruit et de la distorsion sur la ligne. Il faut allier un traitement du signal performant et effectuer un couplage optimal du réseau CPL au réseau électrique.

Toute solution CPL doit inclure une couche physique robuste mais également un protocole d'accès à la couche réseau efficace. Ce protocole contrôle le partage du média de transmission entre de nombreux clients, pendant que la couche physique spécifie la modulation, le codage et le format des paquets.

Deux types de modulation ressortent particulièrement : OFDM (Orthogonal Frequency Division Multiplexing) et Spread Spectrum (ou modulation à étalement de spectre) qui divisent les canaux en sous-porteuses à bas débit, et permettent une occupation optimale de la bande de fréquences.

Le fonctionnement du CPL est simple : un signal électrique compris entre 1,6 et 30 MHz, de faible énergie, est superposé au courant alternatif standard à 50 Hz. Un simple récepteur spécifique suffit alors à décoder le signal CPL.

La méthode d'accès à la couche réseau est, elle aussi, identique à celle des réseaux wi-fi, à savoir la CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Cet algorithme tiré d'Ethernet a été modifié pour s'adapter au canal partagé utilisé notamment par le CPL. Il permet d'écouter le support de transmission avant l'envoi de données afin d'éviter que plusieurs transmissions aient lieu en même temps, et ainsi réduire les collisions.

**CPT -** Code des Postes et Télécommunications.

**Cracker -** Un hacker digne de ce nom ne va pirater le réseau ou les sites que pour souligner leur vulnérabilité, Un cracker a l'ambition avouée de détruire les systèmes qu'il visite.

**CRC -** Cyclic Redundancy Check - Clé de contrôle permettant de déterminer si la transmission a subi une erreur (contrôle de parité).

Le CRC donne une indication sur la validité d'une trame. La valeur du champ CRC de chaque trame est le résultat d'un calcul effectué sur l'ensemble des bits de la trame. Le récepteur effectue le calcul puis compare le résultat obtenu avec la valeur du champ CRC reçu. S'il y a divergence, la trame est considérée comme corrompue et une réémission est requise par le récepteur.

Le taux de CRC est directement lié à la qualité du câblage mis en œuvre dans la liaison. A titre de repère, un réseau qui accuse un taux d'erreur de trame (taux de CRC) de 1% est un réseau qui n'atteint que 20% de son débit maximal. La dégradation des performances en fonction du taux d'erreur CRC n'est pas proportionnelle mais exponentielle.

Le contrôle de redondance cyclique consiste à protéger des blocs de données. A chaque trame est associé un bloc de données, appelé code de contrôle. Le principe du CRC consiste à traiter les séquences binaires comme des polynômes binaires, c'est-à-dire des polynômes dont les coefficients correspondent à la séquence binaire.

Dans ce mécanisme de détection d'erreur, un polynôme prédéfini (appelé polynôme générateur et noté G(X)) est connu de l'émetteur et du récepteur. La détection d'erreur consiste pour l'émetteur à effectuer un algorithme sur les bits de la trame afin de générer un CRC, et de transmettre ces deux éléments au récepteur. Il suffit alors au récepteur d'effectuer le même calcul afin de vérifier que le CRC est valide.

Les polynômes générateurs les plus couramment employés sont CRC-12, CRC-16, CRC CCITT V41 (LDLC), CRC-32 (Ethernet) et CRC ARPA.

**Crédit temps -** Utilisé en téléphonie fixe et mobile, ce terme désigne une base de temps indivisible, débutant à la connexion, et pour laquelle l'appelant est débité quelle que soit la durée effective de la communication.

**Criblage -** Le criblage est une opération qui consiste à établir un ensemble d'équations ou polynômes destinés à générer une matrice dans le but de casser un cryptosystème. Cette opération est réalisée sur des centaines machines indépendantes puissantes et disposant de beaucoup de mémoires.

**CRM -** Customer Relationship Management - En Français : GRC - Le CRM est une approche intégrée pour identifier, acquérir et fidéliser les clients. En permettant de gérer et coordonner les interactions clients sur plusieurs canaux, services, lignes d'activités et lieux géographiques, le CRM aide les entreprises à améliorer leur performance et à optimiser la valeur de chaque interaction client.

Aujourd'hui, les entreprises doivent gérer les interactions clients sur plusieurs canaux de communication, tels que le Web, les centres d'appels, les ventes terrain, ainsi que les réseaux de concessionnaires ou de partenaires. Nombre d'entreprises disposent de multiples lignes d'activités avec de nombreux clients se retrouvant dans différents secteurs. Le défi est d'aider les clients à faire des affaires avec une entreprise comme ils le souhaitent (à tout moment, quels que soient le canal de communication, la langue ou la devise) et de faire en sorte qu'ils aient une expérience positive et identique à chaque interaction.

Les avantages du CRM sont clairement identifiés : en rationalisant les processus et en apportant aux équipes de ventes, de marketing et d'assistance plus d'informations détaillées sur les clients, le CRM permet aux entreprises d'établir des relations plus rentables avec leurs clients et de réduire leurs coûts de fonctionnement.

**Cryptage -** Codage des données empêchant leur lecture par une autre personne que le destinataire prévu. De plus, les données sont uniquement lisibles après avoir été correctement décryptées.

Transformation des données dans un code secret à des fins de protection. Equivalent de chiffrement.

**Cryptologie ou Cryptographie -** Science de l'écriture et de la lecture de messages codés. La protection des données informatiques est un problème crucial pour les entreprises et les institutions, face à la mise en réseau. De même, pour les particuliers et les entreprises, dans le cadre du commerce électronique et de la sécurité des paiements.

La cryptologie est un ensemble de techniques qui permettent de protéger des informations grâce à un code secret. Le but d'un système cryptographique (aussi appelé cryptosystème) est de chiffrer un message intelligible ou clair en un texte chiffré incompréhensible. Le texte chiffré est aussi appelé cryptogramme. Le principe est de permettre au destinataire légitime de déchiffrer le cryptogramme et obtenir le texte clair. Cependant, il est impératif d'interdire l'interception et la modification du message par une tierce personne. Cet espion (aussi appelé cryptanalyste ou décrypteur) ne doit être en mesure de décrypter (ou cryptanalyser) le texte chiffré. Il ne faut pas confondre déchiffrement (opération effectuée par le destinataire légitime) et le décryptement (opération que l'espion tente d'effectuer).

Les systèmes cryptographiques utilisent un algorithme cryptographique associé à une fonction mathématique utilisée pour le chiffrement et le déchiffrement. Pour chiffrer un message en clair, on applique un algorithme de chiffrement au texte de ce message. Pour déchiffrer un texte chiffré, on applique un algorithme de déchiffrement au texte chiffré.

Il existe plusieurs types de cryptosystèmes :

• Les cryptosystèmes à usage restreint - Un algorithme cryptographique est dit à usage restreint si sa sécurité est basée sur le fait que les opérations de chiffrement et de déchiffrement sont tenues secrètes. De

tels algorithmes ne comportent pas intérêt de nos jours, car ils ne sont plus adéquats pour les besoins actuels de sécurité. Un groupe d'utilisateurs important ou variable ne peut utiliser de tels algorithmes car il y aura toujours un utilisateur qui tôt ou tard révélera le secret. Quand cela se produit, la sécurité de tout le système s'écroule. Plus important encore, la plupart des algorithmes restreints sont faciles à casser par les cryptanalystes expérimentés.

• Les cryptosystèmes à usage général - Un système cryptographique est dit à usage général si sa sécurité ne repose pas sur le secret des opérations de chiffrement et de déchiffrement mais plutôt sur une information appelée la clé. Les individus qui utilisent de tels systèmes doivent pouvoir facilement générer leurs propres clés sans avoir recours au concepteur du système de telle sorte que celui-ci ne jouisse d'aucun avantage particulier s'il décide de passer au camp des cryptanalystes. Il existe deux grandes classes de cryptosystèmes à usage général :

Le système à clé secrète ou symétrique. Un système de chiffrement à clé secrète, ou symétrique, repose sur le partage entre deux interlocuteurs en communication, d'une même clé secrète utilisée à la fois pour le chiffrement d'un message et pour son déchiffrement. La clé doit être échangée préalablement à la communication par un canal sûr autre que le canal à protéger.

le système à clé publique ou asymétrique. Le concept de cryptographie à clé publique fut inventé par Whitfield Diffie et Martin Hellman, et indépendamment par Ralph Merkle en 1976. L'idée neuve dans le domaine était que les clés pouvaient être des paires - une clé de chiffrement et une clé de déchiffrement - et qu'il était impossible de générer une clé à partir de l'autre. Cette idée est apparue après une observation pertinente selon laquelle celui qui chiffre un message n'a pas besoin de pouvoir le déchiffrer.

La solution prônée en France est la cryptographie à clé publique : cette solution permet de réaliser les fonctions d'authentification, de signature/vérification et de distribution/échange de clé, en évitant tout partage préalable, entre les interlocuteurs d'une transaction sécurisée, d'un secret commun. Cette solution implique deux conditions : d'une part l'implantation, dans les terminaux, les serveurs, etc., de moyens de cryptologie mettant en œuvre des protocoles de sécurité reposant sur des algorithmes de sécurité, et d'autre part la mise en place d'une infrastructure de certification, soit d'un service offert par un prestataire indépendant - appelé généralement tiers certificateur ou autorité de certification - de délivrance d'un certificat attestant la correspondance entre la clé publique de cet utilisateur et les données d'identification utilisées dans l'application.

Les fonctions de la cryptographie doivent répondre aux besoins suivants :

- Intégrité des données - Le contrôle de l'intégrité d'une donnée consiste à s'assurer que cette donnée n'a pas été altérée accidentellement ou frauduleusement. Le plus souvent le contrôle de l'intégrité ne s'appuie pas à proprement parler sur un outil de cryptologie car son calcul ne requiert pas de convention secrète.
- Authentification - Elle peut être de deux natures : authentification des partenaires ou authentification de l'origine des informations. En pratique, ce service permet principalement de s'assurer que le correspondant connecté est bien le correspondant annoncé ou de s'assurer du signataire de l'acte.
- Non-répudiation - La non-répudiation permet d'obtenir la preuve de l'émission d'une information ou la preuve de sa réception. L'émetteur ou le récepteur ne peut ainsi en nier l'envoi ou la réception.
- Confidentialité - La confidentialité permet de rendre la lecture de l'information inintelligible à des tiers non autorisés lors de sa conservation ou surtout de son de transfert. Le chiffrement des informations constitue la technique la plus utilisée pour répondre à ce service.
- Signature numérique - La signature numérique est une technique qui permet la mise en oeuvre à la fois de l'intégrité des données, de l'authentification et de la non-répudiation.

**CSA - France -** Conseil Supérieur de l'Audiovisuel - Instance de régulation de l'audiovisuel français, autorité indépendante créée en 1989.

**CSMA -** Carrier Sense Multiple Access - Méthode d'Accès à un réseau local dans laquelle une station qui veut émettre vérifie qu'une autre station n'est pas en train de le faire au même moment (collision). Soit cette vérification s'effectue avant l'émission, et l'on cherche à éviter la collision : c'est la méthode CSMA-CA (Collision Avoidance). Soit la vérification a lieu pendant l'émission, et l'on cherche seulement à détecter une collision ; s'il y a collision, la station réémet son message : c'est la méthode CSMA/CD (Collision Detection), utilisée notamment dans les réseaux locaux Ethernet.

**CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) -** Méthode d'accès à un réseau local de type WLAN. Le protocole CSMA/CA tente d'éviter les collisions en imposant un accusé de réception systématique des paquets (ACK), ce qui signifie que pour chaque paquet de données arrivé intact, un paquet ACK est émis par la station de réception.

Ce protocole CSMA/CA fonctionne de la manière suivante : une station qui souhaite émettre explore les ondes et, si aucune activité n'est détectée, attend un temps aléatoire avant de transmettre si le support est toujours libre. Si le paquet est intact à la réception, la station réceptrice émet une trame ACK qui, une fois reçue par l'émetteur, met un terme au processus. Si la trame ACK n'est pas détectée par la station émettrice (parce que le paquet original ou le paquet ACK n'a pas été reçu intact), une collision est supposée et le paquet de données est retransmis après attente d'un autre temps aléatoire.

CSMA/CA permet donc de partager l'accès aux ondes. Ce mécanisme d'accusé de réception explicite gère aussi très efficacement les interférences et autres problèmes radio. Cependant, il ajoute à 802.11 une charge inconnue sous 802.3, aussi un réseau local 802.11 aura-t-il toujours des performances inférieures à un LAN Ethernet équivalent.

**CSMA-CD (Carrier Sense Media Access with Collision Detection) -** Méthode d'accès à un réseau local dans laquelle une station qui veut émettre vérifie qu'une autre station n'est pas en train de le faire au même moment (collision). Chaque utilisateur vérifie que le canal est libre avant de commencer une émission, puis écoute pendant l'émission pour détecter une éventuelle collision.

Cette méthode d'accès "aléatoire" stoppe les transmissions de données dès la détection d'une collision, pour les reprendre selon une temporisation aléatoire.

Cette méthode s'utilise couramment dans les réseaux locaux d'entreprise du type Ethernet, et dans les réseaux radioélectriques de type Aloha.

Principe de base :

Carrier Sense (écoute de porteuse) - Une station ne peut transmettre une trame que si le canal est libre depuis plus d'un intervalle de temps donné

Multiple Access (accès multiples) - Toutes les stations ont accès au même canal

Collision Detection (détection de collisions) - Une station qui transmet une trame écoute en même temps le canal pour détecter une collision éventuelle

Jamming (brouillage) - Une station qui a détectée une collision continue à émettre des bits de brouillage pour que les autres stations détectent aussi la collision

Waiting (attente) - Une station qui a participé à une collision attend un temps aléatoire avant d'essayer de retransmettre sa trame

**CSPR -** Commission de Synthèse et Prospectives des Radiocommunications.

**CST -** Conseil Supérieur de la Télématique. Organisme consultatif chargé de contrôler la régularité de fonctionnement des services télématiques.

**CSTA -** La première est la norme connue sous le nom de CSTA (Computer Supported Telecommunication Applications), préparée par l'ECMA (European Computer Manufacturers Association). L'ECMA regroupait au départ un ensemble de constructeurs européens ; ceci est désormais désuet car il regroupe maintenant des constructeurs d'appareils de télécommunications mondiaux. Les spécifications CSTA ont été publiées pour la première fois en 1995. L'objectif de CSTA est de normaliser l'échange de données de gestion téléphonique entre un PABX et un serveur informatique.

La norme CSTA définit les règles d'échange des messages entre le PABX et le serveur informatique. CSTA est vue comme une application relevant du niveau de la couche 7 dans le modèle OSI. Ainsi, elle s'appuie sur un support de communication des couches basses OSI, comme TCP/IP.

Le protocole CSTA permet notamment les fonctions suivantes :

- Fonctions de commutation - Ces fonctions permettent de d'effectuer les opérations de base comme la connexion et la déconnexion. Elles peuvent également permettre le transfert d'appel, la mise en conférence et également servir des messages. La deuxième phase CSTA a ajouté des services supplémentaires pour la conférence. La phase III a jouté des fonctions de groupage d'appels.
- Fonctions de surveillance : ces fonctions sont similaires à un outil de reporting et permettent de renvoyer des informations concernant un périphérique. La phase III CSTA rajoute une gestion plus fine concernant les informations des périphériques.
- Fonctions informatiques de routage : elles permettent à un PABX d'interroger le serveur informatique pour lui faire effectuer un traitement plus fin des informations afin de router les appels.
- Fonctions bidirectionnelles : ces fonctions permettent de connaître l'état réciproque du serveur téléphonique et du serveur informatique.
- Fonctions d'extension : la norme CSTA prévoit ainsi son extension par des ajouts de services par les constructeurs de PABX. Ainsi, la phase II CSTA a rajouté la gestion des entrées/sorties mais en incluant alors une non compatibilité ascendante avec CSTA I. La phase III a par exemple ajouté des fonctions d'enregistrement d'appels.

**CSU -** Channel Service Unit - Aux Etats-Unis, équipement de terminaison d'une ligne numérique (ligne T1 par exemple) résidant chez l'utilisateur.

**CT -** Commutateur de Transit.

**CT2 -** Norme de radiotéléphone numérique sans fil. Le CT2 définit de petits terminaux de poche permettant d'appeler en communiquant par l'intermédiaires de bornes situées à quelques centaines de mètres, mais pas de recevoir. Le service Bi-Bop de France Télécom s'appuie sur la mise en œuvre de cette norme.

**CTA -** Conseil de la Télématique Anonyme. Organe exécutif du CST

**CTD -** Câble de transmission de données.

**CTI -** Couplage Téléphonie Informatique - Couplage entre un équipement téléphonique et un équipement informatique permettant l'échange de commandes et de messages entre ces équipements. C'est l'intégration de la téléphonie et de l'informatique ayant pour but de faciliter le développement d'applications communes (définition du TENOR). Mais le terme "CTI "a été généralisé. En effet, il est possible de regrouper sous ce terme l'ensemble des techniques logicielles et matérielles qui permettent l'intégration de la téléphonie et de l'informatique.

Le serveur de deuxième génération CTI, aussi appelé Serveur de Commandes et de Gestion des Appels (SCG), s'interface avec le PABX de l'entreprise. Cette interface s'effectue à l'aide d'un lien informatique, et non plus avec deux liens voix et signalisation comme dans le CTI de première phase. De plus, il commande maintenant intégralement le PABX, ce dernier n'ayant plus qu'une fonction de connexion des lignes téléphoniques.

Pour que le serveur puisse commander et remplacer le PABX, il est nécessaire qu'il possède des fonctions de téléphonie, comme le routage des appels, l'association synchronisée des données avec les appels, le contrôle d'appel, l'émission d'appel ou encore la gestion des appels. D'autre part, le SCG ne reprend pas la fonction de traitement vocal, qui est réservé au serveur CTI de première génération (comme le SVI).

A quoi cela sert il dans la vrai vie ?

- Le Couplage CTI permet l'association synchronisée des données avec les appels (screen pop up). En identifiant l'appelant sur la base de son numéro, il est possible d'y associer son dossier informatique pour améliorer la prise d'appel entrants.
- Router les appels - Sur la définition de certains critères, il est possile de "router" un appel au niveau du serveur CTI. On utilise dans ce cas un logiciel de traitement des appels avec table de routage. La décision de routage peut être basée sur l'identification du numéro de l'appelant, de la date, du jour, de l'heure de l'appel entrant, de la disponibilité de l'appelé ou du téléopérateur,etc etc.
- Contrôle des appels - Déclencher un autre appel en cours de communication (double appel), passer ce nouvel appel en conférence (mise en conférence), transfert d'appel, mise en garde d'une communication. Le contrôle des appels peut bien sûr être complété d'un suivi des données informatiques liées aux appels.
- L'émission des appels - Rappel automatique, partage d'annuaire, marketing publicitaire, etc etc
- Gestion des appels - Supervision des communications émises et recues par un poste, traçabilité des appels (avec journalisation des communications), supervision de la productivité individuelle et collective dans les centres d'appels (quantité de communications présentées, décrochées, durée des communications, périodicité, origine, etc etc.

Les différents composants d'une architecture CTI :

L'architecture classique d'un CTI est basée sur deux équipements essentiels : le PABX et le serveur informatique. Le PABX est connecté aux postes téléphoniques et le serveur aux postes informatiques clients.

Le serveur localise l'application de commande et de gestion des appels téléphoniques et le PABX localise la ressource de commutation ou de connexion entre les lignes téléphoniques extérieures et les lignes téléphoniques intérieures.

Le PABX et le serveur communiquent, sur le plan logique, par une pile de protocoles de communication reposant généralement sur les protocoles Ethernet et TCP/IP. Au niveau applicatif de la pile, on trouve un protocole de communication portant sur l'échange de messages spécifiques des commandes téléphoniques : la norme CSTA ou les protocoles propriétaires des fabricants de PABX.

Le serveur de pilotage dispose d'une interface spécifique de programmation qui définit des classes de fonctions et établit la communication entre la couche de communication CSTA et l'application informatique qui définira le script de traitement des appels. Cette interface, l'API CTI de seconde phase, est construite sur la base d'une architecture client/serveur.

Quatre principaux logiciels d'interface sont disponibles : TAPI de Microsoft, TSAPI de Novell, CT-Connect de Dialogic et JTAPI de Sun Microsystems. Une application peut donc être développée à partir de ces API CTI. Néanmoins, on trouve souvent, au-dessus de ces API, des logiciels intermédiaires, ou middleware, qui permettent de simplifier les tâches de programmation terminales et les délais de développement des applications téléphoniques.

Enfin le serveur dialogue sur le réseau local avec des postes clients qui disposent notamment des logiciels

clients TAPI, TSAPI, qui peuvent ainsi interagir avec l'architecture téléphonique. L'usager dispose de son poste informatique et d'un téléphone, tous deux reliés indirectement par le biais de l'architecture CTI de deuxième phase. Pour compléter cette architecture, il est possible d'ajouter un serveur de base de données.

**CTR -** Common Technical Regulation - Norme technique harmonisée au niveau européen qui aura force de loi dans tous les pays membres de la CEE pour les terminaux connectables aux réseaux publics. Prendra progressivement la place des Net dans un cadre réglementaire en cours de mise en place.

Règles techniques communes pour l'accès des équipements terminaux aux réseaux, élaborées en application de la directive communautaire 98/13/CE par le comité TRAC et l'ETSI à la demande du comité ACTE, présidé par la Commission européenne. Ces règles s'appliquent à l'ensemble des Etats membres.

**CTS-WAN -** Conformance Testing Services - Wide Area Network - Projet européen visant à fixer des procédures communes et harmonisées pour les tests de conformité aux normes OSI (Open Systems Interconnection).

**Cut Through -** Mode de fonctionnement d'un commutateur visant à accélérer le processus de commutation par un traitement des trames à la volée dès réception de l'adresse de destination de celle-ci. (voir commutateur et VLAN).

**CVC -** Circuit Virtuel Commuté - Circuit virtuel établi et libéré à l'initiative d'un des correspondants. Ce terme est utilisé dans les réseaux en mode paquet de type ATM, X25 ou Frame relay.

**CVP -** Circuit Virtuel Permanent - Circuit virtuel établi d'une manière permanente entre deux extrémités. Ce terme est utilisé dans les réseaux en mode paquet de type ATM, X25 ou Frame relay.

**CVS -** Commission de Valorisation du Spectre.

**CWDM -** Coarse Wavelength Division Multiplexing - La technologie CWDM apparaît particulièrement bien positionnée pour séduire les entreprises et les opérateurs pour des distances inférieures à 50 km. Le coût d'une solution CWDM est et effet inférieur d'environ 25 % à celui d'une infrastructure DWDM grâce à un espacement plus important entre les longueurs d'oncle (lambdas). Les équipements CWDM ne requièrent pas de coûteux composants optiques, notamment les dispositifs de refroidissement des lasers DFB ou VCESL utilisés dans les équipements DWDM.

| CWDM Versus DWDM | | | | |
|---|---|---|---|---|
| | Nombre de lambdas protégés | Espacement | Refroidissement nécessaire | Application |
| DWDM | 32 | 100-200 GHz | Oui | Bande passante nécessaire supérieure à 16 lambdas ou distance > à 80 kms |
| CWDM | 16 | 2 500 GHz | Non | Bande passante nécessaire inférieure à 16 lambdas et/ou distance < 80 kms sans amplification |

# D

**D2D -** Disk To Disk - Technique de sauvegarde utilisant des disques durs comme support d'archivage. Réservé à l'origine à de gros volumes de données, cette technique de sauvegarde se développe parallèlement à la baisse de prix des disques SATA ou EIDE. Outre des débits importants, cette technique de sauvegarde offre surtout un accès direct aux données sauvegardées (par opposition aux accès séquentiels des lecteurs de bande).

**D2D2T -** Disk to Disk To Tape - Technique de sauvegarde s'appuyant sur D2D dans un premier temps (principalement pour des raisons de débits et d'accès concurrents) pour transférer à postériori les données vers un système de sauvegarde sur bande.

**DAP -** Directory Access Protocol - Protocole permettant d'accéder à un annuaire X500.

**DAS -** Débit d'Absorption Spécifique (équivalent du SAR anglo-saxon). Ce terme est utilisé principalement dans la téléphonie mobile. Il caractérise une incidence vis-à-vis d'un signal radio.

**DAS -** Direct Attached Storage - Stockage attaché - Ensemble des périphériques de stockage directement rattachés à un serveur tels que baies de disques simples (JBOD), baies Raid, baies de stockage, lecteurs de bandes, graveurs, robots de bandes, disques SSD.

**Datagramme -** Bloc ou paquet contenant des données et l'adresse du destinataire. Un datagramme est transmis "à la volée" sur un canal de transmission, sans référence aucune à un ordre de séquencement par rapport aux autres paquets. Cette communication se fait en mode non connecté.

Technique de commutation par paquets, dans laquelle chaque paquet comporte toutes les informations nécessaires à son acheminement. A la différence du mode circuit virtuel, le mode datagramme ne garantit pas l'ordre d'arrivée des paquets.

**Datagramme IP -** Ensemble de données de 30 à 500 octets. Ils sont indépendants les uns des autres et représentent l'unité de base des données sur un réseau TCP/IP. Un Datagramme s'appuie sur la couche UDP du protocole TCP/IP, il est utilisé en mode non connecté.

**Datalene -** Variante du polypropylène expansé. La constante diélectrique est excellente, bonne tenue à l'écrasement et supporte des températures plus élevées que le polypropylène expansé. C'est l'isolant idéal pour les câbles multipaires destinés aux applications informatiques.

**DCE -** Data Communications Equipement - Equipement qui permet d'établir, maintenir et mettre fin à une connexion de transmission de données, par exemple un modem. voir ETCD.

**DCE -** Distributed Computing Environment - Système logiciel permettant le développement et la gestion d'applications distribuées (mode client serveur). DCE est constitués de plusieurs composants obligatoires comme les Remote Procedure Call (RPC) qui permettent de faire appel à des fonctions d'une application à travers le réseau, les Threads, qui permettent d'améliorer les performances d'une application en offrant la possibilité d'exécuter plusieurs procédures en parallèles, le Directory Service (CDS et GDS), qui permet de retrouver les différentes ressources et les différentes applications gérées par DCE, le Time Service (DTS), qui permet la synchronisation des serveurs et qui permet de garder une heure valide sur le réseau, le Security Service, qui permet l'authentification des utilisateurs et des applications clientes et qui permet de gérer l'accès aux ressources du réseau.

DCE est aussi composé d'éléments optionnels comme le Distributed File Service (DFS), qui permet le partage des fichiers au sein d'une ou plusieurs cellules DCE.

DCE se positionne entre le système d'exploitation de la machine et les applications qui utilisent les services de DCE. En tant que middleware, DCE se place entre l'OS et les applications. L'architecture DCE est composée en deux grands ensembles : l'ensemble des composants permettant le développement d'applications distribuées, et l'ensemble des composants permettant la gestion de l'environnement distribué. Les composants gérant l'environnement DCE sont basés sur les éléments de développement de DCE.

On peut aussi présenter DCE par rapport au modèle OSI. DCE joue un rôle dans la couche présentation, car en tant que middleware, DCE a la possibilité d'adapter les données pour l'architecture destinatrice. Cela permet de distribuer des applications sur des architectures différentes. DCE joue aussi un rôle dans la couche session, étant donné qu'une application distribuée devra mettre en place une session avec son serveur pour pouvoir générer des appels de procédures (RPC) à travers le réseau.

**DCF -** Distibuted Coordination Function - Mécanisme régulant le partage des ondes radio entre plusieurs stations connectées sur un réseau radio IEEE 802.11.

**DCOM -** Distributed Component Object Model - Technique de Microsoft utilisée pour le développement objet. Définit les spécifications pour la distribution et l'accès de composants d'une application aux ordinateurs en réseau.

**DCS -** Digital Cellular System ou Digital Communication System - Système cellulaire numérique : norme de radiotéléphonie utilisée notamment par Bouygues Telecom; de type GSM. Réseau de radiocommunication cellulaire utilisant la norme GSM à une fréquence de 1800MHz.

**DCS1800 -** Norme de radiotéléphonie numérique fonctionnant sur la même technologie que la norme GSM mais à une fréquence plus élevée (1800 MHz).

**DE -** Discard Eligibility - Voir Relais de Trame et Frame Relais - Le bit DE sert à indiquer que les trames qui ont été envoyées en excès du CIR, peuvent être retirées si nécessaire.

**Débit -** Quantité d'informations transportées en une unité de temps par un moyen de communication. Un débit s'exprime en Bit par seconde. (ne pas confondre avec Baud). Mesure la quantité d'informations que peut transmettre un canal dans un temps donné, généralement exprimé en bits par seconde (bps) pour les transmissions numériques.

Unité de mesure de transfert des données en descendant (download) ou en montant (upload) exprimé en bit/s ou en octet/s (ou Byte/s). Pour une question de commodité, le Mbit/s (=1 000 000 bit/s) ou le Mo/s (1 000 000 octet/s) sont plus généralment utilisés. A noter aussi qu'il existe un rapport de 8 entre le débit exprimé en Mbit/s et celui en MB/s ou Mo/s.

**Débit binaire -** Bit Rate - Nombre de bits transmis pendant un intervalle de temps rapporté à la durée de cet intervalle. Un débit binaire s'exprime en bit/s ou en multiple de cette unité : kbit/s, Mbit/s, Gbit/s.

**DEC-Connect -** Système de câblage proposé par Digital Equipment à la fois pour les réseaux locaux (Ethernet) et étendus (Decnet).

**Déchiffrement -** Action inverse du chiffrement, qui consiste à retrouver l'information initiale contenue dans le message chiffré à l'aide de la clé secrète appropriée.

**Décibel -** Valeur de mesure logarithmique de l'amplitude d'un signal égale à 20*log(x). Le décibel est le dixième du Bel (en hommage à Alexander Graham Bell).

Quand il est nécessaire de quantifier les gains et les atténuations d'un signal (sonore ou électrique), il est plus commode de parler d'un amplificateur de 20 dB de gain que d'un amplificateur qui amplifie 100 fois.

De même, on utilise cette valeur pour donner l'affaiblissement d'un câble, en mètre ou kilomètre. Le signal original se trouve affaiblit avec la distance, l'affaiblissement peut s'exprimer alors en dB.

Exemples :

- En puissance :

Le dB est 10 fois le logarithme base 10 du rapport de puissance P1/ P2.

L'amplification de puissance exprimée en dB d'un amplificateur qui sort 20 W pour 1 W à l'entrée se calcule comme ceci : A=10 Log x (20/1) = 13dB.

- En tension ou courant :

Le dB est 20 fois le logarithme base 10 du rapport des tensions V1/V2 ou des courants I1/I2

L'amplification de tension exprimée en dB d'un transistor monté en amplificateur sur lequel on mesure 3 V de tension de sortie pour 10 mV de tension d'entrée se calcule de la façon suivante : A = 20 Log x (3/0.01) = 49,5 dB.

Le dBm - Il est commode d'exprimer une puissance par rapport à une référence qui sera en l'occurrence le milliwatt sur une impédance de 50 ohms. Cette notion d'impédance de charge est importante et doit être spécifiée car 0 dBm sur 50 ohm ne correspond pas à 0 dBm sur 75 ohm. 0 dBm sur 50 ohm = 224 mV sur charge de 50 ohm = 1mW

Le dBi exprime en dB le gain d'une antenne par rapport à un aérien isotrope qui émet la même quantité d'énergie dans toutes les directions. Cet aérien n'existe pas.

le dBd exprime en dB le gain d'une antenne par rapport à un aérien dipôle demi-onde. Cet aérien est une réalité physique.

Les catalogues des fabricants et distributeurs ne spécifient pas souvent si nous avons affaire à des dBi ou dBd, et pourtant Une antenne de 10 dBd de gain à un gain de 12.15 dBi.

**DECnet -** Ensemble de produits matériels et logiciels mis au point par Digital Equipment Corporation qui mettent en œuvre l'architecture DNA (Digital Network Infrastructure).

**Décodage -** Transformation inverse du codage restituant l'information sous sa forme initiale.

**Décodeur -** Appareil de décodage.

**Décryptage -** N'est pas l'inverse du "cryptage", mais l'opération, normalement frauduleuse, consistant à retrouver un message chiffré lorsqu'on ne possède pas le code de chiffrement.

Action qui consiste à "casser" le chiffrement d'une information sans avoir accès à la clé secrète qui permet son déchiffrement normal.

**DECT -** Digital European Cordless Telecommunications - Norme européenne pour une radiocommunication vocale numérisée point à point entre un téléphone ou un terminal portable léger et une station de base. La norme DECT prévoit le transfert inter cellule = roaming).

Tableau de synthèse de présentation de la norme DECT :

| | |
|---|---|
| Bande de fréquence | De 1880 MHz à 1900 MHz |
| Espacement des porteuses | 1728 KHz |
| Nombre de porteuses | 10 |
| Multiplexage des porteuses | TDMA / 24 IT par trame |
| Longueur des trames | 10 ms |
| Puissance de transmission | 10 mW (crête 250 mW) |
| Hand Over | Supporté |
| Allocation dynamique des canaux | Supporté |
| Débit | Brut = 1152 kbit / seconde |
| | Champ A (signalisation et contrôle) = 6,4 kbit/sec/IT |
| | Champ B (trafic) = 32 kbit / seconde / IT |

La norme DECT (Digital Enhanced Cordless Telecommunications) est une norme d'accès radio fonctionnant dans une bande de fréquence comprise entre 1880 Mhz et 1900 Mhz.

Le DECT utilise les mêmes technologies que les normes de radiocommunications cellulaires :

- Informations codées numériquement
- Découpage de la zone de couverture en cellules
- Technologie TDMA (Time Division Multiple Access),
- Gestion du handover, etc.

Le DECT utilise un système de saut permanent de fréquence et de recherche de la meilleure transmission ce qui rend le système peu sensible aux interférences.

La norme DECT permet une allocation dynamique des fréquences aux utilisateurs et rend possible le partage des fréquences entre plusieurs opérateurs. Il n'est donc pas nécessaire d'attribuer des fréquences de façon exclusive aux opérateurs. Les fréquences sont attribuées aux opérateurs du réseau ouvert au public à titre non exclusif au fur et à mesure des demandes et ceci sans limitation du nombre d'opérateurs.

Le DECT est également adapté à la transmission de données de façon synchrone ou asynchrone. Plusieurs canaux élémentaires d'une capacité de 32 kbps peuvent être couplés de manière à obtenir des transmissions pouvant aller jusqu'à 1Mbps.

Utilisation du spectre radio :

- Découpage en cellules

Afin de gérer les ressources fréquentielles mis à sa disposition, la norme DECT reprend le principe du découpage en cellules utilisé dans la norme GSM. Un espace géographique est ainsi découpé en zones, elles même découpées en cellules. Une base gère les communications d'une cellule. Plus la taille des cellules est petite, plus la fréquence de réutilisation des fréquences est importante (2 fois le diamètre de la cellule). La norme DECT peut être utilisée en fonctionnement monocellulaire pour la téléphonie sans fil grand public ou en fonctionnement multicellulaire pour la téléphonie sans fil au sein d'une entreprise par exemple.

- Découpage de la bande de fréquence

La norme DECT utilise également le principe de découpage de la bande de fréquence disponible. La bande de fréquence (comprise en 1880Mhz et 1900Mhz) est divisée en 10 porteuses espacées en elles de 1.728Mhz.

- Partage en temps

Chaque porteuse définit précédemment est divisée en 24 slots temporels : 12 slots sont réserve aux informations émises et 12 aux informations reçues. Chaque porteuse assure donc 12 communications full duplex simultanément. Grâce à ces techniques, chaque station est capable de gérer 120 communications full duplex en simultanées.

- Sélection et allocation dynamique d'un canal

Un équipement DECT est capable de sélectionner et d'allouer dynamiquement une fréquence pour une communication. Chaque équipement est donc obligé d'explorer régulièrement (au moins toutes les 30 secondes) son environnement radio. Explorer signifie mesurer la puissance de chaque signal présent sur un canal. Ce scan permet de tenir à jour une liste des canaux libres et occupés (Liste RSSI : Received Signal Strenght Indication). Cette liste permet alors l'allocation du canal optimal lors de l'établissement d'une nouvelle communication. Le portable analyse le canal qui a la RSSI la plus haute afin de voir si la transmission provient d'une base sur laquelle ce dernier a les droits. Quant au canal qui a la RSSI la plus basse, il sera utilisé pour établir une connexion avec la base si nécessaire.

- Le handover

Grâce à l'efficacité de la sélection et de l'allocation dynamique des canaux, un portable à la possibilité, pour échapper aux interférences radio, d'établir une seconde connexion radio à partir de la même base ou à partir d'une autre base. Les deux connexions radio sont alors temporairement maintenues. Après analyse, la base détermine le canal qui possède la meilleure qualité de transmission et libère alors l'autre canal.

Si un portable se déplace d'une base vers une autre, la puissance du signal reçu va alors diminuer graduellement quant au signal émis par la station vers laquelle le mobile se déplace, il va lui augmenter graduellement. Au moment où le signal émis par la nouvelle base dépasse le signal émis par l'ancienne base, le handover s'effectue.

Contrairement à la norme GSM, c'est ici uniquement la station mobile qui gère le handover sans que l'utilisateur ne s'en aperçoive.

**DEEE -** Déchets d'Equipements Electriques et Electroniques - Une directive européenne, appliquée en droit Français le 13 août 2005 rend les entreprises responsables de la collecte des déchets d'équipements électriques et électroniques, du traitement systématique des composants dangereux, de la valorisation des déchets collectés avec une priorité à la réutilisation et au recyclage.

**Défauts -** Les lignes d'abonnés doivent à présent transporter des flux de données à hauts débits. La qualité des lignes doit être optimale pour préserver des débits importants sur de longues distances. Les principaux défauts sont répertoriés ci-dessous :

| Terme utilisé en anglais | Terme utilisé en français |
|---|---|
| Electrical impairments | Défauts électriques |
| Physical impairments | Défauts physiques |
| Central office | Central |
| Rain or ground water | Pluie ou nappe phréatique |
| Splices, mixed gauges | Epissures, fils de différents diamètres |
| RF, background noise, impuls noise NEXT / FEXT | RF, bruit de fond, bruit impulsif NEXT / FEXT |
| Unterminated bridged taps | Branchements en dérivation sans terminaison |
| Length, untwisted drop wires Subscribers | Longueur, fils d'abonnés non torsadés Abonnés |

**Définition -** La définition désigne le nombre de pixels dont est composée une image numérique. Souvent exprimée sous la forme "longueur x largeur". Plus la valeur est élevée, plus l'image comporte de détails. Ce terme est utilisé en photographie numérique ou pour définir la capacité d'affichage d'un écran.

**Dégroupage -** Séparation en plusieurs lots de prestations de télécommunication traditionnellement regroupées en un lot unique, de façon à pouvoir les confier éventuellement à des opérateurs de télécommunication différents.

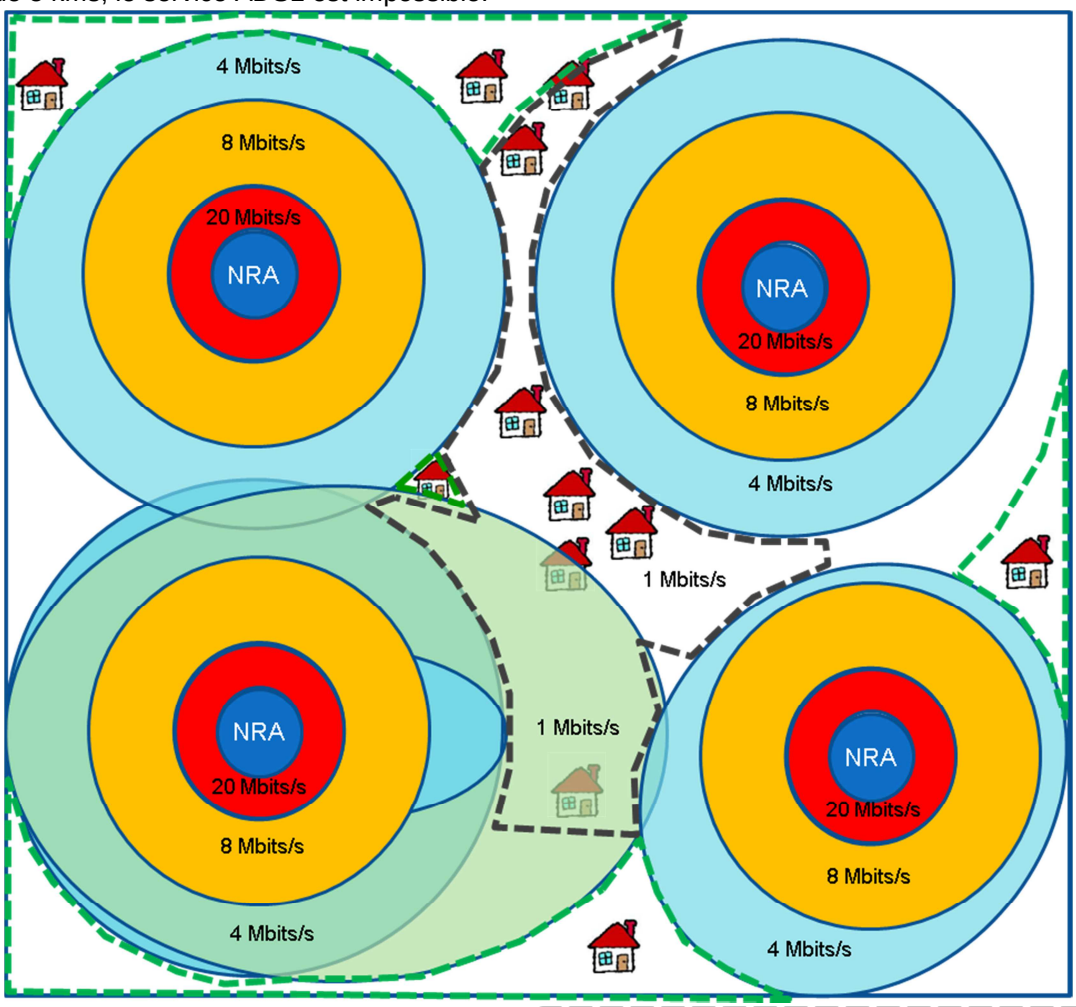
Ainsi, les nouveaux opérateurs raccordent leur réseau directement aux liaisons cuivre de l'abonné sans passer par le répartiteur. Le dégroupage permet aux nouveaux opérateurs de se libérer de leur dépendance par rapport aux opérateurs historiques, propriétaires des infrastructures du réseau public.

Le dégroupage, dans l'approche générale de la déréglementation, consiste pour un opérateur de réseau à désolidariser les différentes capacités de son réseau (commutation locale, commutation de transport, distribution, ...) pour que celles-ci puissent être utilisées séparément par les différents concurrents.

**Dégroupage ADSL -** le dégroupage d'une zone en ADSL est fortement conditionné par la longueur de la ligne téléphonique (voir ADSL 2+)

A proximité immédiate du NRA, les débits sont importants. L'éloignement induit une baisse notable des débits et services disponibles.

Au-delà de 5 kms, le service ADSL est impossible.




**Dégroupage de la boucle locale -** Le dégroupage de la boucle locale ou l'accès dégroupé au réseau local consiste à permettre aux nouveaux opérateurs d'utiliser le réseau local de l'opérateur historique, constitué de paires de fils de cuivre, pour desservir directement leurs abonnés. Dans cette hypothèse, l'usage du réseau local de l'opérateur historique est naturellement rémunéré par l'opérateur nouvel entrant. Ainsi, il n'y aurait plus obligation, pour les clients des nouveaux entrants, de prendre un abonnement auprès de France Télécom pour accéder aux services de leur opérateur. Cette définition générique recouvre plusieurs options possibles. Les travaux préparatoires à la consultation publique conduite par l'Autorité en 1999 en ont identifié cinq :

Trois d'entre elles sont apparues dans le cadre de la réflexion concernant la possibilité d'accéder à la boucle locale de l'opérateur historique sous une forme dégroupée. Cet accès peut correspondre :

A un dégroupage physique de la boucle locale où l'opérateur nouvel entrant accède directement à la paire de cuivre. Il s'agit du dégroupage de la paire de cuivre (option 1),

A un accès des capacités de transmission. Il s'agit de l'accès au débit et de l'accès à un circuit virtuel permanent (options 2 et 3 respectivement).

Les deux dernières s'apparentent à une activité de revente. Il s'agit de la revente de trafic local et la revente d'abonnements (options 4 et 5 respectivement).

**Délimiteurs -** Informations insérées dans un message pour indiquer le début et la fin des blocs ou des paquets. On emploie aussi le mot fanion (flag).

**DELTA Electronik Centralen (EC) -** Bureau de Certification Danois.

**Démodulateur -** Circuit ou composant utilisé dans un terminal satellite pour extraire les signaux de base qui ont été modulés par le diffuseur de programmes. Par extension, le terme de démodulateur est parfois utilisé pour définir l'ensemble du terminal de réception.

**Démodulation -** Procédé permettant de reconstituer le message original à partir d'une onde porteuse modulée par ce message.

**Démultiplexage -** Action de restituer complètement ou partiellement les signaux originaux, ou des groupes de ces signaux, à partir d'un signal composite obtenu par multiplexage.

**DEN -** Directory Enabled Networking - Concept de service d'annuaire global appliqué au réseau. Les équipements réseaux peuvent, avec cette norme, être eux aussi référencés dans les bases de données des services d'annuaires compatibles X500 afin d'être inclus dans la stratégie d'administration globale.

Architecture basée sur un annuaire centralisé. Permet d'optimiser l'utilisation de la bande passante des réseaux.

**Dépairage -** Erreur de câblage entre deux fils issus d'une paire différente, créant une fausse paire.

**Dérèglementation -** Opération juridique ou législative modifiant le sens des règlements dans le sens d'une plus grande liberté des acteurs (opérateurs, industriels, sociétés de services...) et de leur mise en concurrence.

**Dérégulation -** Terme d'origine américaine désignant le mouvement de dérèglementation qui a débuté aux Etats-Unis en 1984 avec le démantèlement d'AT&T et s'étend progressivement à de nombreux autres pays.

**DES -** Data Encryption Standard - Système (Algorithme) de chiffrement d'origine IBM à clé secrète et normalisé par NSA (National Security Agency) et par le National Institute of Standards and Technology (voir NIST et Triple DES).

Le principe de D.E.S est très simple car il s'appuie sur deux opérations élémentaires de cryptage : La permutation et la substitution. L'algorithme n'utilisant que des opérations arithmétiques et logiques standards sur des nombres d'au maximum 64 bits, il était facile de le réaliser avec la technologie de la fin des années 70. Le caractère répétitif de l'algorithme le rend idéal pour l'utilisation de puces spécialisées. Avec un langage évolué tel que le C, D.E.S est facilement réalisable en 200 lignes de codes environ.

D.E.S est un système de chiffrement par blocs ; il chiffre les données par blocs de 64 bits à l'aide d'une clé de longueur 56. Un bloc de 64 bits du texte clair entre par un côté de l'algorithme et un bloc de 64 bits du texte chiffré sort de l'autre côté. Le chiffrement et le déchiffrement utilisent le même algorithme avec des différences uniquement dans le plan de génération des clés.

**DES CBC -** Data Encryption Standard Cipher-Block - Algorithme standard d'IPV6 permettant de chiffrer des données afin d'en assurer la confidentialité.

**Désassemblage** (de paquets) - Opération inverse de l'assemblage consistant à remettre sous leur forme d'origine les informations reçues à travers un réseau à commutation de paquets. Elle est le plus souvent assurée par un PAD (Paquet Assembler Disassembler).

**Désérialisation -** Opération inverse de la sérialisation consistant à transformer un message série (où les bits d'un mot sont présentés successivement sur un canal unique) en un message parallèle (où les bits d'un mot sont présentés simultanément sur plusieurs canaux).

**DEST -** Direction de l'Enseignement Supérieur des Télécommunications de France Télécom. Chapeaute les grandes écoles de formation en télécommunications (Télécom Paris, ENST Bretagne, INT...).

**Détection d'erreurs -** Technique permettant de vérifier si une erreur s'est produite pendant une transmission (exemple = parité).

**DGA -** Délégation Générale pour l'Armement - LA DGA conduit les études et les programmes d'Armement à partir des besoins définis avec les Etats-Majors. Elle a la responsabilité de l'ensemble du processus d'acquisition correspondant.

**DGNF -** Direction de la Gestion Nationale des Fréquences

**DGT -** Ancienne Direction Générale des Télécommunications. Elle a pris le nom commercial de France Télécom en 1986.

**DHCP -** Dynamic Host Configuration Protocol - L'affectation et la mise à jour d'adresses IP peuvent être facilitées par le protocole DHCP qui offre une configuration dynamique des adresses IP et des informations associées. L'administrateur de réseau contrôle le mode d'attribution des adresses IP en spécifiant une durée de bail qui indique combien de temps l'ordinateur peut utiliser une adresse IP attribuée, avant de devoir renouveler le bail auprès du serveur DHCP.

Standard IETF (Internet Engineering Task Force), il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but

principal étant la simplification de l'administration d'un réseau. On voit généralement le protocole DHCP distribuant des adresses IP, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui était utilisé par exemple lorsque l'on installait une machine à travers un réseau.

Les versions actuelles des serveurs DHCP fonctionnent pour IPv4 (adresses IP sur 4 octets) et IPv6.

DHCP fournit les paramètres de configuration pour des machines à connecter sur un réseau. DHCP est constitué de 2 parties : Un protocole pour la livraison de paramètres de configuration de machines spécifiques à partir d'un serveur DHCP et un mécanisme d'allocation d'adresses réseaux à des machines.

DHCP est bâti sur le modèle client -> serveur, où la machine désignée serveur DHCP alloue des adresses réseaux et délivre des paramètres de configuration à des machines configurées dynamiquement. Le terme "serveur" se réfère à une machine fournissant des paramètres d'initialisation au travers du DHCP. Le terme "client" se réfère à une machine qui demande des paramètres d'initialisation au serveur DHCP.

DHCP supporte 3 mécanismes pour l'allocation des adresses IP :

- L'allocation automatique (ou allocation dynamique statique), DHCP assigne une adresse IP permanente à un client.
- L'allocation dynamique, DHCP assigne une adresse IP à un client pour une durée déterminée (ou jusqu'à ce que le client renonce à son adresse, notion de bail).
- L'allocation manuelle, une adresse IP est assignée par l'administrateur réseau, et DHCP est simplement utilisé pour convoyer les adresses désignées jusqu'au client.

Un réseau spécifique utilisera un ou plusieurs de ces mécanismes, cela dépend de la stratégie de l'administrateur réseau.

L'allocation dynamique est la seule des 3 mécanismes qui réutilise automatiquement une adresse qui n'est plus utilisée par un client. De plus, l'allocation dynamique est particulièrement utile pour assigner une adresse à un client qui se connectera au réseau de manière temporaire, ou pour partager une liste limitée d'adresses IP entre un groupe de clients qui ne nécessitent pas une adresse permanente. L'allocation dynamique est aussi un bon choix pour assigner une adresse IP à un nouveau client qui se connectera de manière permanente au réseau où les adresses IP sont suffisamment rares pour qu'il soit important de les récupérer quand les anciens clients sont hors connexion. L'allocation manuelle permet à DHCP d'être utilisé pour éliminer les processus enclins à l'erreur de configuration manuelle de machines avec une adresse IP dans des environnements où (pour diverses raisons) il est préférable de gérer l'attribution des adresses IP en dehors des mécanismes de DHCP.

Fonctionnement du protocole DHCP :

Lorsque l'on connecte une machine à un réseau Ethernet TCP/IP, cette machine, pour fonctionner correctement, doit disposer :

- D'une adresse IP unique dans le réseau et appartenant au même réseau logique que toutes les autres machines du réseau en question,
- D'un masque de sous réseau, le même pour tous les hôtes du réseau,
- D'une adresse de DNS, pour pouvoir résoudre les noms des hôtes.
- De l'adresse de la passerelle qui permet d'accéder sur un réseau complexe à l'un des multiples sous-réseaux.

Il faut dans un premier temps un serveur DHCP qui distribue des adresses IP. Cette machine va servir de base pour toutes les requêtes DHCP. Dans un réseau, on peut donc n'avoir aucune machine avec adresse IP fixe.

Le mécanisme de base de la communication est BOOTP (avec trame UDP). Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP. Pour faire cela, la technique utilisée est le broadcast. Pour trouver et dialoguer avec un serveur DHCP, la machine va simplement émettre un paquet spécial de broadcast (broadcast sur 255.255.255.255 avec d'autres informations comme le type de requête, les ports de connexion...) sur le réseau local.

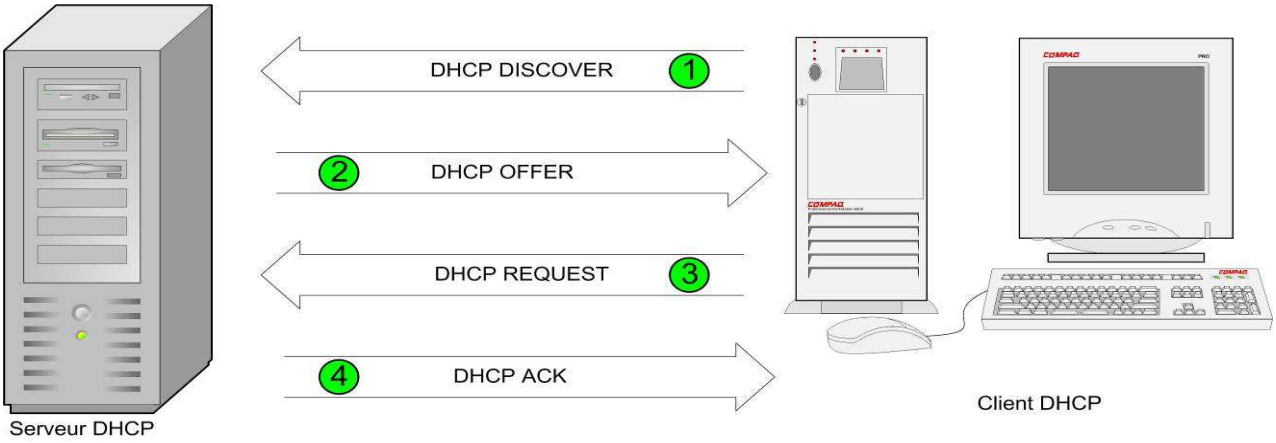
Lorsque le serveur DHCP recevra le paquet de broadcast, il renverra un autre paquet de broadcast (le client n'a pas forcement son adresse IP et que donc il n'est pas joignable directement) contenant toutes les informations requises pour le client.

On pourrait croire qu'un seul paquet peut suffire à la bonne marche du protocole. En fait, il existe plusieurs types de paquets DHCP susceptibles d'être émis soit par le client pour le ou les serveurs, soit par le serveur vers un client :

Le premier paquet émis par le client est un paquet de type DHCPDISCOVER. Le serveur répond par un paquet DHCPOFFER, en particulier pour soumettre une adresse IP au client. Le client établit sa configuration, puis fait un DHCPREQUEST pour valider son adresse IP (requête en broadcast car DHCPOFFER ne contient par son adresse IP). Le serveur répond simplement par un DHCPACK avec l'adresse IP pour confirmation de l'attribution. Normalement, c'est suffisant pour qu'un client obtienne une configuration réseau efficace, mais cela peut être plus ou moins long selon que le client accepte ou non l'adresse IP.

Les adresses utilisées lors de cet échange sont les adresses MAC ainsi que des adresses de "broadcast" IP.

| Message | Utilisation |
|---|---|
| DHCP DISCOVER | Requête de diffusion du client pour localiser les serveurs DHCP disponibles |
| DHCP OFFER | Réponse du serveur au client pour répondre au DHCPDISCOVER avec les paramètres de configuration. |
| DHCP REQUEST | Message client aux serveurs soit (a) qui demande les paramètres à un serveur et décline implicitement les offres de tous les autres, (b) qui confirme la validité des adresses précédemment allouées, par ex : un redémarrage système, ou (c) qui étend le bail sur une adresse réseau en particulier. |
| DHCP ACK | Réponse du serveur au client avec les paramètres de configuration et qui inclut l'adresse réseau déjà attribuée. |
| DHCP NAK | Réponse du serveur au client indiquant que la notion d'un client pour les adresses réseau est incorrecte. (par ex : si un client est déplacé sur un nouveau sous réseau) ou que le bail du client a expiré. |
| DHCP DECLINE | Requête du client vers le serveur indiquant que l'adresse réseau est déjà utilisée. |
| DHCP RELEASE | Requête du client vers le serveur libérant l'adresse réseau et annulant le bail. |
| DHCP INFORM | Requête du client vers le serveur, demandant seulement les paramètres de configuration locaux ; le client possède déjà une adresse IP. |




Lorsque le client DHCP démarre sur le client DHCP, il n'a aucune connaissance du réseau (du moins en principe). Il envoie donc une trame "DHCPDISCOVER", destinée à trouver un serveur DHCP. Cette trame est un broadcast envoyé à l'adresse 255.255.255.255 port source (UDP 67) / port destination (UDP 68). N'ayant pas encore d'adresse IP, il adopte provisoirement l'adresse 0.0.0.0. Comme ce n'est pas avec cette adresse que le DHCP va l'identifier, il fournit aussi sa MAC Address.

Chaque serveur DHCP peut répondre avec un message DHCPOFFER qui inclut une adresse réseau IP valide (et d'autres paramètres de configuration des options DHCP). Cette trame est elle aussi en broadcast car il n'est pas encore possible d'atteindre le client nommément (il n'a pas encore d'adresse IP valide).

Le client reçoit un ou plusieurs messages DHCPOFFER d'un ou plusieurs serveurs. Le client peut choisir d'attendre des réponses multiples. Le client choisit un serveur pour ses paramètres de configuration, basé sur la configuration présente dans le DHCPOFFER. Le client diffuse un message DHCPREQUEST à tous les serveurs (donc toujours en "Broadcast") pour indiquer quelle offre il accepte, il doit inclure l'option 'identifiant serveur' indiquant quel serveur il a sélectionné et qui peut inclure d'autres options spécifiant les valeurs de configuration désirées. L'option "adresse IP demandée" doit être réglée sur la même valeur que l'adresse du message DHCPOFFER provenant du serveur. Le DHCPREQUEST doit utiliser les mêmes valeurs dans l'en-tête du champ "secs" du message DHCP et être envoyé à la même adresse IP de diffusion que le message DHCPDISCOVER originel. Le client clôture à la fin d'un délai d'attente et retransmet le message DHCPDISCOVER si le client ne reçoit pas de messages DHCPOFFER.

Les serveurs reçoivent les diffusions DHCPREQUEST des clients. Les serveurs qui ne sont pas sélectionnés par le message DHCPREQUEST utilisent le message comme notification que le client décline leur offre. Le serveur sélectionné dans le message DHCPREQUEST engage une liaison pour le client dans sa mémoire permanente et répond avec un message DHCPACK qui contient la configuration pour le client demandeur. La combinaison entre "identifiant client" et l'adresse réseau assignée constitue un identifiant unique pour le bail du client et sont utilisés à la fois par le client et le serveur pour identifier un bail auquel il sera fait référence dans tous les messages DHCP.

Détail sur le Bail :

Pour des raisons d'optimisation des ressources réseau, les adresses IP sont délivrées avec une date de début et une date de fin de validité. C'est ce qu'on appel un bail. Un client qui voit son bail arriver à terme peut demander au serveur une prolongation du bail par un DHCPREQUEST. De même, lorsque le serveur verra un bail arrivé à terme, il émettra un paquet DHCPNAK pour demander au client s'il veut prolonger son bail. Si le serveur ne reçoit pas de réponse valide, il rend disponible l'adresse IP.

C'est toute la subtilité du DHCP : on peut optimiser l'attribution des adresses IP en jouant sur la durée des baux. Le problème est là : si aucune adresse n'est libérée au bout d'un certain temps, plus aucune requête DHCP ne pourra être satisfaite, faute d'adresses à distribuer.

Sur un réseau où beaucoup d'ordinateurs se branchent et se débranchent souvent (réseau d'école ou de locaux commerciaux par exemple), il est intéressant de proposer des baux de courte durée. A l'inverse, sur un réseau constitué en majorité de machines fixes, très peu souvent "rebootées", des baux de longues durées suffisent. Le DHCP marche principalement par broadcast, et que cela peut bloquer de la bande passante sur des petits réseaux fortement sollicités.

Dans le bail, il y a non seulement une adresse IP pour le client, avec une durée de validité, mais également d'autres informations de configuration :

- L'adresse d'un ou de plusieurs DNS (Résolution de noms)
- L'adresse de la passerelle par défaut (pour sortir du réseau où le DHCP vous a installé).
- L'adresse du serveur DHCP (nous allons voir pourquoi).

Cette liste est loin d'être complète, il existe en effet une grande quantité d'options qui peuvent êtres transmises.

Lorsque le bail arrive approximativement à la moitié de son temps de vie, le client va essayer de renouveler ce bail, en s'adressant directement au serveur qui le lui a attribué. Il n'y aura alors qu'un DHCPREQUEST et un DHCPACK. Si, au bout des 7/8e de la durée de vie du bail en cours, ce dernier n'a pu être renouvelé, le client essayera d'obtenir un nouveau bail auprès d'un DHCP quelconque qui voudra bien lui répondre. Il pourra alors se faire que le client change d'adresse IP en cours de session.

Il est recommandé de ne pas créer de baux inutilement courts, ceci entraînant une augmentation significative du taux de broadcast sur le réseau. Le compromis est à trouver entre la durée moyenne de connexion des utilisateurs, la réserve d'adresses IP du serveur, le nombre d'abonnés...

Le serveur DHCP :

Un serveur DHCP dispose d'une plage d'adresses à distribuer à ses clients. Il tient à jour une base de données des adresses déjà utilisées et utilisées il y a peu (C'est ce qui explique que l'on récupère souvent la même adresse, le DHCP ayant horreur des changements. Lorsqu'il attribue une adresse, il le fait par l'intermédiaire d'un bail. Sur un réseau d'entreprise où l'on dispose d'assez d'adresses pour le nombre de postes et que ces derniers sont en service toute la journée, le bail peut être d'une semaine ou plus encore.

Après expiration du bail, ou résiliation par le client, les informations concernant ce bail restent mémorisées dans la base de données du serveur pendant un certain temps. Bien que l'adresse IP soit disponible, elle ne sera pas attribuée en priorité à une autre machine. C'est ce qui explique que l'on retrouve souvent la même adresse d'une session à l'autre.

Le DHCP et les Réseaux Complexes :

Si le réseau physique est formé de plusieurs sous réseaux logiques, avec des routeurs entre chaque sous réseau, le tout peut fonctionner avec un seul serveur DHCP...

Les requêtes DHCP doivent pouvoir atteindre le serveur qui est situé sur un autre réseau logique, elles doivent donc passer les routeurs, ce qui n'est théoriquement pas possible, car un "broadcast" n'est pas retransmis (par défaut) par les routeurs.

Il est alors nécessaire d'installer sur un ou plusieurs routeurs un agent de relais (relay DHCP) qui va intercepter les requêtes en broadcast et les transmettre à un serveur DHCP connu de cet agent.

C'est l'agent de relais situé sur la passerelle qui va faire l'intermédiaire et le client réussira tout de même à obtenir une adresse, donnée par un DHCP situé sur un autre réseau, mais relayé par l'agent de relais. Le serveur DHCP sera même capable d'envoyer des paramètres différents, suivant le sous réseau du client...

Configuration des Paramètres :

Le premier service fourni par DHCP est la fourniture d'un espace de mémorisation des paramètres réseaux pour les clients de ce réseau. Le modèle DHCP de mémoire persistante est basé sur la mémorisation, comme point d'entrée, d'une valeur clef pour chaque client, cette clef est un identifiant unique (par exemple un nombre IP sous réseau et un identifiant unique à l'intérieur du sous réseau) et la valeur contient les paramètres de configuration du client.

Le second service fournit par le DHCP est l'allocation temporaire ou permanente d'adresses réseau (IP) aux clients. Le mécanisme pour l'allocation dynamique d'adresses est simple : un client demande l'utilisation d'une adresse pour une certaine période. Le mécanisme d'allocation (la collection des serveurs DHCP) ne garantit pas une ré allocation de l'adresse pendant le temps demandé et tend à retourner la même adresse réseau à chaque client qui fait la demande. Dans ce document, la période pendant laquelle une adresse réseau est allouée à un client est nommée "bail" [11]. Le client peut étendre ce bail avec des requêtes. Le

client peut émettre un message pour libérer l'adresse quand il ne l'utilise plus. Le client peut demander une assignation permanente en demandant un bail permanent, un serveur peut choisir de donner un bail très long mais pas infini pour permettre la détection qu'un client s'est retiré du réseau.

Les références :

La principale documentation sur le DHCP est constituée par les RFCs :

RFC951 (BOOTP), RFC1541 (DHCP), RFC1542 (interaction entre BOOTP et DHCP), RFC2131, RFC2132.

**Diamètre de champ de mode - Diamètre de champ électromagnétique -** La théorie électromagnétique montre que dans une fibre optique, pour un mode donné, une partie de la puissance optique transportée se trouve dans la gaine.

Pour une fibre largement multimode, presque toute la puissance optique est transportée dans le coeur de la fibre.

Pour une fibre monomode, la puissance optique transportée dans la gaine peut être relativement importante.

Le profil de puissance à l'intérieur d'une fibre monomode peut être approximé à une gaussienne. Dans ce type de fibre, la lumière n'est plus « canalisée» dans le coeur, il est d'usage de définir un nouveau paramètre appelé diamètre de mode, 2WO, WO représentant la demi largeur du mode pris à 1/ e2 dans la distribution gaussienne du champ.

Ce paramètre apparaît, en plus du diamètre de coeur, dans les documentations constructeurs sur les fibres monomodes, car c'est lui qui est porteur d'informations en terme de distribution lumineuse dans la fibre et non le diamètre de coeur qui est là un paramètre géométrique.

**Diaphonie -** Crosstalk ou Next - En audio, désigne la perturbation de l'un des canaux stéréophoniques par le canal voisin. Une électronique de qualité séparera au maximum les deux voies. Cette séparation s'exprimera par un nombre de décibels (dB) aussi grand que possible.

Défaut dû à l'influence d'un canal de transmission sur un autre canal.

La diaphonie est aussi mesurée dans l'informatique. On utilise le terme de para diaphonie sur les systèmes de câblage. Il s'agit de mesurer la perturbation induite sur une paire par une autre paire lors de la transmission d'un signal de référence.

Brouillage d'une voie de transmission téléphonique par des signaux provenant d'une ou de plusieurs autres voies.

Entre voies de transmission de signaux vidéo, on parle de diaphonie (cross-view et cross-colour).

En câblage : induction du signal d'une paire sur une autre. Transfert non désiré d'un signal d'un circuit perturbateur vers un circuit perturbé. La diaphonie dépend de la longueur de détorsadage, de la régularité de la torsade, de la proximité des paires, des matériaux utilisés pour le câble et de la qualité de fabrication (centrage du cuivre par rapport à la gaine, maintien de la torsade, etc.).

Influence réciproque entre des conducteurs métalliques voisins; cet effet n'existe pas en fibre optique.

Voir Paradiaphonie

**Diaphotie -** Phénomène analogue à la diaphonie mais applicable à des guides d'ondes lumineux voisins. Ce phénomène ne concerne pas les fibres mono-coeur mais concerne les fibres multi-coeurs.

**DIB -** Directory Information Base - Base de données d'annuaire dans la norme d'annuaire distribué X500. La DIB représente la base de données (ou d'informations) associée à l'annuaire. Elle fait partie intégrante de l'annuaire. Toutes les informations sont donc stockées dans la DIB. Les données sont organisées sous forme d'arbre, aussi appelé DIT.

Un attribut est la plus petite quantité d'information que la DIB contienne. L'attribut est composé d'un type (chaîne de caractères, entier,…) et d'une ou plusieurs valeurs. Chaque valeur peut être marquée par un fanion de contexte, permettant ainsi de savoir quelle en est l'application.

**Dictionnaires de données -** Procédé consistant à remplacer des séquences de données répétitives par d'autres données beaucoup moins volumineuses pour soulager le trafic échangé dans un flux.

**Diélectrique -** Isolant recouvrant une âme conductrice. Autre appellation des isolants utilisés dans la fabrication des coaxiaux. Ex : polyéthylène.

**Diffie Hellman -** Système à clé publique permettant à deux utilisateurs ou équipements réseau d'échanger des clés publiques via un support non sécurisé.

**DIFFSERV -** Differenciated Services Support - DiffServ décrit une qualité de service assurée de bout en bout, lors d'une visioconférence. Il s'agit d'une extension de la fonctionnalité "IP Precedence" qui vient compléter les fonctionnalités de qualité existantes (RSVP, IP Precedence et Type of Service). DiffServ réduit la surcharge des ressources réseau et gère les contraintes d'étranglement grâce à des méthodes telles que la classification et le marquage de paquets.

Concept de classification et de marquage du trafic basé sur le principe que chaque équipement d'un réseau possède une file d'attente, sur lequel peut être mis en place un certain nombre de filtres. En effet, la prioritisation des paquets ne se fait que dans ces files d'attente. Le principe est simple : Chaque paquet possède un champ qui permet de le classifier. Ce champ est alors analysé par un filtre, et le paquet est dirigé vers la file d'attente qui lui correspond. Il peut y avoir une multitude de files d'attente différentes, et chacune de ces files d'attente se voit affecter un débit de sortie et une priorité particulière. De cette manière, il devient facile pour le routeur de donner la priorité à un certain type de trafic. Cette gestion de la priorité est complètement passive, elle ne s'appuie que sur la valeur du champ de classification contenue dans le paquet. Contrairement à RSVP (qui lui se base sur un maintien d'une réservation de ressources par le destinataire du message), cette méthode de qualité de service est beaucoup plus simple et aussi beaucoup moins gourmande en ressources, mais offre moins de fonctionnalités, notamment pour le multicast et la gestion de la variation du nombre de membres d'un groupe.

Diffserv est un mécanisme qui permet de garantir la qualité de service. Les données sont identifiées par un marquage qui fixe les priorités de passage. Diffserv propose trois options selon le niveau de qualité requis.

**Diffusion -** Broadcast - Mode de transmission dans lequel un émetteur transmet vers plusieurs destinataires généralement inconnus.

**Digital Clarity -** Permet de diffuser des images dynamiques à 4 fois la résolution utilisée en visioconférence (4CIF).

**Digital Signal - DS0, DS1, 2, 3...** - Niveau de signal dans la hiérarchie numérique des opérateurs. DS0 désigne le signal élémentaire (56 Kbps), DS1 = 23 + 1 signaux élémentaires soit 1 544 Kbps, DS3 = 44 Mbps... L'appellation DS est en fait surtout utilisée aux USA, la hiérarchie européenne étant différente, on préfère employer l'appellation CEPT 0 (64 Kbps), CEPT 1 (2 048 Kbps), CEPT 2 (8 448 Kbps), CEPT 3 (34 Mbps), etc.

**Diffusion de Rayleigh -** Phénomène provenant d'hétérogénéité du matériau du cœur d'une fibre et donc de son indice de réfraction. Ce phénomène entraîne:

- Une partie prépondérante des pertes linéiques des fibres modernes.
- Un effet dit de rétrodiffusion pour la partie d'énergie réfléchie vers la source d'émission.

Ce phénomène est utilisé pour la technique de mesure par réflectométrie.

**DIGITIP -** Direction Générale de l'Industrie, des Technologies de l'information et des Postes - Direction rattachée au secrétariat d'Etat à l'Industrie ayant pour mission de favoriser le développement et la compétitivité des entreprises industrielles et du secteur des postes et des télécommunications en France et à l'international.

**Din -** Deutsches Institut für Normung - Institut allemand de normalisation, membre de l'ISO, équivalent juridique de l'Afnor française.

**Directivité -** Audio - On relève la dégradation de la courbe de réponse sur le plan horizontal à 30 et 45° de l'axe du "tweeter ". Avec des enceintes à faible déperdition latérale, la zone d'écoute stéréo et "Home Cinéma "sera plus vaste et plus confortable.

**Dispersion -** Ecart entre les temps de parcours des modes dans une même fibre, entraînant une limitation de bande passante.

**Dispersion par mode de polarisation -** Concerne les fibres monomodes - La dispersion par mode de polarisation est due à la différence de temps de propagation entre deux modes orthogonaux sur une liaison longue. La mesure est spécifiée en picoseconde par racine de kilomètre ( ps / km 0.5 ).

**Dispersion Modale** (ou intermodale) - Modal Dispersion - La dispersion modale est due aux parcours différents effectués par les différents modes d'une fibre multimode.

**Dispersion Chromatique -** Chromatic Dispersion - due à la dépendance entre longueur d'onde et indice de réfraction. Elle se traduit par une différence de vitesse de propagation. L'effet est surtout prépondérant dans les fibres monomodes, où son influence est aussi fonction de la largeur spectrale de la source lumineuse utilisée. S'exprime en ps/nm/km.

**Dispersion chromatique Décalée -** Dispersion Shifted - Une Fibre à dispersion décalée est une fibre construite telle que la zone où la dispersion chromatique est minimale, normalement située vers 1300 nm est décalée vers 1550 nm. Ceci pour bénéficier tout à la fois de l'atténuation minimum et de la bande passante maximum.

**Disponibilité -** Une disponibilité de 99,99% sur un service 24/24 & 7/7 autorise une indisponibilité (interruption de service) de 53 minutes par an.

**Dispositif d'éclatement -** En FTTH - Dispositif permettant un nouvel agencement des fibres optiques contenues dans un ou plusieurs câbles en fibre optique vers un ou plusieurs autres câbles en fibre optique, de modularité différente ou de destination différente (par exemple : câble en fibre optique dédié à différents opérateurs ; câble unique dans une colonne montante).

**Dispositif de brassage** - En FTTH - Equipement passif permettant la mise en correspondance par connecteurs entre les fibres situées en aval (vers l'utilisateur final) et les fibres situées en amont (vers les réseaux d'un ou plusieurs opérateurs).

**Distorsion -** C'est la déformation du signal original par ajout d'harmoniques ou intermodulation entre deux fréquences sur une ligne de transmission. Moins il y en a, en %, mieux c'est.

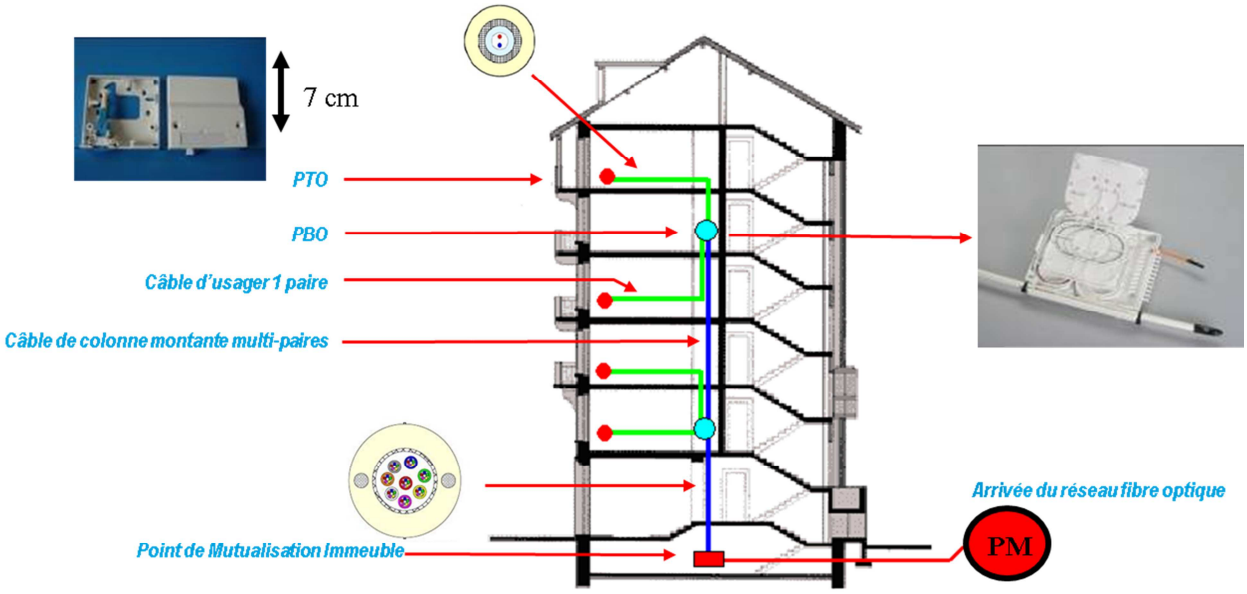
Etant donné que les retards ou les pertes par effet joule sont inévitables sur une ligne de transmission réelle, il est impossible d'obtenir un réseau idéal. Les lignes réelles se distinguent par les distorsions d'amplitude si la grandeur du facteur de transmission dépend de la fréquence, et par les distorsions de phase (retards) si l'angle du facteur de transmission dépend de la fréquence.

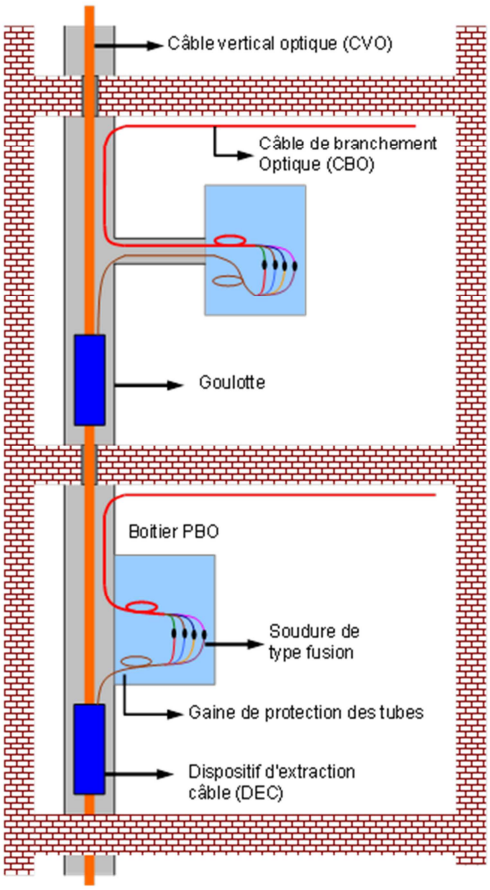
Dans les réseaux linéaires, les distorsions sort linéaires car les spectres du signal d'entrée et de sortie contiennent exactement les même portions de fréquences.

**Distribué -** Désigne un mode de traitement ou une architecture dans lequel une même fonction peut être assurée par plusieurs nœuds et non pas par un unique organe central. Est souvent synonyme de "décentralisé".

**Distribution -** Mode de transmission dans lequel un émetteur transmet vers plusieurs destinataires obligatoirement identifiés.

**Distribution Horizontale -** En FTTH, désigne la partie du réseau qui est destinée à la distribution. En zone dense, le réseau de distribution crée dans les immeubles de plus de 12 logments peut être installé en mono fibre ou en multi fibre.






Les raccordements des PTO sur le PBO

**Distribution Optique d'Abonnés -** L'installation de fibres optiques jusqu'au poste d'abonné (voir FTTH) offre des services de télédistribution et de vidéo à large bande.

**DIT -** Directory Information Tree - Arbre représentant le contenu de la DIB. On peut donc représenter l'information de la DIB sous forme d'arbre où les noeuds représentent des entrées ou des alias.

**DivX -** Format de compression vidéo, dérivé du MPEG-4 par un duo franco/allemand (Gej et Max Morice) qui ont monté le Projet Mayo (Project Mayo) pour continuer son évolution. 'DivX ;-)', est à la vidéo ce qu'MP3 est à l'audio (d'ailleurs le MP3 est utilisé pour le canal son).

**DLCI -** Data Link Channel Identifier - Le DLCI ou identificateur de voie logique permet l'acheminement des trames au niveau de chaque commutateur Frame Relay. L'adressage au sein du réseau s'effectue grâce au contenu du champ DLCI.

Ce champ compte 6bits + 4 bits (soit 10 bits). Il peut y avoir jusqu'à 2^10 = 1 024 valeurs de DLCI.

Tableau d'attribution des valeurs de champ DLCI :

| DLCI (sur 2 octets) | FONCTIONS |
|---|---|
| 0 | Canal de Gestion de l'Interface Locale (LMI) |
| 1-15 | Usage Réservé |
| 16-991 | Disponible pour les PVC ou SVC |
| 992-1007 | Réservé pour la gestion du réseau FR |
| 1008-1022 | Usage Réservé |
| 1023 | Réservé aux messages des couches supérieures (CLLM) |

Le routage des trames dans un réseau Frame Relay s'effectue grâce aux DLCI. Le champ DLCI est modifié au passage de chaque noeud. Le routage s'effectue par un chaînage de numéros DLCI.

L'adressage en Frame Relay s'effectue en donnant un numéro de circuit virtuel entre l'utilisateur et le réseau et n'a qu'une valeur locale. Ces identificateurs locaux sont nommés par le sigle DLCI, ils peuvent désigner des circuits virtuels permanents (PVC) comme des circuits virtuels commutés (SVC).

**DLS -** Data Link Switching - En Mars 1993 sort à l'initiative d'IBM la RFC1434 qui décrit l'implémentation 6111 originale d'IBM du protocole. Protocole de type « switch-to-switch » (SSP) ayant pour but de transporter le trafic entre les réseaux System Network Architecture (SNA) ou Network Basic Input/Output System (NetBIOS) via Transport Control Protocol/Internet Protocol (TCP/IP).

En Octobre 1994, les constructeurs réunis sur l'initiative d'IBM dans le forum « Advanced Peer-to-Peer Networking Implementors Workshop » (AIW), destiné à assurer une interopérabilité de leurs routeurs avec les protocoles System Network Architecture/Advanced Peer-to-Peer Network (SNA/APPN), travaillent sur une nouvelle spécification de DLS : DLSw version 1.

Cette nouvelle version est décrite dans la RFC1795 d'Avril 1995, rendant ainsi obsolète la RFC1434. En effet, DLS ne garantissait pas le contrôle de flux session par session, ni une Management Interface Base (MIB) de gestion de réseau, le support du « Spanning Tree » et des spécifications d'interopérabilité. Cette génération visait à combler ces lacunes.

Cette RFC décrit aussi le SSP utilisé par le standard DLSw entre les routeurs (nommés commutateurs de liaison de données) pour établir une connexion entre homologues, la localisation des ressources, la transmission des données, le contrôle de flux et comment s'effectue la correction d'erreurs.

La RFC 2166 décrit la version 2 de DLSw et ajoute, à la RFC 1795, l'IP multicast, l'User Datagram Protocol (UDP) unicast, les fonctions avancées d'homologues à la demande, et l'activation de connexions d'homologues. Ce standard ne fournit cependant pas toutes les fonctions clés, notamment le besoin de connectivité TCP continue entre deux routeurs dont les utilisateurs ont besoin pour construire les réseaux importants actuels. C'est pour cette raison que CISCO introduit, le 15 Novembre 1994, la troisième génération de liaisons de données : DLSW+, conforme et inter-opérable avec le standard DLSw et la norme « Remote Source Route Bridging » (RSRB).

DLSw+ introduit le concept de « groupes homologues » qui optimise le processus d'exploration, simplifie la configuration des réseaux, et rend possible l'interopérabilité entre tous les réseaux : « any-to-any », mais aussi la multiplication des routeurs en clusters qui permet de réduire les trafics d'exploration pour la définition des chemins.

Les fonctionnalités suivantes ont été ajoutées au standard DLSw :

• L'option de choix du transport, incluant TCP, FST et l'encapsulation directe.

• Des capacités étendues à travers : des groupes d'homologues, des homologues à la demande, des pare-feu d'exploration et la recherche dynamique des chemins. Conversion de media entre Local Area Network (LAN), locaux ou distants, et Synchronous Data Link Control (SDLC) ou Ethernet.

**DME -** Distance Measurement Equipment.

**DMT -** Discrete Multi-Tone - Méthode qui consiste à séparer le signal d'une ligne DSL en 256 bandes de fréquences. Une transformée de Fourrier permet de moduler et démoduler le signal. L'intérêt de cette technologie est de pouvoir faire varier le nombre de bits dans chaque canal par modulation d'amplitude (AM) et donc de permettre à un modem DSL de s'adapter en termes de débit.

**DMZ -** Zone Démilitarisée - Sas entre le réseau interne (LAN) et le réseau externe (WAN), généralement délimité par un coupe-feu. Une DMZ peut héberger un serveur web, un serveur de messagerie, une passerelle relais, etc.

**DNA -** Digital Network Architecture - Architecture de réseaux développée par Digital Equipment Corporation (DEC). DEC phase V est très proche du modèle OSI.

**DNS -** Domain Name Server - Serveur affectant à une machine un nom de domaine validé par le centre d'informations du segment Internet Local (NIC) "Raison_sociale.fr" devient ainsi un nom réservé.

Système de base de données réparties assurant la correspondance d'un nom et d'une adresse Internet (adresse IP). C'est un serveur qui traduit une adresse de la forme nom.domaine.organisation en adresse IP compréhensible par les équipements de réseau.

Le Système de Noms de Domaine est un élément clé d'Internet, fournissant un mécanisme pour résoudre les noms d'hôte en adresses IP.

Le système DNS peut être vu comme l'élément à la fois vital pour Internet (plus de cinquante RFCs décrivent son fonctionnement) et à la fois décentralisé; DNS a été développé avec un esprit d'ouverture, ses premières implémentations furent open source (BIND) et est maintenant sous la direction de l'ISC (Internet Software Consortium) pour les serveurs de noms et l'ICANN pour l'attribution des Top Level Domain (TLD) comme .com alors que l'attribution des noms de domaine est déléguée aux registrars.

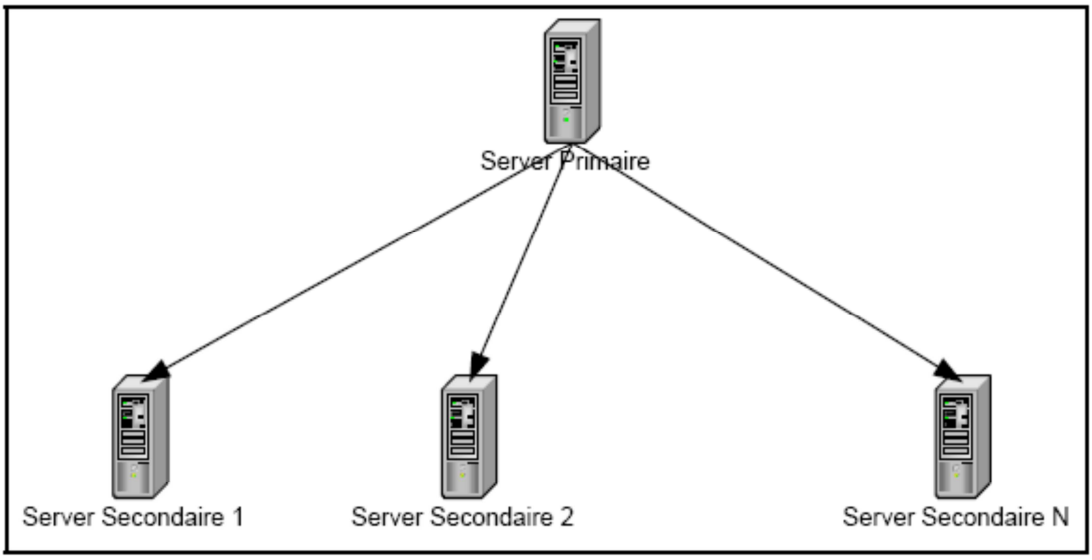
DNS joue un rôle critique dans le bon fonctionnement de l'infrastructure d'Internet en fournissant un mécanisme robuste et distribué de résolution des noms d'hôtes Internet en adresses IP et des adresses IP en noms. On verra que DNS supporte également d'autres fonctionnalités de recherche pour rapatrier des informations des serveurs de noms DNS, noms canoniques, etc. Malheureusement, de nombreux problèmes de sécurité affectent IP et les protocoles qu'il véhicule. La véracité des informations contenues dans le système DNS est critique pour de nombreux systèmes de communication basés sur IP.

Les RFC 882 et 883 jettent les bases de ce qu'on appelle actuellement le Système de Nom de Domaine

(DNS). Ces RFC sont aujourd'hui remplacées par les RFC 1034 et 1035 auxquelles viennent s'ajouter un certain nombre de mises à jour.

Les serveurs de noms :

Les informations sur les domaines sont accessibles via des serveurs de noms, on dit qu'un serveur a l'autorité sur une certaine information si celle-ci est contenue dans son fichier zone. Mais pour faciliter l'administration, sécuriser et répartir la charge du trafic, on a mis au point un système de redondance de l'information grâce à l'utilisation de serveurs maîtres primaires et secondaires (ou encore esclaves). Les serveurs secondaires possèdent les mêmes données sur la zone et ont le même niveau d'autorité sur l'information que les serveurs primaires. La seule différence vient de la manière dont elles reçoivent cette information. En effet, le serveur maître primaire met à jour ses informations de zone localement par la modification "en dur "de son fichier zone (intervention humaine), alors que le serveur maître secondaire quant à lui obtient les mises à jour du fichier zone via une opération que l'on nomme transfert de zone. Il contacte donc régulièrement un serveur primaire et vérifie si son fichier zone est à jour, sinon il le télécharge sans intervention humaine.




Il existe deux autres types de serveurs, les serveurs cache et les serveurs forwarder. Les serveurs cache ne possèdent d'autorité sur aucun domaine, mais se contentent de rechercher des informations pour les programmes resolver et les placent en mémoire cache. Au fur et à mesure que l'on va les interroger sur des noms de domaine, ils vont augmenter la taille de leur fichier de cache et ainsi répondront plus rapidement aux requêtes les plus demandées. Un serveur cache suit les mêmes procédures de résolution de nom à cela qu'il ne consulte jamais son fichier de zone vu qu'il ne possède d'autorité sur aucune zone. La première recherche pour une zone l'amènera donc finalement vers un serveur primaire ou secondaire qui fait autorité sur cette zone.

Les serveurs forwarder servent à limiter le trafic vers l'extérieur du réseau, pour des raisons de coût pour la plupart du temps. En effet, ils agissent comme des serveurs cache pour toutes les informations concernant des requêtes externes. Donc, un serveur qui ne possède pas d'informations dans son fichier de zone ou dans son cache, transmettra directement sa requête au forwarder, celui-ci va donc se bâtir une grande mémoire cache sur les données les plus demandées et n'appartenant pas à la zone. Les requêtes faites à un forwarder sont toutes récursives et demandent donc une réponse complète.

Le fichier zone

Le fichier zone est un fichier de base de données qui contient toutes les informations sur une zone pour un groupe de serveurs (primaire et secondaire) qui fait autorité sur cette zone. C'est un fichier texte, facilement consultable et modifiable. Il peut être organisé différemment en fonction du DNS utilisé mais conserve une structure plus ou moins identique. On peut séparer quatre parties distinctes :

- Les options,
- L'enregistrement SOA qui définit la zone d'autorité,
- Les informations de serveurs de noms,
- Les informations de la zone.

Formatage des enregistrements :

La plupart des enregistrements se présentent de la façon suivante : <nom d'hôte/domaine> <classe de réseau> <type d'information> <TTL> <information>

Dans le protocole officiel du DNS (issu des RFC), la comparaison entre les chaînes de caractères se fait sans tenir compte de la casse. Dans les différentes normes, il est possible d'utiliser des notations en commentaire pour améliorer la compréhension du fichier de zone par l'administrateur.

Le TTL (Time To Live) représente la durée de vie de l'information récupérée auprès d'un serveur. Lorsque ce délai est écoulé, l'information ne doit plus être considérée comme valide, et donc supprimée de la mémoire cache. Cela permet un rafraîchissement régulier des informations en mémoire et ainsi de prendre en compte les modifications des fichiers de zones. La valeur du TTL doit être choisie judicieusement. Il faut établir un bon compromis entre un délai ni trop court, qui obligerait à aller chercher cette information régulièrement et encombrerait le réseau, et ni trop long, car la cohérence du réseau ne serait alors plus assurée. Si cette valeur n'est pas spécifiée dans un enregistrement, il faut prendre celle par défaut du SOA (voir plus bas).

Start Of Authority (SOA)

L'information de l'enregistrement SOA est la plus importante du fichier zone. Elle indique que ce serveur détient l'autorité sur cette zone et possède donc les informations les plus complètes sur cette partie du domaine. Pour chaque fichier zone, il doit y avoir un enregistrement SOA , quelque soit le nombre de zone sur lequel le serveur fait autorité. Cet enregistrement contient trois types d'informations : le nom du domaine, le nom des serveurs de noms, et un ensemble de compteurs de validité.

Pour compléter le champ SOA, suivent cinq valeurs décimales. Elles indiquent différents compteurs d'états et de rafraîchissement. La première valeur représente le numéro de série du fichier de zone. C'est ce numéro qui est pris en compte lors des transferts de zone pour savoir si un fichier a été mis à jour et doit être remplacé sur les serveurs secondaires. La valeur et le style d'incrémentation sont laissés à l'appréciation du l'administrateur du domaine.

La deuxième valeur indique le délai de rafraîchissement du fichier de zone pour les serveurs secondaires. De cette valeur dépend donc la cohérence de l'information dans la zone, mais il faut aussi veiller à ne pas mettre un temps trop court pour éviter au serveur maître d'être surchargé par des messages de test de mise à jour. Cette valeur dépend bien évidemment de la fréquence de mise à jour du domaine. Si l'on ne rajoute pas souvent de machine, on peut se contenter d'un délai de quelques jours, mais il ne faut pas alors s'attendre ce que les modifications soient rapidement prises en compte.

La troisième valeur indique le temps qu'un serveur secondaire va attendre avant de recontacter le serveur primaire si celui-ci ne répond pas lors d'un rafraîchissement. Cette valeur devrait être inférieure à celle du rafraîchissement, mais cela n'est pas une obligation.

La valeur suivante est celle de l'obsolescence de l'information. Si le serveur n'arrive pas à contacter un serveur maître avant cette durée, on considère que les données qu'il possède sont trop anciennes et plus à jour. Le serveur arrête tout simplement ses fonctions. Mieux vaux une rupture de service que de propager des informations erronées qui pourraient entraîner le chaos dans le réseau. Cette durée doit être supérieure à celle du rafraîchissement, sinon le serveur esclave s'arrête systématiquement à chaque mise à jour.

La dernière valeur est celle du Time to live des informations fournies pas le serveur. C'est la valeur par défaut qui est donnée si celle-ci n'est pas précisée dans l'enregistrement. Au bout de ce temps l'information fournie n'est plus valide, le serveur doit l'effacer de sa mémoire cache, et devra recommencer une recherche si on lui redemande.

Les serveurs de noms :

Les informations qui suivent le champ SOA indiquent la liste des serveurs de noms en activité. On a vu précédemment que pour s'assurer une plus grande marge de sécurité, il vaut mieux posséder plusieurs serveurs de noms. Rien n'empêche un même serveur d'avoir l'autorité sur plusieurs zones. Mais dans ce cas il faudra un fichier par zone, chacun commençant par un enregistrement SOA différent.

Une bonne stratégie pour le choix d'un serveur de noms est d'utiliser une machine possédant des liens sur plusieurs réseaux. De cette façon, si un des réseaux tombe, pour une quelconque raison, le serveur de noms est toujours disponible, via au moins un autre chemin. La syntaxe est la suivante pour définir des serveurs de noms : <nom de domaine> <classe> NS <nom de machine>

Les différents types d'information

La partie suivante va décrire les différents types d'informations que l'on trouve généralement dans les bases de données des serveurs de noms. Il faut se rappeler que le DNS est avant tout un système de partage et de diffusion de l'information, et qu'en théorie il pourrait contenir tout type d'information.

Enregistrement d'adresse (A) : C'est l'enregistrement le plus utilisé dans le DNS. Il fournit tout simplement l'adresse IP d'une machine à partir de son nom. Une machine peut posséder plusieurs adresses IP distinctes, dans ce cas, elles seront toutes fournies en même temps si on fait une demande d'adresse de la machine. Certains serveurs possèdent une fonction de tri d'adresse, en cas de plusieurs champs d'adresses fournis pour une même machine, le serveur renverra en priorité celle qui est la plus proche du réseau demandeur. La syntaxe est la suivante : <nom de machine> IN A <adresse IP de la machine>

Enregistrement d'alias (CNAME) : Les Alias permettent de donner de fournir des noms supplémentaires à des machines : d'ajouter un nom logique à un nom canonique (Canonical NAME). Ceci peut être utile pour des entreprises qui n'ont pas les moyens de posséder un parc informatique important, mais veulent en donner l'illusion. Syntaxe : <nom d'alias> IN CNAME <nom de machine>

Une astuce classique consiste, pour l'administrateur du réseau, lorsque l'on a une machine qui possède plusieurs interfaces (adresses réseaux) à créer autant d'alias qu'il existe d'adresses, un pour chaque interface. Ainsi chaque interface sera accessible, mais cela uniquement pour des soucis d'administration.

**DNSSEC -** Extensions de sécurité du protocole DNS - Améliorations apportées au protocole conçues pour être interopérables avec les implémentations DNS qui ne proposent pas ces améliorations. L'IETF a exploité le fait que les RR (Resource Record) avaient été prévus pour être extensibles à de nouveaux RR. L'IETF a défini un nouveau système de RRs pour les informations relatives à la sécurité et apporter une authentification forte des zones DNS voulant implémenter DNSSEC. Ces enregistrements s'ajoutent aux RRs existant, cela permet à des serveurs n'ayant pas de fonctions DNSSEC de répondre aux requêtes d'une zone sécurisée par DNSSEC.

De façon à être massivement adopté, le groupe de travail DNSSEC de l'IETF permet une compatibilité totale avec les serveurs et clients DNS antérieurs. En mars 1997, l'IAB (Internet Architecture Board) s'est réuni pour discuter de l'architecture sécurisée d'Internet. Cette réunion a permis d'identifier des mécanismes sécurisés et d'autres en développement, pas encore standardisés, pouvant jouer un rôle dans l'architecture sécurisée d'Internet. Un des protocoles majeurs était DNSSEC qui permettait de résoudre le problème de cache empoisonné (Cache Poisoning) [RFC 2316].

Les objectifs de DNSSEC

Un des principes fondamentaux de DNS est d'être un service public. Il requiert des réponses correctes aux requêtes mais les données sont considérées comme étant publiques. Ainsi, les besoins d'authentification et d'intégrité existent, mais pas le contrôle d'accès ni la confidentialité. L'authentification et l'intégrité des informations contenues dans les zones DNS sont fournies par l'utilisation de signatures cryptées par un système de clés publiques.

Les clients et serveurs implémentant DNSSEC peuvent alors garantir l'authenticité des données reçues ainsi que le fait de ne pas avoir été altérées.

Même si le groupe de travail DNSSEC n'a pas choisi d'intégrer la confidentialité pour les transactions DNS, il est possible d'utiliser les clés publiques que fournit DNS dans des applications de niveau supérieur pour garantir la confidentialité. Les PKI pourraient alors jouer un rôle pour stocker les clés publiques.

Etendue de DNSSEC

L'intérêt de DNSSEC s'étend à trois services : la distribution de clés, l'authentification de l'origine des données et l'authentification des transactions et requêtes.

- Distribution de clés : ce service permet de rapatrier la clé publique d'une entrée DNS pour vérifier l'authenticité des données de la zone DNS ; mais il permet également d'apporter des nouvelles fonctions avec lesquelles les clés associées aux entrées DNS peuvent être utilisées dans un autre but que DNS. Les PKI permettent de supporter différents types de clés ainsi que divers algorithmes de génération de clés.
- Authentification de l'origine des données : c'est le principal objectif de la mise au point de DNSSEC. Il réduit nettement la possibilité de Cache Poisoning : les divers RRs sont en effet signés. La signature électronique contient le hash crypté d'un RR. Ce hash est signé (crypté) par la clé privée du serveur origine. Le destinataire vérifie ensuite la validité des données reçues avec la signature associée au RR. Il décrypte le hash avec la clé publique du signataire puis crée son propre hash des données reçues en utilisant le même algorithme et compare ensuite les deux valeurs de hash. Si les deux valeurs sont identiques, les données sont intègres et l'origine est authentifiée.
- Authentification des requêtes et transactions DNS : cela permet de garantir que la réponse à une requête correspond bien à la question et que cette réponse provient bien du serveur duquel on l'attendait. La réponse et la requête sont signées et la signature est également renvoyée avec la réponse. Une autre utilisation de DNSSEC concerne DDNS où les mises à jour dynamiques du DNS se font avec authentification forte [RFC 2137].

Les enregistrements de ressources DNSSEC

L'IETF a créé plusieurs nouveaux RRs pour supporter les nouvelles fonctions de sécurité de DNSSEC. Les plus importants sont les RRs KEY, SIG et NXT. Le RR KEY est utilisé pour stocker les clés publiques, une clé publique par RR KEY. C'est ce RR qui est utilisé pour vérifier la signature d'un champ d'un RR. La signature est stockée dans un le RR SIG ; elle est utilisée pour prouver l'authenticité et l'intégrité des données contenues dans un champ d'un RR. Le RR NXT (pour nonexistent) est utilisé pour certifier la non-existence d'un champ d'un RR.

Il existe également un autre RR, le RR CERT mais il n'apporte pas de fonctionnalités de sécurité supplémentaires à DNS. Il est en fait utilisé pour les applications au-dessus de DNS pour stocker les certificats de clé publique [RFC 2538]. De la même façon qu'une application génère une requête de type A pour résoudre un nom d'hôte, une application sécurisée voulant discuter de manière cryptée avec une autre génère une requête CERT pour rapatrier le certificat de clé publique de l'autre entité. Une première application est le projet LADON17, qui intègre DNSSEC pour l'authentification avec SSH (Secure Shell, un protocole sécurisé très utilisé dans le monde Unix remplaçant telnet, pouvant servir de VPN).

- RR KEY : La clé d'un nom DNS est contenue dans un RR KEY. Tout type de requête sur un nom DNS, contenu dans une zone sécurisée, génère une réponse contenant les informations demandées. Le RR KEY associé au nom DNS fait partie de la réponse. Le resolver reçoit ainsi les deux informations permettant la validation sans avoir besoin de générer une requête supplémentaire

pour rapatrier la clé. Le RR KEY contient des informations relatives (dans la section RDATA) aux caractéristiques de la sécurité mise en oeuvre ainsi que l'utilisation autorisée pour le propriétaire. Il comporte ainsi le type d'algorithme, la clé publique, le type de protocole et des flags pour indiquer si le nom DNS possède ou non une clé publique par exemple. Plusieurs algorithmes sont supportés comme RSA/MD5, Diffie-Hellman, DSA (Digital Signature Algorithm) et les algorithmes à courbe elliptique. Seul le support de DSA est requis. Le champ protocole sert à indiquer pour quel type de protocole la clé publique est supportée : TLS (Transport Layer Security), email, DNSSEC et IPsec sont déjà supportés, les autres valeurs (5 à 254) restent libres d'être attribuées par l'ICANN.

- RR SIG : La signature est contenue dans le RR SIG. Il permet l'authentification d'un RR et fournit l'expiration de la signature. Dans une zone sécurisée, à un RR peuvent être associés plusieurs RR SIG ; en effet, certains sites situés dans des pays où il existe des restrictions à l'exportation de matériel cryptographique peuvent choisir entre plusieurs algorithmes pour effectuer la signature. De même que le RR KEY, la partie RDATA du RR SIG contient des informations sur le type d'algorithme utilisé, le type de RR signé, ainsi que plusieurs champs relatifs à l'expiration.
- RR NXT : Le système DNS fournit la possibilité de cacher des réponses négatives. Une réponse négative indique qu'un RR n'existe pas pour une requête. DNSSEC permet de signer la nonexistence de ces RRs afin que la non-existence dans une zone puisse être authentifiée.

Toutes ces fonctionnalités impliquent des responsabilités supplémentaires pour les serveurs DNS implémentant DNSSEC. En effet, s'ajoutent aux fonctions de base d'un serveur DNS (gérer les informations de la zone sur laquelle il a autorité, gérer le cache DNS, répondre aux requêtes des clients) la gestion des clés privées [RFC 2541] qui doivent être inaccessibles en dehors du serveur DNS lui-même (on remarque que ces clés privées ne sont générées qu'une seule fois, à la création du couple clé privé/clé publique donc il faut faire attention à ne pas être intercepté lors de la création de ces clés), la gestion de l'expiration des RRs SIG en concurrence avec le TTL originel du système DNS (le TTL est néanmoins conservé pour la compatibilité ascendante).

**DOD -** Department of Defense - Equivalent du ministère de la Défense aux Etats-Unis. Joue un grand rôle de normalisation dans le domaine des réseaux et de la sécurité. A notamment été à l'origine du succès du protocole TCP/IP.

**Dolby Digital -** Procédé d'encodage de la piste son sur un support numérique développé par les laboratoires Dolby. Il remplace la piste analogique Droite par un signal Dolby Digital (appelé à l'époque AC3 en 1995) qui est modulé en analogique FM. Cependant, ce signal AC-3 RF est un signal modulé pour "rentrer" sur le support analogique et ne ressemble pas à un signal numérique Dolby Digital classique comme celui du DVD. Avant le décodage Dolby Digital proprement dit, ce signal AC3-RF doit donc être démodulé pour prendre la forme d'un signal numérique. Cette démodulation est faite soit dans l'ampli s'il en est capable, soit par un petit boitier appelé démodulateur AC3-RF. Les amplis Dolby Digital intègrent de plus en plus rarement la fonction de démodulation RF. Un ampli qui en est capable possède une prise cinch appelé AC3-RF.

**DOM -** (Document Object Model) - Spécification d'un ensemble de fonctions permettant d'analyser le code d'un document XML ou HTML afin de construire un arbre représentant sa structure et de mettre à jour les différents éléments de l'arbre.

**Domaine -** Entité logique définie par l'administrateur de réseau lui permettant de gérer plusieurs serveurs physiquement distincts.

Les domaines sont des entités administratives qui permettent la gestion décentralisée des noms de domaine. Le système de noms de domaine (DNS) est organisé hiérarchiquement. Le NIC a été désigné par l'Agence de la Défense et des Communications (DCA) pour s'occuper du registre des noms de domaine pour la partie du DDN et DARPA de l'Internet.

**Domaine de collision -** (Ethernet) Segment de réseau Ethernet que se partagent plusieurs ordinateurs. Pour éviter les collisions, chaque ordinateur n'envoie ses données qu'après avoir "écouté" les autres ordinateurs de son segment et s'il est sûr qu'aucun autre n'est en train d'émettre.

**Domaine MPLS -** Ensemble contigu de nœuds qui effectuent du routage et de la commutation MPLS et qui se trouvent dans un domaine de routage ou dans un domaine administratif.

**Domotique -** Regroupe l'ensemble des nouvelles technologies utilisées pour automatiser l'habitat : sécurité, gestion de l'énergie et communications tant internes qu'externes.

**DON -** Disque Optique Numérique.

**Dopant -** (en optique) Particule de matériau ajouté à la silice du coeur lors de la fabrication de la préforme et permettant ainsi de créer un verre différent d'indice de réfraction « n1 » plus ou moins élevé.

Dans toutes les activités sportives : Particules permettant d'améliorer les performances sans recourir à un entrainement spécifique.

**Dorsale -** Partie principale d'un réseau de télécommunication, caractérisée par un débit élevé, qui concentre et transporte les flux de données entre des réseaux affluents.

**DoS -** Deny Of Service - Attaque par interruption de service **-** Action malveillante visant à empêcher le fonctionnement normal de tout ou partie d'un réseau ou d'un système hôte. Cette attaque peut être comparée à une personne qui composerait sans arrêt le même numéro de téléphone pour saturer cette ligne.

Le terme français équivalent (déni de service) est beaucoup moins employé que l'original anglais. Pourtant, il aurait l'avantage d'être très clair pour décrire un type d'attaque électronique dont l'objectif est de retirer à la victime la possibilité de se servir d'un ou plusieurs moyens informatiques qui sont la cible de l'attaque DoS.

Tous les types de service peuvent être victimes de ce type d'attaque qui consiste à saturer la cible avec des demandes plus ou moins réelle au point de la rendre incapable de traiter son activité normale. Dans le cas d'un serveur de courrier électronique ou d'un utilisateur de courrier électronique, une attaque DoS peut par exemple consister à bombarder la victime avec un nombre considérable de messages (on peut penser à des chiffres allant de quelques milliers à quelques millions de messages). L'agresseur s'attend à ce que la victime soit submergée par le déluge de messages, devenant ainsi incapable de traiter son courrier d'une manière normale. Dans les cas extrêmes, on peut s'attendre à ce qu'un serveur soit amené à s'arrêter totalement, ou à ce qu'un utilisateur ne trouve d'autre porte de sortie que de détruire ou faire détruire tous les messages reçus (utiles ou non).

De nombreux autres types d'attaques DoS sont envisageables (et utilisés). Le terme DDoS (Distributed Denial of Service ou déni de service distribué) est utilisé dans le cas où l'attaque est coordonnée entre plusieurs ordinateurs rendant ainsi presqu'impossible de s'en prémunir.

Les attaques de ce type qui ont été observées sur des serveurs de grande taille se sont révélées très efficaces et sont considérées comme un véritable moyen de guerre électronique contre lequel il est difficile de se défendre.

**Dosimétrie -** Mesure, ou détermination par le calcul, des valeurs de champs électromagnétiques ou du DAS (débit d'absorption spécifique) dans le corps d'êtres humains ou d'animaux exposés à un champ électromagnétique.

**Downlink -** Terme anglais désignant le lien descendant entre un satellite et une station au sol.

**Downspeeding -** Ce concept permet au système si il perd un ou plusieurs de ces canaux pendant la communication, de recalculer en quelques secondes le débit restant et de conserver la connexion en optimisant le codage au débit restant.

**DPNSS -** Digital Protocol for Networking Switch Signaling - Système de signalisation privée d'autocommutateurs développé par Gec-Plessey sous la supervision de British Telecom.

**DPSAI -** Direction de la planification du spectre et des affaires internationales.

**DQDB -** Distributed Queue Dual Bus - Réseau en fibre optique mis au point en Australie et retenue comme proposition de norme (IEEE 802.6) pour les réseaux métropolitains (MAN). La topologie est un double bus avec des débits de 34 à 622 Mbps.

Développé par une université australienne et soutenu par Telecom Australia, ce protocole a été normalisé par l'IEEE 802.6 et l'ISO 8802.6 comme norme de réseau métropolitain. Il a été développé parallèlement à ATM et utilise le format des cellules de 53 octets dont 48 octets de charge utile.

DQDB permet des transfert isochrone et asynchrone en mode connecté ou non.

DQDB utilise un double bus unidirectionnel. Sur chaque bus, une tête de bus (HoB, Head of Bus) génère une trame toutes les 125 µs contenant n slots (cellules de 53 octets). Le nombre n de slots dépend du débit du réseau. Les têtes de bus sont généralement situées sur une même station.

Le premier bit de chaque slot (bit Busy) indique si le slot est libre ou occupé.

**Drain -** (en câblage) - Fil de continuité d'écran, facilite le raccordement à la connectique. Elément conducteur qui est assemblé en contact électrique avec le blindage d'un câble lors de la fabrication.

**Drapeau -** Structure particulière de bits servant à délimiter un bloc de données. On utilise aussi les termes fanion, flag ou délimiteur.

**DRCS -** Dynamically Reconfigurable Character Set - Jeu de caractères alphamosaïques dynamiquement redéfinissables. En France, on peut avoir des DRCS avec les minitels 2 et certains minitels 12.

**DRG -** Direction à la Réglementation Générale - Organisme dépendant du ministère des Postes et Télécommunications responsable des règlements s'appliquant aux réseaux publics et aux réseaux privés ouverts à des tiers, tant en termes d'Accès techniques que de règles commerciales.

**Driver -** Logiciel ou programme qui pilote les données destinées à un port de communication à des fins de transfert.

**DRM -** Digital Right Management - Gestion numérique des droits d'auteurs.

**DSA -** Distributed System Architecture - Architecture de communication du constructeur Bull. Englobe diverses possibilités de construction de réseaux centralisés, hiérarchisés ou distribués. Depuis quelques années, Bull emploie l'expression ISO/DSA pour mettre en avant la mise en conformité progressive de DSA avec les protocoles normalisés de l'ISO (International Standard Organisation) dans le cadre du modèle OSI (Open System Interconnection).

**DSL Forum -** Le Digital Subscriber Line Forum rassemble les principaux fabricants d'équipements xDSL

**DSLAM -** Digital Subscriber Line Access Multiplexer - Multiplexeur DSL - Concentrateur de lignes DSL, placé dans les répartiteurs téléphoniques. Il aiguille les flux DSL vers le réseau ATM de l'opérateur. Situé sur le réseau de l'opérateur local, au niveau du répartiteur, il fait parti des équipements utilisés pour transformer une ligne téléphonique classique en ligne ADSL permettant la transmission de données, et en particulier l'accès à Internet, à haut débit. La fonction du DSLAM est de regrouper plusieurs lignes ADSL sur un seul support, qui achemine les données en provenance et à destination de ces lignes.

**DSML -** Directory Services Markup Language - Langage normalisant la communication avec les annuaires LDAP par la structuration des données au format XML. Il permet aux applications d'avoir accès aux données dans les annuaires.

**DSP -** Directory System Protocol - Protocole utilisé pour accéder à un annuaire dans le cadre de la norme X500.

**DSS -** Digital Signature Standard - Algorithme de signature numérique développé par la National Security Agency (voir NSA).

**DSSS -** Technologie à étalement du spectre en séquence directe - Transmission radio au sein de la bande de fréquence des 2,4 GHz sans licence. La technologie DSSS est une technique de modulation développée dans les années 1940 pour étaler un signal de transmission sur une large bande de fréquence radio. Cette technique est idéale pour la transmission de données car elle est moins sensible au bruit radioélectrique et ne crée que peu d'interférences

**DTCG -** Direction Technique du Contrôle du spectre et de la Gestion de réseaux

**DTD -** (Document Type Definition) - Spécification d'un ensemble de balises utilisables dans un document XTML dont le respect garantit la validité du document. La DTD définit aussi la structure (schéma) du document, et contient la valeur par défaut de certains attributs.

Document (non XML) permettant de décrire les structures des documents XML. Les DTD permettent de valider un document XML bien formé. Elles peuvent être internes ou externes aux documents.

**DTE -** Data Terminal Equipment - Equivalent d'ETTD (Equipement Terminal de Traitement de Données) dans le vocabulaire officiel du CCITT.

**DTMF -** Dual Tone Multifrequency Signaling - Système de signalisation utilisé pour transmettre la numérotation dans les systèmes de commutation analogique classiques. Utilise une combinaison matricielle de deux fréquences de base formant quatre groupes de fréquences pour former les différents numéros d'un téléphone à touche.

Le processus DTMF aussi connu sous le nom de processus à double tonalité, processus de numérotation dans les appareils téléphoniques. Dans le central téléphonique IP, la numérotation DTMF agit comme une sorte d'extension virtuelle qui doit être appelée de façon à ce que la fonction de non sélection automatique à l'arrivé puisse être exécutée. Lorsqu'un appel est émis, l'abonné virtuel répond et la numérotation directe peut être exécutée via le DTMF. Pour ce faire, cependant, le téléphone doit prendre en charge les tonalités DTMF.

**DTS -** Standard audio. Codage 5.1 de qualité car moins compressé que le Dolby Digital et de meilleur qualité.

**DUA** - Directory User Agent - Application OSI représentant l'utilisateur accédant à un annuaire.

**Duplex -** Transmission des informations dans les deux sens simultanément.

**Duplexeur -** Multiplexeur sur deux voies. Dispositif permettant de superposer deux voies de transmission sur un seul canal et, par exemple, d'utiliser une liaison 4 800 bps comme deux liaisons de 2 400 bps.

**DV -** Format de bande vidéo numérique pour l'enregistrement de son et de vidéo numérique sur une bande 1/4" Metal Evaporated. Des minis bandes DV peuvent contenir jusqu'à 60 minutes de vidéo, alors que les bandes standard DV peuvent en contenir jusqu'à 270 minutes.

**DVB -** Digital Video Broadcast - Groupe Européen spécialisé dans la radio télédiffusion numérique. 2 variantes existent :

- DVB-T pour Terrestrial = C'est la Télévision Numérique Terrestre (TNT) - Diffusé en MPEG-2 sur un multiplex (fréquence) de 24 Mbit/seconde. Chaque programme requiert une bande passante de 4 à 5 Mbit/seconde d'où une capacité de 5 chaines TV par multiplex (fréquence).
- DVB-H pour Handheld = C'est la TNT adapté aux spécificités des terminaux mobiles (écran réduit, autonomie des batteries et mobilité) - Diffusé en IP (protocole IPDC - IP Data cast) sur un multiplex de 11 Mbit/seconde. Chaque programme requiert une bande passante de 128 à 384 kbit/seconde d'où une capacité de 25 à 80 flux vidéos par multiplex (fréquence). Norme Européenne validée par l'ETSI, utilisant la norme de compression MPEG-2 ou MPEG-4. Utilise les bande UHF IV et V.

**DVD -** Digital Versatil Disk aussi appelé DVD-Vidéo.

**DVD+R/RW -** Dernier arrivé sur le marché, le DVD+RW est très proche physiquement et chimiquement du DVD-RW. Ainsi, il se compose lui aussi d'une couche d'enregistrement composée d'un alliage d'argent et d'indium ou de germanium. Les différences chimiques et physiques entre les deux formats sont minimes (jitters, profondeur de gravure…).

**DVD-R/RW -** Digital Versatil Disk Writing Device - Le DVD-R et le DVD-RW sont deux des formats validés par le DVD-Forum. Techniquement, la couche d'enregistrement d'un DVD-RW se compose, en fonction de la marque, d'un alliage d'argent et d'indium ou de germanium. Le DVD-R se voit doté d'une couche de polycarbonate. Comme un CD-RW, un DVD-RW autorise jusqu'à 1 000 enregistrements et conserve les données pendant 100 ans (en théorie).

**DVD-RAM -** Premier type de DVD réinscriptible à avoir été normalisé. À l'origine dédié au monde professionnel, ce média dispose de nombreux avantages. Il est réinscriptible 100 000 fois contre 1 000 pour le DVD-RW et le DVD+RW. De plus, il dispose d'un caddie protecteur, augmentant ainsi sa durée de vie. Enfin, le DVD-Ram existe en plusieurs versions: 2,6 Go, 3,9 Go, 4,7 Go et même 9,4 Go, alors que DVD-R/RW et DVD+RW ne dépassent pas les 4,7 Go.

Ce media est véritablement une excellente alternative aux produits de stockage magnéto-optiques déjà utilisés dans le monde de l'entreprise. Malheureusement, il n'est pas non plus exempt de défauts. Tout d'abord, il s'agit du plus cher d'entre tous. Enfin, sa compatibilité est très limitée. Il doit être sorti de son caddie pour être lu ailleurs que dans un lecteur dédié. De plus, un seul lecteur de DVD-Rom (GD 8000 d'Hitachi) sur le marché supporte le DVD-Ram. Pire, aucune platine de salon en dehors des produits réservés n'accepte ce format.

**DVI -** Digital Visual (ou Vidéo) Interface - L'interface fut standardisée en 1999 et conclua les efforts des constructeurs pour trouver un connecteur capable de faire transiter un signal vidéo numérique. En effet, les écrans plats, par exemple, fonctionnent entièrement en mode numérique contrairement aux bons vieux moniteurs cathodiques. Or, les cartes graphiques convertissent, via leur Ramdac (Ranz Digital Analog Converter, les données numériques qu'elles produisent en un signal analogique compréhensible par un moniteur cathodique. Du coup, pour pouvoir afficher le signal vidéo analogique provenant du port VGA de la carte graphique, les écrans plats sont équipés d'un convertisseur analogique/numérique, ce qui grève le prix de l'écran. Cette double conversion numérique/ analogique par la carte vidéo puis analogique/numérique par le convertisseur intégré à l'écran, a pour effet de dégrader la qualité de l'image. L'intérêt de l'interface DVI, quand elle est présente à la fois sur la carte et sur l'écran, est d'obtenir un signal numérique d'un bout à l'autre.

Il existe trois sortes de connecteurs DVI :

- Le DVI-D uniquement numérique,
- le DVI-1 analogique et numérique
- le DVI-A uniquement analogique.

**DVMRP -** Distance Vector Multicast Routing Protocol v1 & v2 - Protocole d'échange de routeurs à routeurs dédié au Multicast. Voir Multicast. Echange des informations de routage entre routeurs voisins (inspiré de RIP). Dépendant d'un protocole de routage Unicast, il requiert son propre protocole de routage unicast intégré (similaire à RIP). DVMRP construit un arbre de distribution séparé pour chaque source / Groupe. Il utilise le Reverse Path Forwarding pour propager et élaguer (propagation = diffuser les paquets sur toutes les interfaces de sortie de l'arbre de diffusion, en supposant au départ que chaque branche mène à des membres du groupe) (élaguer = Eliminer les branches de l'arbre sans membre du groupe multicast, coupant la transmission sur les LANs sans récepteur intéressé, élague aussi les chemins redondants non optimaux de chaque récepteur vers la source).

DVMRP est plus efficace pour les distributions denses de récepteurs Multicast, a été largement utilisé sur le MBONE (réseau Multicast Européen // Internet), mais induit des facteurs significatifs de facteur d'échelle (convergence lente comme RIP dont il s'inspire), beaucoup d'informations d'état sur le routage Multicast maintenues sur les routeurs, partout (Sources, Groupe), ne supporte pas les arbres partagés, n'est pas adapté sur des architectures avec un nombre de saut supérieur à 32.

DVMRP est inapproprié pour les grands réseaux avec peu de récepteurs intéressés due au mécanisme propager et élaguer et/ou dans le cas de groupes faiblement représentés sur un WAN.

**DWDM -** Dense Wavelength Division Multiplex - La technologie WDM (qui consiste à injecter n canaux de différentes longueurs d'onde dans une seule fibre) est dite DWDM lorsque l'espacement intercanal utilisé est égal ou inférieur à 0,8 (100 GHz) ou lorsque plus de 16 canaux sont utilisés. Des tests ont déjà été effectués avec des espacements de 0,4 (50 GHz) et 0,2 nm (25 GHz).

Les systèmes commercialisés aujourd.hui proposent 4, 8, 16, 32 et même 80 canaux optiques à 2,5 Gbits/s par canal. Un système à 16 canaux de 2,5 Gbits/s, soit 40 Gbits/s permet l'acheminement de 500 000 conversations téléphoniques simultanément sur une seule paire de fibre optique.

La norme ITU-T G692 définit la plage de longueurs d'ondes dans la fenêtre de transmission de 1530 à 1565 nm. L'espacement normalisé entre deux longueurs d'ondes est de 1,6 (200Ghz) ou 0,8 nm (100 Ghz).

On parle aussi de multiplexage dense en longueur d'onde dès qu'on injecte plus d'une dizaine de canaux dans la bande 1530-1560 nm.

La technologie DWDM introduit des phénomènes non linéaires qui ont notamment pour conséquence de limiter en pratique la distance entre amplificateurs entre 50 et 100 Km.

La distance entre les amplificateurs est limitée par la diaphonie entre canaux ou XPM (Cross Phase Modulation). Un autre paramètre fait malheureusement son apparition : le mélange quatre ondes dit FWM (Four Wave Mixing) qui crérait de l'intermodulation optique entre les différents canaux.

L'effet Raman SRS (Stimulated Raman Scattering) augmente les écarts de puissance reçus entre canaux et par conséquent produit une trop grande dispersion du rapport signal/bruit.

Avec de la fibre optique monomode G 652, les effets non linéaires n'apparaissent pas dans la fenêtre 1550 nm tant que le nombre de canaux reste inférieur ou égal à 32 canaux et que la puissance par canal reste inférieure à 1 mW.

Différentes techniques permettent de corriger ces phénomènes : c'est le cas de la DCF (Dispersion Compensating Fiber) qui consiste à introduire dans la liaison un tronçon de fibre produisant une dispersion négative (environ -100 ps/nm.km) de compensation.

Un des éléments clef est l'amplificateur à fibre dopée erbium EDFA (Erbium Doped Fibber Amplifier). Il compense les pertes d'insertion dues aux multiplexage/démultiplexage des longueurs d'onde. Ceci est dû à des phénomènes non linéaires (XPM, FWM, SRS) qui se développent lors de la propagation du signal dans la fibre.

Les travaux récents du C.N.E.T (Centre National d'Etudes en Télécommunications) sur la transmission soliton montrent que l'on peut repousser cette limite (distance inter-amplificateur) à 1000 kilomètres. Un soliton est une onde qui se propage sans déformation remarquable de sa forme ni variation de sa vitesse. Ce phénomène a été remarqué pour la première fois sous la forme d'une vague dans un canal, mais il existe dans de nombreux domaines, dont la lumière.

| CWDM Versus DWDM | | | | |
|---|---|---|---|---|
| | Nombre de lambdas protégés | Espacement | Refroidissement nécessaire | Application |
| DWDM | 32 | 100-200 GHz | Oui | Bande passante nécessaire supérieure à 16 lambdas ou distance > à 80 kms |
| CWDM | 16 | 2 500 GHz | Non | Bande passante nécessaire inférieure à 16 lambdas et/ou distance < 80 kms sans amplification |

# E

**EAI - Entreprise Application Integration -** Logiciel servant à fédérer et faire communiquer tous les éléments du système d'information d'une entreprise : application grands systèmes, ERP, CRM, bases de données,…

**EAP -** Extensible Authentication Protocol - RFC 2284 - Extension de RADIUS qui permet aux adaptateurs des clients sans fil de communiquer avec les serveurs RADIUS. Authentification pour les connexions point à point (PPP) utilisée pour les WLAN 802.1x.

Le protocole EAP est une extension du protocole PPP. Contrairement à PPP, le protocole EAP permet d'utiliser différentes méthodes d'identification et son principe de fonctionnement rend très souple l'utilisation de différents systèmes d'authentification.

EAP possède plusieurs méthodes d'authentification, dont les plus connues sont :

- EAP-MD5 (Message Digest 5)
- EAP-PEAP
- EAP-TLS
- EAP-TTLS

**EBCDIC -** Extended Binary Coded Decimal Interchange Code - L'un des plus courants des codes alphanumériques, largement utilisé dans les matériels IBM. Il propose sur 8 bits 256 combinaisons pour les majuscules, les minuscules, la ponctuation et les caractères spéciaux. Cède cependant du terrain au code ASCII.

**EBPP -** Electronic Bill Presentment and Payment - La facturation en ligne ou EBPP recouvre deux notions : la présentation des factures et leur règlement. Ce service combine généralement des services de messagerie pour la notification, et Web, pour la présentation.

**e-Business -** Outils logiciels permettant à une entreprise d'utiliser l'Internet pour traiter les commandes à ses fournisseurs et la vente à ses clients. Ces derniers peuvent être soit d'autres entreprises en relation BtoB soit des consommateurs finaux en relation BtoC

**ECB -** Electronic CodeBook mode - Le mode ECB correspond à l'utilisation de l'algorithme D.E.S décrit dans les documents officiels : étant donné un texte clair découpé en blocs de 64 bits x1x2x3 … xn , chaque bloc xi de 64 bits est chiffrer avec la clé K, constituant le texte chiffré y1y2y3 … yn.

**ECC -** Electronic Communications Commitee - Nouveau Comité des communications électroniques qui regroupe les anciennes activités de l'ECTRA et de L'ERC au sein de la CEPT.

**ECC Chipkill -** Système de vérification de l'intégrité du contenu de la mémoire par contrôle de parité de type ECC, mais capable de détecter et de corriger des erreurs jusqu'à 4 bits.

**Echantillon -** Valeur d'un signal à un instant déterminé - échantillonnage (sampling) - Prise d'échantillons d'un signal, à intervalles de temps réguliers.

**Echantillonnage -** Technique consistant à ne prélever sur un signal que des échantillons d'information à des intervalles de temps réguliers et suffisamment proches pour conserver une image fidèle du signal d'origine. L'échantillonnage est généralement utilisé pour numériser un signal analogique (voix, son...). Les valeurs des échantillons discontinus sont ensuite codées pour former un signal numérique.

**Echo -** Défaut de transmission par la réflexion d'une partie du signal du récepteur vers l'émetteur. En informatique, désigne aussi une technique consistant à ce que l'émetteur attende le retour d'un accusé de réception du message émis, alors renvoyé par le récepteur, pour s'assurer que celui-ci a bien été reçu.

**ECMA -** European Computer Manufacturer Association - Association regroupant la plupart des grands constructeurs informatiques présents en Europe (y compris ceux d'origine non européenne), elle joue un rôle important comme espace de discussion pour l'élaboration des normes. Elle émet ainsi des recommandations qui, sans avoir de statut officiel, sont généralement suivies et précèdent l'adoption comme normes internationales.

**Écran -** Feuillard de métal enroulé autour d'un câble assurant une protection contre les hautes fréquences parasites ou contre les perturbations éléctromagnétiques.

**Ecran à cristaux liquides -** Les écrans à cristaux liquides (LCD) ne consomment que peu d'énergie et sont généralement faciles à lire. Ils sont réalisés par scellement d'un joint liquide entre deux morceaux de verre et/ou un filtre. L'écran se compose de centaines ou de milliers de points qui sont chargés ou non et donc réfléchissent ou ne réfléchissent pas la lumière de façon à former des lettres, des caractères et des chiffres. Certains écrans LCD sont dotés d'un panneau électroluminescent qui est placé derrière eux ; ils sont alors dits "rétro éclairés".

**ECTRA -** European Committee of Telecommunications Regulatory Affairs ou Comité européen des affaires réglementaires des télécommunications - Organe de la CEPT chargé des affaires réglementaires, qui dispose d'un bureau permanent appelé ETO (Office européen des télécommunications).

**ECTUA -** European Council of Telecommunications Users Associations - Association européenne fédérant les principales organisations d'utilisateurs de services de télécommunications. L'Afutt (Association Française des Utilisateurs du Téléphone et des Télécommunications) est membre de cette fédération.

**EDGE -** Enhanced Data Rate for GSM Evolution - Norme GSM permettant des débits plus importants que le GPRS. Technologie intermédiaire entre le GSM et l'UMTS offrant un accès rapide à l'internet à une vitesse de 200 Kbits/s pour un utilisateur stationnaire. Elle offre des performances comparables à celles de l'UMTS, mais dans la bande des fréquences des réseaux GSM et avec leur technologie d'accès TDMA.

Edge a été standardisée au niveau européen (Etsi/ 3GPP) comme au niveau international (ITU). Contrairement à l'UMTS, son exploitation ne nécessite ni licence spécifique (Edge fonctionne sur 800, 900, 1 800 et 1 900 MHz) ni bouleversement des réseaux existants ; l'infrastructure nécessaire à la transmission en mode paquet a déjà été mise en place lors du passage au GPRS.

La norme met en oeuvre de nouveaux schémas de codage assortis d'une nouvelle technique de modulation appelée 8-PSK (8 Phase Shift Keying) , ce qui lui permet d'augmenter nettement son débit. Cette modulation autorise le transfert de 3 bits par impulsion, là où le GPRS ne peut en gérer qu'un (modulation GSMK).

Edge peut cependant aussi effectuer du GSMK en cas de défaillance, car le protocole est capable d'adapter dynamiquement la modulation et les schémas de codage. Edge compte cinq schémas supplémentaires permettant d'augmenter le débit par canal jusqu'à près de 60 Kbit/s, soit un débit maximal théorique de 473,6 kbit/s (160 pour le GPRS), volontairement plafonné à 384 kbit/s par l'ITU pour pouvoir l'intégrer à la famille IMT2000 des normes 3G.

**EDI -** Electronic Data Interchange - Echange de Données Informatisé - Technique permettant de remplacer les échanges de documents papier par des échanges inter ordinateurs grâce à des réseaux de télécommunications. Cette technique connaît un fort développement à travers de nombreux organismes de normalisation ou structures interprofessionnelles.

**EDICON -** Electronic Data Interchange Construction - Projet britannique d'EDI dans la construction.

**EDICT -** Réseau à valeur ajoutée britannique de la société Istel, actif notamment dans le transport.

**EDI-Express -** Service d'Echanges de données informatisé (EDI) proposé par la société GEISCO.

**EDIFRANCE -** Structure rattachée à l'Afnor rassemblant l'ensemble des partenaires économiques français impliqués dans la mise en place d'EDI (Echange de données informatisé).

**EDIG -** European Defense Industry Group - Association européenne regroupant les industriels de la défense.

**Effet de mémoire -** La durée de vie d'une batterie risque de diminuer progressivement si la batterie est rechargée avant d'être complètement déchargée. C'est ce qu'on appelle l'effet de mémoire ; il se rencontre le plus souvent avec les piles Nickel Cadmium. Il constitue un problème de moindre importance avec les batteries à l'hydrure de nickel, et quasiment insignifiant avec les batteries lithium ion.

**Effet Photoélectrique -** Phénomène d'émission d'électrons après absorption de photons par un matériau.

**EFR -** Enhanced Frequency Rate - Technologie améliorant la qualité du son des communications avec les mobiles.

**EGP -** Exterior Gateway Protocol - C'est le protocole utilisé par les routeurs pour interconnecter des réseaux TCP/IP étendus. La dernière version en date est BGP-4 qui est largement utilisée par tous les ISP à travers le monde.

**EIA -** Electronic Industry Association. Organisme de certification américain.

**EICTA -** European Information and Communications Technology Industry Association - Association européenne regroupant les industriels des technologies de l'information et des télécommunications.

**EIGRP -** Enhanced Interior Gateway Routing Protocol - Protocole de routage CISCO - C'est une version avancée du protocole vecteur de distance. Il est basé sur le DUAL (Diffusing Update Algorithm).

L'algorithme DUAL est basé sur un mélange de l'algorithme de vecteurs de distance et de l'algorithme d'état de liaison. Ce mélange de ces deux algorithmes est bien sûr réalisé en oubliant les défauts de ces deux algorithmes. Le principe du calcul de la métrique de chaque route prend en compte de nombreux paramètres comme la bande passante, la fiabilité de la ligne ou le nombre de noeuds à traverser pour atteindre un réseau.

Le protocole EIGRP utilise quatre types de paquet de contrôle : les paquets Hello pour signaler sa présence, les paquets Update pour les mises à jour de table de routage, les paquets Query et les paquets Request.

Le coeur de l'EIGRP est son algorithme de convergence : le DUAL. Les diverses technologies fonctionnant avec : Neighbor discovery/recovery, le protocol dependent modules, le protocole de transport RTP et les divers paquets transportés

Ce protocole présente de nombreuses fonctionnalités évoluées comme la summarization, l'autosummarization, le filtrage de routes, les routes par défaut, la redistribution de routes et supporte de nombreuses architectures telles qu'IPX ou Appletalk.

Enfin, l'EIGRP propose avec le système de signature MD5 d'accroître la sécurité du réseau en permettant d'authentifier la source des requêtes de mise à jour arrivant sur un routeur et donc d'éliminer les imposteurs.

**EIR -** Equipment Identity Register - Réseau mobile - L'EIR contient les identités des mobiles (IMEI). Il permet de vérifier qu'un équipement est autorisé sur le réseau. L'IMEI est définie à l'usine qui produit le terminal.

Il existe trois listes pour les mobiles :

• Liste blanche : mobiles autorisés.

• Liste grise : mobiles présentant un dysfonctionnement insuffisant pour interdire l'accès au réseau.

• Liste noire : mobile non autorisés (volés, non homologués).

Le système d'administration reçoit l'IMSI de tout abonné utilisant un terminal figurant sur la liste noire.

**EIR -** Excess Information Rate - Débit de débordement autorisé au-dessus duquel toute trame de données peut être détruite.

**EISI -** Externalisation de l'Instrumentation du Système d'Information - Voir "map factory"

**EJB -** Enterprise JavaBean - Standard Java définissant, côté serveur, la structure des composants logiciels et les interfaces permettant aux programmeurs de développer et de gérer des applications distribuées, indépendamment du système utilisé. Les EJB offrent pour ce faire des services techniques de niveau système.

**Electroluminescence -** Transformation directe d'une énergie électrique en énergie lumineuse.

**Embrouillage -** Scrambling - Transformation d'un signal numérique en un signal numérique aléatoire ou pseudo-aléatoire, de même signification et de même débit binaire en vue d'améliorer la transmission du signal sur un support donné.

Transformation réversible d'un signal numérique, en vue d'en faciliter la transmission ou l'enregistrement, en un signal numérique de même signification et de même débit binaire, dont le spectre est voisin de celui d'un signal aléatoire.

Opération inverse : le désembrouillage. Certains modems utilisent un dispositif d'embrouillage.

**Emulation -** Technique permettant d'imiter le fonctionnement d'un équipement donné sur un autre équipement à l'origine non conçu pour cet usage. Surtout utilisé pour permettre à un terminal d'une marque donnée de dialoguer avec un ordinateur d'une autre marque.

**Emuler -** to emulate - Transformer les conventions constituant un protocole pour simuler un protocole différent.

**EN -** Norme européenne.

**EN 50167 -** Norme européenne relative aux câbles de capillarité.

**EN 50168 -** Norme européenne relative aux câbles de rocade.

**EN 50169 -** Norme européenne relative aux cordons.

**EN 50173 -** Norme européenne relative au pré-câblage.

**Encrypteur -** Equipement permettant de coder (ou chiffrer) des données pour des raisons de sécurité.

**ENST -** Ecole Nationale Supérieure des Télécommunications - Compte deux établissements, ENST Bretagne à Brest, et Télécom Paris dans la capitale.

**En-tête d'authentification -** En-tête IPsec permettant de vérifier que le contenu d'un paquet n'a pas été modifié pendant le transport.

**Entropie -** La théorie de l'information définit la quantité d'information d'un message comme le nombre minimal de bits nécessaires pour coder toutes les significations possibles de ce message. Formellement, l'entropie en bits d'un message M est H(M) = Log2 (n) = Logx(n) / Logx(2), où n est le nombre de significations différentes que peut prendre le message.

**ENUM -** Protocole défini par l'Internet Engineering Task Force qui permet de créer des noms de domaine Internet à partir des numéros de téléphone et de les associer à des services de communication (service téléphonique, mail, fax, messagerie unifiée...). Il s'agit du premier projet réellement convergent entre le monde de l'Internet et celui des télécommunications mêlant des aspects de numérotation avec des aspects de nommage et d'adressage sur Internet.

**Enveloppe -** Partie des informations entourant les données contenues dans un message ou une trame à des fins de contrôle.

**Epissure -** Opération consistant au raccordement entre deux fibres optiques de façon permanente.

Il existe plusieurs façon de procéder à des épissures :

- Epissure mécanique - Réunion de deux fibres optiques jointes bout à bout par une action mécanique.
- Epissure fusion - Soudure par fusion - Réunion de deux fibres optiques jointes bout à bout, obtenue en ramollissant ou en fondant les extrémités des deux fibres optiques, à l'aide d'une source de chaleur. La qualité de la soudure dépend du bon positionnement des coeurs des deux fibres optiques mises en continuité.

Les épissures « fusion , si elles sont permanentes, donnent de meilleurs résultats dans la durée, et offrent une meilleure tenue dans le temps.

**Equilibre Modal -** Dans une fibre multimode l'état d'équilibre de la lumière est atteint par un mélange de modes après une certaine distance. La répartition d'énergie lumineuse sur les divers modes ne varie plus au delà de cette longueur. En laboratoire afin de s'affranchir de l'emploi de grandes longueurs de fibres, on peut également utiliser des mélangeurs ou des filtres de modes.

**Equipements d'accès WAN -** Centraux téléphoniques publics pour téléphonie fixe bande étroite, plates-formes de réseaux intelligents, commutateurs RNIS, DSLAMs, BAS, Softswitchs voix/données, commutateurs voix/données d'accès, BTS LMDS et CPE LMDS.

**Equipements Data Wan -** Equipements ATM, commutateurs, brasseurs, concentrateurs, équipements X25, équipements Frame Relay, équipements de routage de cœur de réseau IP.

**Equipements LAN -** Equipements pour réseaux locaux et étendus d'entreprise tels que commutateurs (Ethernet, Token Ring, Frame Relay, ATM), modems, multiplexeurs, concentrateurs, routeurs d'agence, passerelles, équipement d'accès distant. Ne sont pas inclus dans ce segment les serveurs et les PABX.

**Equipements terminaux -** Matériel qui permet à l'utilisateur de transmettre, de traiter ou de recevoir des informations (téléphone, fax, modem, etc.).

**Equipements Transmission WAN -** Equipements de multiplexage, répéteurs, amplificateurs, équipements de distribution, de brassage WDM, SDH, PDH et SONET.

**ERC -** European Radiocommunications Committee - Organisme dépendant de la CEPT, chargé de la coopération réglementaire dans le domaine des radiocommunications et dont le bureau permanent est l'ERO (Office européen des radiocommunications).

**Erlang -** Unité de mesure de l'intensité du trafic sur une liaison - Un erlang correspond à l'occupation de la ligne pendant une heure. Cette valeur sert à évaluer l'occupation optimale d'une ligne. Elle résulte d'un calcul multipliant le nombre moyen de communications par la durée moyenne des communications et divisant le tout par la valeur correcte pour obtenir une heure de communication.

Exemple : 80 sites doivent recevoir des données entre 22h00 et minuit. Chaque communication doit durer 3 minutes. Quelle sera la quantité de lignes nécessaire ?

E = (Quantité x durée) / durée exprimée en minutes.

Soit (80x3)/120 = 2 erlang

Il faudra donc deux liaisons pendant 2 heures pour écouler tout le trafic.

Symbole : E.

L'ingénieur danois A.K. Erlang est l'un des pionniers de la théorie du trafic.

**ERMES -** European Radio Messaging System) - Norme européenne utilisée en radiomessagerie, visant à unifier les systèmes de radiomessagerie des principaux pays européens.

**ERP -** Entreprise Ressource Planning - En Français = PGI - Voir PGI - Progiciel de Gestion Intégré - Constitue une solution complète qui couvre la totalité des domaines de l'entreprise où l'informatique est un atout stratégique.

**Escon -** Enterprise Systems CONnection - Canal de communication en fibre optique développé par IBM permettant la communication entre machines distantes, réparties sur de grandes étendues (plus de 60 km), avec un taux de transfert allant de 10 à 17 Mo/s.

**ESSID -** Extended Service Set Identifier - Identifiant de 32 caractères au maximum qui correspond au nom du réseau Wi-Fi.

**Esterel -** Société regroupant la SNCF, les transporteurs aériens français, la SNCM, le Club Méditerranée et le Syndicat des agences de voyages pour fournir à ces dernières un réseau et des terminaux pour la réservation des voyages. Elle utilise Transpac et un réseau privé de commutation baptisé Esterpac.

**Etablissement** (d'une ligne ou d'un circuit) - Mise bout à bout de différents tronçons pour constituer une ligne permanente (ligne spécialisée) ou temporaire (commutée).

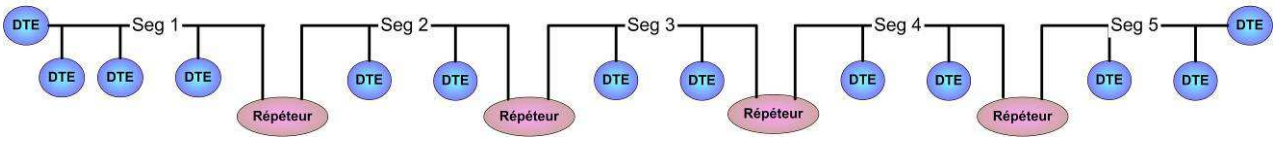
**ETCD -** Equipement de terminaison de circuit de données (en anglais DCTE, Data Circuit Terminating Equipment). Expression qui dans le vocabulaire officiel des télécommunications désigne un appareil adaptant les signaux émis par un équipement terminal aux caractéristiques de la ligne. Exemple : modem.

Un ETCD n'est pas toujours un modem.

**Ethernet -** Réseau local conçu à l'origine par Xerox, DEC et Intel, aujourd'hui normalisé par ISO. Il fonctionne normalement à 10 Mbps par seconde sur un câble coaxial et une topologie en bus. La méthode d'accès utilise un protocole à contention avec détection de collision dit CSMA/CD. Mais il existe aujourd'hui des réseaux de type Ethernet adaptés à d'autres supports (paires torsadées, fibre optique) et à d'autres topologies (étoile notamment).

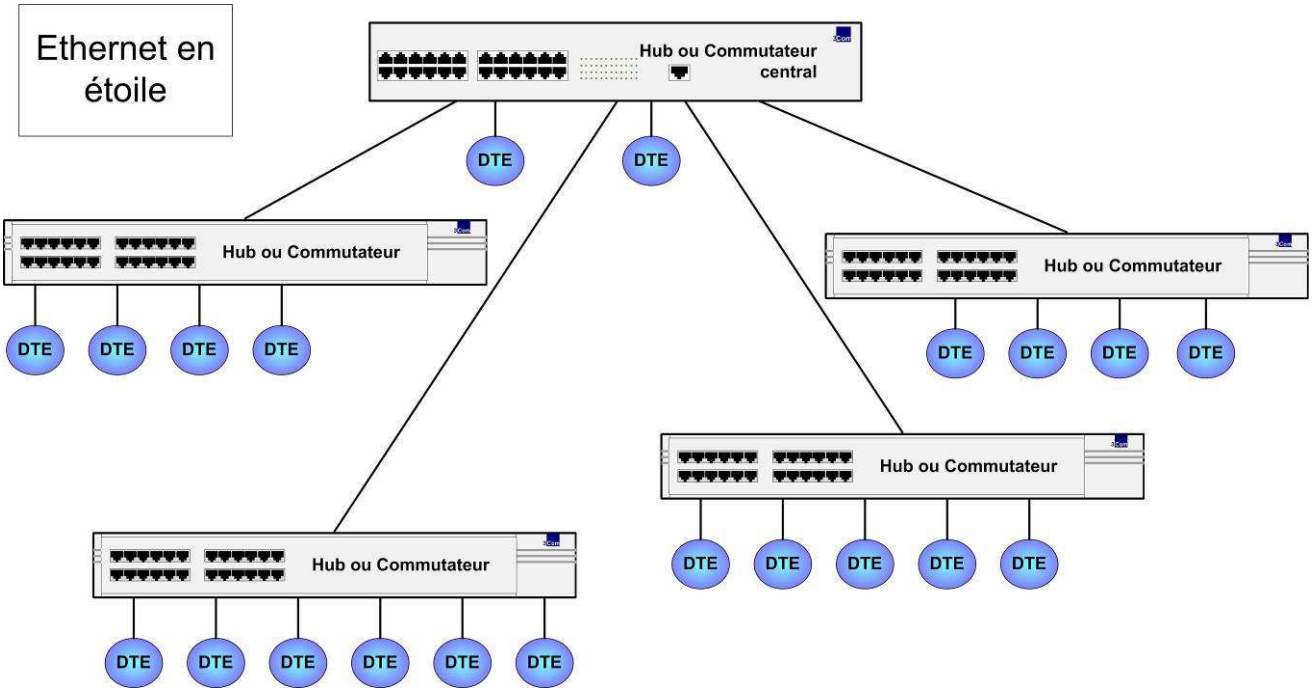
A l'origine, le réseau de l'Ether devait donner naissance à un principe de transmission de données par ondes radio. Le projet fut abandonné au profit d'une longue carrière… dans le filaire.

Ethernet en bus




La vitesse normalisée d'ETHERNET est de 10 Mbit/s. Pour le média, si un câble coaxial particulier avait été défini par la normalisation originale (câble jaune) ,10 Base 5, on trouve aujourd'hui d'autres câbles à meilleur prix, notamment un câble coaxial fin (Thinnet), 10Base 2, et surtout plusieurs solutions de câblage sur paires torsadées téléphoniques, 10 base T. Il existe également une version avec fibre optique appelée 10 Base F. La plus répandue d'entre elles, 10Base T, permet un câblage en étoile, plus facilement administrable. Aujourd'hui cohabite une nouvelle version d'Ethernet qui à une vitesse de 100 Mbit/s, normalisée sous la norme IEEE 802-3u, également appelée FAST ETHERNET. L'accès au média se fait par l'intermédiaire d'un module appelé "transceiver". La longueur d'un segment Ethernet est en 10Base5 de 500m, en 10Base2 de 180m, en 10BaseT de 100m et en 10BaseF de 2000m. Cinq segments maximum peuvent être reliés entre eux. Chaque segment étant relié à l 'autre par un répéteur.

Ethernet en étoile




Trame Ethernet :

Préambule - 7 octets de synchronisation (7 x 10101010)

Délimiteur de début de trame - 1 octet (10101011)

Adresses destinataire et source - Adresses MAC codées sur 6 octets (48 bits)

Longueur de la trame LLC ou type de la trame - Problème de compatibilité

Zone de donnée + Bourrage - Entre 1 et 1500 octets

Contrôle d'erreur - Cyclic Redundancy Code : 4 octets, soit un polynôme générateur de degré 32 appliqué aux champs « adresses », « taille ou type », « donnée + padding »

Quelques points de repères :

Délai inter-trame de 96 temps bits

- 9.600 ms pour un réseau à 10 Mbps

- 0.960 ms pour un réseau à 100 Mbps
- 0.096 ms pour un réseau à 1 Gbps

Fenêtre de collision ou slot-time

Temps d'émission d' une trame de taille minimale
- 512 temps bits pour les réseaux à 10 et 100 Mbps
- 4096 temps bits pour les réseaux à 1 Gbps

Temps d'attente maximal avant retransmission
- 1023 * slot-time = 0.052 secondes pour les réseaux à 10 Mbps
- 1023 * slot-time = 0.0052 secondes pour les réseaux à 100 Mbps
- 1023 * slot-time = 0.0042 secondes pour les réseaux à 1 Gbps

Notions fondamentales :

Segment Ethernet - Deux stations appartiennent au même segment si elles sont connectés directement entre elles par un support de transmission

Domaine de collisions - Deux stations appartiennent au même domaine de collisions si deux trames émises simultanément par ces stations rentrent nécessairement en collision.

Domaine de broadcast - Deux stations appartiennent au même domaine de broadcast si toute trame de broadcasts émise par l'une est reçue par l'autre – Adresse MAC de broadcast = X 'FF-FF-FF-FF-FF-FF

Les réseaux Ethernet 10, 100 et 1000 n'utilisent pas le même codage de transmisssion.

**ETL -** Établissement américain de test et certification.

**ETL -** Extraction Transformation Loading - Système permettant d'extraire et de formater des données dans le but d'alimenter un infocentre.

Outil destiné à l'alimentation d'un entrepôt de données en 3 étapes :

- extraction des données de diverses sources (bases de données de production, fichiers, Internet, etc.),
- nettoyage et transformation des données
- chargement de l'entrepôt de données.

**ETNO -** Association des exploitants de réseaux publics de télécommunications européens ayant un rôle d'instance de coopération entre opérateurs.

**ETS -** European Telecommunications Standard - Norme technique européenne de télécommunications ayant un caractère volontaire. Les ETS sont actuellement mis au point par l'Etsi.

**ETSI -** European Telecommunications Standard Institute - Organisme créé par les administrations des télécommunications des pays européens avec le soutien de la Communauté européenne et chargé de proposer, de discuter et de mettre en œuvre des normes pour le compte de la Cept (Conférence européenne des postes et télécommunications). A son siège en France à Sophia Antipolis.

**ETTD -** Equipement Terminal de Traitement de Données - DTE, Data Terminal Equipement - Expression qui dans le vocabulaire officiel des télécommunications désigne un appareil connecté à un réseau capable de recevoir et/ou d'émettre des données.

Exemple: interface R (adaptation de terminaux analogiques au RNIS, Réseau numérique à intégration de services), interface S (adaptation d'un terminal RNIS à ce réseau), interface T (entre le système de transmission et la distribution interne de l'abonné).

**Eutelsat -** Organisation européenne fournissant des services internationaux, notamment téléphoniques, de communications par satellite.

**Euteltracs -** Service de localisation et de gestion de flottes de véhicules mobiles par satellite (couvre l'Europe, l'Afrique du Nord et une partie du Moyen-Orient).

**Evanouissement -** Diminution momentanée de la puissance d'un signal radioélectrique à l'entrée d'un récepteur. Par extension, variation de la puissance du signal due aux conditions de propagation des ondes. Le terme "fading" a été utilisé en ce sens en radiodiffusion sonore.

**Ewos -** European Workshop for Open Systems - Organisme européen d'étude pour le développement et les spécifications de test de "profils fonctionnels" -superpositions de protocoles des 7 couches du modèle OSI capables d'inter fonctionner réellement. Il est commun aux organisations suivantes: Cen, Cenelec, Cosine, Ecma, Emug, Ositop, RARE et Spag.

**Exigences Essentielles -** Les exigences essentielles sont imposées, par voie de directive européenne, afin de garantir la protection de l'Intérêt Général. Les exigences essentielles sont obligatoires. Seuls les produits conformes aux exigences essentielles peuvent être placés sur le marché et/ou mis en service. Les exigences essentielles doivent être appliquées en fonction des risques inhérents à un produit donné.

**Exploitation -** Ensemble des activités nécessaires pour mettre en œuvre une installation, par exemple un réseau de télécommunication. L'exploitation comprend notamment les manœuvres, commande, surveillance et maintenance, ainsi que des travaux de toutes sortes.

**ExpressCard -** l'ExpressCard a pour objectif d'être plus compacte, plus performante et moins chère à produire que la PCCard CardBus. L'ExpressCard prévoit l'utilisation d'un port relié simultanément au bus PCI Express 1x (2,5 Gbit/seconde) et USB 2.0 (480 Mbit/seconde) sans contrôleur spécifique, ce sera le bus PCI ou USB qui prendra en charge la gestion du périphérique.

A noter que l'ExpressCard sera proposé dans 2 formats ; l'ExpressCard 54 pour les ordinateurs de bureau et L'ExpressCard 34 pour les ordinateurs portables.

**Extensibilité -** Aptitude d'un codeur de son ou d'image à produire un signal numérique dont on peut utiliser une partie plus ou moins grande correspondant à une qualité plus ou moins bonne. L'extensibilité est obtenue par un codage dit hiérarchique.

**Extranet -** Réseau de télécommunication constitué d'un intranet étendu pour permettre la communication avec certains organismes extérieurs, par exemple des clients ou des fournisseurs. Un réseau extranet est un réseau externe utilisant la technologie IP (Internet Protocol). Il permet à une entreprise ou à un organisme d'échanger des informations numériques avec ses principaux correspondants (filiales, clients, fournisseurs, etc.) en bénéficiant de la norme IP pour la transmission des informations et d'une présentation conviviale des informations, le langage HTML autorisant une lecture non linéaire des pages consultées, grâce à l'utilisation de liens hypertexte (on peut passer d'une rubrique à l'autre par un simple "clic" de souris).

# F

**Fac similé -** Fax ou document télécopié.

**Facilité -** Anglicisme pour complément de service.

**Facteur d'amortissement -** Audio - Il révèle de la capacité d'un amplificateur à bien maîtriser l'enceinte acoustique. Un faible pourcentage révèle une bonne maîtrise.

**Facturation pour le compte de tiers -** Service qui permet aux opérateurs entrants de confier à l'opérateur historique la facturation des services qu'ils offrent à leurs clients via l'interconnexion. Dans le cas des services spéciaux, ce service, qui ne peut concerner que les services payants, non les services gratuits pour l'appelant, apparaît comme indispensable à l'exercice d'une concurrence effective, en raison du développement de ce marché.

**Fading de proximité -** Embouteillage, feu rouge... c'est toujours à ce moment que l'autoradio décide de museler le doux babil de Philippe Meyerglosant sur la modernité de notre époque. Il est victime du fading de proximité, ou "opposition de phase provoquée par une réflexion".

Tout signal radioélectrique est rayonné selon un plan horizontal (antennes de type "râteau" des télés) ou vertical ("fouets" des émetteurs en ondes courtes). De l'émetteur au récepteur, l'onde croise des obstacles. Dans certains cas, ces écueils font "rebondir" l'onde. Le récepteur va donc recevoir un signal accidenté en retard de phase ou rotation de polarisation. Dans le premier cas, une partie de l'information radio ayant pris un "retard" certain par rapport à une autre ayant trouvé un signal plus direct va venir se "soustraire" au "bon" signal proportionnellement au décalage de phase constaté à l'arrivée. Cette opposition de phase peut aller jusqu'à l'extinction du signal. Dans le second cas, la polarisation verticale ou horizontale, caractérisée par l'antenne d'émission, sera "infléchie": elle risque de parvenir avec un angle fantaisiste... parfois à 90' de l'origine (cas le plus défavorable). Pour éviter cela, les AP (Points d'accès Wi-Fi) disposent de deux antennes, distantes de quelques centimètres et recevant les signaux directs ou réfléchis. Cette double réception permet, après comparaison de phase et sommation, de s'affranchir des signaux retardataires et destructeurs. En outre, les antennes étant parfois articulées, l'une à 90' par rapport à l'autre, on réalisera cette comparaison pour choisir la polarisation la plus favorable en un point particulier. Reste enfin OFDM, qui effectue, sur le signal reçu, un traitement de comparaison/ reconstitution éliminant les derniers miasmes créés par ces rebonds.

**FAH -** Fournisseur d'Applications Hébergées - ASP (Application Service Provider) - Prestataire de service qui loue sur son site des applications de tout type aux entreprises, accessibles par Internet.

**FAI ou ISP -** Fournisseur d'Accès à Internet - Internet Service provider - Société proposant des abonnements à Internet. Les FAI proposent souvent en **complément** de l'accès des services complémentaires (news, portail, messagerie, proxy cache,…).

**Faisceau -** Terme utilisé en imagerie, endoscopie et transport de lumière. Un faisceau est un assemblage ordonné ou non de fibres.

**Faisceau hertzien -** Liaison par radio à très haute fréquence. Utilisé pour transmettre des émissions de télévision ou de radio, quelquefois pour le téléphone dans des régions difficiles d'Accès ou en secours du réseau terrestre, encore assez rarement pour les données.

Ne fonctionnant qu'en ligne droite et nécessitant des pylônes de relais pour être en "vue directe" entre émetteur et récepteur (ou entre émetteur et relai), la portée (distance entre émetteur et récepteur) dépend de la puissance, de l'environnement, de la météo, de la fréquence utilisée et des antennes. L'utilisation de relai d'amplification permet d'accroitre la portée.

Mode de transmission par ondes radioélectriques dans la gamme des ondes centimétriques (gigahertz). Ces ondes sont transmises en ligne droite entre deux points en vue optique, à partir d'antennes montées sur des tours ou pylônes.

**Fanion -** Flag - Séquence particulière de bits servant à délimiter des trames. Dans la procédure HDLC, le fanion est la suite des huit bits 01111110.

**FAQ -** Frequently Asked Questions - On l'appelle aussi Foire Aux Questions. Document qui répertorie les questions souvent posées par les usagers d'un service.

**Farad -** Unité de mesure de capacité. Le farad, du nom du physicien Michael Faraday, est l'unité dérivée de capacité électrique du système international (SI).

Le Farad est la capacité d'un condensateur électrique entre les armatures duquel apparaît une différence de potentiel de un volt lorsqu'il est chargé d'une quantité d'électricité de un coulomb.

**Fast Ethernet -** Désigne un réseau Ethernet 100 BASE TX à 100 Mbits. Voir Ethernet et 100 Base T.

**Fast Packet Switching -** Commutation de paquets rapide - Bien que l'expression soit une marque déposée du principal fournisseur de cette technologie, l'américain Stratacom, le Fast Packet désigne une famille de techniques cherchant à marier les avantages de la commutation de circuits et de la commutation de paquets, du multiplexage en fréquence et du multiplexage temporel. Ces techniques combinent commutation à haute vitesse, gestion statistique de la largeur de bande et prise en compte de trains de données de longueurs très variables. Font partie de cette famille: le Frame Relay, DBDQ et l'ATM.

**Fast TCP -** Des chercheurs de l'université de Pasadena (Californie) ont développé une variante du protocole TCP censée démultiplier les débits sur Internet. Fast TCP implique des modifications logicielles et matérielles au niveau des PC, sans remettre en cause les infrastructures Internet existantes. La technique des chercheurs consiste à mesurer le temps que les paquets mettent pour arriver à leur destination, et à ajuster le débit en fonction de ce qu'est capable de supporter la liaison Internet.

**Fausse positive -** (anti-spam) - Alerte ou action qui bloque involontairement un courrier "utile". Son défaut: il suffit d'une seule erreur pour annuler tous les bienfaits de la solution anti-spam elle-même.

**FC -** Fibre Channel - Norme de transmission de données en mode série standardisée par l'ANSI, développée sur les spécifications SCSI-3, et utilisée pour le stockage. Fibre Channel est caractérisée par la forte bande passante garantie délivrée (de 266 Mbit/s à 4,24 Gbit/s selon les générations) sur support physique de cuivre ou fibre optique et sur des distances pouvant atteindre 10 km.

La norme utilise un protocole de transmission respectant le codage 8B 10B (détection et contrôle d'erreur, synchronisation) et un contrôle de flux de deux type : bout en bout et/ou mémoire à mémoire, en fonction de la classe de service négociée.

**FC Fabric -** Matrice FC - Type d'architecture Fibre Channel utilisant un ou plusieurs commutateurs.

**FC-AL -** Fiber Channel Arbitrated Loop - Type d'architecture Fibre Channel où les composants (jusqu'à 126) sont connectés en boucle et partagent la même bande passante. Le débit peut aller jusqu'à 100 Mbit/s en utilisant de la fibre optique.

**FCC -** Federal Communications Commission - Organisme administratif déterminant la réglementation et la tarification des télécommunications américaines.

**FCS -** Frame Check Sequence - Code de détection d'erreurs ajouté à une trame. Le Frame Check Séquence est utilisé pour contrôler que la trame à été reçue sans erreurs et consiste en deux octets contenant un code cyclique redondant utilisant le polynôme générateur de l'UIT-T.

**FDDI -** Fiber Distributed Data Interface - Norme de transmission pour constituer des réseaux locaux ou des interconnexions de réseaux locaux en fibre optique, donc ultra-rapides : spécifie un double anneau fonctionnant à 100 Mbps.

Elaborée par le groupe de travail X3T9.5 de l'ANSI au début des années 80 et reprise par l'ISO sous la référence ISO 9314. Ses caractéristiques générales définissent des réseaux en double anneaux sur une infrastructure en fibres optiques multi modes qui offrent des débits de 100 Mbps sur une distance maximale de 100km (technique LAN et MAN). FDDI peut supporter jusqu' à 1000 nœuds distants de plus 2 km chacun. Deux versions sur paires torsadées offrent un débit de 100 Mbps avec des distances inter-nœuds d'au plus 100m : TPDDI (Twisted Pair DDI) et CDDI (Cooper DDI (cuivre)).

Architecture Protocolaire :

Couches et protocoles définis.

Une couche Physique scindée en deux sous-couches :

- la sous-couche PMD (Physical Medium Dependant) couvre la génération et la réception des signaux sur les supports et précise les types de connecteurs et câbles à utiliser.
- la sous-couche PHY (PHYsical Layer Protocol) décrit l'interface permettant à la sous-couche MAC supérieure de transmettre et recevoir des trames et les techniques de codage utilisées pour transmettre les données

Une sous-couche MAC pour la couche Liaison : Définie une technique de contrôle d'accès base sur la circulation d'un jeton (comme pour Token-ring) et peut être utilisée au-dessous de la sous-couche LLC définie par la norme ISO 8802.2

Une couche ou protocole SMT (Station ManagemenT) a cheval sur les couches Physique et Liaison et chargée de la gestion de l'anneau (initialisation, reconfiguration en cas de panne, insertion ou retrait de stations).

Aspects Physiques :

Fibres optiques multi modes 62.5-125 microns (cœur gaine) à la longueur d'onde de 1200 nm (alternatives : fibres 50-125 ou 82.5-125)

Raccordement au double anneau FDDI Double pour les nœuds a double attachement (DAS = Dual Attached Station) reliées aux 2 anneaux Simple pour les nœuds a simple attachement (SAS = Simple Attached Station) reliées uniquement a l'anneau primaire du double anneau FDDI

Techniques de codage :

Technique de double codage : A toute séquence de 4 bits, on associe d' abord une séquence de 5 bits afin d'assurer la présence de transitions (codage 4B5B). On utilise ensuite un code NRZI (Non Return To Zero Inverted) (sans changement d'état pour la transmission d'un bit à 0 et alternativement positif et négatif pour la transmission d'un bit à 1. Cette technique de codage en deux phases ne requiert qu'une rapidité de modulation de 125 Mbauds.

Méthode d'accès :

Principes du protocole du jeton temporisé, proche de la méthode d'accès Token-ring. Pour transmettre des données, une station doit posséder le jeton unique circulant sur l'anneau. De même, chaque station est chargée de retirer les données qu'elle a déposées dans l'anneau.

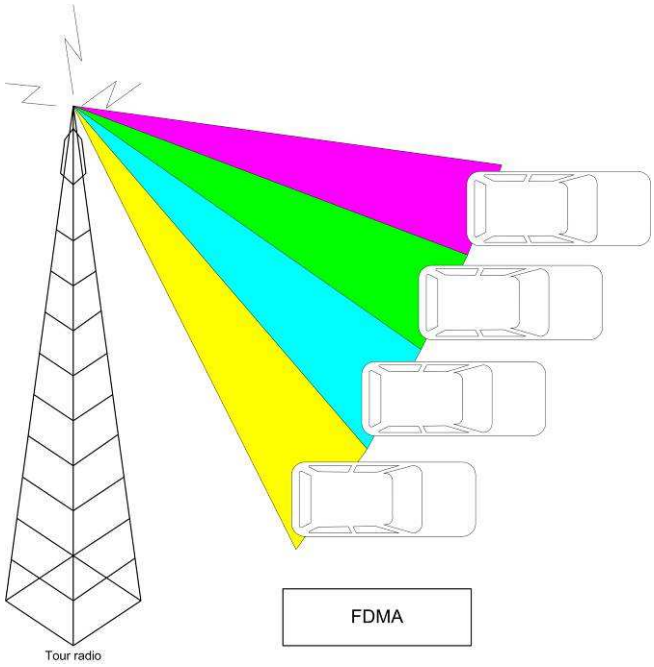
Différences par rapport à Token-Ring : Quand une station a fini de transmettre des données, elle n'attend pas leur retour pour transmettre le jeton (pour pallier à des temps d'attente trop longs). Les données sont séparées en deux classes de trafic :

- Classe synchrone : garantie à chaque station l'utilisation d'une fraction donnée de la bande passante offerte par le réseau (à chaque passage du jeton)
- Classe asynchrone : permet d'allouer sur demande de la bande passante synchrone non utilisée (si le jeton arrive en avance par rapport aux attentes)

Pas de station monitrice spécifique, chaque station d'un réseau FDDI participant à la surveillance de l'anneau Une transmission continue de symboles IDLE (en absence de jeton et données) permet de contrôler le bon fonctionnement des liaisons entre stations.

**FDM -** Frequency Division Multiplexing - Voir multiplexage en fréquence.

**FDMA -** Frequency Division Multiple Access - Voir UMTS - Technique de multiplexage d'information utilisant la division de fréquence. Chaque récepteur dispose de sa fréquence divisée.




**FEC -** Forwarding Equivalence Class - Désigne un groupe de paquets IP acheminés de la même manière, en suivant le même chemin avec les mêmes traitements d'acheminement.

**FECN -** Forward Explicit Congestion Notification - Bit situé dans l'entête de trame initialisé par un commutateur pour avertir le destinataire que la trame qu'il va recevoir a subi des problèmes de congestion.

**Femtocell -** Téléphonie Mobile 3G - Ce terme désigne un équipement radio de type CDMA permettant d'améliorer la couverture radio des réseaux 3G.

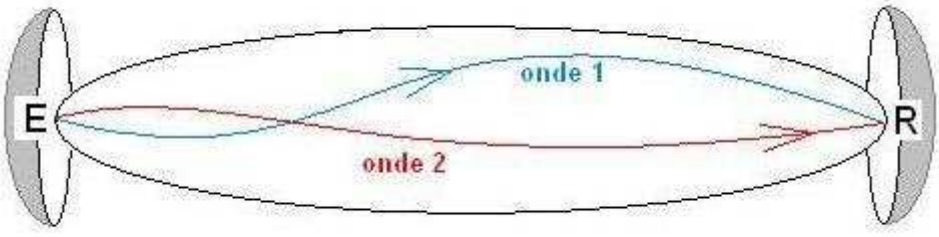
Ces équipements, souvent dédiés à un usage domestique, pemettent d'améliorer la couverture radio indoor des réseaux 3G des opérateurs mobile. Ils supportent quelques utilisateurs (moins de 5 utilisateurs simultanés très souvent) et existent dans des versions CDMA (3G) et HSDPA / HSUPA (3,5G). Ils fonctionnent dans les même bandes de fréquences que les réseau 3G actuels (2,1 GHz).

Les communications « portées » par ses boitiers sont facturées par les opérateurs au même titre que les appels passés sur une infrastructure opérateur mobile.

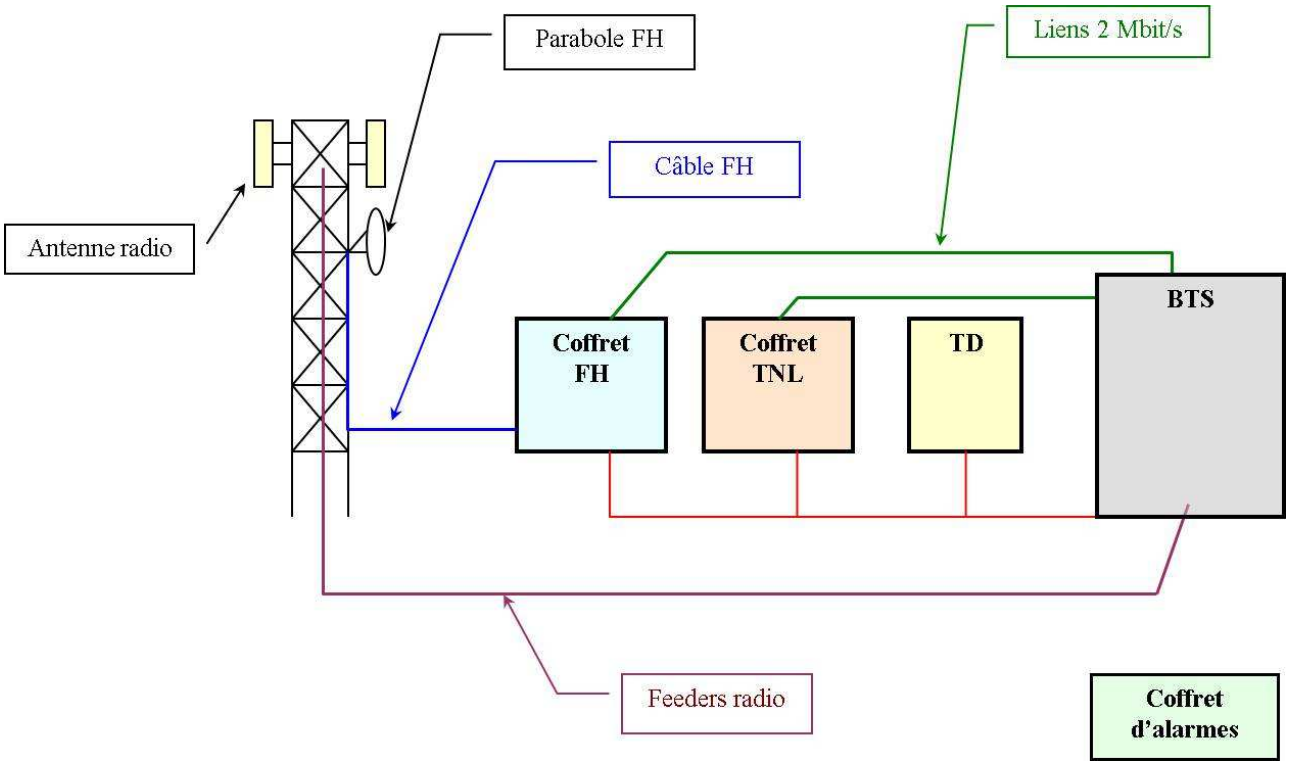
**Fenêtre optique -** La fenêtre optique est une zone du domaine des longueurs d'onde optiques pour laquelle la fibre optique présente des affaiblissements faibles. Il existe trois fenêtres utilisées: 850 nm, 1300 nm et 1550 nm.

**FH - Faisceau Hertzien -** Système de transmission sans fil utilisé pour transmettre en vue directe des données d'un point A a un point B en utilisant un faisceau radio.

un faisceau hertzien est une liaison haute fréquence "point à point " destinée à véhiculer sur une porteuse harmonique un signal analogique ou un signal numérique, enfermé dans un ellipsoïde de Fresnel.




Ce type de transmission est très utilisé dans les opérateurs mobile notamment pour assurer la liaison le raccordment des sites radios avec le cœur de réseau.




Exemple de mise en œuvre d'une liaison tyupe FH dans le cadre d'une installation de téléphonie sans fil.

**FHSS -** Technologie à étalement du spectre à saut de fréquence - Transmission radio au sein de la bande de fréquence des 2,4 GHz sans licence. La technologie FHSS est limitée à un taux de transfert de 2 Mbit/s et uniquement recommandée pour des applications très spécifiques telles que celles que l'on utilise sur les navires. Pour toutes les autres applications LAN sans fil, la technologie DSSS est le meilleur choix.

**Fibre à gradient d'indice -** Fibre optique ayant un profil d'indice à gradient.

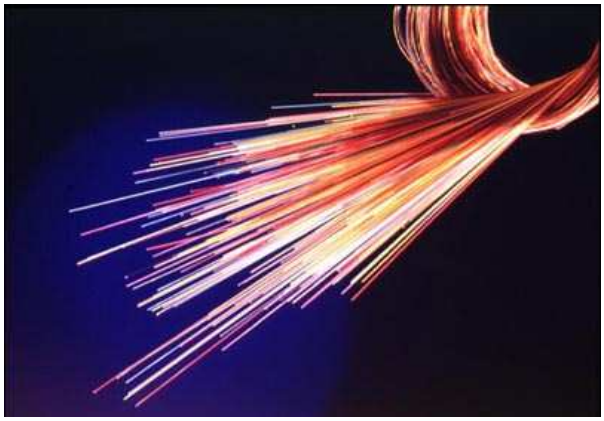
**Fibre à maintien de polarisation -** Fibre optique dans laquelle on maintient la polarisation. Utilisée dans les applications de capteurs.

**Fibre Noire -** Désigne, dans un câble à fibres optiques posé, une fibre non munie d'organes d'émission-réception. Par opposition, on dit d'une fibre qu'elle est "éclairée" lorsque celle-ci est raccordée à des équipements.

**Fibre Optique -** Câble généralement fait de silice, capable de véhiculer des signaux sous forme lumineuse.

Guide d'onde optique en forme de filament,composé de substances diélectriques.

Filament de silice ou de matière plastique permettant de transporter un rayonnement optique. Dans les fibres optiques multimodes à diamètre relativement élevés, plusieurs modes de propagation ne permettent pas des délais aussi élevés que dans les fibres optiques monomodes qui ont un coeur en verre très fin et qui ne permettent qu'un seul mode de propagation leur donnant un débit très élevé.



La fibre s'impose dès qu'il faut allier haut débit (gigabit) et distance (plusieurs centaines de mètres voire des kilomètres). Entre autres qualités, la fibre a les atouts suivants : la qualité de transmission en milieu perturbé (la fibre ne véhicule que de la lumière, pas de courant), les coûts en cas de croissance rapide du trafic (pas besoin de recâblage) et la sécurité (toute dérivation entraîne une perte de puissance facile à détecter).

Depuis plus de cent ans, TYNDALL a montré comment, dans une fontaine lumineuse, un faisceau de lumière pouvait être guidé dans un milieu transparent. Il suffit qu'un deuxième milieu, d'indice de réfraction inférieur, entoure le premier milieu. La lumière se réfléchit alors à la surface de séparation des deux milieux, c'est la réflexion totale, bien plus parfaite que la réflexion sur une surface métallique.

Les deux phénomènes principaux dans la transmission optique sont les phénomènes de réfractions à l'introduction de la lumière dans la fibre et les phénomènes de réflexion entre le coeur et la gaine. Lorsqu'un faisceau lumineux heurte obliquement la surface qui sépare deux milieux plus ou moins transparents, il se divise en deux : une partie est réfléchie tandis que l'autre est réfractée, c'est à dire transmise dans le second milieu en changeant de direction. L'indice de réfraction est une grandeur caractéristique des propriétés optiques d'un matériau. Il est obtenu en divisant la vitesse de la lumière dans le vide (Cv=299 792 Km/s) par la vitesse de cette même onde dans le matériau.

La demande en bande passante générée par l'augmentation exponentielle des données et les progrès réalisés dans le domaine des composants optroniques ont accéléré les mutations technologiques et laissent entrevoir de beaux jours aux entreprises spécialisées dans les équipements destinés aux réseaux de fibre optique.

En effet, parallèlement aux progrès des fibres optiques de silice, les composants optoélectroniques ont permis de mettre en œuvre des systèmes de transmission de plus en plus performants en terme de portée maximale, de débit d'information et de fiabilité.

Ces composants appelés composants d'extrémité sont d'une part des sources émettrices de lumière (DEL : diode électroluminescente ou DL: diode à laser), d'autre part des photos détecteurs.

Les fibres Multimode, si elles sont moins coûteuses que les fibres monomodes, sont en contrepartie plus limitées en terme de distance, notamment lorsque l'on monte en débit. Les nouvelles fibres OM3 en cours de définition et de normalisation par l'ISO/ IEC devraient changer cela. Elle est de type 50 (diamètre au cœur de la fibre en microns) /125 (diamètre extérieur) comme la fibre OM2. En utilisant une longueur d'onde de 850 ns, de nouvelles fibres optiques ont atteint la vitesse de 10 Gbits/seconde sur une distance de 300 m ou 1 Gbit/seconde sur 1 Km.

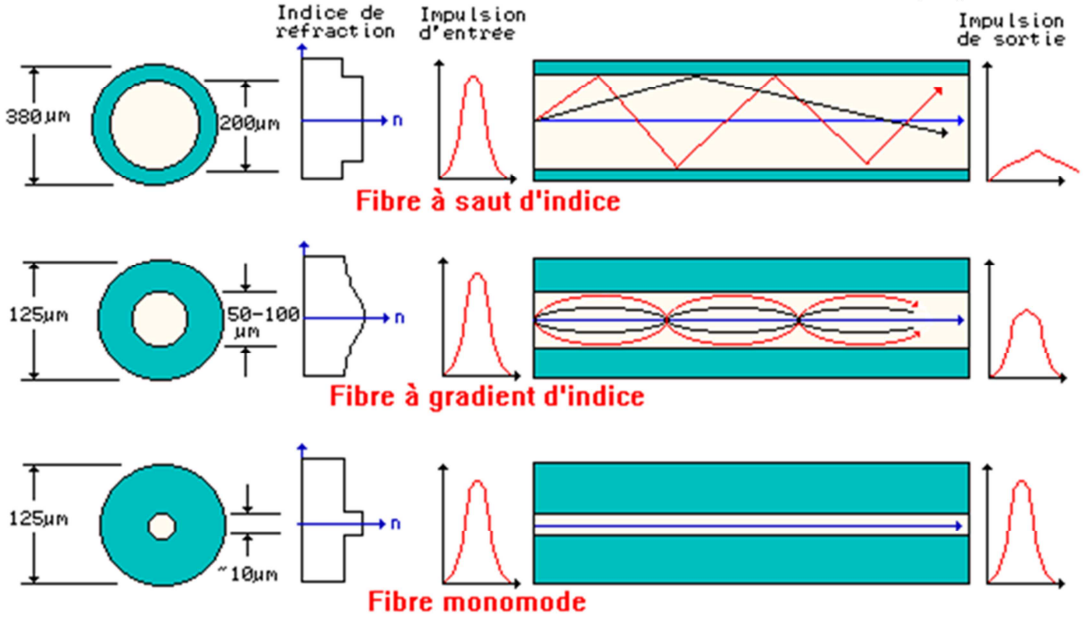
Grâce à ces performances, la fibre commence également à supplanter le câble dans les réseaux d'entreprises. Notamment avec l'arrivée de l'Ethernet rapide avec le futur standard 10 Gbit Ethernet (10GE).

| Limites de distance maximale pour les transmissions Ethernet à haut débit sur fibre optique (limites définies en 2002) | | | |
|---|---|---|---|
| Type de Fibre | Ethernet 100 Mbit/seconde | Ethernet 1 Gbit/seconde | Ethernet 10 Gbit/sec. |
| Monomode (OS1) cœur 50 µm | 2000 m | 2000 m | 2000 m |
| Multimode (OM1) Cœur 50 ou 62,5 µm | 2000 m | 300 m | N/A |
| Multimode (OM2) Cœur 50 ou 62,5 µm | 2000 m | 500 m | N/A |
| Multimode (OM3) Cœur 50 µm | 2000 m | 500 m | 300 m |

Code couleur et numérotation des fibres :

Modulo 12 :
1 = Rouge
2 = Vert
3 = Bleu
4 = Jaune
5 = Blanc
6 = Gris
7 = Marron
8 = Violet
9 = Turquoise
10 = Noir
11 = Orange
12 = Rose

Modulo 24 (de 13 à 24) :
13 = Jaune + marquage
14 = Blanc + marquage
15 = Gris + marquage
16 = Turquoise + marquage
17 = Orange + marquage
18 = Rose + marquage
19 = Jaune + marquage
20 = Blanc + marquage
21 = Gris + marquage
22 = Turquoise + marquage
23 = Orange + marquage
24 = Rose + marquage




- Avantages : débits très important sur des distances très importantes, insensibilité aux perturbations électromagnétiques
- Inconvénients : installation et mesures complexes
- Utilisation : backbone de réseaux, réseau structurant, réseau nationaux et internationaux
- Débit : quelques dizaines Mbits/s jusqu'à 10 Gbits/s sur une distance très longue

Terminologie :

- Axe de la fibre : Lieu géométrique des centres du coeur le long d'une fibre optique.
- Centre du coeur : Dans une section droite d'une fibre optique, centre du cercle qui s'ajuste le mieux avec la limite extérieure de la zone de coeur. Le centre du coeur peut être différent dans une même section droite, des centres de la gaine et de la surface de référence.
- Centre de la gaine : Dans une section droite d'une fibre optique, centre du cercle qui s'ajuste le mieux avec la limite extérieure de la gaine. Le centre de la gaine peut être différent dans une même section droite, des centres du coeur et de la surface de référence..
- Coeur - Région centrale d'une fibre optique dans laquelle la plus grande partie de l'énergie rayonnante est transmise.
- Diamètre du coeur : Diamètre du cercle qui définit le centre du coeur.
- Diamètre de la gaine : Diamètre du cercle qui définit le centre de la gaine.
- Domaine de tolérance du cœur : Dans une section droite d'une fibre optique, région comprise entre le cercle ayant pour centre le centre du coeur qui est circonscrit à la zone de coeur et le plus grand cercle concentrique premier qui peut être inscrit dans la zone de coeur.
- Domaine de tolérance de la gaine Dans une section droite d'une fibre optique, région comprise entre le cercle ayant pour centre le centre de la gaine qui est circonscrit à la gaine et le plus grand cercle concentrique au premier qui peut être inscrit dans la gaine.
- Erreur de concentricité coeur 1 gaine - Pour une fibre optique multimodale, rapport de la distance entre le centre du coeur et le centre de la gaine au diamètre du coeur. Pour une fibre optique unimodale, rapport de

la distance entre le centre du coeur et le centre de la gaine. Toutefois il est plus intéressant de considérer la concentricité 2 wo / centre de la gaine.

**Fibre optique dédiée -** Chemin continu en fibre optique, compris entre le point de mutualisation et la prise optique, mis à disposition d'un opérateur de façon permanente, que celui-ci fournisse ou non un service à l'utilisateur final concerné.
D'un certain point de vue, on peut considérer que toutes les fibres installées depuis le point de mutualisation et vers les abonnés sera dédié, puisque le cheminement de la fibre court du point de mutualisation à la prise optique installée dans le logement de l'usager.

**Fibre optique partagée -** Chemin continu en fibre optique, compris entre le point de mutualisation et la prise optique, mis à disposition d'un opérateur, pour ce qui est nécessaire à la fourniture effective de services de communications électroniques à l'utilisateur final concerné.
La liaison fibre est dédiée à l'usager mais les opérateurs commerciaux devront la « partager » pour pouvoir offrir leurs services aux usagers.

**Fibre Optique Monomode -** Voir Monomode

**Fibre Optique Multimode -** Voir Multimode

**Fibre plastique** - Fibre optique dont le coeur et la gaine sont entièrement en matières plastiques.

**Fibre de silice gainée de plastique - Fibre silice / plastique -** Fibre optique dont le coeur est en silice et la gaine en matières plastiques (PCS - HCS).

**Fibre toute silice -** Fibre optique dont le coeur et la gaine sont entièrement en silice.

**Fibre préconnectorisée -** Fibre optique dont l'une au moins des extrémités est équipée d'un connecteur. Son utilisation permet d'éviter des opérations de soudure. Par extension, on parle de câble en fibre optique préconnectorisé ou encore de pigtail, bin que le terme pigtail soit plus souvent utilisé pour décrire des demi jarretières optiques.

**FIFO -** First in First out - Mode de gestion des files d'attente où le premier message arrivé est aussi le premier transmis.

**Filterspec -** Fonction définissant l'ensemble de paquets de données devant bénéficier de la qualité de service et servant à fixer les paramètres du système de classification des paquets.

**Filtrage -** Recherche dans le trafic réseau de certaines caractéristiques, telles que l'adresse source, l'adresse de destination ou le protocole, afin de déterminer, selon les critères définis, si le trafic de données concerné est accepté ou bloqué. Filtrage de paquets = Mécanisme de contrôle paquet par paquet du trafic routable.

**Filtre -** Splitter - Voir ADSL - Ce dispositif a pour but de séparer les fréquences de la téléphonie analogique et son signal dit POTS des fréquences xDSL. Pour cela il agit comme passe-haut pour le signal xDSL et comme passe-bas pour le signal POTS. Sur une ligne DSL il y a un filtre des deux côtés, chez l'utilisateur mais aussi dans le répartiteur. Ces filtres côté NRA sont à la charge de France Telecom.

**Fips -** Programme destiné à la division non destructrice de partitions de disques durs. Pour ce faire, il s'appuie sur les interruptions Bios.

**Firewall -** Garde barrière - coupe-feu - pare-feu - Système de protection des serveurs privés. Il interdit que des intrus se connectent. Ce système "filtre" les données entrantes et sortantes et intervient en couches 3 et supérieures du protocole ISO. Le rôle du Firewall est de :

- Restreindre l'accès à certains réseaux
- Empêcher les attaquants de se rapprocher des autres mesures de défenses
- Empêcher les utilisateurs de quitter les zones sécurisées.

Il existe trois grandes familles de Firewall :

- Firewalls à liste de contrôle d'accès (ACL Firewall). Un firewall peut effectuer des translations d'adresses, mais ne se limite pas à cela. Il utilise aussi des listes de contrôle d'accès (ACL). Le firewall inspecte chaque paquet entrant de niveau 3 et prend la décision de le transférer au réseau interne ou de le détruire. Le système de filtrage de paquet routent les paquets entre les hôtes internes et externe mais le fait de manière sélective. Il autorise ou bloque les paquets suivant la politique de sécurité du site.
- Les services mandataires. Ce sont des applications spécialisées qui tourne sur le firewall ou un équivalent (serveur proxy) ayant accès à Internet. Ces programmes s'introduisent dans le modèle client serveur est font d'intermédiaires.
- Firewalls à inspection d'état (Stateful Firewall). Un firewall à inspection d'état va au-delà des fonctionnalités d'un simple firewall. L'IOS Stateful Firewall de Cisco permet d'inspecter dynamiquement chaque paquet de niveau 4. Il piste tous les trafics qui utilisent des ports dynamiques comme FTP et garde en mémoire les flux autorisés. Les protocoles standards, tels que HTTP, HTTPS, SMTP, FTP et DNS sont inspectés, ce qui permet de contrôler les applets Java et de les bloquer si nécessaire. Un firewall à inspection d'état protège également des attaques de déni de service (DoS), lorsqu'une personne malintentionnée essaie de surcharger un réseau ou un serveur Web local en envoyant de multiples demandes invalides. Cette technologie reprend le filtrage de paquet et le proxying en y ajoutant le désencapsulage des paquets jusqu'au niveau 7 et l'introduction dynamique de règles de retour.

**FireWire -** ou IEEE 1394 dans le monde PC ou i.LinK chez Sony - Protocole de transmission de données. Grâce à ses transferts à haut débit 400 Megabits par secondes (Mbps) et maintenant 800 Megabits par secondes (Mbps) et à ses capacités Plug & Play à chaud, FireWire est l'interface idéale des équipements vidéo et audio numériques actuels, mais aussi des disques durs externes et d'autres périphériques haute performance. Il donne la possibilité de gérer simultanément jusqu'à 63 périphériques.

**Firmware -** Logiciel résidant en ROM. Le firmware est entre le hardware et le software. Il est principalement utilisé pour contrôler directement le matériel et fourni par la firme qui fabrique ce matériel. Exemple type : un driver de périphérique intégré.

**FLO -** Forward Link Only - Standard propriétaire de Qualcomm. Protocole de diffusion concurrent du DVB-H aux Etats-Unis. Utilisant le spectre UHF, avec une bande de fréquence de 6 MHz sur le canal UHF 55 (716-722 MHz.

**Flow-based -** Technique propriétaire de commutation qui consiste lorsqu'elle reçoit un flux de données à n'analyser que le premier paquet afin d'y trouver l'adresse de destination. Le reste des paquets étant acheminés vers celle-ci sans autre analyse.

**Flowspec -** Fonction définissant la qualité de service fournie à un flot de données et servant à fixer les paramètres de la fonction d'ordonnancement des paquets respectant cette qualité de service.

**FM -** Frequency Modulation - Modulation de fréquence.

**FNF -** Fichier National des Fréquences

**FOIRL -** Fiber Optic Inter Repeater Link - Méthode de signalisation pour des transmissions sur fibre optique.

**Forfait illimité -** Désigne une offre d'accès à Internet par le réseau téléphonique commuté, illimité en temps de connexion avec une tarification forfaitaire pour l'abonné final.

**Forum -** Service permettant discussions et échanges sur un thème donné : chaque utilisateur peut lire à tout moment les interventions de tous les autres et apporter sa propre contribution sous forme d'articles

**Fourreau -** Tube en PVC ou PEHD (polyéthylène haute densité) à la fois, solide, étanche est assez souple pour être enterré et constituer l'infrastructure passive des réseaux enterrés.

**Fournisseur d'accès -** Organisme offrant à des clients d'accéder à l'internet, ou, plus généralement, à tout réseau de communication.

**Fournisseur de service -** (Téléphonie mobile) - Entreprise affiliée à un opérateur réseau qui fournit des services de téléphonie mobile à ses clients.

Personne physique ou morale qui fournit un ou plusieurs services aux utilisateurs d'un système de télécommunication.

Les services offerts peuvent être : la fourniture de compléments de service / les forums / les messageries / la fourniture de contenu / l'hébergement de contenu / l'accès à un réseau de télécommunication...

**FPLMTS -** Future Public Land Mobile Telecommunications Systems - Projet de l'UIT qui constitue la troisième génération de communications mobiles (après l'analogique et le numérique). Appelé aussi IMT 2000.

**FRAD -** Frame Relay Access Device - Equipement d'accès à un réseau Frame Relay (relay de trame).

**Frame -** Terme anglo-saxon équivalent de trame.

**Frame Relay -** Frame Relay est en fait un protocole réseau de télécommunication de niveau 2 qui permet de véhiculer des trames de données de formats variables (de 262 à 4096 octets de données utiles) sur des réseaux partagés offrant des débits de 64 Kbits/s à 40 Mbits/s.

Frame Relay utilise la couche 2 du modèle OSI (niveau trame) .La gestion dynamique de la bande passante permet une meilleure gestion des rafales de trames envoyées par les réseaux locaux. Son principal intérêt est d'offrir de la bande passante à la demande (bandwidth on demand) à l'usager par le biais du multiplexage statistique. Il est transparent aux protocoles, il permet de véhiculer des flux tels que : SNA, X.25, IP, IPX... mais est aussi capable de transporter de la voix.

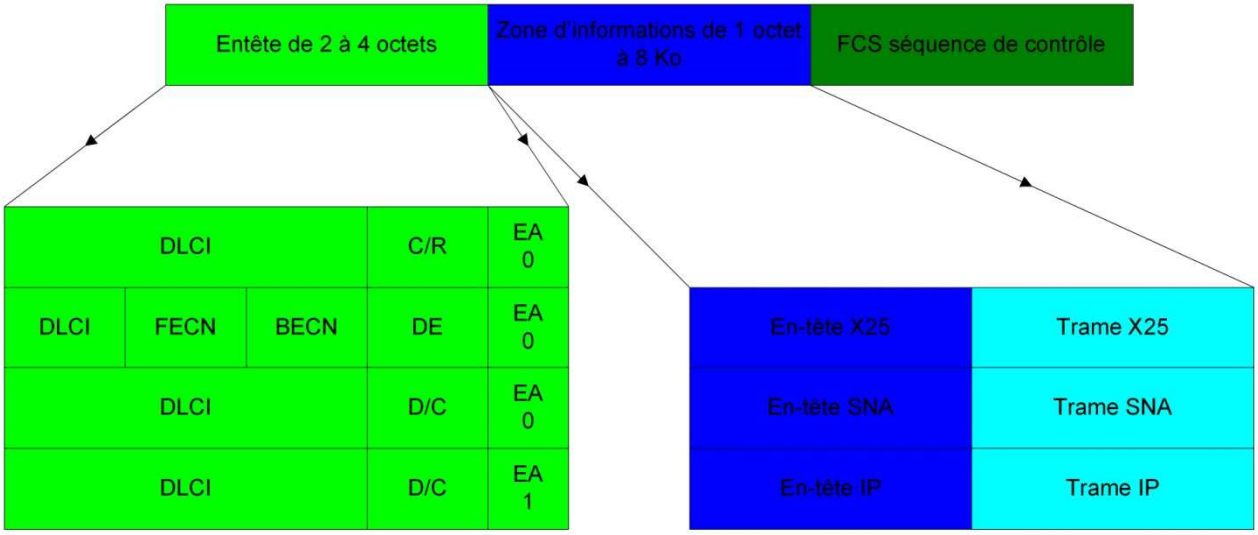
Né en 1991 outre-Atlantique, on pensait au départ que ce protocole de relais de trames (de l'expression anglaise Frame Relay) servirait de technologie de "relais" en attendant que s'impose partout la technologie ATM. En fait, il s'est imposé discrètement et sûrement dans les réseaux d'entreprises et dans les services des opérateurs. De plus, il a évolué: conçu au départ pour transporter les données, il peut aussi transporter la voix.

C'est le côté pertinent du protocole qui a fait son succès. Pertinent, parce qu'il est arrivé au moment où les utilisateurs avaient besoin de débits beaucoup plus élevés que ce que ne leur offrait, en France tout du moins, la technologie X25. Pertinent aussi parce que les débits proposés (2 Mbits/s) convenaient à leurs besoins réels contrairement aux débits surdimensionnés (155 Mbits/s et plus) de l'ATM. Pertinent enfin, car il est arrivé dans un environnement réseau hautement fiable, donc prêt à accueillir un protocole déchargé en grande partie des fonctions de contrôle d'erreurs et de flux qui sont le propre du protocole X25. Ainsi allégé, le relais de trames a pu se concentrer sur la vitesse de traversée des données dans le réseau, vitesse devenue un véritable besoin dans l'interconnexion de réseaux locaux.

Par rapport à X25, on estime que le gain en vitesse de commutation est de l'ordre de 5 à 10. Et si l'on admet que le temps de commutation est égal au temps d'émission sur le lien, alors le gain de performance vis à vis de X25 peut être environ de 10. Cette rapidité tient au fonctionnement du protocole mais aussi au fait que l'essentiel des mécanismes de contrôle et de reprise sur erreur est confié aux équipements émetteurs et destinataires (FRAD et routeurs).

Contrairement à X25, obligé de segmenter à tous crins les données en paquets dés le départ pour des raisons de contrôle, le relais de trames les découpe en trames beaucoup plus longues que les paquets X25 (jusqu'à 8 Ko) et de longueurs variables. Cela permet d'acheminer un plus gros volume d'information plus rapidement, et ce, qu'il s'agisse de trames Ethernet, X25, SNA ou de paquets IP. L'encapsulation de ces protocoles est réalisée par les FRAD (BSC, SNA, X25) et par les routeurs (IP, IPX).

Le relais de trames fonctionne en mode connecté par le biais de circuits virtuels permanents, établis entre la source et le destinataire. Les trames sont indépendantes les unes des autres, mais elles partagent entre elles un identifiant de circuit virtuel appelé DLCI, numéro stocké par ailleurs dans les tables de routage des commutateurs qui équipent le réseau de relais de trames. Le DLCI se trouve dans l'en-tête de chacune des trames (2, 3 ou 4 octets). L'en-tête contient aussi le champ d'adresse, codé sur 10, 16, 17 ou 23 bits. Le DLCI de numéro 0 désigne le canal de signalisation utilisé pour l'ouverture et la fermeture des circuits virtuels. La signalisation se fait hors bande, ce qui contribue à maintenir des hauts débits durant la transmission.




Dans l'en-tête, le bit DE sert à identifier les trames à éliminer en cas de congestion. Les bits FECN et BECN servent à alerter les FRAD en cas d'encombrement du réseau. La zone d'information de la trame permet d'encapsuler toutes sortes de protocoles (asynchrone, BSC, SNA, X25, IP, IPX,…)

En-tête de trame Frame Relay

Le relais de trames garantit le séquencement des trames, un débit minimal (le CIR), ainsi qu'un débit de débordement maximal (dit EIR) au delà du débit autorisé. Le CIR représente le débit moyen sur lequel le réseau s'engage à transporter les informations avec la qualité de service demandée par l'utilisateur. La valeur du CIR est une des bases de la tarification du service de relais de trames.

Enfin, dans la mesure où le relais de trames est un protocole déchargé du traitement des anomalies, que se passe-t-il en cas d'erreur de transmission et de congestion sur le réseau? La détection des erreurs est réalisée par un champ de contrôle d'erreurs (2 octets) contenu dans la trame. Mais le protocole se contente d'avertir les terminaux d'extrémité (FRAD et routeurs) qui, eux, ont à charge d'utiliser des protocoles de niveau supérieur (TCP entre autres) pour demander la réémission des trames manquantes. Concernant la gestion des congestions, le relais de trames dispose de deux outils dans la structure de sa trame pour alerter le destinataire de la transmission: le bit BECN (Backward Explicit Congestion Notification) pour l'informer que les trames qu'il va émettre vont rencontrer un problème de congestion, et le bit FECN (Forward Explicit Congestion Notification) pour lui indiquer que la trame reçue contient des anomalies.

Les caractéristiques intéressantes du Frame Relay sont les suivantes :

- Faible Latence, Débit de Commutation Elevé. Pour réaliser ces objectifs le Relais de Trames utilise un protocole de liaison simplifié.
- Bande Passante à la Demande. Il est préférable d'avoir une flexibilité d'allocation de la bande passante de manière à optimiser l'utilisation des ressources réseau. La moitié de la bande passante est allouée à l'établissement de la communication. Par l'intermédiaire d'un procédé de réservation rapide de la bande passante, l'utilisateur peut renégocier la bande passante allouée.
- Partage Dynamique de la Bande Passante. Le partage dynamique des ressources permet d 'optimiser l'utilisateur de la bande passante normalement allouée à d'autres utilisateurs, si celle-ci est libre. Les utilisateurs dont le trafic en rafales est très important devront avoir une bande passante suffisante pour assurer les pointes de trafic.

La gestion des congestions dans un réseau Frame Relay :

L'originalité du Frame Relay réside dans la possibilité d'ajuster la bande passante aux besoins du moment et notamment à partir de 4 paramètres :

- Le CIR (Committed Information Rate), qui permet d'ajuster la bande passante minimale moyenne sur chaque circuit virtuel.
- Le Bc (Committed Burst Size), qui indique le débit maximal autorisé sans perte de données.
- Le Be (Committed Excess But Size), qui indique le débit maximal autorisé sans garantie de service.
- Le temps pour la période d'observation (généralement 1 seconde).

Le contrôle de flux est assuré par un contrat de débit moyen à respecter par l'utilisateur : le CIR (Committed Information Rate). Ce contrôle est très simple : il consiste à demander à l'utilisateur d'émettre un flux de débit constant ou presque. Cela permet à l'opérateur d'avoir une connaissance des flux qui vont transiter dans les noeuds de commutation et de pouvoir planifier l'ouverture ou le refus de nouvelles demandes de liaison virtuelles.

Le CIR est garanti pour des périodes de longueur T. Si T est relativement long, le trafic peut excéder le CIR pendant une partie de ce temps et être en dessous dans une autre partie. Cependant, il est prévu de faire

rentrer des trames en plus du contrat ; pendant une courte période de temps (généralement 1 seconde), le débit pourra être supérieur à celui précise dans le CIR. La quantité d'informations maximale qui sera transportée pendant la période T est dénommée CBS (Committed Burst Size). En d'autres termes T * CIR = CBS. Sur la période T, le trafic supplémentaire peut atteindre en moyenne la valeur EBS (Excess Burst Size). En résume, sur la période de longueur T, la quantité totale d'informations peut atteindre CIR + EBS.

Durant cette période T, l'utilisateur peut dépasser le trafic négocié dans le CIR. Dans le même temps, l'utilisateur se sert du DE (Discard Eligibility) pour indiquer les trames supplémentaires qui forment la quantité EBS. L'utilisateur qui dépasse son contrat de trafic aura intérêt à marquer les trames qui ne sont pas importantes par rapport à la qualité de service ; l'opérateur peut détruire ces trames dans le réseau en cas de surcharge. Le bit DE = 1 indique que la trame peut être détruite.

Deux bits supplémentaires ont également été introduits dans la structure de trames pour permettre la mise en place de contrôle de flux : le bit FECN (Forward Explicit Congestion Notification) et le bit BECN (Backward Explicit Congestion Notification) Le premier permet à un noeud congestionné de faire connaître son état au récepteur. Quant au deuxième bit, il a pour but de faire remonter la connaissance de l'état de congestion d'un noeud à l'émetteur.

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 noeud congestionné, ils sont automatiquement mis à 1. Le récepteur et l'émetteur sont donc informés de l'état de congestion d'un noeud par la réception de ces deux bits à 1.

**Freeware -** Logiciel mis gratuitement à disposition par son créateur. Il ne doit pas être confondu avec les logiciels commerciaux diffusés de manière bridée en termes de fonctionnalités (dit de démonstration), ou en termes de durée d'utilisation (partagiciel, shareware en anglais). Ils sont parfois financés par la publicité qu'ils contiennent (Adware).

**Fréquence -** Quantité d'éléments d'un signal transmis pendant un temps donné, généralement la seconde. Se mesure en hertz ou cycles par seconde. La fréquence d'une onde électromagnétique correspond au nombre d'oscillations par seconde. Elle se mesure en Hertz (1 Hz = 1 cycle par seconde). Pour les radiofréquences on utilise en fait ses multiples : le mégahertz (MHz) (1 million de Hertz) et le Gigahertz (GHz) (mille fois plus). 1 MHz correspond à une longueur d'onde de 300 m.

Nombre de cycles complets parcourus en une seconde par un courant alternatif, généralement exprimé en Hertz (Hz). Terme qualifiant également un endroit du spectre de radiofréquences (800 MHz, 900 MHz ou 1900 MHz, par exemple).

**Fréquence d'Echantillonnage -** Sampling Frequency - Nombre d'échantillons d'un signal qui sont prélevés par unité de temps.

**Fréquence vocale -** Désigne la bande passante nécessaire pour transmettre la voix (300 à 3 400 hertz). Les téléphones dits "à fréquence vocale" sont ceux où la numérotation se transmet en faisant correspondre à chaque touche du cadran un signal de fréquence donné. Ce mode de numérotation est plus rapide que la numérotation décimale (où chaque touche génère une suite d'impulsions) et permet d'utiliser aisément les touches pendant la communication.

**Fresnel -** Voir Pertes de Fresnel.

**FRIF -** Fichier de Référence International des Fréquences.

**Frontal -** Front-end Processor - Ordinateur assurant l'adaptation entre les réseaux de télécommunication et les ordinateurs sur lesquels tournent les applications (macroordinateurs, ou hôtes).

**FSAN -** Full Service Access Network - Groupe de travail international constitué entre plusieurs exploitants mondiaux et des grands industriels dont l'objectif est de favoriser la convergence des interfaces des réseaux numériques pour le développement de services à haut débit.

**FSTP -** Foiled Shielded Twisted Pair. En câblage, désigne un câble doté d'un blindage général ruban + tresse.

**FTAM -** File Transfer Access Method - Norme ISO de transfert de fichiers (IS 8571).

**FTP -** File Transfert Protocol - Système de manipulation et de transfert de fichiers à distance. Composé de deux entités : le serveur et le client. Ce n'est pas un protocole autonome, il ne s'occupe que de la manipulation des fichiers. Pour le transfert des blocs de données, il s'appuie sur la couche de protocoles TCP/IP. Outre le transfert de fichiers, il autorise la suppression de fichiers, la consultation de répertoires...

FTP garantit un certain niveau de sécurité: le client doit ouvrir une session sur le serveur pour s'identifier. Couramment utilisé sur Internet, le protocole FTP permet à n'importe quel utilisateur de démarrer une session de transfert de fichiers, et ce, de façon anonyme.

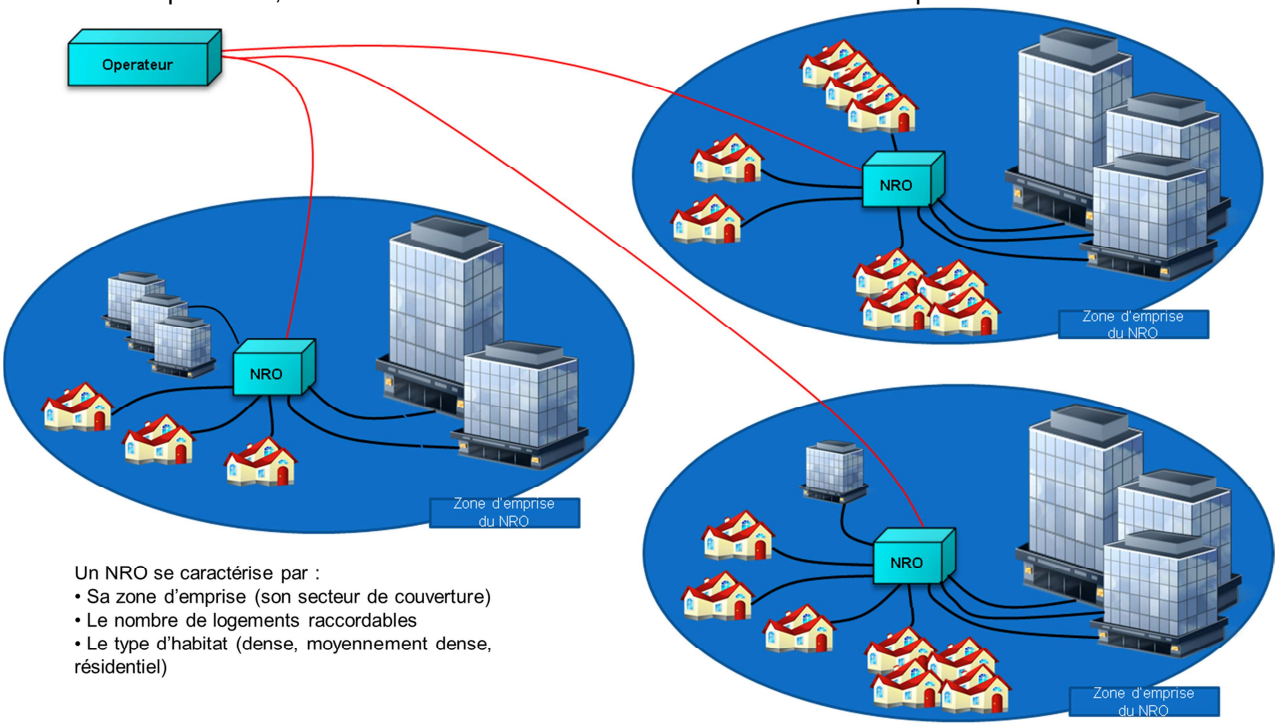
**FTP -** Foiled Twisted Pair - En câblage, désigne un câble doté d'un écran général.

**FTTC - FTTCab -** Fibre To The Curb or to the Cabinet - Ces expressions ont trait au mode de raccordement économique des abonnés en fibre optique. Faut-il se contenter d'une répartition à partir d'un coffret (Cabinet) ou aller jusqu'au pied de l'immeuble (Curb : trottoir) ?

**FTTH -** Fiber To The Home - Réseau d'accès par fibre optique jusqu'à l'abonné. il existe plusierus standards : l'EPON (Ethernet Based PON), qui vise à utiliser une couche Ethernet MAC légèrement modifiée comme protocole support, et le GPON (Gigabit PON), un type de PON pouvant fonctionner à des débits supérieurs au gigabit.

On va différencier deux architecteures de raccordements des abonnés : Point à Point ou arbre PON (point à multipoint).

Technologie d'accès reposant sur les standards PON (Passive Optical Network). Elle utilise des composants passifs du réseau de l'opérateur vers l'abonné, sur environ 20 km. Elle permet donc des coûts de maintenance peu importants. Et le standard BPON (Broadband Passive Optical Network) offre la possibilité de transporter sur trois longueurs d'onde WDM un flux descendant à 622 Mbit/s, un flux ascendant à 155 Mbit/s et de transporter des signaux vidéo analogiques ou numériques. C'est ainsi l'une des rares technologies à pouvoir transporter des flux de télévision haute définition, exigeant un débit minimal de 20 Mbit/s sur chaque canal, ou à offrir des services de visioconférence de haute qualité.




Contrairement à la plupart des réseaux de télécommunications, les réseaux optiques passifs (PON) n'utilisent pas de composants actifs alimentés en électricité (processeurs, mémoire...) sur l'infrastructure en fibre reliant les locaux de l'opérateur aux abonnés. Des composants passifs, les coupleurs, filtrent les longueurs d'onde transportées par les fibres et les aiguillent vers les clients. C'est à l'initiative de sept opérateurs, en 1995, que les premiers travaux pour standardiser les PON ont débuté sous la houlette du FSAN Consortium. L'IUT a ensuite défini le premier standard PON, dénommé APON, dont le protocole support est ATM. Il a ensuite été renommé en BPON (Broadband PON) pour montrer qu'il pouvait aussi transporter d'autres flux qu'ATM, comme Ethernet ou la vidéo à des débits de 655 Mbit/s.

**FTTH EFM -** (dite P2P) **-** 1000BASE-LX-10 - 802.3ah - Technologie de raccordement appréciée pour sa qualité de service mais également parce que c'est une technologie d'avenir parce que non limitante en terme de raccordement. Une technologie fibre FTTH en Point à Point signifie qu'une fibre relie directement (ou via soudure mais pas de multiplexage) un abonné à son NRO, d'où un débit et une qualité supérieure.

**FTTx -** Il existe une grande variété d'architectures dite Fiber To The xxx :

- FTTB : Fiber To The Building (Fibre jusqu'au bâtiment)
- FTTC: Fiber To The Curb (Fibre jusqu'au trottoir)
- FTTCab : Fiber To The Cab (Fibre jusqu'au sous-répartiteur)
- FTTH : Fiber To The Home (Fibre jusqu'au domicile)
- FTTLA : Fiber To The Last Amplifier (Fibre jusqu'au dernier amplificateur)
- FTTN : Fiber To The Neighbourhood (Fibre jusqu'au quartier)
- FTTN : Fiber To The Node (Fibre jusqu'au répartiteur)
- FTTP : Fiber To The Premises (Fibre jusqu'aux locaux - entreprises)

*Liste non exhaustive*

La fibre optique est utilisée depuis très longtemps pour ses capacités de transmission : rapidité (propagation à la vitesse de la lumière), largeur de bande passante, insensibilité aux perturbations électromagnétiques…

Deux grands principes d'architectures cohabitent aujourd'hui en France :

- Principe de l'architecture finale en Cuivre (issue des réseaux câbles) :

FTTB ou FTTLA - La terminaison de la liaison est assurée avec un câble coaxial en cuivre.

Ce sont les offres très haut débit de Numéricâble, Bouygues Telecom, Darty, Auchan…. Toutes ses offres utilisent le réseau de Numéricâble en France.

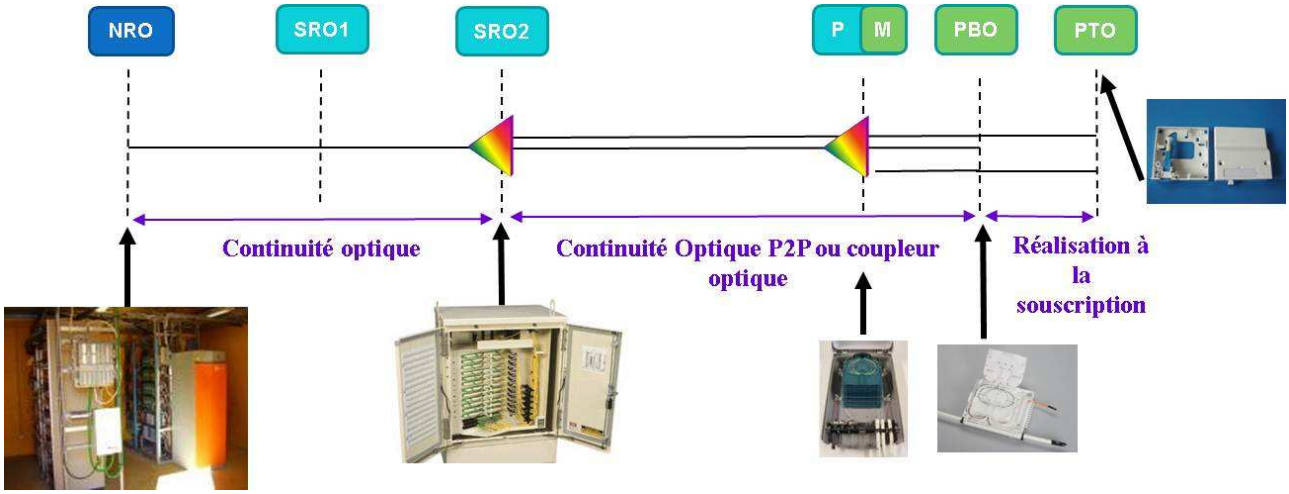
- L'architecture fibre jusqu'a l'usager :

FTTH - La fibre pénètre dans le logement. Le réseau de transport est intégralement construit en fibre optique jusque dans le logement.

Ce sont les offres très haut débit de Bouygues, Free, Orange, Quentiop, SFR, La majorité des DSP…

On distingue 2 grandes familles d'architecture dans le FTTH :

- FTTH GPON (Gigabit Passive Optical Network) - Liaisons de type 1 vers N. On parle aussi la notion d'arbre optique. Architecture optique retenue par Bouygues, Orange, SFR,…




⇒ Il est possible de raccorder 64 à 128 PTO à une seule fibre du NRO (dépend de l'équipement dans le NRO)

⇒ Il est possible de « cascader » les coupleurs optiques si les équipements actifs du NRO le permettent

⇒ Il n'est pas nécessaire de « tirer » une fibre par logement

⇒ Les contraintes d'affaiblissement sont à prendre en compte pour l'installation des coupleurs

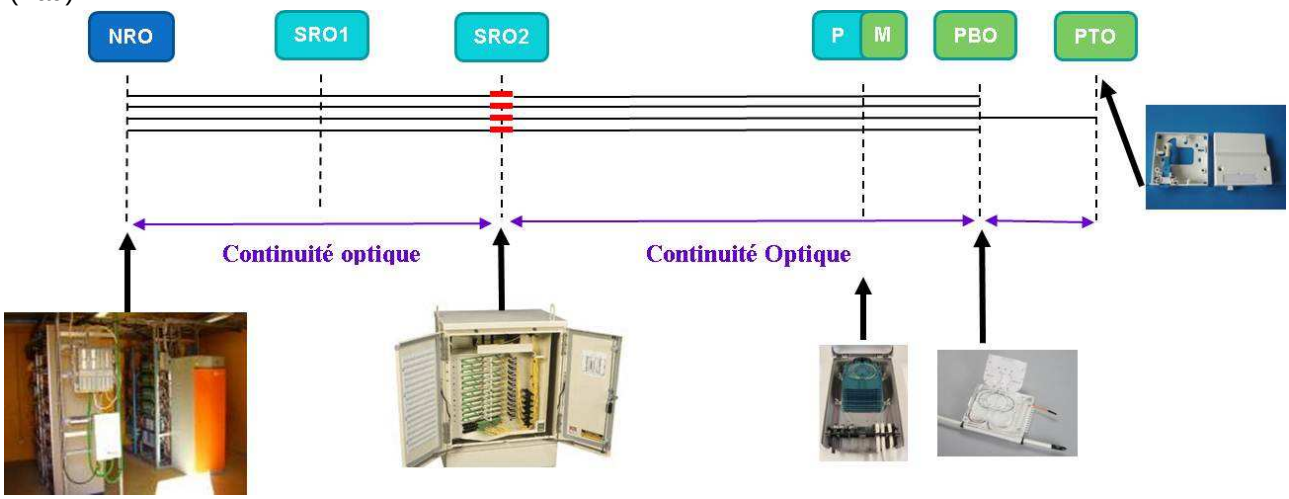
⇒ Il faut au moins 1 fibre en départ NRO pour chaque opérateur commercial

⇒ Les coûts sont amortis si les arbres sont « remplis ». S'il n'y a qu'un seul abonné, le coût est plus important.

⇒ Gestion plus complexe de la mutation des clients d'un opérateur vers un autre

⇒ Débit plus limité (2,5 Gb /sec) partagé par les 64 utilisateurs maximum de la liaison (40 Mbit/sec sauf évoltion vers une technologie WDW-PON).

- FTTH Point to Point (ou P2P) - Liaison de type 1 vers 1. c'est l'architecture retenue par Free, SPTHD (Pau)…




A chaque PTO est associé une fibre du NRO

⇒ Il y a autant de fibres que de logements
⇒ Il n'y a pas de partage de la fibre
⇒ Les contraintes d'affaiblissement sont limitées
⇒ On peut faire de l'Ethernet nativement sur la liaison (jusqu'à 1 gigabit / sec / PTO)
⇒ Gestion plus simple = on peut facilement muter un client
⇒ Il existe moins de contraintes pour la gestion du débit (pour les entreprises)

Architecture de réseau GPON vs P2P :

- Affaiblissement dû à la distance entre NRO et PTO très faible contrairement à l'ADSL
- Construction PTO vers premier point de mutualisation identique (coût, structure)
- Connectique au NRO, à la PTO.
- Possibilité de débit identiques (2,5 Gb) en fonction des technologies
- Coûts en fin de déploiement avec les équipements actifs équivalents

| | Positif | Négatif |
|---|---|---|
| P2P | - 1 fibre / PTO<br>- Exploitabilité<br>- Distances<br>- Débits<br>- Maintenance plus aisée<br>- Conception et calibrage facile (1 FO / destination)<br>- Mutualisation<br>- Sécurité de transmission | - Couts si beaucoup de connexion (zone très dense = Génie Civil Plus important et NRO plus importants)<br>- Déploiement long<br>- Câbles plus gros |
| GPON | - 1 fibre / 64 PTO<br>- Modularité<br>- Déploiement rapide<br>- Câbles plus petits | - Couts si peu de connexion<br>- Exploitabilité<br>- Affaiblissement dans les coupleurs passifs<br>- Maintenance plus contraignante<br>- Conception plus contraignante (1 ou 2 coupleurs et où ; dimensionnement si plusieurs FAI)<br>- Sécurité de transmission. |

**Full-Duplex -** Bidirectionnel simultané - Mode de transmission d'une ligne ou d'un équipement où les informations transitent en même temps dans les deux sens. Se dit d'une liaison où les informations transitent en même temps dans les deux sens.

# G

**G.SHDSL -** Single-pair High-speed Digital Subscriber Line - Appelé aussi ligne numérique d'abonné à très haut débit de transmission. Le standard G.SHDSL définit, sur la paire de cuivre téléphonique, des débits de transmission symétriques qui varient de 192 kbit/s à 2,32 Mbit/s en fonction de la distance. Il remplace avantageusement les traditionnelles liaisons louées à moindre coût. Il ne faut pas confondre SDSL et G.SHDSL, qui offrent pourtant plus ou moins les mêmes débits. Le SDSL n'est pas normalisé, contrairement au G.SHDSL.

**GAAI -** Generic Access to A/Gb Interface - Le 3GPP (The Third Generation Partnership Project) a intégré le concept de l'UMA à la release 6 de l'UMTS, en parlant de "generic access". Voir UMA.

**Gaine optique - Gaine -** Région d'une fibre optique, constituée d'une substance diélectrique qui entoure le coeur.

**GAMOT -** Guichet d'Accueil Maintenance Opérateur Tiers. Il s'agit du SAV de France Télécom. En effet, les opérateurs ne peuvent intervenir directement sur les installations FT. De ce fait, lors d'un problème de câblage (par exemple), l'opérateur doit demander, grâce à cette procédure, à l'opérateur historique d'intervenir pour corriger le problème.

**GARP -** Generic Attribute Registration Protocol - Mécanisme standard servant à propager l'information au niveau 2 du modèle en couche des réseaux, et à faciliter la configuration automatique des réseaux locaux virtuels ainsi que leur propagation.

**GCT -** Groupe Consultatif Terminaux - Groupe réunissant, sur une base volontaire, différentes parties intéressées par les équipements terminaux de télécommunications, tels que des opérateurs, des syndicats de constructeurs, des laboratoires d'essai et des utilisateurs, animé par l'Autorité et qui est chargé de préparer les règles techniques nationales relatives à l'évaluation de conformité des équipements terminaux.

**GED - Gestion Electronique de Documents -** Ensemble des méthodes, outils et standards permettant de créer, transférer et utiliser des documents sous forme électronique, en évitant ainsi de devoir utiliser le format "papier" dans les échanges d'information.

**Générateur de trafic -** Appareil de test permettant la génération à vitesse constante d'un nombre de trames de taille définie. Ce type d'appareil est utilisé pour simuler de la charge ou reproduire des conditions d'utilisations particulières.

**G-EPON -** Gigabit - Ethernet Passive Optical Network- Technologie de raccordement d'abonnés à un réseau optique qui consiste à multiplexer les données pour déployer un réseau "en grappe" (comme une arborescence en étoile hiérarchisée). Les fibres rejoignent toutes une autre fibre et sont multiplexées à l'aide de petits splitters passifs pour être multiplexées selon la technologie TDMA (Time Division Multiple Access). La technologie PON permet un déploiement rapide et à moindre coût puisqu'une fibre dessert plusieurs clients. Cette technologie PON connaît des limites en débit. La fibre étant multiplexée, plusieurs foyers partagent la même au moyen de splitter passif. C'est le choix qu'à fait France Télécom pour ses expérimentations.

**Gestionnaire de réseau - Voir NMS -** Désigne soit l'ensemble des logiciels assurant le contrôle d'un réseau, notamment d'un réseau local, soit, le plus souvent, le responsable supervisant le fonctionnement d'un réseau. On dit aussi "administrateur de réseau".

**GFU -** Groupe Fermé d'Utilisateurs - Le code des postes et télécommunications définit un réseau indépendant comme un réseau à usage privé ou partagé. Il "est appelé à usage privé, lorsqu'il est réservé à l'usage de la personne physique ou morale qui l'établit et à usage partagé, lorsqu'il est réservé à l'usage de plusieurs personnes physiques ou morales constituées en un groupe ou plusieurs groupes fermés d'utilisateurs, en vue d'échanger des communications internes au sein d'un même groupe". L'Autorité a précisé cette définition en indiquant qu' "un GFU est entendu comme un groupe qui repose sur une communauté d'intérêt suffisamment stable pour être identifiée et préexistante à la fourniture du service de télécommunications". La notion de groupe fermé d'utilisateur est également utilisée en dehors du champ des réseaux indépendants, par exemple pour définir un service de réseau privé virtuel sur un réseau ouvert au public.

**GGSN -** Gateway GPRS Support Node - Noeud assurant la connexion avec d'autre réseau que le GSM, comme IP ou X25.

**Gigabit Ethernet -** Technologie utilisant des câbles en cuivre ou en fibre optique pour le transfert de données à une vitesse pouvant atteindre 1 Gbit/s, dans un réseau local utilisant le protocole Ethernet.

Le Gigabit Ethernet fonctionne en full-duplex dans le mode switch-to-switch et dans le mode switch-to-end-station (de commutateur à commutateur ou à station) et en half-duplex pour les stations raccordées directement à un hub.

Pour maintenir un diamètre de réseau suffisant en half-duplex (200 mètres), la fenêtre de collision a été modifiée, la trame minimale étant portée à 64 octets. l'IFG reste à 96 bits.

**Gigabps -** Un milliard de bits par seconde. S'écrit aussi Gbps.

**Gigahertz -** Un milliard de hertz (voir Fréquence). S'écrit aussi GHz.

**Gigue -** Jitter - Défaut d'un signal dont l'amplitude et la fréquence varient autour de ses valeurs normales et perçues comme un "tressautement".

Variations des instants significatifs définissant un signal numérique par rapport aux positions qu'ils devraient occuper dans le temps.

**Globalstar -** Constellation de 48 satellites LEO (1414km d'altitude) répartis sur 8 plans d'orbite et qui est dédié à un service mondial de radiocommunication mobile.

**Gopher -** Protocole développé par l'Université du Minnesota (USA). Il permet à des clients d'accéder à des fichiers et à des répertoires via Internet. Ce protocole n'est pratiquement plus utilisé aujourd'hui.

Ce protocole considère le réseau Internet comme un immense livre. Les pages à lire sont constituées par l'information diffusée par les serveurs. L'utilisateur peut feuilleter les pages du livre au hasard. On présente souvent Gopher comme un outil de navigation, en fait c'est l'ancêtre. Gopher est basé sur le modèle client/serveur, fonctionnant avec le protocole TCP/IP.

Le serveur assure la diffusion de l'information; le client interroge le serveur pour accéder aux données. Le serveur présente les documents à diffuser sous la forme d'une arborescence. Un serveur Gopher indique la nature de l'information qu'il délivre; c'est au client de reconnaître le format du document reçu et de réagir en conséquence. Cette technique permet donc de diffuser une grande variété de documents (Texte, Image, Son, Binaire ...).

**GOSIP -** Government OSI Procurement Specification - Spécifications conformes à l'OSI imposées par certains gouvernements pour tous les achats publics. Les Etats-Unis, plusieurs pays européens et la CEE utilisent de telles spécifications.

**GPRS -** Global Packet Radio System - Technique de commutation de paquets sur GSM. Réseau de télécommunication mobile à commutation par paquet. Evolution du GSM permettant la transmission de données multimédia par paquets, à des débits importants, dans le contexte des infrastructures radio existantes.

Sur un plan technique, la transmission de données sur réseau GSM s'effectue de manière simple puisqu'il suffit de composer le numéro du site vers lequel le transfert doit s'effectuer. Le réseau GSM achemine l'appel en question au circuit d'interconnexion IWF (Inter Working Function). Ce dernier achève le transfert vers le terminal distant. L'IWF fonctionne en effet comme une passerelle. Muni d'une batterie de modems comme les serveurs d'accès distants des fournisseurs d'accès Internet, l'IWF effectue les traductions entre l'ensemble de protocoles GSM et les protocoles utilisés par les différents types de réseaux filaires: RTC, RNIS, X25 ou autre (voir schéma). Les données peuvent être envoyées sur le réseau GSM en mode transparent ou en mode non transparent.

En mode transparent, une liaison est établie sans correction d'erreur et les données sont envoyées en asynchrone. La transmission des données s'effectue après un bref délai (latence).

En mode non transparent, la liaison s'établit entre émetteur et récepteur avec correction d'erreur. La connexion entre le terminal et le réseau GSM utilise le protocole RLP (Radio Link Protocol) de correction d'erreur. L'IWF établit alors la connexion avec le modem distant en utilisant le protocole V42. Ce second mode présente deux avantages, une augmentation du débit de données d'environ 20 % et une meilleure gestion des appels par le réseau GSM.

Le GPRS est une technique de commutation de paquets qui porte le débit à 19,8 Kbits/s / Time Slot. La norme, qui s'appuie sur le fait que seuls les paquets utiles sont transmis, prévoit des possibilités telles que le partage de ressources entre plusieurs utilisateurs au moyen d'une allocation de bande passante appropriée. Au travers du couplage de plusieurs intervalles temporels sur un même canal radio, il sera possible d'atteindre 156,4 Kbits/s de débit pour chaque canal.

Les débits théoriques de 171,2 kbps par mobile, près de 18 fois ceux du réseau GSM, permettent aux téléphones mobiles et assistants personnels dotés de systèmes communicants, une connexion quasi instantanée et surtout permanente à l'internet.

Actuellement, une communication vocale nécessite un seul canal pour l'émission et la réception. Pour transmettre des données, plusieurs canaux sont mobilisés, augmentant d'autant les débits. Selon les spécifications techniques définies par l'ETSI (European Telecommunications Standards Institute), le GPRS utilise 8 canaux (time slot) simultanément pour atteindre les vitesses de transmission promises.

Seulement cette vitesse est très théorique. D'abord, les premiers téléphones ne peuvent gérer que 4 canaux, notamment pour des raisons d'autonomie. L'utilisation de chaque canal requiert pratiquement autant d'énergie qu'une communication classique en GSM. Quatre canaux utilisés simultanément consomment donc 4 fois plus, et 8, 8 fois plus. Inutile de préciser que dans ces conditions, la durée de vie d'une batterie perd toute chance d'excéder une heure, voire une demi-heure en communication.

Chaque station de base, qui sert de relais aux communications, possède un nombre déterminé de canaux à répartir entre les utilisateurs. Plus ils sont nombreux, moins ils disposent de canaux, et plus les débits sont

faibles. Une partie de ces canaux étant par ailleurs réservés aux appels vocaux, même seul sur un relais, un utilisateur GPRS peut voir sa vitesse de transmission bridée, surtout qu'un appel vocal est prioritaire.

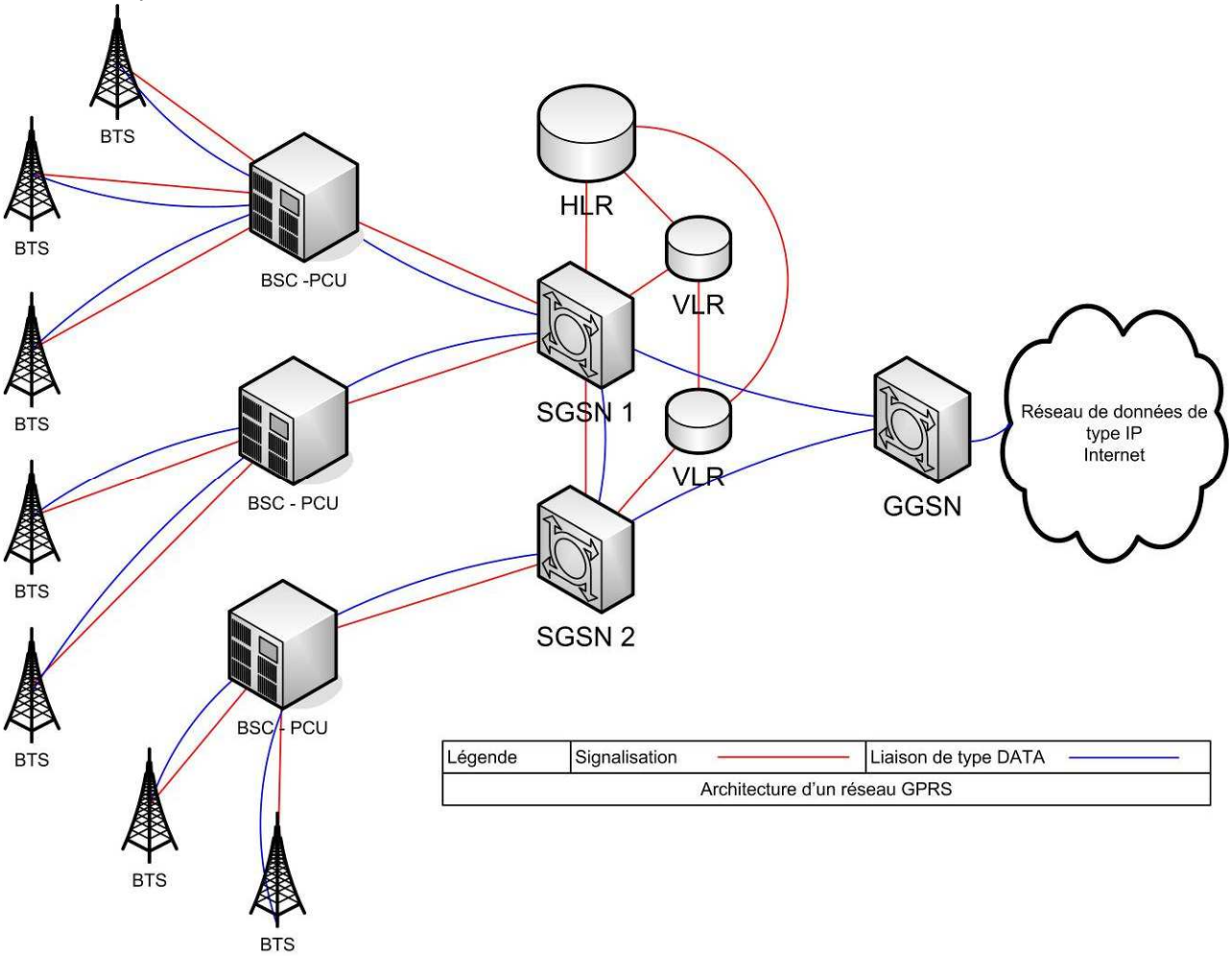
Enfin, la dernière limitation tient à la structure du réseau. Contrairement au GSM, le GPRS s'appuie sur une technologie de transmission par paquets, comme le protocole TCP/IP sur lequel repose l'internet. Un document est envoyé par petits morceaux, les paquets de données. Ce n'est que lorsque la totalité des informations ont été transmises, que le destinataire peut les réceptionner. Pour éviter les pertes de paquets inhérentes à ce type de réseau et renforcées par le caractère sans fil du GPRS, des protocoles de corrections d'erreur ont été mis en place. Mais, ces derniers ralentissent d'autant la vitesse de transmission. Appelés Coding Shemes, ils correspondent chacun à un débit réel : CS1: 9,05 kbps, CS2: 13,4 kbps, CS3: 15,6 kbps, CS4: 21,4 kbps.

En pratique, à cause des interférences radio de toutes sortes, des problèmes de couverture réseau, les CS1 et CS2 seront les plus souvent utilisées. Ainsi en réception, le débit d'un mobile GPRS oscillera entre 36 et 53 kbps, environ. En émission, un seul canal sera disponible, et le débit ne dépassera donc pas 9 kbps, soit celui du GSM. On est donc loin des vitesses annoncées.

L'utilisation d'un protocole de transmission par paquets, permet une connexion permanente au réseau, un peu comme le câble ou l'ADSL pour l'Internet, et ouvre la voie à un nouveau mode de facturation. Les communications vocales classiques resteront facturées à la durée, et les appels de données au volume. C'est-à-dire qu'on peut effectivement rester toujours connecté sans rien payer tant qu'aucune information ne transite.

En revanche, la technologie permet de garder une connexion permanente entre le mobile et l'entreprise. En effet, l'utilisation d'applications telles que l'accès à distance à des bases de données ou au système d'information se trouve facilitées. D'ailleurs, les opérateurs déploient en priorité des services à destination des professionnels.

Techniquement il existe trois types de téléphone GPRS regroupés en classe : a, b et c. Les terminaux de classe "a" traitent la voix et des données simultanément et regroupe la plupart des modèles proposés. Ceux de classe "b" traitent voix et données alternativement. Les mobiles de classe "c" ne traitent que les données et s'apparentent davantage à des modems qu'à des téléphones, ils seront sans doute intégrés dans des ordinateurs portables.




Le terminal communique avec une BTS GSM, mais contrairement aux appels data par commutation de circuit qui sont connectés au réseau vocaux par une MSC, les paquets GPRS sont identifiés par un PCU

(Packet Controler Unit) puis envoyés vers le SGSN (Serving GPRS Support Node).

Le SGSN est un noeud à l'intérieur de l'infrastructure GSM qui envoie et reçoit des donnés avec les stations mobiles. C'est aussi un routeur qui gère les terminaux présents dans une zone de donnée. Le SGSN communique avec le GGSN (Gateway GPRS Support Node). C'est le système qui assure les connections avec d'autres réseaux comme Internet,

Un réseau GPRS peut utiliser plusieurs SGSN mais ne nécessite qu'une seule GGSN pour assurer une connexion avec un réseau extérieur.

Les SGSN et GGSN sont des entités fonctionnelles. Elles sont séparées pour le principe mais dans la pratique elles peuvent être réunies dans un même équipement. Chaque fonction possède une adresse IP fixe. On appelle réseau fédérateur l'ensemble constitué par les GGSN, SGSN, les routeurs IP et les liaisons entre les équipements.

Quand le terminal GPRS envoie des paquets de donnés, ils transitent par le SGSN en direction du GGSN. Ce dernier les convertis pour les transmettre à travers le réseau désiré qui peuvent être soit des réseaux IP ou X25. Les paquets IP envoyés depuis l'Internet et adressés au terminal GPRS sont reçus par le GGSN, transmis au SGSN et acheminés vers le terminal. Pour faire transiter les paquets IP ou X25, le SGSN et le GGSN les encapsulent en utilisant un protocole spécialisé, le GPRS Tunnel Protocol qui agit au-dessus des protocoles standard TCP/IP.

**GPS -** Global Positioning System - Les récepteurs GPS permettent de localiser (au mètre près dans sa définition militaire) grâce à un réseau américain de 24 satellites, un engin mobile à n'importe quel point du globe.

**Graduation -** Codage de son ou d'image produisant un signal numérique dont on peut utiliser une partie plus ou moins grande correspondant à une qualité plus ou moins bonne.

La graduation est employée notamment lorsque le débit de transmission peut être plus faible que celui qui est nécessaire pour acheminer le signal complet ou lorsque certains récepteurs sont incapables de traiter le signal complet.

La graduation est aussi dite "codage hiérarchique".

**Grappe -** Ensemble d'équipements, notamment de terminaux-écrans, regroupés pour partager un canal de transmission ou un concentrateur. ETTD constitué d'un ensemble de périphériques souvent situés dans le même local.

**GRC -** Gestion de la Relation Client - En Anglais : CRM - Moyens informatiques et télécoms permettant à une société de gérer les relations avec ses clients. Voir CRM

**GRE -** Generic Routing Encapsulation - Protocole de tunnellisation développé par Cisco permettant d'encapsuler des paquets utilisant de nombreux protocoles différents dans des tunnels IP, afin de créer un lien point à point virtuel entre des points distants et des routeurs Cisco via un réseau IP.

**GRI -** Groupe des Régulateurs Indépendants - Organisme informel regroupant des représentants des différentes autorités de régulation des pays de l'Union Européenne et des pays de l'espace économique européen.

**GRID -** Grille - Réseau constitué d'ordinateurs interconnectés dont les ressources sont exploitées de façon à disposer, à moindre coût, d'une capacité de traitement importante.

Chaque ordinateur effectue séparément les traitements qui lui sont demandés par un serveur et renvoie les résultats qui sont intégrés à d'autres.

Les ordinateurs peuvent être reliés au moyen de l'internet ou appartenir au réseau d'un même organisme, d'une même entreprise.

On trouve aussi le terme "grille de calcul".

**Groupe de travail -** Regroupement en une seule et même entité (sous-réseau) de plusieurs postes de travail, serveurs et autres équipements réseau voués à une même fonction, utilisant les mêmes applications et/ou partageant des ressources communes. Un groupe de travail peut être fondé sur une localisation géographique ou une fonction commune à tous ses membres (par exemple, ingénierie, marketing, production ou administration).

**Groupe primaire -** Terminologie utilisée en multiplexage - Assemblage de 12 voies (par exemple téléphoniques) occupant des bandes de fréquence adjacentes en vue de leur modulation et démodulation.

Terminologie utilisée en Informatique - Groupe de taille limitée dont tous les membres se connaissent et ont entre eux des rapports directs.

**Groupe secondaire -** 5 groupes primaires = 60 voies

**Groupware -** Expression américaine désignant les applications informatiques mettant en jeu le travail collectif autour des mêmes projets.

**GSIT -** Groupement pour un Système Interbancaire de Télé compensation - Réunissant les principales banques françaises, il gère un réseau à valeur ajoutée, le SIT, destiné à la compensation et à l'échange automatisé de documents bancaires.

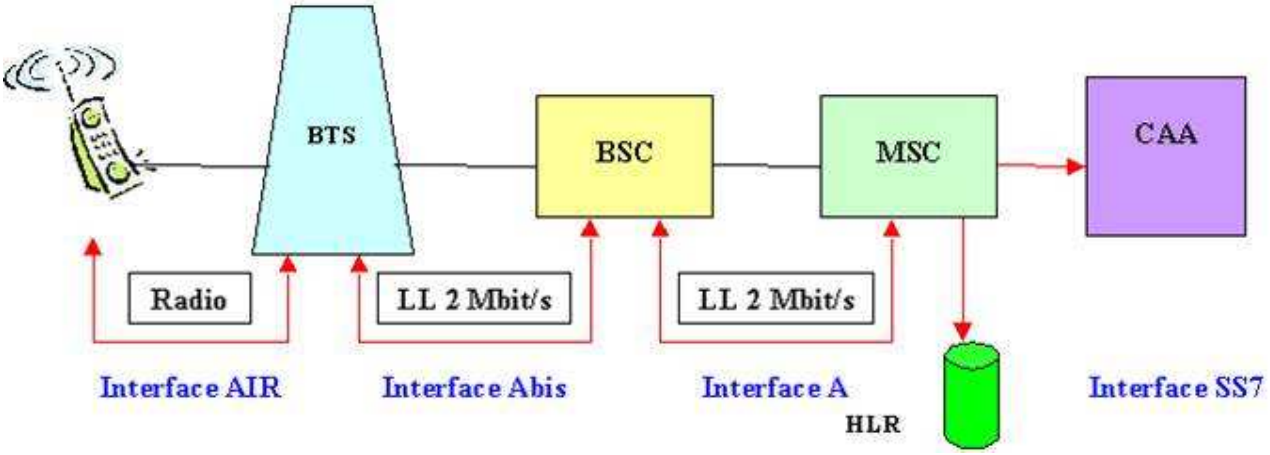
**GSM -** (Global System for Mobile communications): norme européenne de téléphonie mobile. C'est le plus connu des systèmes de téléphonie mobile terrestres de seconde génération. Il en existe d'autres : DECT ou CT2 (sans fil), LAN (autres sans fil), TETRA (PMR numérique), et TFTS (à bord des avions). La troisième génération s'appelle UMTS (Universal mobile télécommunication system) qui offre des améliorations permettant les hauts débits nécessités par le multimédia. L'UMTS est basé sur le CDMA (code division multiple access) alors que le GSM est basé sur le TDMA (Time division multiple access). Avec le GSM le combiné émet par impulsions et le pic de puissance est 8 fois la puissance moyenne. Le CDMA utilise une transmission en continu si bien que la puissance moyenne sera supérieure, mais cette puissance moyenne sera cependant moitié moindre (125 mW) qu'avec le GSM.

La norme GSM a vu le jour en 1982, lors d'une réunion du Groupe Spécial Mobiles, rebaptisé par la suite Global System for Mobile communications. Née en Europe, cette norme a su conquérir le monde où elle compte désormais plus de 150 millions d'utilisateurs. A l'origine, la norme utilisait uniquement une bande de fréquence radio autour des 900 MHz. Elle a été étendue à deux autres bandes autour des 1800 et 1900 MHz sous les noms de DCS 1800 (technologie utilisée par Bouygues Télécom et, depuis peu, par Cegetel et France Télécom Mobiles) et de DCS 1900 (norme utilisée principalement aux États Unis).

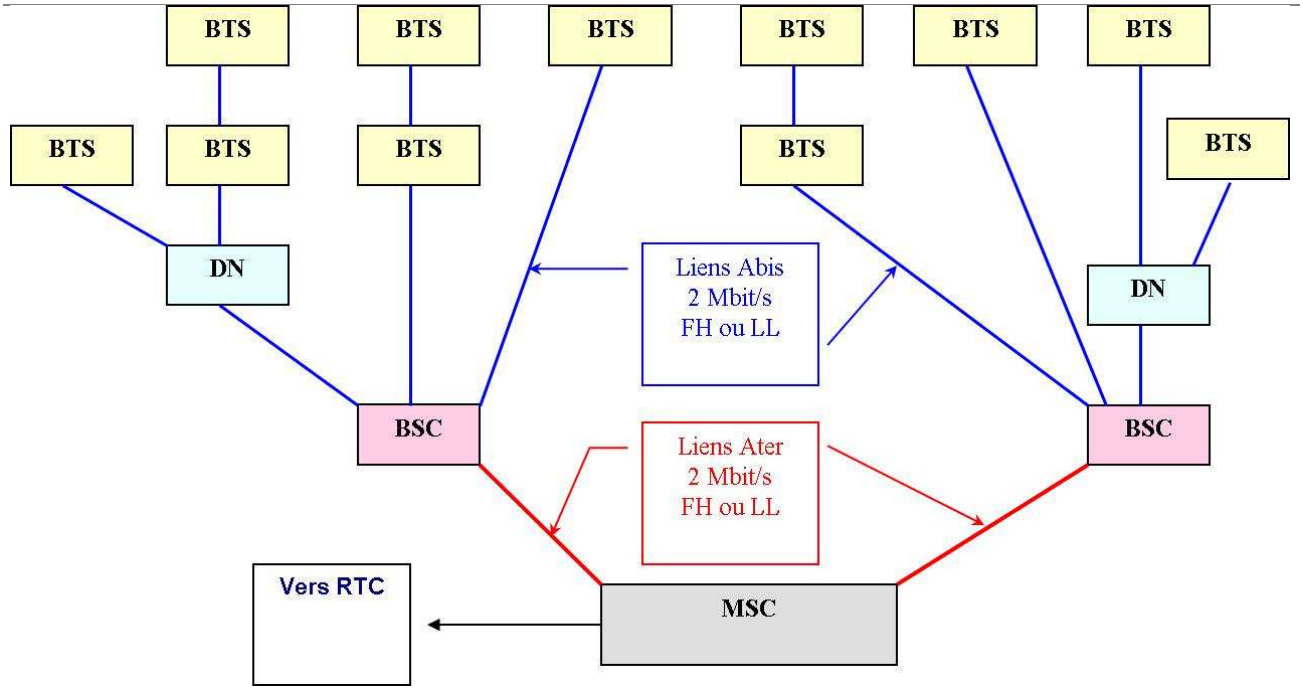
Si les premières ébauches du GSM avaient pour vocation de transmettre la voix et seulement la voix, les différentes évolutions qui ont suivi (GSM Phase 1, Phase 2 puis Phase 2 Plus) ont permis de développer de nombreux services à valeur ajoutée (messagerie, réservations) autour de cartes SIM dont la capacité s'accroît régulièrement. La carte SIM du GSM Phase 1 ne pouvait contenir qu'une vingtaine de numéros alors que celle du GSM Phase 2 Plus peut stocker un répertoire d'une centaine de numéros ou supporter deux numéros de téléphone (et donc deux forfaits) sur le même mobile.

Techniquement, un coup de téléphone sur un mobile, comment ça se passe? L'appel est transmis par radio vers la plus proche station de base (BTS) du réseau, voyageant de cellule en cellule. La taille des cellules dépend de l'environnement. En GSM 900 MHz, la taille des cellules varie de 300 m de rayon en environnement urbain, à 30 km en terrain découvert. Les cellules du GSM 1800 MHz ont, quant à elles, un rayon de 100 m à 4 km. Une fois passé par les stations de base, l'appel est relayé vers un multiplexeur (BSC). Le trajet en ondes radio prend alors fin: en effet, une fois arrivé au multiplexeur, l'appel est ensuite routé vers son destinataire via le réseau filaire. Évidemment, si l'appel est destiné à un autre mobile, il ressortira du réseau filaire pour courir à nouveau dans les airs.

Les schémas ci-après présentent l'architecture d'un réseau de téléphonie mobile avec les différentes interfaces :




Le réseau de téléphonie mobile en « coupe »




Architecture de réseau de téléphonie mobile.

Fondé sur la transmission numérique, le GSM compile un ensemble de technologies dont le codage de la parole et le partage en temps. Pour ce dernier, la technique actuellement utilisée est le TDMA (Time Division Multiple Access) qui permet de diviser chaque porteuse de fréquences utilisées en intervalles de temps appelés "slots". Chaque slot permet de transmettre un certain nombre de bits jusqu'à la station de base. Dés que l'abonné veut passer un appel, il compose un numéro et le terminal à l'écoute du canal de recherche demande une ressource sur le canal. En réponse, le réseau lui alloue un canal de signalisation. Le commutateur local (MSC) obtient de l'enregistreur les données de l'abonné (basé sur le réseau filaire, l'enregistreur stocke ces données et vérifie si l'abonné est autorisé à utiliser le réseau), puis achemine l'appel sur le canal de trafic alloué à la station mobile.

| GSM 900 et 1800 - Principales différences | | |
|---|---|---|
| | GSM 900 | GSM 1800 |
| Bande de fréquence | 890-915 MHz<br>et 935-960 MHz | 1710-1785 MHz<br>et 1805-1880 MHz |
| Nombre d'intervalle de temps par trame TDMA | 8 | |
| Ecart duplex | 45 MHz | 95 MHz |
| Rapidité de modulation | 271 Kbits/seconde | |
| Débit de parole | 13 Kbits/seconde | |
| Débit maximum de données | 12 Kbits/seconde | |
| Accès multiple | Multiplexage fréquentiel et temporel | |
| Rayon des cellules | 300 m à 30 Km | 100 m à 4 Km |

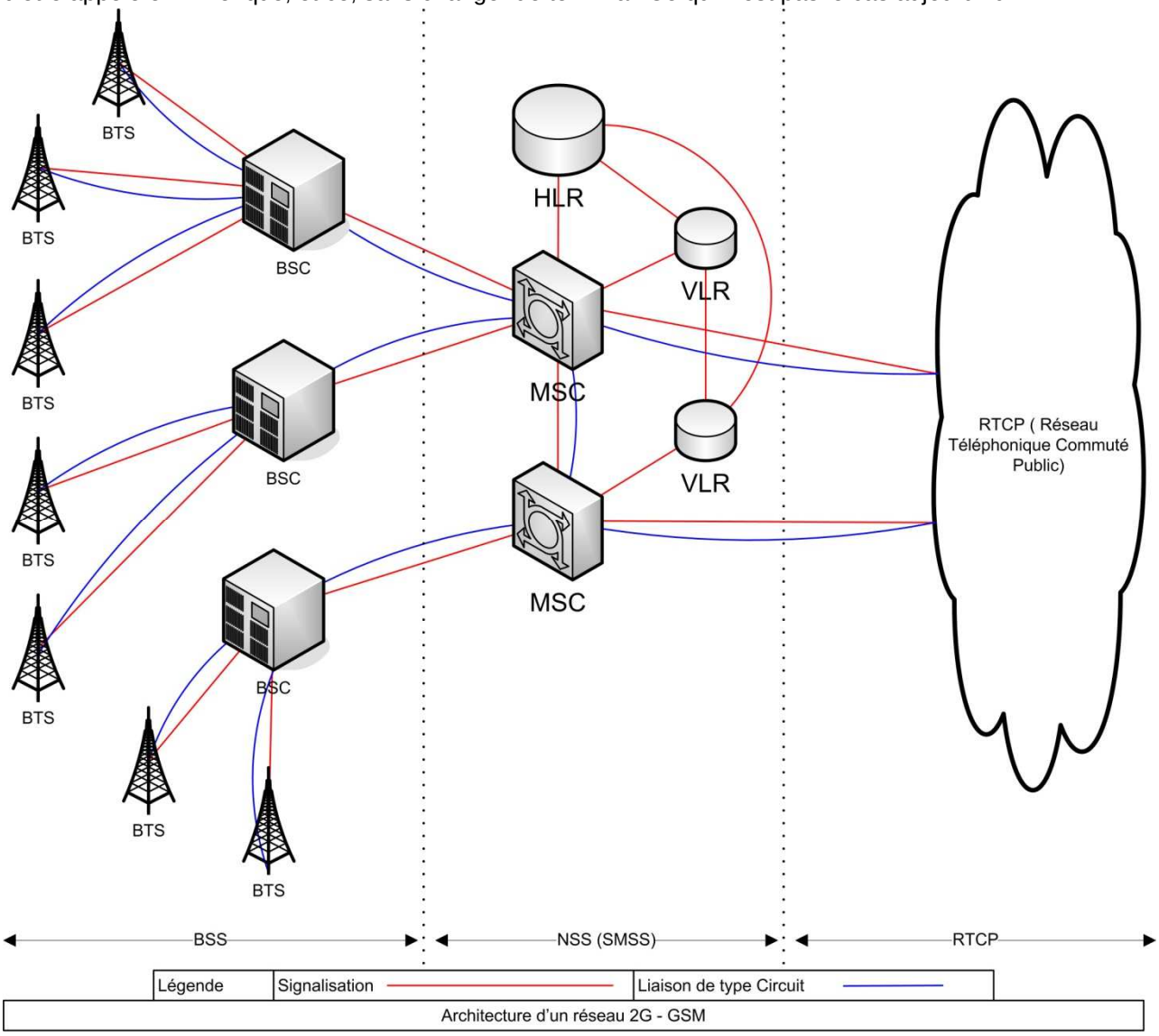
Il en va de même pour un appel en provenance du réseau fixe. Cet appel est transmis à l'enregistreur, qui se charge de localiser le mobile appelé.

Pour un appel international, le schéma de principe est le même. Dans ce cas (ce service porte le nom de "service d'itinérance" (roaming), l'abonné est enregistré sur le réseau d'un opérateur local qui interroge le réseau d'origine de l'abonné pour savoir si la fonction d'itinérance est activée pour cet utilisateur. Cette fonction d'itinérance (à titre indicatif, rappelons que le premier contrat d'itinérance a été signé le 17 juin 1992 entre Telecom Finland et Vodafone) est facilitée lorsque les réseaux GSM sont homogènes et fondés sur la même architecture, quelles que soient les fréquences utilisées.

En combinant l'usage du GSM 900 et du GSM 1800, les opérateurs cherchent à accroître à la fois la couverture géographique et la qualité de leurs réseaux. Pour bénéficier de cette avancée, l'abonné devra toutefois s'équiper d'un terminal bi-bande, c'est à dire, qui fonctionne sur les deux fréquences.

L'histoire ne s'arrête pas là puisque les téléphones "tri-bande" font depuis peu leur apparition. Ils permettront

(au travers d'accords d'itinérance avec les opérateurs de téléphonie mobile outre-Atlantique) d'appeler et d'être appelé en Amérique, et ce, sans changer de terminal. Ce qui n'est pas le cas aujourd'hui.



Architecture d'un réseau 2G - GSM

Un réseau de radiotéléphonie est constitué de trois sous ensembles :

- Le sous-système radio (BSS) - Généralement composé des équipement dénommés BTS et BSC (voir les définitions dans le présent document).
- Le sous-système d'acheminement (NSS) - Généralement composé des équipements HLR, VLR et MSC (voir les définitions dans le présent document).
- Le sous-système d'exploitation et de maintenance (OSS) - Généralement composé des équipement de provisionning, de supervision et d'exploitation.

L'équipement terminal peut être inclus ou exclu du sous-système radio suivant s'il est connecté ou non.

Sécurité et authentification :

La norme GSM utilise cinq éléments pour assurer le chiffrement et l'authentification des abonnés :

• Les nombres aléatoires RAND.
• Une clé Ki qui authentifie et sert à créer la clé de chiffrement Kc.
• Un algorithme A3 fournissant un nombre SRES basé sur le RAND et Ki.
• Un algorithme A8 pour déterminer la clé Kc à partir de RAND et Ki.
• Un algorithme A5 pour le chiffrement/déchiffrement des données à partir de Kc.

La clé Ki est personnelle, elle est attribuée à chaque abonné lors de l'abonnement. Les algorithmes sont communs à tous les usagers d'un même réseau. SRES, RAND et Kc sont utilisés en triplets.

**GSO -** Geostationary Satellite Orbit - Désigne une orbite géostationnaire pour un satellitte.

**GTB -** Gestion technique du bâtiment. Terme souvent utilisé dans les appels d'offres sur la mise en œuvre de système de câblage.

**GTC -** Gestion technique centralisée. Terme souvent utilisé dans les appels d'offres sur la mise en œuvre de système de câblage.

**GTI -** Garantie de Temps d'Intervention - Dans un contrat de support ou d'assistance, cette garantie définit le délai maximum d'intervention sur incident.

**GTR -** Garantie de Temps de Rétablissement - Dans un contrat de support ou d'assistance, cette garantie définit le délai maximum de rétablissement du service.

**GTR -** Groupe de travail sur les radiocommunications professionnelles, crée au sein de la Commission consultative des radiocommunications.

**Guichet Unique -** Procédure par lequel un exploitant de réseau ou un fournisseur de services offre à un client une prestation commerciale globale permettant d'accéder à un ou plusieurs services de télécommunication et fait appel, s'il en est besoin, aux moyens d'un ou plusieurs autres exploitants ou fournisseurs.

**Guide d'onde -** Médium, diélectrique ou conducteur dans lequel se propagent des ondes électromagnétiques.

**GVRP -** GARP VLAN Registration Protocol - Protocole définissant l'enregistrement dynamique des réseaux locaux virtuels au moyen de l'étiquetage conforme au standard IEEE 802.1q.

C'est un protocole qui transporte dans ses attributs des règles de filtrage permettant d'informer les stations et de réduire le trafic aux commutateurs où au moins une station est abonnée au VLAN. Ce protocole s'appuie sur l'arbre construit par l'algorithme du spanning tree.

Protocole transportant dans ses attributs les informations d'appartenances aux VLANs. Son but est de limiter le trafic sur un réseau commuté employant les VLANs mais il est également utilisé pour la maintenance et la mise à jour des informations de chaque équipement participant à la gestion des VLANs.

GVRP permet aux équipements "VLAN-aware" de faire savoir aux autres équipements qu'ils gèrent tel ou tel VLAN sur un segment LAN. L'objectif est de limiter dynmiquement la diffusion de trames ne concernant aucune station sur un segment non concerné par le VLAN d'appartenance de la station de destination.

GVRP permet à tous les éléments du réseau de faire des déclarations d'appartenance ou de révocation aux VLANs et c'est ainsi que les équipements se mettent en permanence à jour en propageant l'information à leurs proches voisins. L'implémentation de GVRP se fait en utilisant le logiciel fourni par le constructeur et dynamise donc les règles établies par l'administrateur.

# H

**H.261 -** Norme CCITT de compression de l'image (288*180 pixels ou 144*180 pixels) et du son pour un transfert sur RNIS (et donc à un débit de n*64 kbit/s).

**H.262 -** Norme CCITT correspondant au volet vidéo de MPEG-2.

**H.264 -** Codec vidéo intégré au format de compression vidéo MPEG-4. H.264 permet de réduire la taille des fichiers de 33% par rapport à ses concurrents.

Les créateurs du format de compression vidéo, baptisé H.264, affirment qu'il permet de diffuser des vidéos via l'internet avec une qualité égale à celle d'un DVD, mais en utilisant moins de ressources que les formats concurrents.

Le MPEG-4 permet de compresser des fichiers numériques audio et vidéo volumineux, afin de les transférer aisément sur internet. Lancé récemment, il est le successeur des formats MPEG-1 et MPEG-2, deux technologies qui ont permis au format de fichiers MP3 de connaître un immense succès.

Selon les premiers tests, ce nouveau format est capable de délivrer une vidéo d'une qualité équivalente à celle d'un DVD en utilisant un peu moins d'1 Mbps. Même si cela ne signifie pas qu'un internaute disposant d'une connexion câblée ou ADSL classique puisse dès à présent parvenir à la même qualité, le H.264 marque des points dans ce domaine, confronté aux formats concurrents. D'autant que ses créateurs affirment que ce codec permet de réduire le poids des fichiers de 33% par rapport à ses rivaux.

Seul bémol, le H.264 s'appuie sur une architecture qui nécessite considérablement plus de puissance processeur que les formats utilisés jusqu'à présent. Comparé à son prédécesseur, le MPEG-2, il utilise environ deux à trois fois plus de puissance.

**H.320 -** Recommandations décrivant les systèmes terminaux visiophoniques à bandes étroites (réseau RNIS).

**H.323 -** Norme de conférence adoptée en 1996 par l'IUT-T pour les réseaux IP (réseaux locaux ou Internet) à commutation de paquets, réseaux dont le débit varie en permanence et permettant la transmission en temps réel de la voix, des données et des images sur des réseaux à commutation de paquets. Dérivée de H.320, elle répond aux besoins d'interopérabilité entre les équipements de visioconférence, sur des intranets ou sur Internet.

Le protocole H323 a pour origine le développement de la visionconférence sur IP, dans la continuité de la norme H320 régissant les systèmes de visioconférence sur RNIS. Issu des travaux de l'ITU-T, la norme H323 est une norme chapeau qui s'appuie sur de nombreuses autres normes, dont les principales sont :

- H.245 pour la gestion des flux multimédias,
- H.225 qui décrit le protocole RAS (Registration Admission Status) régissant le protocole d'inscription d'un terminal, mais aussi définit la signalisation d'appels (qui, en s'appuyant sur Q.931, est très proche du RNIS).

H.323 définit 3 composants : Les terminaux (qui peuvent être des postes téléphoniques, des softphones sur PC Multimédia ou des terminaux de visioconférence), le gatekeeper (dans le mode "routé" généralement implémenté le gatekeeper contrôle toutes les étapes nécessaires à l'établissement de la communication) et les gateways (passerelles assurant l'interface entre le réseau IP et le réseau commuté ou les postes analogiques ou encore le système DECT).

**Hack -** Méthode utilisée pour obtenir l'accès illégal et non autorisé à un réseau, en vue de dérober des documents ou des données confidentielles ou par simple démonstration technique.

**Hacker -** Traduit en français, de façon peut être imparfaite, par pirate. Un hacker agit pour la beauté du geste, la grandeur du défi, le goût du jeu... et la volonté parfaitement égocentrique de (se) prouver qu'il est le meilleur. Officiellement, il ne veut ni détruire, ni agir sur commande. Mais des hackers "retournés" peuvent devenir de très bons corsaires.

**Half-Duplex -** Mode de communication bidirectionnel non simultané. Désigne une transmission où le même canal est utilisé alternativement dans un sens puis dans l'autre. On dit aussi à l'alternat

**HandOver -** Passage transparent d'une cellule à l'autre. Le terme handover est utilisé dans les réseaux mobiles, soit pour les communications téléphoniques en mode circuit, soit pour les communications de données en mode paquet.

Mécanisme grâce auquel un mobile peut transférer sa connexion d'une station de base vers une autre (handover inter station de base) ou, sur la même station, d'un canal radio vers un autre (handover intra station de base). On l'appelle également Transfert automatique inter/intra cellulaire ou Handoff (aux Etats-Unis).

Il existe plusieurs modes de gestion du hand-over entre un réseau de téléphonie 3G et un réseau de téléphonie 2G : Le mode blind, le mode compress.

**HD -** Haut Débit - Liens à haut débits (numériques).

Le tableau ci-dessous permet de comparer les technologies / les débits / les portées des diverses offres techniques récentes.

| Technologie | Standard | Débit | Distance | Fréquence |
|---|---|---|---|---|
| Wi-Fi | 802.11a | 54 Mbit/seconde | 100 m | 5 GHz |
| Wi-Fi | 802.11b | 11 Mbit/seconde | 100 m | 2,4 GHz |
| Wi-Fi | 802.11g | 54 Mbit/seconde | 100 m | 2,4 GHz |
| WiMax | 802.16 | 75 Mbit/seconde | 10 km | > 11 GHz |
| WiMax | 802.16e | 30 Mbit/seconde | 3,5 km | 2-6 GHz |
| UMTS | 3G | 2 Mbit/seconde | 6 km | 1900-2100 MHz |
| Edge | 2,5G | 348 kbit/seconde | 6 km | 900-1800 MHz |
| ADSL | xDSL | 8 Mbit/seconde | 5 km | 25 à 1,1 kHz |
| ADSL2+ | xDSL | 25 Mbit/seconde | 2,5 km | 25 à 2,2 kHz |
| SDSL | xDSL | 2 Mbit/seconde | 2,5 km | |

**HD -** Haute Définition (TV) - En TV Haute Définition, le nombre de lignes qui composent une image est de 1920 x 1080 points, à comparer au 576x720 points du DVD Vidéo.

**HDCD -** High Definition Compatible Digital - Format audio breveté pour CD et DVD . Il s'agit d'une bidouille rajoutant 4 bits pour coder les sons sur 20 bits au lieu de 16 normalement, et c'est compatible avec les formats normaux.

**HDCP -** High-Bandwidth Digital Content Protection - Système de protection de contenus numériques en haute définition qui permet de contrôler les flux audios et vidéos lors de leur transfert via une connexion numérique (DVI ou HDMI) d'un appareil vers un autre appareil.

**HDLB -** Haut Débit Large Bande - Projet de France Télécom d'un réseau à fibre optique pour le transport de données à 34 et 140 Mbps.

**HDLC -** High Level Data Link Control - Protocole de niveau 2 du modèle OSI. Ce protocole travaille en bipoint et assure le contrôle de la liaison entre deux équipements. Famille de protocoles évolués orientés bit (pas de notion de caractère) fonctionnant en mode synchrone bidirectionnel, utilisant une procédure de sécurité de type code cyclique et une anticipation des échanges (envoi des trames sans attendre les accusés de réception) permettant d'optimiser les lignes. Ce type de protocole normalisé par l'ISO (International Standard Organisation) est très utilisé, notamment dans les réseaux X25 ou le RNIS (Réseau numérique à intégration de services).

Commande de Liaison de Données à Haut Niveau - Protocole de liaison de données. Classes de procédures de transmission normalisées définies par l'ISO. Ces procédures assurent la transmission de suites d'éléments binaires et non de caractères... La version utilisée par X25 est LAP_B (Link Access Protocol Balanced).

**HDMI -** High Definition Multimedia Interface - Prise Multimédia à haute définition permettant de transporter de la vidéo numérique en haute définition ainsi que du son numérique en 5.1.

**HDSL et SHDSL -** High Symetric bit rate Digital Subscriber Line et Synchronised HDSL. Systèmes numériques à débit symétrique pour ligne métallique d'abonné de type "liaisons louées "en point-à-point. Plusieurs variétés de ces systèmes sont disponibles pour des débits utiles compris entre 194 kbit/s et 2 Mbit/s.

**Header -** en-tête en français.

**Helpac -** Nom du réseau à commutation de paquets proposé en Grèce.

**Hermès -** Réseau européen d'Echanges de données informatisés (EDI) pour les chemins de fer internationaux.

**Hertz -** Unité de fréquence correspondant à un cycle par seconde. Symbole : Hz. Ses multiples sont, entre autres, le kilohertz (kHz), le mégahertz (MHz) et le gigahertz (GHz).

Du nom du physicien allemand Heinrich Hertz, un pionnier de la radioélectricité, qui a mis en évidence les ondes radio dans les années 1880.

**Hertzien -** Désigne les transmissions utilisant comme support les ondes électromagnétiques dans leur ensemble et plus particulièrement les liaisons radio haute fréquence.

**Hétérogène -** Réseau constitué d'équipements de types ou de marques différents.

**HI8 -** Version améliorée du format Video8 utilisant le format S-Vidéo enregistré sur une bande Métal Particle ou Métal Evaporated. En raison d'une résolution à plus forte luminance et d'une largeur de bande plus grande, le résultat donne des images plus nettes qu'avec le format Video8.

**HiperLAN2 -** Elaborée sous la tutelle de l'European Telecommunications Standards Institute, HiperLAN est une norme exclusivement européenne. Hiperlan1 apporte un débit de 20 Mbps et Hiperlan2 de 54 Mbps sur un rayon d'action semblable à celui de Wi-Fi et HomeRF (100 mètres). Originalité d'HiperLAN 1 et 2: elles exploitent la gamme de fréquence de 5 GHz alors que 802.11a ou Bluetooth sont "installés" sur les 2,4 Ghz.

**Hippi -** High-Performance Parallel Interface - Interface Parallèle Haute Performance - Procédé de transmission unidirectionnelle en mode point à point d'un débit maximal de 800 Mbit/s, souvent déployé sur une paire de câbles pour obtenir des connexions en full duplex. Hippi peut relier de nombreux hôtes en utilisant des commutateurs Hippi. La distance de transmission maximale est de 25 mètres, mais avec des répétiteurs et sur fibre optique, cette distance peut atteindre 20 kilomètres.

**HLR -** Home Location Register - Base de données qui contient toutes les informations concernant les abonnés d'un PLMN donné : identité internationale de l'abonné utilisé par le réseau (IMSI), le numéro de téléphone de l'abonné (MSISDN), les services et options auquel il a souscrit.

Toutes ces données sont enregistrées lors de la souscription d'un abonnement.

Le HLR sert aussi à localiser un abonné en mémorisant le VLR dans lequel il est enregistré. L'abonné est relié à un HLR unique même si sa localisation change, en général l'abonné est relié au HLR de la ville dans laquelle l'abonnement a été souscrit. Le HLR est déterminé par le MISDN ou l'identité IMSI de l'abonné.

**Hoaxing -** Pratique qui consiste à faire courir des rumeurs, à diffuser des informations fausses ou déformées. Internet en serait un vecteur privilégié, notamment par le biais des journalistes, qui utilisent de plus en plus Internet comme source d'information mais qui ont de moins en moins le temps de vérifier ladite information.

**HomeRF -** Home Radio Frequency - Soutenu initialement par des acteurs comme Compaq, HP, IBM, Intel et Microsoft, HomeRF a été imaginé avant tout pour un usage domestique. Ses performances théoriques sont semblables à celles de Wi-Fi (débit de 11 Mbits/s). En outre, un réseau HomeRF permet aussi de soutenir des liaisons DECT, technologie de transport de la voix en mode numérique sur les réseaux sans-fil.

C'est une norme basée sur 802.11b et DECT. Elle permet indifféremment de faire transiter des flux audio ou des données. La norme autorise des portées de 50 mètres sans utiliser d'amplificateur.

**Homologation -** Procédure d'autorisation délivrée par une administration pour mettre en service un type d'équipement. En France, c'est la Direction à la réglementation générale, dépendant du ministère des Postes et Télécommunications, qui assure officiellement ce rôle.

**Horloge -** Dispositif électronique permettant de synchroniser le fonctionnement du processeur ou du microprocesseur.

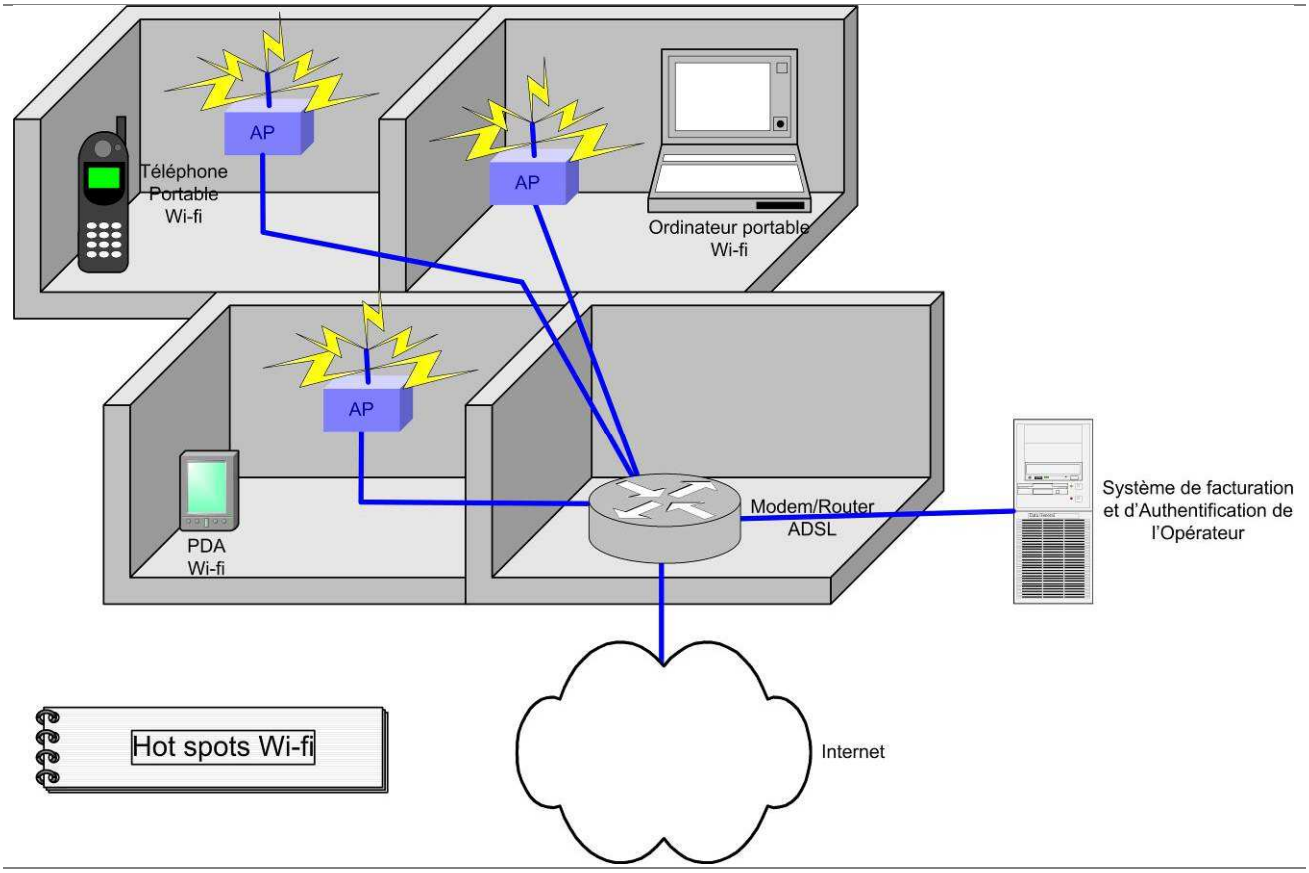
**Host masquerade -** (Masque IP) - Nom donné au mode de traduction d'adresse qui permet aux hôtes d'un réseau privé d'utiliser une seule adresse IP pour envoyer des données sur le réseau. Le routeur assure la traduction en modifiant l'entête du paquet (TCP, UDP ou ICMP). Cette traduction effectuée, le paquet sera, pour le récepteur, estampillé à l'adresse IP du routeur.

**Hot Plug -** Capacité à brancher et à débrancher un composant d'un système informatique à chaud, indispensable pour les systèmes à tolérance de panne.

**Hot Spot -** Bornes publiques Wi-Fi - Le principe consiste à installer dans les hots spots, c'est à-dire les sites radio Wi-Fi que constituent tous les lieux (les passages publics) des bornes Wi-Fi permettant à n'importe quel passant de se connecter à Internet avec son portable, son PDA ou son téléphone mobile. Le tout grâce à une liaison à haut débit sans fil utilisant le standard de réseau local 802.11. Ce marché est naturellement dynamisé par l'essor des technologies (le réseau sans fil d'entreprise) et par l'émergence de communautés libres Wi-Fi promettant un accès à Internet (presque) gratuit grâce à la mise en réseau de leurs sympathisants et un partage des frais d'accès.

Le faible coût d'installation est l'un des grands avantages de la technologie Wi-Fi. On petit monter, en théorie, un hot spot couvrant une surface de 500 m² avec une simple borne Wi-Fi et un modem ADSL.

Un Hot Spot est composé d'au moins un équipement AP (point d'accès réseau radio ou borne d'accès réseau), d'un routeur, d'un commutateur et d'un système de facturation. La composition du Hot Spot varie selon l'architecture, la surface à couvrir, l'opérateur…




**Hôte -** Host computer - Terme souvent utilisé pour désigner un ordinateur relié à un réseau et assurant des fonctions autres que le transport (en particulier des fonctions de niveau application).

**HSCSD -** High Speed Circuit Switched Data - Système de commutation de données par circuits permettant d'améliorer les débits fournis par les réseaux GSM (voir "commutation").

**HSDPA -** High Speed Download Packet Access - Evolution de l'UMTS qui fait évoluer les débits en réception (dans le sens réseau -> terminal) à 2 Mbit/seconde (puis, si l'on croit les fournisseurs de terminaux ; 3 Mbits et jusqu'à 14 Mbit/seconde).

L'UMTS FDD (Frequency Division Duplex), appelé aussi WCDMA (voir UMTS) utilise un duplexage fréquentiel (transmission bidirectionnel sur deux fréquences) par opposition à l'UMTS TDD (Time Division Duplex), aussi appelé HSDPA, qui met en œuvre un duplexage temporel (transmission bidirectionnelle sur la même fréquence en alternance). Ces deux technologies sont en fait inclues dans la norme originale de l'UMTS.

L'UMTS TDD se positionne, à l'instar du WiMax, en concurrence des accès Internet haut débit radio de type Wi-Fi et fixe (DSL). Le TDD-CDMA repose sur des infrastructures radio, des jeux de composants, et des terminaux dédiés.

La transmission s'effectue par «canaux partagés» (High Speed Downlink Shared Channels), chacun permettant de gérer jusqu'à quinze codes de transmission. Suivant les besoins des utilisateurs connectés et la capacité de leur terminal, ils se verront attribuer un ou plusieurs codes au cours de la connexion et pourront passer d'un canal à l'autre en 2 millisecondes (entre 10 et 20 ms pour l'UMTS).

HSDPA utilise en complément une technique de modulation de fréquence supplémentaire par rapport à l'UMTS (ce dernier se contentait du Quadrature Phase Shift keying (QPSK)). HSDPA y ajoute la 16-quadrature amplitude modulation (16-QAM). 16-QAM permet de doubler la capacité de transfert par rapport à QPSK, mais nécessite en contrepartie de très bonnes conditions radio. Pour gérer ce type de contraintes, HSDPA est assorti de mécanismes d'adaptation immédiate des paramètres de transmission. En cas de dégradation de l'environnement, les ressources (codes, intervalles de temps, etc.) seront réallouées au mieux et une plus ou moins grande partie de la bande passante sera utilisée pour des données de correction d'erreurs.

L'exploitation optimale de toutes ces techniques (utilisation de quinze codes, avec double modulation QPSK/16-QAM, sans transfert de données d'erreur) offre le débit maximal théorique de 14,4 Mbit/s.

**HSPA** - High Speed Packet Access - Terme générique adopté par l'UMTS Forum pour nommer les améliorations de l'interface radio UMTS.

HSPA désigne les améliorations apportées à la fois au flux descendant (HSDPA) et au flux ascendant (HSUPA). Dans le cadre de l'évolution des technologies GSM vers la 3G, le HSPA permet d'accélérer le transfert des données, de renforcer l'efficacité spectrale et d'accroître la capacité des systèmes des opérateurs. En ce qui concerne les utilisateurs, le HSPA donne accès à tout un monde de services mobiles haut débit multimédias.

La première manière de procéder réside dans la technologie Mimo (Multiple Input Multiple Output), qui consiste à utiliser plusieurs antennes en réception et en émission. Ce procédé permet dé recourir à plusieurs flux de données simultanés, puis d'assembler le tout à l'arrivée en fonction des différences de temps de trajet dues aux réflexions. Il est possible alors de passer d'un débit de 14 à 28 Mbit/s.

La deuxième piste pour doper le débit du HSPA est le recours à un système de modulation plus performant. Chaque porteuse est réglée en utilisant des modulations numériques appelées constellations QPSK, QAM-16, QAM-64... Les bits sont transmis sous forme de symboles numériques, le nombre de bits inclus dans chaque symbole désigne la taille de la constellation. En optimisant la modulation de QAM-16 à QAM-64, il devient possible de véhiculer 6 bits au lieu de 4, soit une augmentation de 50 %, qui influe directement sur le débit, lequel pourra passer de 28 à 42 Mbit/s.

**HSRP -** Hot Standby Router Protocol - Permet aux stations de travail utilisant IP de communiquer sur l'inter réseau même si leurs routeurs par défaut sont indisponibles. Ce protocole garantit une disponibilité élevée du réseau et un changement de topologie réseau totalement transparent. Protocole propriétaire de Cisco System.

**HSS -** Home Subscriber Server - Ce serveur gère les annuaires de domaines. Voir IMS

**HSUPA -** High Speed Uplink Packet Access - Evolution de l'UMTS qui fait évoluer les débits en émission (dans le sens terminal -> réseau). Cette évolution est un défi pour les fabricants de terminaux, puisqu'elle induit une consommation énergétique importante.

**HTML -** HyperText Markup Language - Est une application spécifique de SGML utilisée pour le Web, définissant un type de document comprenant des balises pour les éléments constituant le document (titres, chapitres, paragraphes, listes, illustrations, etc.). Simple, et largement utilisé, le HTML laisse peu à peu la place à des langages plus puissants tels que xHTML, XML, etc.

Langage simple de mise en forme de documents hypertexte qui utilise des balises, ou tags, pour indiquer comment une partie spécifique d'un document doit être interprétée par une application de visualisation telle qu'un navigateur Web.

Format de document utilisé pour créer à l'aide d'un langage spécifique des documents reconnus comme standard par un environnement WWW.

**HTTP -** HyperText Transfer Protocol - Ce protocole défini un ensemble de commandes pour manipuler les documents HTML.

Protocole le plus utilisé sur Internet depuis 1990. La version 0.9 était uniquement destinée à transférer des données sur Internet. HTTP permet un transfert de fichiers (entre autres au format HTML) localisés grâce à une chaîne de caractères nommée URL entre un navigateur et un serveur web.

**Hub -** Le hub est un processeur de communication implanté dans le local technique. Le Hub est le périphérique d'interconnexion de plus bas niveau (niveau 1) . Son rôle est de retransmettre les trames arrivant sur un de ses port vers tous ses autres ports. Le problème majeur du HUB est donc que toutes les machines qui y sont raccordées se partagent la bande passante. De plus, tous les segments et équipements raccordés à un HUB font partie du même domaine de collision. Le Hub permet l'interconnexion des postes de travail par la distribution en étoile des réseaux informatiques.

Son rôle est d'optimiser l'utilisation du câblage structuré dans l'entreprise, d'interconnecter les réseaux existants, d'intégrer les technologies existantes, de contrôler et administrer l'ensemble du réseau, de diminuer le nombre de produits dans le domaine de l'interconnexion de réseau.

Il se caractérise par les fonctionnalités suivantes : SOUPLESSE (médias courants (paires torsadées), connecteurs indépendants des modules, topologie Ethernet, Token-ring et FDDI, coexistence de plusieurs réseaux de topologie différente, fédération des réseaux locaux par les ponts/routeurs, technologie Port Switching (commutation par port), ...) SECURITE (redondance de l'alimentation sur les châssis, redondance modulaire sur les châssis, contrôle des connexions via SNMP, contrôle des connexions, ...) PUISSANCE (gestion dynamique de la bande passante sur les châssis, gestion de hauts débits sur les châssis, performances de commutation, performances des matrices de fond de panier, ...).

**Huffman -** Mathématicien à l'origine d'un algorithme de compression très utilisé pour le stockage des données et les télécommunications. Le code de Huffmann est utilisé en télécopie.

**Hyperchannel -** Hypercanal - Mode d'interconnexion à haute vitesse, typiquement à 50 Mbps, proposé par la société Network System Corporation pour interconnecter directement des ordinateurs de même marque ou de marque différente. Très utilisé en France dans le domaine de la recherche.

**Hypertexte -** Technique de consultation d'informations ou organisation des informations par des liens déterminés à l'avance. Ces liens (img ou texte cliquables) permettent d'accéder directement à l'information recherchée. Les pages Web sont construites de cette façon et le passage d'une page à une autre s'effectue par des liens hypertextes.

**Hz -** Symbole de hertz - Unité de fréquence.

# I

**IAB -** Internet Activities Board - Instance principale de la communauté TCP/IP; supervise le développement et la standardisation des protocoles.

**IAD -** Integrated Access Device - Equipement d'Accès Intégré - Équipement dont la fonction est d'intégrer la voix aux données qui sont transmises sur une ligne numérique (DSL), installée pour donner accès à un réseau télécom.

Ce terme est principalement utilisé par les papys des télécoms (et il ne faut pas me montrer du doigt !) et tous ceux qui ne veulent pas utiliser le terme de "box". En fait, les "LiveBox", "FreeBox", "AOLBox", "NeufBox" et consoeurs sont des IAD évolués.

**IAM -** Identification des Appels Malveillants - Malicious Call Identification, MCID - Complément de service permettant à un abonné demandé de solliciter que l'identité de la ligne appelante soit enregistrée par l'exploitant du réseau.

**IANA -** Internet Assigned Numbers Authority - Internet Address Naming Authority. Organisme vérifiant l'unicité des adresses sur le réseau Internet. Cet organisme assure la cohérence des adresses utilisées sur le réseau public et le respect des règles et format de trames utilisées.

**IAPP -** Inter Access Point Protocol - Interopérabilité inter constructeurs et support du hand-over.

**ICANN -** Internet Corporation for Assigned Names and Numbers - Organisme responsable de l'enregistrement des nouveaux sites connectés au réseau Internet. Il gère les numéros d'adresses IP de tout le réseau.

L'ICANN est une organisation à but non lucratif qui a été créée pour assurer la responsabilité de l'allocation des adresses IP, l'ajout de nouveaux protocoles et le management du système de noms de domaine. La direction de l'ICANN est assurée par 9 directeurs et un président.

Les statuts de l'ICANN définissent trois organisations suppléantes (OS) pour aider à la l'élaboration de recommandations sur la politique et la structure d'Internet dans trois domaines spécifiques. Ces OS aident à promouvoir le développement administratif d'Internet et encouragent les participations internationales pour l'administration technique de l'Internet.

Les différentes OS sont :

- Address Supporting Organization (ASO), s'occupe du système d'adressage IP qui identifie d'une manière unique les ordinateurs reliés à Internet.
- Domain Name Supporting Organization (DNSO), est la branche qui travaille sur la gestion du DNS.
- Protocol Supporting Organization (PSO), touche à tous les aspects protocolaires de l'Internet : les standards techniques en matière d'échanges de données entre ordinateurs sur le réseau.

**ICMP -** Internet Control and error Message Protocol - Un routeur ou un hôte destinataire peut avoir à communiquer vers l'émetteur d'un datagramme, par exemple, pour signaler une erreur de traitement du datagramme. C'est le protocole Internet Control Message Protocol (ICMP) qui en est "chargé". Il s'appuie sur le support de base fourni par IP comme s'il s'agissait d'un protocole d'une couche supérieure. ICMP n'en reste pas moins une partie intégrante du protocole IP, et doit de ce fait être implémenté dans chaque module IP.

Les messages ICMP sont envoyés dans diverses situations: par exemple, lorsqu'un datagramme ne peut pas atteindre sa destination, lorsque le routeur manque de réserve de mémoire pour retransmettre correctement le datagramme, ou lorsque le routeur décode de viser l'hôte destinataire via une route alternative pour optimiser le trafic.

Le protocole IP n'est pas, dans sa définition, absolument fiable. Le but de ces messages de contrôle est de pouvoir signaler l'apparition d'un cas d'erreur dans l'environnement IP, pas de rendre IP fiable. Aucune garantie que le datagramme soit acheminé ni qu'un message de contrôle soit retourné, de peut être donnée. Certains datagrammes pourront se perdre dans le réseau sans qu'aucun message de contrôle ne le signale. Les protocoles de niveau supérieur s'appuyant sur une couche IP devront implémenter leurs propres mécanismes de contrôle d'erreur et de retransmission si leur objet nécessite un circuit de communication sécurisé.

Les messages ICMP reportent principalement des erreurs concernant le traitement d'un datagramme dans un module IP. Pour éviter de ne pas entrer dans un cercle vicieux de réémission de message de contrôle en réponse à un autre message de contrôle et ce sans fin, aucun message ICMP ne sera réémis en réponse à un message ICMP. De même les messages ICMP ne seront transmis qu'en réponse à un traitement erroné du fragment zéro dans le cas d'un datagramme fragmenté. (Le fragment zéro est celui dont l'offset vaut zéro).

Formats de message :

Les messages ICMP sont émis en utilisant l'en-tête IP de base. Le premier octet de la section de données du datagramme est le champ de type ICMP; Sa valeur détermine le format du reste des données dans le datagramme ICMP.

ICMP est un protocole qui fonctionne un peu comme TCP, il est surtout utilisé pour la transmission de messages d'erreurs sur le réseau. Quand un nœud du réseau n'est pas joignable pour une raison x ou y, un message de ce type sera envoyé à l'émetteur du paquet IP.

Les messages d'erreur ICMP sont transportés sur le réseau sous forme de datagramme, comme n'importe quelle donnée. Ainsi, les messages d'erreur peuvent eux-mêmes être sujet d'erreurs.

Toutefois en cas d'erreur sur un datagramme transportant un message ICMP, aucun message d'erreur n'est délivré pour éviter un effet "boule de neige" en cas d'incident sur le réseau.

Tableau des messages ICMP et codes :

| Type | Code | Message | Signification du message |
|---|---|---|---|
| 8 | 0 | Demande d'ECHO | Ce message est utilisé lorsqu'on utilise la commande PING. Cette commande, permettant de tester le réseau, envoie un datagramme à un destinataire et lui demande de le restituer |
| 3 | 0 | Destinataire inaccessible | Le réseau n'est pas accessible |
| 3 | 1 | Destinataire inaccessible | La machine n'est pas accessible |
| 3 | 2 | Destinataire inaccessible | Le protocole n'est pas accessible |
| 3 | 3 | Destinataire inaccessible | Le port n'est pas accessible |
| 3 | 4 | Destinataire inaccessible | Fragmentation nécessaire mais impossible à cause du drapeau (flag) DF |
| 3 | 5 | Destinataire inaccessible | Le routage a échoué |
| 3 | 6 | Destinataire inaccessible | Réseau inconnu |
| 3 | 7 | Destinataire inaccessible | Machine inconnue |
| 3 | 8 | Destinataire inaccessible | Machine non connectée au réseau (inutilisé) |
| 3 | 9 | Destinataire inaccessible | Communication avec le réseau interdite |
| 3 | 10 | Destinataire inaccessible | Communication avec la machine interdite |
| 3 | 11 | Destinataire inaccessible | Machine inaccessible pour ce service |
| 3 | 12 | Destinataire inaccessible | Communication interdite (filtrage) |
| 4 | 0 | Source Quench | Le volume de données envoyé est trop important, le routeur envoie ce message pour prévenir qu'il sature afin de demander de réduire la vitesse de transmission |
| 5 | 0 | Redirection pour un hôte | Le routeur remarque que la route d'un ordinateur n'est pas optimale et envoie l'adresse du routeur à rajouter dans la table de routage de l'ordinateur |
| 5 | 1 | Redirection pour un hôte et un service donné | Le routeur remarque que la route d'un ordinateur n'est pas optimale pour un service donné et envoie l'adresse du routeur à rajouter dans la table de routage de l'ordinateur |
| 5 | 2 | Redirection pour un réseau | Le routeur remarque que la route d'un réseau entier n'est pas optimale et envoie l'adresse du routeur à rajouter dans la table de routage des ordinateurs du réseau |
| 5 | 3 | Redirection pour un réseau et un service donné | Le routeur remarque que la route d'un réseau entier n'est pas optimale pour un service donné et envoie l'adresse du routeur à rajouter dans la table de routage des ordinateurs du réseau |
| 11 | 0 | Temps dépassé | Ce message est envoyé lorsque le temps de vie d'un datagramme est dépassé. L'en-tête du datagramme est renvoyé pour que l'utilisateur sache quel datagramme a été détruit |
| 11 | 1 | Temps de ré-assemblage de fragment dépassé | Ce message est envoyé lorsque le temps de ré-assemblage des fragments d'un datagramme est dépassé. |
| 12 | 0 | En-tête erronné | Ce message est envoyé lorsqu'un champ d'un en-tête est erronné. La position de l'erreur est retournée |
| 13 | 0 | Timestamp request | Une machine demande à une autre son heure et sa date système (universelle) |
| 14 | 0 | Timestamp reply | La machine réceptrice donne son heure et sa date système afin que la machine émettrice puisse déterminer le temps de transfert des données |
| 15 | 0 | Réponse d'adresse | Ce message permet de demander au réseau une adresse IP |

| | | | |
|---|---|---|---|
| | | réseau | |
| 16 | 0 | Réponse d'adresse réseau | Ce message répond au message précédent |
| 17 | 0 | Demande de masque de sous-réseau | Ce message permet de demander au réseau un masque de sous-réseau |
| 18 | 0 | Réponse de masque de sous-réseau | Ce message répond au message précédent |

**ICNIRP -** Commission Internationale de Protection contre les Rayonnements Non Ionisants.

**ICS -** IBM Cabling System. Système de précâblage et de câblage d'immeuble préconisé par IBM. Utilisait du câblage blindé, connecteur hermaphrodite, impédance de 150 Ohm. Très développé sur les réseaux Token Ring, sa mise en œuvre nécessitait une très bonne connaissance de certaines normes pour les calculs de longueur de l'anneau.

**I-CSCF -** Interrogation Call Session Control Function - Serveur assurant la couche transport entre les différents opérateurs. Voir IMS

**IDATE -** Institut de l'Audiovisuel et des Télécommunications en Europe - Organisme d'étude à but non lucratif dans le domaine des télécommunications et de l'audiovisuel.

**IDEA -** International Data Encryption Algorithm - IDEA est un algorithme de chiffrement par bloque utilisé à la fois pour le chiffrement que le déchiffrement.

**Identification de l'appelant -** Fonctionnalité qui affiche le nom et/ou le numéro de téléphone de la personne qui vous appelle sur l'écran de votre téléphone mobile ou d'un dispositif séparé (comme c'est souvent le cas sur un téléphone fixe). La quasi-totalité des téléphones numériques - et de nombreux appareils analogiques aussi - offre cette possibilité, qui peut être activée par votre opérateur mobile.

**Identifieur -** Identifier ou ID - Enchaînement particulier de caractères utilisés pour reconnaître l'origine d'un message, d'un paquet ou d'un bloc d'informations.

**Identité -** Identification précise des utilisateurs, hôtes, applications, services et ressources du réseau. Les nouvelles technologies, telles que les certificats numériques, les cartes à puces, les services "répertoire" jouent un rôle de plus en plus important dans les solutions d'identification.

**IDS -** Intrusion Detection System - Système de Détection d'Intrusions - Sentinelle de sécurité en temps réel (semblable à un détecteur de mouvement) protégeant le périmètre du réseau, les extranets et les réseaux internes de plus en plus vulnérables. Les systèmes IDS analysent le flux de données du réseau à la recherche de signatures d'attaques ou d'activités considérées comme non autorisées, déclenchent l'alarme et lancent les actions nécessaires face à cette activité.

Système alliant des ressources logicielles et matérielles surveillant en temps réel les flux de données entrant dans un système d'information pour te protéger. Il compare les objets surveillés avec une base de signatures d'attaques connues et détecte des anomalies de fonctionnement.

Deux principales méthodes sont appliquées pour détecter les intrusions, suivant deux approches : l'approche comportementale et l'approche par scénarios.

- L'approche comportementale - Cette approche correspond à chercher à savoir si un utilisateur a un comportement déviant de ses habitudes. Il existe différentes méthodes mises en oeuvre pour détecter un utilisateur déviant de ses habitudes. Une méthode statistique se base sur l'observation du comportement normal d'un utilisateur, en considérant un certain nombre de variables aléatoires, une autre méthode se base sur le comportement passé de l'utilisateur et une troisième méthode consiste à prévoir la prochaine commande de l'utilisateur avec une certaine probabilité. L'avantage de cette approche est qu'elle détecte un très grand nombre d'intrusions. On peut également détecter des intrusions "nouvelles ", c'est à dire des attaques inconnues jusqu'alors. Par contre, l'inconvénient réside dans les choix des paramètres à prendre en considération.
- L'approche par scénarios - Cette deuxième approche se base sur la reconnaissance des signatures des attaques. Approche la plus utilisée dans les IDS. Les signatures d'attaques sont recherchées dans les différents audits de sécurité. Les différentes attaques connues sont répertoriées, ainsi que les actions indispensables à ce type d'attaque. Ces deux points forment ensemble la signature de l'attaque. En analysant les audits, on compare les actions effectuées sur le système avec les signatures d'attaques connues afin de les détecter. Si on reconnaît une signature parmi les actions effectuées par un utilisateur, on peut en déduire qu'il est en train d'attaque le système. Il existe plusieurs méthodes utilisées pour gérer les signatures des attaques. Tout d'abord, la plus fréquente, est la reconnaissance de signature par pattern matching (reconnaissance de formes), où les signatures d'attaques sont représentées comme une suite de lettres d'un alphabet, chaque lettre correspondant à un événement. La deuxième méthode se base sur l'utilisation des algorithmes génétiques pour analyser les traces des audits. Une troisième méthode est de considérer la signature d'attaque comme une séquence de changement d'état du système. L'inconvénient est justement que par cette approche, on ne peut détecter que les attaques déjà connues

Placement des IDS :

On peut placer les IDS à différents endroits sur le réseau, en fonction de la partie du réseau qu'on souhaite protéger. Néanmoins, il y a des points essentiels à protéger contre les intrusions externes. On place donc généralement les IDS :

Dans le périmètre du réseau - de préférence de chaque coté du firewall, pour le renforcer. On peut aussi placer l'IDS sur les connexions aux autres réseaux pour filtrer ce qui arrive et repart du réseau.

- Sur le backbone du WAN - on renforce ainsi la sécurité sur ce qui passe vers ou en provenance du WAN
- Dans les "fermes à serveurs" ou sur les "brins du réseau" contenant les serveurs. Il paraît judicieux de placer un IDS à ce niveau pour protéger les serveurs.
- Dans les DMZ : les DMZ (de-militarized zone : segment de réseau avec une protection partielle et contrôlée permettant l'accès entre autres de l'Internet) sont des points particulièrement sensibles sur un réseau. En effet, la plupart des attaques externes se font par l'intermédiaire des services en ligne, regroupés dans la DMZ. En plaçant un IDS à cet endroit, on protège l'accès aux services en ligne et on réduit le nombre d'attaque provenant de ces services.

**IDSL -** ISDN bit rate Digital Subscriber Line - Système numérique à débit RNIS à 144 kbit/s pour ligne métallique d'abonné. Ce système d'accès n'a pas encore été développé en France. L'ETSI s'y intéresse, ce qui pourrait donner un essor nouveau aux services déjà développés en RNIS.

**IEC -** International Electrotechnical Commission. Commission de normalisation Internationale.

**IEEE -** Institute of Electrical and Electronics Engineers - Association d'ingénieurs en électronique américains jouant un rôle important comme forum d'étude et de discussion sur la normalisation. Elle a notamment joué un rôle prépondérant dans la normalisation des réseaux locaux avec les normes IEEE 802, 802.3 (Ethernet), 802.4 (bus à jeton), 802.5 (anneau à jeton).

**IETF -** Internet Engineering Task Force - Consortium chargé d'introduire des procédures pour les nouvelles technologies Internet. Groupe de travail de l'IAB, il est responsable des développements à court terme et de la publication des RFC (Requesf For Comments) qui sont les standards de la communauté Internet.

Centre de décisions concernant les grands sujets d'actualité d'Internet. Sous ensemble de IAB (Internet activities board).

**IGMP - Internet Group Management Protocol -** Protocoles Multicast Stations → Routeurs (voir Multicast).

- IGMP v1 (RFC 1112)

Adresse de groupe abstraite : pas de notion de machine ni de réseau.

Le groupe est dynamique : de 0 à une quasi-infinité de membres

Les membres d'un groupe sont indépendants d'une localisation physique.

Un membre doit envoyer un rapport à l'adresse 224.1.1.1 pour rejoindre le groupe.

Le routeur envoie périodiquement des requêtes générales à l'adresse 224.0.0.1 pour déterminer l'appartenance aux groupes.

Pour maintenir le groupe, un membre (par groupe et par sous réseau) rapporte au routeur, les autres membres annulent leur rapport.

Les ordinateurs quittent le groupe sans en référer au routeur. Si pas de réponse aux requêtes périodiques du routeur, le groupe disparaît sur temporisation.

- IGMP v2 (2236)

Compatibilité descendante avec IGMP v1 +

Requête spécifique à un groupe - Le routeur vérifie que le dernier récepteur intéressé a quitté un groupe avant de cesser l'envoi de ses données sur un sous réseau.

Message pour quitter explicitement un groupe - Un ordinateur envoie un message de résiliation s'il quitte le groupe et s'il est le dernier membre (réduit le temps de latence de disparition d'un groupe par rapport au IGMP v1).

Mécanisme d'élection du routeur requérant - Sur les réseaux multi accès, un routeur requérant IGMP est élu sur la base de la plus petite adresse IP. Seul le routeur requérant envoie des requêtes générales.

Requêtes Générales - Intervalle de temps de réponse - Les requêtes générales spécifient le temps de réponse maximum imparti aux ordinateurs pour répondre (amélioration de la réactivité des ordinateurs).

- IGMP v3 & 4 (Internet Group Management Protocol v3 & 4 - en cours d'élaboration)

Autoriseront l'écoute d'un sous-ensemble de participants au groupe Multicast.

**IGMP Snooping -** Ce mécanisme donne à un commutateur une capacité de niveau 3, il examine chaque paquet pour savoir si c'est un message IGMP (rejoindre ou quitter), découvre dynamiquement les routeurs et les sources Multicast, inter opère avec les commutateurs utilisant CGMP. IGMP Snooping peut être traité par le hardware de certains commutateurs (moindre altération des performances). (voir multicast).

**IGP -** Interior (ou Internal) Gateway Protocol - C'est le protocole utilisé par les routeurs sur un réseau TCP/IP local. Il permet d'interconnecter différentes classes IP entre elles.

On utilise différents protocoles de routage qui agissent au niveau de la couche 3 du modèle OSI (la couche réseau). Ils permettent aux équipements concernés de construire des tables de routage pour aiguiller les informations. Les protocoles de routage choisissent le meilleur itinéraire entre deux machines (le plus rapide, le moins cher, le plus fiable, etc.). Si un élément ne fonctionne pas, un autre chemin va être choisi.

On distingue les protocoles de routage interne et externe. IGP (Interior Gateway Protocol) est un type de protocole utilisé pour router des données au sein d'un système autonome. Même Internet peut être vu comme l'agrégation de différents systèmes autonomes pouvant ainsi utiliser des protocoles de routage différents. Chaque réseau possède au moins un routeur (supportant les protocoles de routage interne et externe) qui transmet les données vers l'extérieur. Parmi les protocoles de routage IP on peut citer RIP, OSPF, BGP, EGP, ainsi qu'IGRP et EIGRP qui sont des protocoles propres à Cisco.

**IHM -** Interface Homme Machine

**IIOP -** Internet Inter-Orb Protocol - C'est à partir de la version 2 de Java qu'apparaît IIOP. Travaillant de concert avec RMI (Remote Method Invocation), ce protocole normalisé par l'OMG permet de manipuler des objets distants de manière transparente. RMI-II0P est utilisé dans l'architecture Corba.

**Ilot -** Unité géographique de l'INSEE, qui représente en général un pâté de maisons. Par extension, ensemble cohérent de logements répartis dans plusieurs immeubles.

**IMEI -** L'identité internationale d'équipement mobile (IMEI) est un nombre de 15 chiffres (divisé en quatre parties) qui identifie un téléphone mobile ou un communicator. L'IMEI figure sur l'étiquette située à l'arrière du téléphone. L'IMEI est automatiquement transmise par le téléphone à la demande du réseau. L'opérateur réseau peut être amené à demander l'IMEI pour déterminer si un appareil à un problème, a été volé, ou bien encore pour collecter des statistiques sur la fraude ou les dysfonctionnements.

**Immeuble Intelligent -** Expression générale pour désigner les nouvelles techniques en matière d'immeubles "pré-câblés", c'est-à-dire livrés avec une infrastructure de câblage à priori, permettant de recevoir divers équipements de téléphonie, d'informatique ou de contrôle technique (contrôle d'accès, climatisation...).

**Impédance -** Unité de mesure, exprimée en ohms, décrivant les propriétés de résistance d'un milieu à la propagation des signaux électriques.

Pour les câbles coaxiaux, l'impédance caractéristique définit les impédances des circuits de chacune des extrémités de la liaison (entrée-sortie).

**Impédance de transfert -** Valeur exprimée en Ohm qui caractérise l'efficacité du blindage d'un câble coaxial.

**Impulsion -** Signal caractérisé par une rapide variation de niveau.

**IMS -** IP Multimédia Subsystem - Technologie qui définit l'architecture cible de cœur de réseau d'un opérateur. Cette technologie met en œuvre des fonctions techniques (mécanismes et contrôles) entre plusieurs matériels en recourant au protocole de signalisation SIP, mais utilisant entre autres les protocoles IP, SIP (Session Initiation Protocol) et RTP (Real Time Transport Protocol).

IMS fournit une couche intermédiaire au cœur des réseaux pour passer du mode appel "classique" (circuit) au mode "session", permettant ainsi d'ouvrir plusieurs sessions au cours d'une même communication.

Les équipements mis en œuvre dans une architecture IMS :

- HSS - Home Subscriber Server - Ce serveur gère les annuaires de domaines.
- BGCF - Break out Gateway Control Function - Cette passerelle contrôle la compatibilité des équipements et renvoie les appareils non compatibles vers des passerelles spécifiques, permettant d'assurer la conversion entre le flux voix RTP et la téléphonie standard.
- I-CSCF - Interrogation Call Session Control Function - Serveur assurant la couche transport entre les différents opérateurs.
- MGCF - Media Gateway Control Function - Passerelle permettant d'assurer la conversion entre des flux d'origines différentes. Aussi appelé MGW.
- MRFC - Media Resource Function Controler - Passerelle qui détecte et oriente les différents en function de le source, de leur distination, de leur priorité, de leur type, de leur urgence…
- P-CSCF - Proxy Call Session Control Function - Serveur permettant d'identifier les types d'appel entrants dans une architecture IMS.
- S-CSCF - Services Call Session Control Function - Serveur permettant d'identifier l'appelant et détectant le type de service associés.

**IMSI -** International Mobile Subscriber Identity - Identité internationale d'abonné mobile - Numéro d'abonnement inscrit sur la carte SIM.

Confidentialité de l'IMSI : La norme GSM utilise donc des identités temporaires appelées TMSI. La correspondance entre le TMSI et l'IMSI est effectuée par le VLR. En théorie l'IMSI n'est donc envoyée sur le réseau qu'une seule fois lors de la mise sous tension du mobile. Il arrive que celle ci re-transite si le matériel tombe en panne. Par la suite seul les TMSI successifs transitent sur le réseau. L'allocation d'un nouveau TMSI est effectuée au moins à chaque changement de VLR, pour des raisons de sécurité un opérateur peut décider de le changer plus fréquemment.

**IMT 2000 -** International Mobile Telecommunications 2000. D'abord appelé FPLMTS, ce projet de l'UIT est la norme commune internationale des systèmes cellulaires de troisième génération offrant notamment des services multimédia : UMTS.

**Indice d'étanchéité IP - Indice de protection IP -** Cet indice est utilisé et communiqué pour des terminaux "durcis". L'indice de protection IP caractérise le niveau d'étanchéité des produits. Le premier chiffre correspond au niveau de protection contre les corps solides et le second contre les liquides. Plus le chiffre est élevé, plus la protection l'est aussi. Les PDA durcis résistent également aux chocs. Les constructeurs indiquent alors la hauteur de chute sur un sol en béton à laquelle le système résiste.

| Indice | Premier chiffre | Second chiffre |
|---|---|---|
| 0 | Aucune protection | Aucune protection |
| 1 | Protection contre les corps solides supérieurs à 50 mm | Protection contre les chutes verticales égouttes d'eau |
| 2 | Protection contre les corps solides supérieurs à 12 mm | Protection contre les chutes d'eau avec une inclinaison maximale de 15° |
| 3 | Protection contre les corps solides supérieurs à 2,5 mm | Protection contre l'eau en pluie |
| 4 | Protection contre les corps solides supérieurs à 1 mm | Protection contre les projections d'eau |
| 5 | Protection contre la poussière | Protection contre les jets d'eau |
| 6 | Protection totale contre la poussière | Protection contre les vagues |
| 7 | | Protection contre les effets de l'immersion |
| 8 | | Protection contre les effets de l'immersion prolongée |

**Indice de réfraction** - Refractive index - Rapport de la vitesse de la lumière dans le vide, à celle prise dans le médium considéré et noté «n».

- du coeur d'une fibre: noté n1 d'une valeur plus grande que celle de n2
- de la gaine optique d'une fibre: noté n2
- de groupe: indice moyen pondéré donné pour une fibre multimode gradient d'indice pour laquelle les influences de la vitesse fonction de la longueur d'onde et des vitesses différentielles des modes ne justifient pas d'utiliser des valeurs distinctes comme en monomode.

**Infogérance -** Synonyme : "I.T. Management" - Service consistant pour une SSII à prendre en charge la responsabilité complète de la gestion du service informatique de son client.

**Infrarouge -** Bande d'ondes électromagnétiques utilisée pour la transmission d'informations sans fil sur de très courtes distances.

**Infrastructure -** Equipements et lignes qui permettent l'interconnexion de systèmes de télécommunications. Désigne souvent les supports physiques existants (fibre optique, boucle locale, câbles privés...).

**Infrastructure Alternative -** Réseaux de communication établis pour leur propre usage par certaines compagnies (ferroviaires, aéroports, sociétés d'autoroutes)

**Inmarsat -** INternational MARitime SATellite Organisation - Organisation internationale gérant un réseau de satellites pour les communications de voix et de données avec les navires.

**INRIA -** Institut National de la Recherche en Informatique et en Automatique.

**INS -** Information Network System - Réseau numérique à large bande proposé par l'ancien opérateur public japonais NTT.

**INT -** Institut National des Télécommunications - Etablissement d'enseignement supérieur situé à Evry dans la région parisienne dépendant de la Direction de l'enseignement supérieur des télécommunications (comme l'ENST Bretagne et Télécom Paris) et formant principalement des ingénieurs.

**Intégration -** L'intégration est une opération qui consiste à assembler les différentes parties d'un système tout en assurant le bon fonctionnement de l'ensemble. Il s'agit donc de coordonner les activités et les fonctionnalités de plusieurs organes, en vue d'un fonctionnement harmonieux.

**Intégrité** - Moyen permettant de garantir que les données n'ont pas été modifiées, si ce n'est par les personnes explicitement autorisées à le faire. Le terme "intégrité du réseau" signifie qu'aucun service ou aucune activité contraire à la politique de sécurité n'est permise.

**Intégrité -** Non-altération d'un message pendant sa télétransmission.

**Intégrité des données -** Processus permettant de garantir que les données n'ont pas été modifiées ou détruites lors du transport via le réseau.

**Intelsat -** Nom des satellites de télécommunications intercontinentaux gérés par l'organisation du même nom. Cette société est une structure communautaire réunissant une grande partie des opérateurs de télécommunications dans le monde.

**Interactif -** Equivalent de conversationnel. Désigne un mode de transmission où les deux extrémités sont en dialogue permanent et aléatoire. Qualifie les matériels, les programmes ou les conditions d'exploitation qui permettent des actions réciproques avec des utilisateurs ou avec des appareils.

**Intercom -** Petit système téléphonique de commutation privé de faible capacité ne nécessitant pas de logiciel centralisé et où les connexions peuvent être directement obtenues par simple appui sur une touche. Sur de nombreux autocommutateurs privés, cette fonction peut être disponible pour une partie de l'installation.

**Interconnexion -** Capacité de connexion entre les différents réseaux de télécommunications, permettant de mettre en relation les clients de tous les opérateurs.

Mécanisme de connexion entre les différents réseaux de télécommunications, dont l'objectif est de permettre à chaque abonné d'un opérateur de joindre tous les abonnés de tous les opérateurs.

Ce terme désigne aussi le raccordement des réseaux privés à celui de FRANCE TELECOM. Le développement de la concurrence est lié aux conditions techniques et surtout financières selon lesquelles cette interconnexion est réalisée. Le catalogue d'interconnexion doit être approuvé par l'ART.

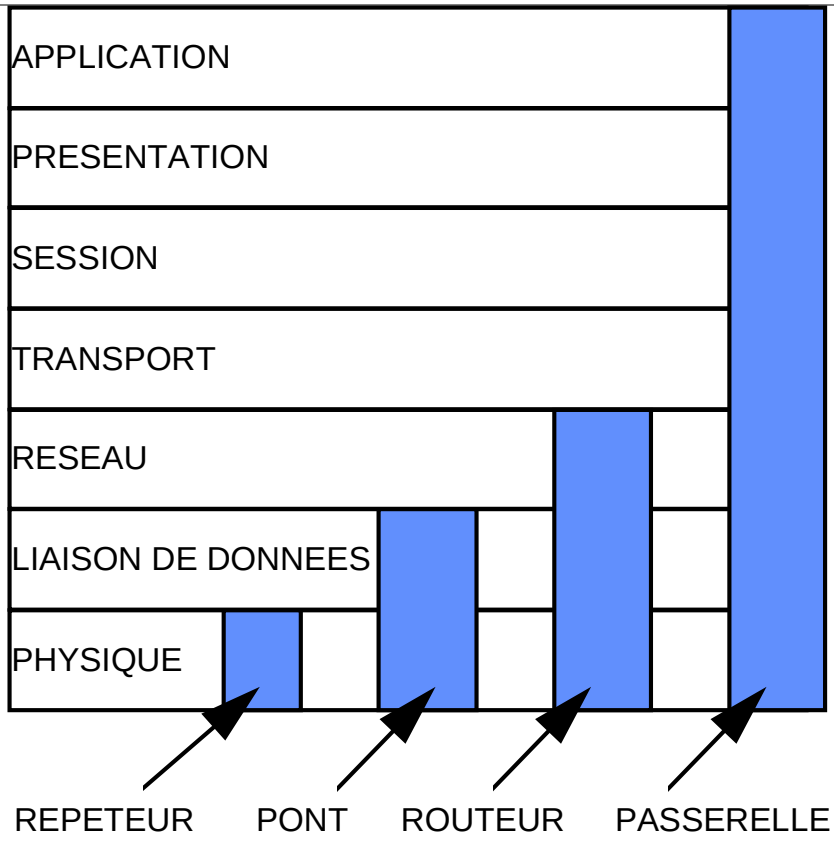
**Interconnexion de réseaux -** On parle souvent du réseau d'entreprise ou du réseau national, ou du réseau local. Il est clair qu'il ne s'agit là que de facilités de langage, et que le réseau unique est un cas exceptionnel. Le travail essentiel des architectes de réseaux consiste précisément à interconnecter les réseaux les uns aux autres, qu'ils soient locaux ou à longue distance, privés ou publics. Ces architectures d'interconnexion sont dominées par les notions de ponts, de routeurs et autres passerelles.

C'est à travers ces équipements que se dessine aujourd'hui l'entreprise étendue. Elle dispose donc bien d'un réseau au sens logique, dans la mesure où "tout le monde pourra communiquer avec tout le monde". Mais l'architecture de ce réseau logique unique n'est possible que parce que des dispositifs interconnectent les différents réseaux physiques.

Si l'on considère que l'organisation des données à transmettre est identique dans les réseaux locaux, dans les réseaux étendus privés et, avec X25, dans les réseaux publics, puisqu'il s'agit toujours de trames de type HDLC ou X25, on ne sera pas surpris que les mêmes types d'équipements, à la capacité près, servent à interconnecter des réseaux locaux, des réseaux téléinformatiques privés et des réseaux publics. Trois types de dispositifs permettent de remplir la fonction d'interconnexion : les ponts, les routeurs et les passerelles. Ils se distinguent par les niveaux auxquels ils fonctionnent dans le modèle OSI. Ponts, routeurs et passerelles montent respectivement au niveau 2, au niveau 3 et au niveau 7.

Comparaison pont-routeur :

| | PONT | ROUTEUR |
|---|---|---|
| Rapidité | Elevée | Moyenne |
| Coût | Bas | Elevé |
| Protocoles | Indifférents | Dépendants |
| Couches OSI | 2 | 3 |
| Economie en débits | Faible | Forte |
| Complexité | Faible | Forte |
| Maillage | Moyennement adapté | Parfaitement adapté |




Notion de routage :

Tous ces équipements, ponts "intelligents", routeurs, sont inséparables de la notion de routage, c'est-à-dire de la recherche du chemin le plus efficace, à travers les différents nœuds d'un réseau, pour que les trames atteignent leur destinataire. La "science" du routage, l'une des plus complexes et des plus vivantes, figure parmi les disciplines "nobles" des réseaux et des télécommunications. Le routage consistera à tenir à jour, dans les nœuds d'un réseau (*pont ou routeur*), des tables contenant les différents chemins. Les algorithmes et les formules foisonnent. On distinguera des systèmes de routage statique, où les tables sont fixées une fois pour toutes, des routages adaptatifs, où les tables sont modifiées en fonction de la charge des nœuds, où les routages locaux, dans lesquels chaque nœud ne connaît que sa propre table, des routages globaux, où un nœud aura une connaissance plus ou moins complète de l'ensemble des autres tables et de la topologie générale du réseau.

Deux types de routage émergent pour l'interconnexion de réseaux, l'arbre recouvrant ou Spanning Tree, et le routage par l'émetteur ou source routing, utilisés dans des ponts intelligents.

Le premier, assez simple, est un routage de proximité s'appliquant aux ponts dits transparents : à l'arrivée de chaque trame, le pont consulte une table qui contient les chemins correspondants à tous les nœuds immédiatement voisins. Le pont décidera d'abandonner ou de router la trame sur l'un de ses nœuds contigus. Au départ, les tables sont vides et les trames routées sur tous les nœuds, elles se garniront peu à peu par apprentissage ; chaque nœud notant l'adresse source des trames qui lui parviennent, il "apprend" la topologie de la partie d'arbre qui le concerne par décantations successives. Ce type de pont est dit transparent, parce qu'on peut le connecter sans aucune opération préalable de programmation et que les trames sont retransmises telles quelles. Cette méthode est utilisée notamment dans le monde des réseaux locaux DEC et Ethernet en mode sans connexion.

| SPANNING TREE | SOURCE ROUTING |
|---|---|
| Transparent | Non transparent |
| Configuration automatique | Configuration manuelle |
| Routage non optimisé | Routage optimal |
| Apprentissage arrière | Pas d'apprentissage |
| Incidents gérés par le pont | Incidents gérés par les stations |
| Complexité dans le pont | Complexité dans les stations |

L'autre méthode, celle du source routing, a la préférence du monde anneau à jeton. Dans cette méthode, il n'y a pas d'apprentissage, les différents réseaux et sous-réseaux sont numérotés, et chaque table de

routage est contenue dans la station émettrice d'une trame. La trame est précédée du chemin qu'elle doit emprunter. Si un pont constate qu'il figure dans ce chemin, il retransmet la trame, sinon il l'abandonne.

Ces algorithmes sont suffisants lorsqu'on reste dans le domaine des réseaux locaux et que l'on ne construit pas un réseau trop complexe. Avec les routeurs ils sont suffisants. Aussi les fabricants de ponts-routeurs et de routeurs ont-ils adopté des méthodes plus perfectionnées. Problème : ces méthodes sont nombreuses, mais incompatibles. Dans le monde TCP/IP, on trouve en particulier le RIP (*Routing Information Protocol*). Le RIP est aujourd'hui dépassé par l'IGRP (*Interior Gateway Routing Protocol*), un prolongement plus perfectionné du précédent, mais qui est un protocole propre à Cisco. L'ISO a retenu, pour les réseaux normalisés OSI, un protocole IS-IS (*Intermediate System to Intermediate System*). Un autre protocole, OSPF (*OpenShort Path First*), est candidat à jouer les rassembleurs dans l'environnement TCP/IP.

**Interconnexion directe -** L'interconnexion directe ou service de terminaison d'appel, consiste, pour un opérateur, à terminer un appel vers un abonné de France Télécom. L'appel est acheminé par l'opérateur jusqu'au point d'interconnexion ; il est ensuite pris en charge par France Télécom sur son réseau à partir du point d'interconnexion jusqu'au poste de cet abonné.

**Interconnexion en ligne -** Voir "colocalisation"

**Interconnexion forfaitaire -** Désigne une offre d'interconnexion entre les réseaux des opérateurs tiers et le réseau de France Télécom, selon laquelle les charges payées par les opérateurs tiers pour la collecte de trafic sur la boucle locale sont fixes par circuit et ne sont plus facturées à la minute.

**Interconnexion indirecte -** L'interconnexion indirecte ou service de collecte d'appel consiste, pour un opérateur, à collecter un appel d'un abonné de France Télécom qui utilise un préfixe pour sélectionner cet opérateur. L'appel est pris en charge par France Télécom depuis le poste de l'abonné jusqu'au point d'interconnexion, puis par l'opérateur nouvel entrant à partir de ce point.

**Interface -** Désigne tout dispositif assurant l'adaptation entre deux équipements et le contrôle des liaisons entre ces équipements.

Frontière entre deux systèmes ou entre deux parties d'un même système.

Dans le vocabulaire officiel du CCITT, désigne des modes d'adaptation normalisés entre des terminaux de transmission de données (ETTD) et un réseau. Exemple : interface R (adaptation de terminaux analogiques au RNIS Réseau numérique à intégration de services), interface S (adaptation d'un terminal RNIS à ce réseau), interface T (entre le système de transmission RNIS et la distribution interne de l'abonné)...

Eviter d'appeler interface un équipement d'adaptation entre deux systèmes; cet équipement possède, en effet, deux interfaces, une avec chaque système.

**Interface d'interconnexion -** Ensemble des règles techniques, nécessaires à la mise en œuvre concrète de l'interconnexion grâce à l'établissement d'un dialogue entre les réseaux, qui définissent les modalités physique d'interconnexion, les services et fonctionnalités avancées accessibles entre les réseaux concernés, les mécanismes de commande de ces services ainsi que leurs modalités de facturation et d'exploitation.

**Interface radio -** Dispositif permettant à un terminal mobile de communiquer avec le réseau. La normalisation de l'interface radio de l'UMTS a fait l'objet de nombreuses discussions au sein de l'ETSI en 1997. Le comité SMG a adopté, le 29 janvier 1998, la norme UTRA (UMTS Terrestrial Radio Access) pour l'interface radio terrestre (par opposition à l'interface radio des systèmes par satellite). La norme UTRA, qui résulte d'un compromis, comprend deux composantes au départ concurrentes : la norme WCDMA et la norme TD/CDMA. L'UTRA a été retenue par l'UIT en mars 1999 comme l'une des normes de l'interface radio pour l'IMT 2000.

**Interférence -** Mixage partiel entre plusieurs signaux électriques ou électromagnétiques. Les ondes électromagnétiques émises par un moteur ou un relais peuvent provoquer des interférences, c'est-à-dire perturber le signal électrique transmis par un câble voisin.

**Intermodulation -** Défaut erratique produit quand un courant d'une certaine fréquence induit un signal parasite de même fréquence sur un autre conducteur, par exemple entre deux câbles téléphoniques.

**Internet -** Interconnected Networks - Réseaux Interconnectés - Le réseau des réseaux. Internet est le plus grand réseau informatique du monde. Il est fait d'une interconnexion de l'ensemble des réseaux fonctionnant sous le protocole Internet (IP), une famille de protocoles de communication appelés TCP/IP : Transmission Control Protocol / Internetworking Protocol et Internet Protocol Suite.

Internet est aussi un réseau mondial constitué de milliers de réseaux hétérogènes, et interconnecté au moyen des protocoles TCP/IP, des réseaux locaux d'agences gouvernementales, institutions, d'éducation, hôpitaux, des commerciaux, …, des réseaux fédérateur de Campus, des réseaux Régionaux, des réseaux nationaux, des réseaux intercontinentaux (Américains, Européen, Eunet, Ebone), et Asiatiques, … Internet c'est enfin une communauté de personnes utilisant différents services (Courrier électronique, Web, Transfert de fichiers FTP, …)

Réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers.
Il fonctionne en utilisant un protocole commun qui permet l'acheminement de proche en proche de

messages découpés en paquets indépendants. Ce réseau international regroupe plus de 60 000 réseaux d'ordinateurs utilisant le même protocole de communication : TCP-IP. L'acheminement est fondé sur le protocole IP (Internet Protocol), spécifié par l'Internet Society (ISOC). L'accès au réseau est ouvert à tout utilisateur ayant obtenu une adresse auprès d'un organisme accrédité. La gestion est décentralisée en réseaux interconnectés.

Protocole de la couche 3 (Voir ISO) utilisé pour transmettre des données entre deux sous-réseaux différents. Normalisé par l'ISO sous le nom ISO 8073.

Attention, dans la mesure où historiquement l'un des premiers protocoles ayant permis cette fonction était le protocole IP (Internet Protocol) de la Défense américaine, l'expression désigne aussi ce protocole non officiellement normalisé. Un groupement baptisé IETF (Internet Engineering Task Force) est également souvent nommé groupement Internet; il a pour mission le développement des protocoles d'interconnexion de réseaux dans le cadre de TCP/IP.

Historique :

- 1969 : Début du réseau (D) ARPANET (4 calculateurs) DARPA = Defense Advanced Research Projects Agency
- 1972 : Démonstration de ARPANET, IMP - Interface Message Processor - mode connecté (X.25), NCP - Network Control Program - non connecté (ancêtre de TCP)
- 1977 - 1979 : Les protocoles TCP/IP prennent leur forme définitive,
- 1980 - L'université de Berkeley intègre TCP/IP dans Unix (BSD)
- 1980 - janvier 1983 : Tous les réseaux raccordés à ARPANET sont convertis à TCP/IP
- 1983 - TCP/IP devient le Standard de facto pour l'interconnexion de réseaux hétérogènes,
- 1988 - Mise en place du Backbone de la NSFnet (12 réseaux régionaux)
- 1992 - EBone et RENATER
- 199x - explosion de l'offre et de la demande de services Internet, y compris pour les particuliers
- 1995 - Arrêt du Backbone NSFnet, Mise en œuvre des NAPs (Network Access Points)

Principes d'Internet :

- Mode Client-Serveur
- Fonctions intelligentes à la périphérie (terminaux)
- Fonctions simples dans le cœur du réseau (routeurs),
- Mode "connecté "ou "non connecté "
- Mode Datagramme
- Routage dynamique
- Commutation de paquets
- Réseau "Best Effort "

**Internet 2 -** Plus de 180 universités américaines, regroupées au sein de l'UCAID (University Corporation for Advanced Internet Développement), travaillent au sein de ce réseau privé fondé en 1996. Des accords de coopération se sont mis en place avec Renater en France et Canarie au Canada.

**Internet commuté -** Désigne l'accès à Internet à partir du réseau téléphonique commuté, réseau public de France Télécom qui achemine les appels téléphoniques classiques.

**InterNIC -** Internet Network Information Center - Organisation chargée de l'enregistrement des adresses IP et des noms de domaine.

L'InterNIC est l'organisation qui s'occupe de gérer les noms de domaine sous .COM, .ORG ou .NET. Son site Internet peut renseigner sur la liste des divers NIC nationaux. InterNIC est un service du département du commerce américain.

**Interopérabilité -** L'interopérabilité des services correspond à la possibilité des différents services de fonctionner indifféremment sur des réseaux différents. Dans le cadre de l'interconnexion, les fonctionnalités techniques disponibles à l'interface d'interconnexion déterminent ainsi en partie l'interopérabilité des services entre les différents opérateurs.

**Interpac -** Filiale de Transpac destinée à fournir des services internationaux de commutations par paquets à partir de la France. Elle utilise le réseau Infonet.

**INTIS -** INternational Transport Information System - L'un des plus importants systèmes d'Echange de données informatisé (EDI) dans le domaine portuaire, proposé par les autorités du port de Rotterdam.

**Intranet -** Un réseau intranet est un réseau fondé sur la technologie IP (Internet Protocol) réservé aux communications internes d'une entreprise ou d'un organisme. Il permet de bénéficier de la norme IP pour l'échange des informations et d'une présentation conviviale des informations, le langage HTML autorisant une lecture non linéaire des pages consultées, grâce à l'utilisation de liens hypertexte (on peut passer d'une rubrique à l'autre par un simple "clic" de souris). Son utilisation est ainsi facilitée par une présentation conviviale et pratique, comparable à celle des sites Web que l'on peut consulter sur le réseau mondial Internet.

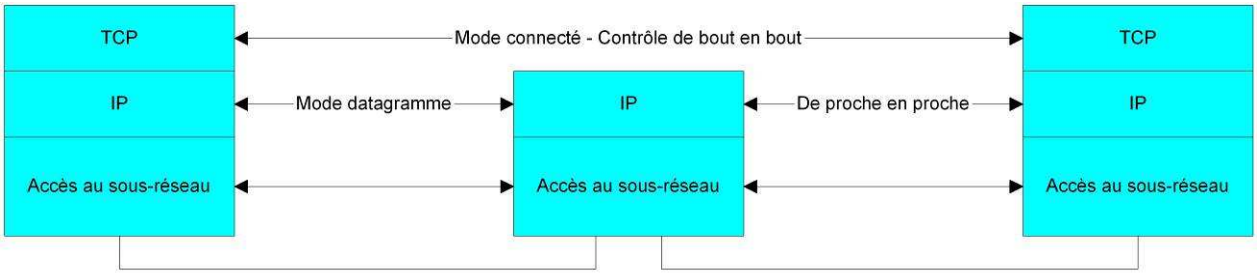
**IntServ -** Integrated Services - Mécanisme qui garantit la qualité de service. Il réserve de la bande passante dans les équipements que traversent les données, de bout en bout, en utilisant la signalisation RSVP. IntServ propose trois options selon le niveau de qualité requis.

**Inversion de phase -** Technique de modulation dans laquelle ce sont les changements de phase qui sont significatifs.

**Invitation à émettre -** Equivalent de la technique du polling, ou scrutation. Procédure centralisée permettant une communication multipoint et où chaque terminal est tour à tour invité à envoyer son message (où à répondre qu'il n'a pas de message à transmettre).

**Invitation à recevoir** (selecting) - Technique identique à la précédente lorsque c'est l'équipement maître qui désire envoyer un message à un terminal.

**IP (IPv4) -** Internet Protocol v4 - Protocole d'interconnexion de deux sous-réseaux développé dans le cadre de la Défense américaine. A été l'un des premiers protocoles permettant d'interconnecter des sous-réseaux ayant des caractéristiques physiques différentes.




IP spécifie un service réseau en mode datagramme. Ce service, non fiable, est sécurisé par la couche transport (TCP) qui met en œuvre un mode connecté de bout en bout autorisant un mécanisme de détection et de reprise sur erreur, un contrôle de séquencement ainsi qu'un contrôle de flux

Protocole de base du réseau Internet, IP permet la transmission de données à travers des réseaux hétérogènes en les découpant par paquets.

La fonction ou rôle du Protocole Internet est d'acheminer les datagrammes à travers un ensemble de réseaux interconnectés. Ceci est réalisé en transférant les datagrammes d'un module Internet à l'autre jusqu'à atteindre la destination. Les modules Internet sont des programmes exécutés dans des hôtes et des routeurs du réseau Internet. Les datagrammes sont transférés d'un module Internet à l'autre sur un segment particulier de réseau selon l'interprétation d'une adresse Internet. De ce fait, un des plus importants mécanismes du protocole Internet est la gestion de cette adresse Internet.

Lors de l'acheminement d'un datagramme d'un module Internet vers un autre, les datagrammes peuvent avoir éventuellement à traverser une section de réseau qui admet une taille maximale de paquet inférieure à celle du datagramme. Pour surmonter ce problème, un mécanisme de fragmentation est géré par le protocole Internet.

**IP Multicast -** Protocole de distribution d'information en ligne où la séparation des paquets est réalisée le plus tard possible dans le but d'optimiser le trafic du réseau sur les distances importantes. (voir Multicast).

**IP/TV -** Cisco Propriétaire - IP/TV a été spécialement conçu pour offrir des solutions de flux continu de données multimédia de haute qualité. Ajouté à la technologie multicast IP, IP/TV permet d'optimiser l'efficacité du réseau ainsi que la qualité du flux vidéo. Le logiciel de gestion de contenu permet d'organiser plusieurs flux multicasts de même contenu de sorte à exploiter au maximum l'efficacité du multicast lorsqu'il s'agit de flux destinés à de grandes audiences. IP/TV 2.0 offre par ailleurs une solution de vidéo à la demande (VOD) en utilisant l'unicast pour visionner en individuel des données multimédias stockées sur le serveur de vidéos. Enfin, IP/TV supporte la majeure partie des standards dédiés à la vidéo sur Internet, comme le multicast, ce qui lui garanti une bonne interopérabilité et permet de participer activement à l'élaboration et aux tests de ces nouveaux standards.

La solution de Cisco se décompose en serveurs dédiés et à la mise en place de services de communication vidéo de qualité sur des réseaux d'entreprises. Ces serveurs peuvent offrir de la vidéo en direct, de la vidéo planifiée, de la vidéo à la demande (VOD) et d'autres fonctionnalités pour la vidéo. Elles offrent un large éventail d'applications pour les communications en entreprise comme la formation, la communication Internet, la formation à distance…

La famille de serveurs est constituée de serveurs de contrôle, de broadcast, d'archivage et du système de démarrage vidéo.

**IPBX -** Internet Protocol-Private Branch Exchange - Autocommutateur privé d'entreprise utilisé pour la téléphonie sur IP.

**I-PNNI -** Integration Private Network Network Interface (ATM).

**IPNS -** ISDN PABX Networking Specification - Système opérationnel de signalisation entre autocommutateurs privés proposé par les principaux constructeurs européens à l'initiative d'Alcatel et de Siemens. Il permettra d'interconnecter des autocommutateurs de marques différentes.

**IPOA -** IP over ATM - Cette architecture a été proposée par l' IETF's IPOA WG. Ici, un groupe de stations ATM est divisé sous réseaux IP logiques (LIS : Logical IP Subnet), interconnectés par des routeurs. Chaque ILS a un serveur ARP (Address Resolution Protocol) ATM pour la résolution entre l'adresse IP et l'adresse ATM. Il n'y a pas de service de broadcast au sein du LIS. Dans cette architecture aussi, les noeuds dans différents LIS communiquent via des routeurs même s'ils sont directement connectés.

**IPS -** Intrusion Prevention System - Fonction intégrée ou pas à un autre équipement, un IPS et un outil qui analyse, la totalité du trafic et bloque en temps réel, sans intervention humaine, les attaques caractérisées.

Sa capacité à observer les flux applicatifs en fait le complément idéal d'un coupe-feu (FireWall). Toujours installé en coupure, ils se caractérisent par une simplicité de mise en œuvre qui nécessite cependant un temps d'adaptation au contexte dans lequel il est inséré. Cet outil complète les outils spécialisés placés en passerelle tels que Antivirus, anti pourriels, Firewall, etc. etc.

**IPSEC -** Protocole qui permet d'encrypter les données qui vont transiter sur un réseau RPV (Réseau Privé Virtuel). Ce protocole a été défini par l'IETF. Ensemble de normes de sécurité offrant des services de confidentialité et de d'authentification au niveau de la couche IP (Internet Protocol).

Certaines entreprises souhaitent que les données soient cryptées afin d'échapper aux regards d'éventuels pirates ou de concurrents mal intentionnés. IPsec est le complément naturel du protocole L2TP. Il adresse les besoins de confidentialité des données transmises sur Internet. Le standard IPsec est complexe du fait des nombreuses fonctions qui lui incombent. II inclut en effet les services de confidentialité (encryptage), d'authentification (certification de l'émetteur), d'intégrité (détection des tentatives de détournement d'information) et de protection des réémissions. 11 permet ainsi de se protéger contre les réémissions non autorisées d'informations.

IPsec peut être utilisé au niveau des équipements terminaux ou au niveau de passerelles de sécurité, permettant ainsi des approches de sécurisation "lien par lien" ou "de bout en bout". IPsec peut être utilisé pour créer des réseaux privés virtuels mais aussi pour sécuriser des accès distants. Enfin, pour en finir avec ses caractéristiques, signalons que IPsec comporte deux modes, le mode transport, qui protège juste les données transportées, et le mode tunnel, qui protège en plus l'en-tête IP. Avec IPsec, il est donc possible de renforcer de manière significative la sécurité d'un VPN et de se prémunir efficacement contre tout détournement des informations transitant sur le réseau.

IPsec fait appel à deux mécanismes de sécurité pour le trafic IP: les mécanismes AH (Authentication Header) et ESP (Encapsulating Security Payload).

- AH est un entête conçu pour assurer l'intégrité et l'authentification des datagrammes IP sans chiffrement des données. Son but est d'ajouter aux datagrammes IP classiques un champ supplémentaire permettant, lorsqu'ils arrivent à destination, de vérifier l'authenticité des données incluses dans le datagramme.
- ESP a, quant à lui, pour objectif d'assurer la confidentialité des données. II peut aussi être utilisé pour garantir leur authenticité. À partir d'un datagramme IP, l'ESP génère un nouveau datagramme dans lequel les données, et éventuellement l'en-tête original, sont chiffrés.

AH et ESP utilisent tous les deux un certain nombre de paramètres (algorithmes de chiffrement, clés, mécanismes sélectionnés...) sur lesquels les équipements doivent s'entendre afin d'être sûrs de pouvoir communiquer. Ces paramètres sont gérés grâce à la Security Association (SA), une base de données où sont stockées les informations décrivant l'ensemble des paramètres associés à une communication donnée. Cette base de données contient donc la clé utilisée pour le cryptage des données. IPsec spécifie en outre une méthodologie pour la gestion des clés: il s'agit de l'Internet Key Exchange (IKE). Cette méthodologie décrit une série d'étapes afin de définir les clés utilisées pour l'encryption et pour le décryptage des données. II s'agit en fait de définir un langage commun afin que les deux parties puissent s'entendre.

**IPSS -** International Paquet Switching Service - Service international de commutation de paquets proposé par le réseau britannique PSS.

**IPv6 -** Dès 1993, l'IETF (Internet Engineering Task Force) constitue un groupe de travail IPng (Internet Protocol next generation) dont la principale mission consiste à trouver une solution à la pénurie des adresses IP (couche 3 réseau), les 32 bits réservés à l'identification logique des équipements terminaux et la structure de découpage n'étant plus adaptés.

IPng est une nouvelle version d'IP qui s'inscrit comme l'évolution naturelle et normale du protocole IP en place IPv4. Protocole IPv4 qui, tout en ayant permis l'énorme croissance de l'Internet, souffre de plusieurs faiblesses. IPng est conçu pour fonctionner aussi bien sur des réseaux à très hauts débits comme ATM que sur des réseaux à faible bande passante tels que les réseaux sans fils.

Les spécifications d'IPng sont assujetties à un certain nombre de critères techniques. La liste de ces critères est impressionnante :

- Etre bâties autour de standards ouverts et accessibles au public.

- Définir une méthode de migration claire et réaliste.
- Permettre la gestion d'au moins un milliard de réseaux, soient mille milliards de stations, avec auto configuration des adresses et mise en place d'un adressage global et unique de chaque équipement, même en présence d'une structuration topologique.
- Utiliser les méthodes de routage RIP, OSPF, etc.
- Etre indépendantes du réseau physique, le Flow Label d'IPng doit même pouvoir correspondre avec les circuits virtuels ATM.
- Supporter les diverses topologies de réseaux interconnectés et un service de type datagramme (orienté sans connexion).
- Exploiter de façon optimisée les réseaux à hautes performances d'où le choix d'un en-tête sans contrôle de parité et cadré sur des multiples de 4 octets.
- Garantir la sécurité de certaines opérations, comme l'authentification ou le cryptage spécifique du niveau 3 réseau.
- Supporter la diffusion de groupe (multicast).
- Gérer plusieurs classes de services (avec le Flow Label).
- Incorporer des protocoles de contrôle semblables à ceux de IPv4 (Ping, Traceroute).
- Permettre l'encapsulation de divers protocoles dans IPng.
- Offrir un service fiable et robuste.

Tous ces éléments sont décrits dans la RFC 1752 publiée en Janvier 1995 et complétés par l'IPng Overview disponible dès Octobre 1994.

Synthèse des principales caractéristiques apportées dans IPv6 :

- Un espace d'adressage limité (32 bits).
- Une explosion des tables de routage principalement due à la faible profondeur de la hiérarchie d'adressage.
- L'impossibilité actuelle d'indiquer dans les paquets IPv4 le type de données transportées, son urgence mais aussi la quasi-absence de moyens d'auto configuration, d'adressage des mobiles, de mécanismes de sécurité.
- IPv6 vise à résoudre l'ensemble de tous ces problèmes en proposant les éléments suivants.
- La très forte progression des réseaux et machines installés sur l'Internet (jusqu'à $10^{12}$ réseaux et $10^{15}$ machines).
- Des schémas de routage prudents, adaptables à de nombreuses topologies, bénéficiant de performances élevées.
- Un schéma de transition directe d'IPv4 à IPv6.
- Un service résistant, en mode datagramme ; mais aussi différentes classes de service.
- Une auto configuration possible.
- Un fonctionnement sûr.
- Des noms uniques au niveau mondial.
- Un accès libre aux différents standards existant.
- Une diffusion restreinte (multicasting).
- Des possibilités d'extension.
- La prise en compte de la mobilité.
- L'inclusion d'un protocole de contrôle.
- Des réseaux fermés (tunneling).

En résumé, lors de sa conception, IPv6 devait logiquement être considéré comme l'évolution normale de l'Internet facilitée par son entière compatibilité avec IPv4 et, par conséquent connaître un déploiement stratégique très rapide. Or, la transition vers IPv6 sera vraisemblablement longue et peut-être même douloureuse. Elle ne connaîtra pas, dans tous les cas, un phénomène de "flag day", grand jour où tout basculerait, comme espéré initialement.

En effet, si dans les organismes de recherche, les travaux sur IPv6 semblent très convaincants, il convient de bénéficier d'un autre soutien et non des moindres, à savoir celui des grands constructeurs.

**IPv6 - DESCRIPTION DES PRINCIPALES CARACTÉRISTIQUES [RFC 1752] -** IPv6 est la nouvelle version d'IP et représente une très forte évolution par rapport à IPv4. Les principales fonctionnalités d'IPv4 sont conservées dans IPv6 excepté certaines fonctions peu ou pas utilisées qui ont été supprimées ou rendues optionnelles. En outre, quelques priorités ont été ajoutées.

Il est possible de dégager huit grandes caractéristiques inclues dans IPv6.

- Des possibilités étendues d'adressage et de routage.

La taille de l'adresse IP augmente de 32 à 128 bits afin de supporter un plus grand nombre de nœuds adressables, davantage de niveaux d'adressage hiérarchique ainsi qu'une auto configuration plus simple des adresses.

Un mécanisme adaptable de diffusion ainsi qu'un nouveau type d'adresses en "cluster" sont définis dans

IPv6.

- Un format d'en-tête simplifié.

Des champs du format de l'en-tête IPv4 ont été abandonnés ou rendus optionnels, ainsi l'en-tête IPv6 est simplifié et réduite à un traitement commun dans tous les routeurs ce qui diminue donc le coût de traitement dans ces routeurs.

- Des possibilités d'extension des en-têtes et des options

Dans IPv6, les options sont rangées dans des en-têtes supplémentaires situés entre l'en-tête IPv6 et l'en-tête du paquet de transport (T-PDU, Transport Protocol Data Unit ou Unités de données du service de transport). La plupart des options dans les en-têtes IPv6 ne sont ni examinées, ni traitées par les routeurs intermédiaires. Contrairement à IPv4, les options IPv6 peuvent être de longueur arbitraire, il n'existe pas de taille limite.

Une des caractéristiques d'IPv6 est la possibilité de coder, dans les options, l'action qu'un routeur ou une station de travail doit réaliser si l'option est inconnue, ce qui permet l'ajout de fonctionnalités supplémentaires dans un réseau déjà opérationnel avec un minimum de perturbations.

- Des possibilités d'authentification et de confidentialité

IPv6 intègre des extensions permettant l'authentification des usagers et l'intégrité des données grâce à des outils de cryptographie.

- Des possibilités d'auto configuration

IPv6 dispose de plusieurs formes d'auto configuration comme la configuration "plug and play" d'adresses de nœuds sur un réseau isolé grâce aux caractéristiques offertes par DHCP.

- Des possibilités pour le "Source Route"

IPv6 intègre une fonction étendue de source routing grâce à SDRP (Source Demand Routing Protocol) afin d'étendre le routage à des routes inter domaine et intra domaine.

- Une transition d'IPv4 à IPv6 simple et flexible

La transition d'IPv4 à IPv6 répond à quatre objectifs essentiels :

  - Un besoin de modernisation,
  - Un besoin de redéploiement,
  - Un adressage facile,
  - Une diminution du coût de démarrage.

- Des possibilités de qualité de service

L'introduction de flux étiquetés (avec des priorités), les services de contraintes "temps réel" sont de nouveaux éléments rendant possible la qualité de service.

**IPv6 - FORMAT D'EN-TÊTE [RFC 1752] -** Bien que plus longue que la version 4 d'IP, l'en-tête de IPv6 a été simplifiée. Un certain nombre de fonctions présentent dans l'en-tête d'IPv4 ont été soit disposées dans des en-têtes supplémentaires, soit abandonnées.

Les champs que l'on retrouve dans un en-tête IPv6 sont les suivants :

- Version (4 bits) - Ce champ défini le numéro de version du Protocole IP. (IPng est la version 6).
- Flow Label (28 bits) - Ce champ, étiquette de flux, peut être utilisé par une station pour "marquer" certains paquets afin qu'ils suivent un routage (service) particulier dans un réseau, tel un service de qualité sans défaut, ou un service "temps-réel".
- Payload Length (16 bits) - Ce champ représente la longueur des données après l'en-tête IPv6 en octets. Pour étendre cette valeur à plus de 64 Koctets, la valeur est donnée dans une option nœud-par-nœud. Le champ "longueur données" est alors à 0.
- Next Header (8 bits) - Ce champ identifie le type d'en-tête suivant immédiatement l'en-tête IPv6. Ce champ est le même que le champ protocole d'IPv4.
- Hop limit (8 bits) - Ce champ est utilisé pour détruire les paquets qui pourraient rester dans le réseau à la suite de boucles dues aux tables de routage, ce champ est décrémenté de une unité à chaque nœud qui retransmet le paquet (équivalent au Time To Live d'IPv4 - durée de vie).
- Source Address (128 bits) - Ce champ contient l'adresse de l'émetteur du datagramme.
- Destination address (128 bits) - Ce champ contient l'adresse du destinataire du paquet. Il est possible que l'adresse ne soit pas celle du destinataire final si une option de routage est présente.

**IPv6 - FORMAT D'EN-TÊTES SUPPLÉMENTAIRES [RFC 1752]** - Des informations complémentaires sont codées dans des en-têtes qui doivent être placées dans le paquet entre l'en-tête IPv6 l'en-tête de la couche transport. Il y a un petit nombre d'extensions d'en-tête, chacun identifié par une valeur de Next Header distincte. Un paquet IPv6 peut comporter aucune, une ou plus d'en-têtes supplémentaires,

Mise à part une exception, les en-têtes supplémentaires ne sont nullement examinés ou manipulés par les nœuds atteints par le paquet le long de son chemin, jusqu'à ce que le paquet arrive au nœud (ou à chaque groupe de nœuds dans le cas du multicast) identifié par le champ adresse destinataire de l'en-tête IPv6. A ce moment là, le premier en-tête supplémentaire, ou l'en-tête transport dans le cas d'absence d'en-tête supplémentaire, est traité. Le contenu de chaque en-tête déterminera s'il faut, ou pas, traiter l'en-tête suivant.

La seule exception est l'en-tête de l'option nœud-par-nœud, elle porte des informations qui doivent être examinées par les nœuds du réseau. Cet en-tête "Hop-by-Hop" Options, lorsqu'elle est présente, doit suivre immédiatement l'en-tête IPv6.

Chaque en-tête supplémentaire est d'une longueur d'un multiple de 8 octets, afin de conserver un alignement de 8 octets pour les en-têtes suivants.

Ordre des en-têtes supplémentaires

Lorsqu'il y a plus d'un en-tête supplémentaire utilisé dans le même paquet, les en-têtes doivent apparaître dans l'ordre suivant :

- IPv6 Header
- Hop-by-Hop Options Header
- Routing Header
- Fragment Header
- Authentication Header
- End-to-End Options Header

Chaque type d'en-tête ne doit apparaître qu'une seule fois dans le paquet (excepté dans le cas d'une encapsulation IPv6 dans IPv6, où chaque en-tête IPv6 encapsulé doit être suivi par son propre en-tête supplémentaire).

Option nœud-par-nœud

L'en-tête d'options nœud-par-nœud comporte des informations analysées par les différents nœuds du chemin pris par le paquet. L'en-tête des options nœud-par-nœud est identifié par une valeur de Next Header égale à 0. Les champs de l'en-tête sont les suivants :

- Next Header (8 bits): identifie le type d'en-tête suivant immédiatement l'en-tête d'options nœud-par-nœud. Les valeurs sont identiques au champ de protocole de IPv4.
- Hdr Ext Len (8 bits): longueur de l'en-tête des options nœud-par-nœud en multiple de 8 octets, à l'exclusion des 8 premiers.
- Options: ce champ contient une ou plusieurs options codées en TLV (Type-Length-Value). Ce premier est de longueur variable, il est un multiple de 8 octets.

Options d'en-tête IPv6

Deux des en-têtes supplémentaires actuellement définis, celle des options nœud-par-nœud et celle des options bout-en-bout, doivent porter un nombre variable d'options codées TLV suivants les options suivantes:

- Option Type (8 bits): identifiant de la nature de l'option.
- Opt Data Len (8 bits): longueur du champ de données de cette option en octets.
- Option Data (longueur variable): données de l'option. Champ de longueur variable.

Les identifiants Option Type sont codés de manière à ce que les deux bits de poids fort provoquent l'opération suivante si un nœud ne reconnaît pas le Option Type:

| | |
|---|---|
| 00 | ne traite pas cette option et poursuit le traitement de l'en-tête |
| 01 | détruit le paquet |
| 10 | détruit le paquet et envoie à l'adresse source un message ICMP de non reconnaissance, et indique la faute en donnant le Option Type. |
| 11 | non défini |

Dans le seul cas des options nœud-par-nœud, le troisième bit de poids fort de Option Type indique si les données de cette option doivent être soumises au calcul d'assurance intégrité lorsque l'en-tête d'authentification est présente. Les données de l'option modifiées en cours de routage sont exclues de ce calcul.

0 inclus un calcul d'intégrité

1 exclus du calcul d'intégrité

Les champs Option Data des options de bout-en-bout ne changent jamais en route et donc, sont toujours inclus dans le calcul d'intégrité.

En-tête de routage

L'en-tête de routage est utilisé par une source pour établir une table de nœud(s) intermédiaire(s) (ou ensemble de groupes) que doit emprunter le paquet pour arriver à destination. Cette forme particulière d'en-tête de routage est conçue pour supporter le "protocole de routage à la demande de la source" (Source Demand Routing Protocol, SDRP) [Estrin94b].

Les champs de l'en-tête sont les suivants :

- Next Header: identifie le type d'en-tête suivant immédiatement l'en-tête de routage. Les valeurs sont identiques au champ de protocole de IPv4.
- Routing Type: indique le type de routage supporter par cette en-tête. La valeur est 1.
- MRE (Must Report Errors) flag: si ce bit est à 1 et qu'un routeur ne puisse émettre, conformément à

la liste Source Route, le paquet (avec un routage incomplet), le routeur génère un message d'erreur ICMP. Dans le cas où le bit MRE est à 0, le routeur ne génère pas de message d'erreur ICMP.

- F (Failure of Source Route Behavior) flag (1 bit): si ce bit est positionné à 1, il indique que si un routeur ne peut acheminer plus loin un paquet (avec un routage incomplet), comme spécifié dans le Source Route, le routeur fixe la valeur du champ Next Hop Pointer à la valeur du champ Source Route Length. Ainsi la destination suivante du paquet sera uniquement basée sur l'adresse de destination (destination address). De même si le bit F est à 0, alors dans les mêmes conditions, le routeur détruira le paquet.
- Reserved (6 bits): initialisé à 0 à l'émission, ignoré à la réception.
- Source Route Length (8 bits): c'est le nombre d'éléments/nœuds dans un en-tête de routage SDRP. La longueur de cet en-tête peut être calculée à partir de cette valeur (longueur=SrcRouteLen*16+8). Ce champ ne doit pas excéder la valeur de 24.
- Next Hop Pointer (NextHopPtr - 8 bits): il pointe les éléments/nœuds à atteindre. Il est initialisé à 0 pour pointer le premier élément/nœud de Source Route. Quand il est égal au Source Route Length, alors le Source Route est terminé.
- Strict/Loose Bit Mask (24 bits): ce masque est utilisé pour prendre une décision d'aiguillage à un nœud. Si la valeur de Next Hop Pointer est N, alors que le $N^{ième}$ bit du Strict/Loose Bit Mask est à 1, cela indique que le prochain nœud est un nœud Strict Source Route Hop. Tandis que s'il est à 0, le prochain nœud est un Loose Route Hop.
- Source Route (multiple de 128 bits): c'est une liste d'adresses IPv6, indiquant le chemin à suivre par le paquet. Le Source Route peut contenir un ensemble d'adresses de types unicast et cluster.

En-tête de fragmentation :

L'en-tête de fragmentation est utilisé par la source pour envoyer des paquets plus grands que ne peut acheminer le réseau à leurs destinataires. A la différence de la version 4 d'IP, la fragmentation est exécutée seulement par les nœuds source et non plus par les routeurs qui acheminent les paquets le long du chemin. L'en-tête de fragmentation est repéré par une valeur de Next Header égale à 44 juste après le précédent en-tête. Les champs de l'en-tête sont les suivants :

- Next Headr (8 bits): identifie le type d'en-tête suivant immédiatement l'en-tête de fragmentation. Les valeurs sont identiques au champ de protocole de IPv4.
- Reserved (8 bits), Res (2 bits) : initialisés à 0 à l'émission, ignorés à la réception.
- Fragmentation Offset (13 bits): il indique la position du premier octet dans le datagramme total (non fragmenté). Le premier fragment à la place 0. La valeur du champ est un multiple de 8 octets.
- M flag (1 bit): si le bit est à 1, il reste un ou des fragments. Tandis que s'il est à 0 il n'y en a plus.
- Identification (32 bits): une valeur assignée au paquet d'origine qui est différente de tous les autres paquets fragmentés récemment avec la même adresse source, les mêmes adresses de destination et valeur du Fragment Next Header. Ce champ permet d'identifier le datagramme pour sécuriser le réassemblage des paquets. Le numéro d'identification est porté par l'en-tête de tous les différents fragments.

En-tête d'authentification

L'en-tête d'authentification est utilisé pour authentifier et assurer l'intégrité des paquets. La non-répudiation est obtenue par un algorithme d'authentification exécuté sur l'en-tête d'authentification. Mais elle n'est pas obtenue par tous les algorithmes d'authentification exécutés sur cet en-tête. L'en-tête d'authentification est déterminé par la valeur 51 du champ Next Header, et les champs de l'en-tête sont les suivants :

- Next Header (8 bits): identifie le type d'en-tête suivant immédiatement l'en-tête d'authentification. Les valeurs sont identiques à celles du champ de protocole de IPv4.
- Authentication Data Length (Auth Data Len - 8 bits): c'est la longueur du champ Authentication Data, multiple de 8 octets.
- Reserved (16 bits): initialisé à 0 à l'émission, ignoré à la réception.
- Security Association ID (SAID - 32 bits): lorsqu'il est combiné avec l'adresse source, il identifie au(x) destinataire(s) le type de sécurité établi, associé au paquets concernés.
- Authentication Data (longueur variable): information sur l'algorithme spécifique nécessaire à authentifier la source du paquet et à assurer son intégrité conformément à la sécurité associée. La longueur de ce champ est variable et est un multiple de 8 octets.

En-tête de confidentialité

L'en-tête privé cherche à donner une confidentialité et une intégrité en cryptant les données à protéger et en les plaçant dans la section données de l'en-tête de confidentialité (Privacy Header). Suivant les exigences de sécurité de l'utilisateur, soit la trame de couche transport (e.g. UDP ou TCP) est cryptée, soit le datagramme entier d'IPv6 l'est. Cette approche par encapsulation est nécessaire pour assurer une confidentialité du datagramme complet original. S'il est présent, l'en-tête de confidentialité est toujours le dernier champ non-crypté dans un paquet.

Le Privacy Header travaille entre stations, entre une station et une Gateway (passerelle) de sécurité, ou entre des gateways de sécurité. Ceci permet sans d'importants coûts financiers et de performance d'assurer

un réseau digne de confiance en transitant du trafic sécurisé sur des segments du réseau qui ne le sont pas.
Les champs de l'en-tête sont les suivants :

- Security Association Identifier (SAID - 32 bits): identifie le type de sécurité au datagramme. Si aucune association de sécurité n'a été établie, la valeur de ce champ est 0x0000. Une association de sécurité est unilatérale. Une communication sécurisée entre deux stations doit avoir normalement deux SAID (un pour chaque sens des échanges). La station destinataire utilise la combinaison de la valeur du SAID et de l'adresse origine pour distinguer la correcte association.
- Initialization Vector (longueur dépendant du SAID): ce champ est optionnel et sa valeur dépend du SAID utilisé. Par exemple, le champ peut contenir des données de synchronisation de cryptographie pour un algorithme de codage. Il peut aussi contenir un vecteur d'initialisation cryptographique. L'implantation d'une en-tête de confidentialité utilisera une valeur de SAID pour déterminer si le champ n'est pas vide, et si c'est le cas, évalue la longueur du champ et l'utilise.
- Next Header (8 bits), crypté: identifie le type d'en-tête suivant immédiatement l'en-tête de confidentialité. Les valeurs sont identiques à celles du champ de protocole de IPv4.
- Reserved (17 bits), crypté: ignoré à la réception.
- Length (8 bits), crypté: longueur de l'en-tête privé, à l'exclusion des 8 premiers octets, donnée en un multiple de 8 octets.
- Protected Data (longueur variable), crypté: ce champ peut contenir un datagramme complet encapsulé IPv6, une séquence d'option(s) IPv6 ou pas, et enfin le paquet de la couche transport. Ou bien, il est constitué du paquet de la couche transport précédé ou pas d'une série d'option(s).
- Algorithme-dependant Trailer (trailer - longueur variable suivant SAID), crypté: ce champ est utilisé pour faire du bourrage (nécessité de certains algorithmes) ou pour enregistrer des données d'authentification à utiliser avec un algorithme de cryptographie qui fournit la confidentialité sans l'authentification. Ce champ n'est présent que si l'algorithme utilisé le nécessite.

En-tête de bout-en-bout

L'en-tête d'options bout-en-bout donne une information optionnelle qui doit être contrôlée par le(s) nœud(s) destinataire(s) du paquet. L'en-tête des options bout-en-bout est identifié par une valeur de Next Header de TBD suivant immédiatement l'en-tête précédent, et a le même format que l'en-tête d'option nœud-par-nœud, à l'exception de la capacité d'exclure une option de calcul d'intégrité.

**IPv6 - La Mobilité -** Le concept de mobilité signifie, dans le cas présent, la séparation des identificateurs et des adresses, ces deux éléments possédant un format similaire. L'identificateur d'un nœud mobile ne change jamais quelque soit ses déplacements tandis que son adresse est spécifique à son point de rattachement à Internet (l'identificateur est un numéro attribué à un nœud unique. Chaque nœud dispose de son propre identificateur indépendamment du nombre d'interfaces réseaux dont il bénéficie. Non seulement un identificateur est unique et définitif quelque soit le nœud de rattachement à l'Internet, mais il bénéficie du même format qu'une adresse classique ce qui lui permet éventuellement de se substituer à une adresse). L'adresse est seulement utilisée pour le routage des paquets et non pour l'identification du nœud à l'inverse de l'identificateur qui peut même éventuellement servir d'adresse par défaut.

Deux options ont été rajoutées dans les options de l'en-tête de type Hop-by-Hop afin de rendre possible la mobilité. L'une est utilisée pour la communication de données et l'autre pour le contrôle.

TCP/UDP identifie un nœud par son identificateur et non son adresse. Afin d'optimiser le routage, chaque nœud dispose d'une partie cachée ou Address Mapping Table (AMT). IPv6 résout le problème de l'identificateur et de l'adresse en utilisant AMT, puis en renvoyant le paquet avec la prise en compte de son adresse complète.

Les entrées AMT (table constituée d'entrées pour chacune desquelles il y a l'information de routage entre l'identificateur et l'adresse. Chaque nœud doit disposer d'une AMT pour la résolution d'adresse) sont créées puis mises à jour en fonction de la réception ou de l'envoi de paquets selon les options de mobilité choisies après, bien entendu, l'authentification du paquet.

Les formats d'en-tête pour l'option de mobilité :

Deux options pour la mobilité sont possibles via les propriétés de l'en-tête IPv6 Hop-by-Hop. La raison principale pour laquelle ces options sont inclues dans l'en-tête IPv6 Hop-by-Hop est la possibilité de créer et de mettre à jour des entrées AMT sur chaque nœud le long du chemin suivi par le paquet envoyé.

- Format de l'entête avec l'option de mobilité pour les données utilisateur :
  - Option Type - Ce champ prend pour valeur 0x2 ?, ce qui signifie que cette option ne relève pas de la propriété d'évaluation de l'intégrité obtenue via l'en-tête d'authentification dans la mesure où les données de l'option peuvent évoluer.
  - Option Data Length - La longueur est de 64 octets.
  - Source Identifier - Ce champ dont la taille est de 128 bits identifie uniquement le nœud source sans considérer sa localisation (c'est-à-dire en-dehors de l'adresse source de l'en-tête IPv6).
  - Source Address Version - Ce champ dont la taille est de 32 bits signale le numéro de version des identificateurs et adresses sources. Cette information doit être invariablement incrémentée à chaque

nouvelle adresse attribuée.

- Holding Time - Ce champ dont la taille est de 32 bits signale le temps nécessaire, en secondes, durant lequel un nœud conserve l'entrée AMT du nœud source du paquet considéré.
- Timestamp - Ce champ dont la taille est de 32 bits signale le temps nécessaire au nœud, en secondes, pour transmettre un paquet.
- Authentication Data - Ce champ dont la taille est de 128 bits authentifie, en fournissant le résultat de l'évaluation de l'algorithme MD5, le nœud source du paquet et garantie l'intégrité de l'option de mobilité pour les données.
- Destination Identifier : Ce champ dont la taille est de 128 bits identifie uniquement le nœud de destination final sans se préoccuper de sa localisation (c'est-à-dire en-dehors de l'adresse destination de l'en-tête IPv6).
- Destination Address Version : Ce champ dont la taille est de 32 bits signale le numéro de version des identificateurs et adresses destinations.

- Format de l'entête avec l'option de mobilité pour le contrôle

Option Type : Ce champ prend pour valeur 0x0 ?, ce qui signifie que cette option relève de la propriété d'évaluation de l'intégrité obtenue via l'en-tête d'authentification.

- Option Data Length - La longueur est de 108 octets.
- Identifier - Ce champ dont la taille est de 128 bits identifie uniquement le nœud pour lequel l'entrée AMT doit être créée ou mise à jour.
- Address - Ce champ identifie le nœud pour lequel l'entrée AMT doit être créée ou mise à jour.
- Address Version - Ce champ dont la taille est de 32 bits signale le numéro de version des identificateurs et adresses.
- Holding Time - Ce champ dont la taille est de 32 bits signale le temps nécessaire, en secondes, durant lequel un nœud conserve l'entrée AMT du nœud désigné par le champ identificateur (Identifier).
- Timestamp - Ce champ dont la taille est de 32 bits signale le temps nécessaire, en secondes, au nœud source pour transmettre un paquet. Ce champ permet aussi de prévenir les attaques récidivistes.
- Authentication Data - Ce champ authentifie, en fournissant le résultat de l'évaluation de l'algorithme MD5 et/ou la signature digitale RSA, et garantie l'intégrité de l'option de mobilité pour les données.

Les méthodes d'authentification :

Les options de mobilité utilisent deux méthodes d'authentification, "keyed MD5" et "RSA digital signature".

Keyed MD5 est utilisée dans le cadre de l'authentification end-to-end d'un paquet via l'option de mobilité pour les données utilisateurs ce qui nécessite de partager une clé secrète commune entre le nœud authentifiant et le nœud authentifié. La taille de la clé est de 128 bits, les calculs couvrent les champs suivants : Source Address (dans l'en-tête IPv6), Source Identifier, Source Address Version, Holding Time et Timestamp.

La méthode RSA digital signature est utilisée pour l'authentification de nœuds intermédiaires utilisés pour l'envoi de paquets avec l'option de mobilité pour le contrôle. La taille de la clé est de 512 bits, les calculs couvrent les champs suivants : Identifier, Address, Address Version, Holding Time et Timestamp.

La connexion à un réseau :

Lorsqu'un nœud est connecté à un réseau, il lui est attribué une adresse IPv6 temporaire dans le sous réseau par le mécanisme d'auto configuration d'adresses. A l'inverse, l'identificateur du nœud mobile ne change pas. Le nœud mobile transfert un paquet IPv6 via l'option de mobilité pour le contrôle située dans son réseau maison. Lors de toute cette procédure, les entrées AMT pour le nœud mobile sont créées et mises à jour à la fois sur les nœuds intermédiaires et ceux du réseau maison.

- Les procédures utilisées sur le nœud mobile

Lorsqu'un nœud mobile est connecté à un réseau, il transmet un paquet IPv6 via l'option de mobilité pour le contrôle à son réseau maison. Chaque champ de ce réseau est rempli de la manière suivante.

- Identifier - l'identificateur du nœud mobile.
- Address - l'adresse temporaire IPv6 de l'interface utilisée.
- Address Version - le numéro de version de l'adresse et de l'identificateur IPv6 temporaires.
- Holding Time - le temps, en secondes, pour lequel l'entrée AMT du nœud mobile doit être conservé.
- Timestamp - l'instant auquel le paquet est transmis.
- Authentication Data - la signature digitale RSA qui couvre les cinq champs précédents.

- Les procédures utilisées sur un nœud intermédiaire

Lorsqu'un nœud intermédiaire reçoit un paquet via l'option de mobilité pour le contrôle, il peut exécuter les procédures suivantes après ou avant l'envoi des paquets.

- Authentification - le nœud intermédiaire authentifie le paquet s'il connaît la clé publique du nœud mobile spécifié par le champ Identifier de l'option de mobilité. Si l'authentification réussit alors la

modification AMT est exécutée.

- Modification AMT - le nœud intermédiaire crée une entrée AMT pour le nœud mobile spécifié par le champ Identifier de l'option de mobilité s'il ne la connaît pas déjà ; ou bien, il met à jour l'entrée AMT existante à condition qu'elle ne soit pas obsolète (le numéro de l'option de mobilité ne doit jamais être plus grand que celui de l'entrée AMT).

Dans le cas où l'entrée AMT est obsolète, le nœud intermédiaire peut diffuser le paquet reçu à toutes ses interfaces.

- Les procédures utilisées sur un nœud situé à la frontière (Boundary Node) du réseau maison

Lorsqu'un paquet avec une option de mobilité pour le contrôle est reçu, un nœud situé à la frontière du réseau maison du nœud mobile désigné par le champ Identifier de l'option exécute les procédures d'authentification et de modification AMT, puis diffuse le paquet dans le réseau maison s'il s'agit d'un réseau de type diffusion. Si le nœud situé à la frontière dispose d'une entrée AMT obsolète, il transmet alors le paquet à l'adresse désignée par le champ Address de l'entrée AMT obsolète.

La communication des données :

Dans les données de communication, l'option de mobilité pour les données des utilisateurs est intégrée dans chaque paquet IPv6. TCP/UDP désigne le nœud de destination avec l'identificateur. La résolution d'adresse pour le nœud de destination est exécutée soit au niveau du nœud source, soit au niveau du nœud intermédiaire, ou bien au niveau d'un nœud localisé au sein du réseau maison du nœud de destination, puis le paquet est routé vers le nœud de destination.

- Les procédures appliquées au nœud source

Le nœud source crée un paquet IPv6 via l'option de mobilité pour les données des utilisateurs. Dans l'option, les champs relatifs au nœud source (Source Identifier, Source Address Version, Holding Time et Timestamp) sont remplis avec les valeurs appropriées, puis les données d'authentification sont calculées et attribuées au champ Authentication Data.

Une requête de transmission de la couche supérieure précise le nœud de destination et son identificateur (champ Destination Identifier) mais pas l'adresse. Le nœud source essaie de résoudre la correspondance de l'identificateur et de l'adresse grâce à la technique AMT. Si l'entrée AMT pour le nœud de destination existe, l'adresse et son numéro de version sont attribués respectivement au champ de destination de l'en-tête IPv6 ainsi qu'au champ du numéro de version de l'adresse de destination de l'option.

- Les procédures appliquées au nœud intermédiaire

Il existe deux procédures dans le cas d'un nœud intermédiaire avec l'option de mobilité des données des utilisateurs, à savoir la modification AMT et la résolution d'adresse.

Lors de la modification AMT, l'entrée AMT pour le nœud mobile désigné par le champ Source Identifier de l'option peut être créée ou modifiée. Dans un premier temps, le nœud intermédiaire authentifie le paquet si ce dernier connaît la clé commune du nœud source. Si l'authentification réussit, les procédures suivantes sont exécutées. Si une entrée AMT pour le nœud mobile désigné par le champ Source Identifier de l'option n'existe pas, elle est alors créée. S'il n'y a pas d'entrée AMT (information obsolète), alors des modifications sont réalisées en accord avec les valeurs de l'option.

Dans le cas de la résolution d'adresse, l'adresse de destination dans l'en-tête IPv6 et le numéro de version de l'adresse de destination de l'option peuvent être modifiés. Si l'entrée AMT pour le nœud de destination du paquet existe, alors il faut comparer le numéro de version de l'adresse de destination du paquet avec le numéro de version de l'adresse de l'entrée. Si l'entrée AMT dispose d'informations plus récentes, alors le champ Destination Address de l'en-tête IPv6 et le numéro de version de l'adresse de destination de l'option sont modifiés conformément à l'entrée.

- Les procédures appliquées au nœud de destination

Le nœud de destination exécute la procédure de modification AMT décrite ci-dessus puis la signale à la couche supérieure de réception du paquet avec l'identificateur du nœud source mais pas son adresse.

**IPv6 - La qualité de service -** Le champ étiquette de flux dans l'en-tête IPv6 peut être utilisé par une station de travail pour étiqueter certains paquets qui demandent un traitement particulier de la part des routeurs IPv6, pour assurer par exemple des qualités de service très fiables ou des services "temps-réel". Cet étiquetage est important afin de supporter les applications qui ont des contraintes sur les quantités de données ou sur les délais par exemple. L'étiquette de flot est un champ de 28 bits divisé en deux sous-champs :

- TClass 4 bits de nature de trafic (traffic class),
- Flow ID 24 bits d'identifiant de flots.

Un flot est une séquence de paquets envoyés depuis une source particulière à une destination particulière (unicast ou multicast) pour lequel la source désire un traitement particulier par les routeurs concernés. La nature de cette manipulation spéciale doit être acheminée aux routeurs par un protocole de commande, par un protocole de réservation de ressources, ou une information contenue dans les paquets du flot eux-mêmes (e.g. option nœud-par-nœud).

Il peut y avoir plusieurs flots actifs émis par la source pour un destinataire, aussi bien qu'un trafic n'est pas

associé à aucun flot. Un flot est identifié par une combinaison de l'adresse de la source et un Flow ID non nul. Les paquets qui n'appartiennent pas au flot porte un Flow ID de zéro.

Un Flow ID est assigné à un flot par le nœud de la source du flot. De nouveaux ID doivent être choisis (pseudo-) aléatoirement et uniformément depuis le rang 1 à FFFFFF en hexadécimal. Un flow ID ne doit pas être réutilisé par une source pour un nouveau flot de données tant que des données (ou des états) associés à l'usage précédent existeront dans chaque routeur.

Le sous-champ TClass donne un moyen, séparément du Flow ID pour une source, d'identifier la priorité de distribution désirée de ses paquets, relativement aux autres paquets du même émetteur. L'indication de type de trafic (valeur de TClass) est divisée en deux "gammes" : les valeurs de 0 à 7 sont employées pour étiqueter des paquets à flots contrôlés (par exemple les paquets d'une connexion TCP), et les valeurs de 8 à 15 sont utilisées pour étiqueter les paquets de flots non contrôlés comme des paquets "temps-réel" envoyés sans contrôle de flux de retour depuis les récepteurs.

Pour le trafic à flots contrôlé, les valeurs TClass suivantes sont recommandées pour les catégories d'application particulières :

0 = trafic non caractérisé

1 = trafic "entonnoir" (par exemple netnews)

2 = transfert de données intempestives (e.g. email)

3 = (reserved)

4 = transfert volumineux attendus (comme FTP, NFS)

5 = (reserved)

6 = trafic interactif (e.g. telnet)

7 = trafic contrôlé d'Internet (e.g. protocoles de routage, SNMP)

Pour le trafic à flux non contrôlés, la plus petite valeur (8) devrait être utilisée pour les paquets que l'émetteur est plus disposé à "jeter" dans des conditions de congestion (e.g. trafic vidéo de haute-fidélité), et la plus haute valeur (15) pour les paquets que l'émetteur est le moins disposé à "jeter" (e.g. trafic audio de basse qualité). Il n'y a pas d'ordre relatif entre les classes de flux contrôlés et celles des flux non contrôlés.

**IPv6 - La Sécurité dans IPv6 - [RFC 1752]** - Dans le domaine de la sécurité, IPv6 doit arriver à rendre deux services :

- Intégrer un système d'authentification de l'utilisateur et garantir l'intégrité des données.
- Offrir un système de cryptage applicable soit à la totalité du datagramme IP, soit à l'unité des données du niveau 4 transport.

Ces systèmes doivent être suffisamment décorrélés des algorithmes employés, afin que l'armée ou l'industrie puisse les mettre en œuvre facilement.

Il semble que les groupes de travail se soient accordés sur un certain nombre de points tels que la séparation du moyen d'authentification de celui du cryptage des informations. Une infrastructure de gestion des clés est requise afin de rendre possible l'utilisation d'en-têtes d'authentification et de cryptage. Cependant, cet aspect n'est pas encore réellement au point d'autant plus que l'effet pervers de ces techniques de sécurité est l'ajout de coûts supplémentaires et la baisse des performances du système.

Quelques définitions :

- L'authentification : Elle permet de savoir si la donnée reçue est la même que celle envoyée et, de la même façon, si le demandeur désiré est bien identifié.
- L'intégrité : Elle assure la bonne transmission de la donnée, de sa source à sa destination sans aucune altération intermédiaire.
- La confidentialité : Elle garde les communications confidentielles afin que seuls les participants puissent identifier ce qui a bien été envoyé.
- Le cryptage : Il s'agit d'un mécanisme communément utilisé pour permettre la confidentialité des informations.
- SAID : ou encore <<Security Association IDentifier>>
- Security Association : L'ensemble des informations de sécurité relatives à la connexion d'un réseau donné ou à un ensemble de connexions ; ce qui inclue des clés de cryptage, des clés de durée de vie, des algorithmes, des degrés de sensibilité (non-classé, secret, propriétaire), mais aussi des services de sécurité (authentication-only, Transport-Mode Encryption, IP-Mode Encryption) ou toutes les autres possibilités envisageables.
- L'analyse du trafic : Elle correspond à une sorte d'attaque du réseau où l'adversaire est capable de faire des déductions sur le réseau lui-même grâce à l'analyse des données repérées sur le trafic (telles que la fréquence de transmission, qui parle à qui, la taille des paquets, le Flow IDentifier utilisé, etc.).

Les mécanismes de sécurité dans IPv6

Le premier objectif est d'obtenir des mécanismes de sécurité sûrs et disponibles pour tous les utilisateurs qui le désirent. Les algorithmes développés pour ces fonctionnalités ne doivent, bien entendu, pas affecter les

autres aspects de l'implémentation IP.

Il existe deux mécanismes de sécurité dans IPv6. Le premier est le mécanisme de l'en-tête d'authentification (Authentication Header), le second, une technique d'encapsulation affectée à la sécurité appelée ESP (Encapsulating Security Payload) permettant l'intégrité, l'authentification et la confidentialité. Cependant, les mécanismes de sécurité IPv6 ne sont pas efficaces face à des attaques de type analyse du trafic, pour le moment.

- Le mécanisme de l'en-tête d'authentification (Authentication Header). L'en-tête d'authentification IPv6 cherche à rendre possibles l'intégrité et l'authentification des datagrammes IPv6. Ceci est obtenu par la mise en place d'une fonction d'authentification du cryptage sur le datagramme IPv6 ainsi que l'utilisation d'une clé secrète d'authentification. L'utilisateur qui émet inclut des données d'authentification dans les paquets IPv6 à traiter ; quant à l'usager qui les reçoit, il vérifie la justesse des données d'authentification. Certains champs de l'en-tête, qui évoluent lors de la transition (cas du champ Hop Limit), sont omis lors de l'authentification. Cependant, cette omission n'a pas de véritables conséquences sur la sécurité elle-même. La non-répudiation peut devenir nécessaire pour certains algorithmes d'authentification utilisant l'en-tête d'authentification (par exemple, les algorithmes asymétriques lorsque les clés de l'émetteur et du récepteur sont utilisées lors de la procédure de calcul de l'authentification). La confidentialité et la protection de l'analyse du trafic ne sont pas traitées par le mécanisme de l'en-tête d'authentification. Ainsi, les informations d'authentification sont analysées à partir des champs du datagramme IPv6 qui n'évoluent pas durant son transfert de la source à la destination. Tous les éléments (en-têtes, données, etc.) sont intégrés à l'analyse. La seule exception concerne certains champs comme le <<Hop Count>> (en-tête IPv6) ou la <<Next Address>> (en-tête de routage IPv6) qui sont omis.

En outre, il est fort probable que le mécanisme de l'en-tête d'authentification risque d'accroître les coûts du processus IPv6 ainsi que l'attente de la communication.

Enfin, le mécanisme de l'en-tête d'authentification apporte une véritable sécurité dans l'Internet sans affecter l'exportabilité des données ni augmenter trop significativement les coûts d'implémentation. Il est, bien entendu, fortement recommandé d'utiliser ce mécanisme de sécurité de l'origine à la destination finale.

Toutes les stations de travail IPv6-only doivent implémenter la technique de l'en-tête d'authentification avec au minimum l'algorithme MD5 utilisant une clé de 128 bits sachant que d'autres algorithmes pourront être implémentés.

- La technique ESP (Encapsulating Security Payload ou l'en-tête de confidentialité) pour IPv6 permet d'apporter l'intégrité, l'authentification et la confidentialité dans les datagrammes IPv6. Ceci s'obtient soit par l'encapsulation d'un datagramme IPv6 dans son intégralité, soit par le cryptage de la majorité des composants ESP au niveau de l'en-tête IPv6 sachant que la partie non codée de l'en-tête est utilisée afin de transporter les données protégées à travers le réseau. Le destinataire du datagramme enlève, se débarrasse de l'en-tête et des options IPv6 non codées, décrypte les éléments ESP, traite puis retire les en-têtes ESP ; enfin, il obtient le datagramme IPv6 d'origine décodé ou la donnée de spécification normale du protocole IPv6.

  o Description des modèles ESP

Il existe deux modèles ESP. Le premier, connu comme un modèle IP (IP-mode), encapsule le datagramme IP au sein de l'en-tête ESP. Le second modèle ou Transport-mode, encapsule généralement une structure UDP ou TCP dans IP et non l'en-tête IPv6.

  o Utilisation d'ESP

ESP évolue soit entre deux stations de travail, soit entre une station et un Gateway (passerelle) de sécurité, soit encore entre deux gateways de sécurité. Les gateways de sécurité permettent à des réseaux correctement reliés à ces derniers de ne pas se préoccuper du cryptage et d'éviter ainsi l'accroissement des coûts monétaires et la baisse des performances dus au cryptage tout en bénéficiant de la fonction de confidentialité.

Lorsque les stations de travail implémentent directement ESP sans l'intermédiaire des gateways de sécurité, il leur est alors possible d'utiliser le Transport-mode. Ce mode réduit à la fois la largeur de bande consommée et le coût du protocole pour l'utilisateur qui n'a pas besoin de garder confidentielle l'intégralité du datagramme IPv6.

  o Les impacts d'ESP sur la performance

Le mécanisme ESP a des impacts notables sur les performances du réseau. En effet, la mise en œuvre du protocole s'avère plus complexe si la technique ESP est utilisée dans la mesure où elle requiert davantage de temps et de puissance de la part processus. L'accroissement du retard est dû au cryptage et au décryptage de chaque datagramme IPv6 contenant ESP. Les conséquences relatives au coût sont variables selon les spécificités de l'implémentation telles que l'algorithme de cryptage utilisé, la taille de la clé, etc. Pour ces deux raisons, il est probable que les utilisateurs préféreront utiliser le mécanisme de l'en-tête d'authentification (Header Authentication) à la place de la technique ESP.

En outre, afin d'assurer l'interopérabilité au sein du monde Internet, toutes les implémentations ESP pour IPv6 doivent accepter l'utilisation de Data Encryption Standard (DES) dans le mode Clipher-Block Chaining

(CBC) ; cependant, d'autres modes et algorithmes peuvent être rajoutés.

- La combinaison des mécanismes de sécurité

Il est possible de combiner à la fois les mécanismes Authentication Header IPv6 et ESP pour IPv6 afin d'obtenir le niveau de sécurité désiré. La technique de l'en-tête d'authentification permet toujours l'intégrité et l'authentification ainsi que la non-répudiation en utilisant certains algorithmes (RSA). Le mécanisme ESP fournit toujours l'intégrité et la confidentialité mais aussi l'authentification via des algorithmes spécifiques de cryptage. Ainsi, le mélange des deux mécanismes permet de profiter véritablement de tous les éléments de sécurité : intégrité, authentification, non-répudiation et confidentialité.

D'autres mécanismes de sécurité permettent aussi de se protéger contre l'analyse de trafic, il faut les implémenter au niveau de la couche IP.

La gestion des clés (Key Management) :

Le protocole de gestion des clés couplé à d'autres mécanismes de sécurité via SAID peut être utilisé pour IPv6. IPv6 n'est pas destiné à fournir une gestion des clés de type <<in-band>>, où les données de gestion des clés sont portées par un en-tête IPv6 spécifique. En revanche, IPv6 utilisera dans un premier temps une gestion des clés de type <<out-of-band>> où les données de gestion des clés sont portées par un protocole de couche supérieure tel que UDP ou TCP sur un numéro de port spécifique. De manière générale, ceci permet le découpage du mécanisme de gestion des clés pour d'autres systèmes de sécurité ainsi que la substitution de nouvelles méthodes de gestion des clés (à la place des anciennes) sans avoir à modifier tous les autres outils de sécurité.

- La distribution d'une clé manuelle

La forme la plus simple de gestion des clés est la gestion manuelle des clés où un individu configure manuellement chaque système avec sa propre clé mais aussi les clés des autres systèmes de communication. Ceci s'avère relativement pratique dans un environnement statique et de petite taille. En prenant l'exemple d'un environnement réseau de type LAN, au sein d'un simple domaine administratif, il est pratique de configurer les clés de chaque routeur de telle sorte que les données routées puissent être protégées et qu'il soit possible de réduire le risque d'intrusions étrangères au sein d'un routeur. Cependant, ce n'est pas une approche viable à moyen ou long terme.

- La distribution d'une clé automatique

Le déploiement et l'utilisation des fonctions de sécurité dans IPv6 nécessitent un protocole de gestion des clés au standard Internet. A l'origine, un tel protocole devait proposer une gamme de services dans le monde Internet et pas seulement se réserver à la sécurité dans IPv6. Il existe des travaux en cours afin d'ajouter des clés signées sur des stations de travail via DNS ; les clés DNS permettant d'authentifier les messages de gestion des clés par rapport aux autres éléments de la gestion des clés utilisant un algorithme asymétrique.

Enfin, il convient de signaler qu'une <<Multicast Key Distribution>> est en cours d'élaboration pour IPv6.

A l'heure actuelle, de nombreux travaux sur IPv6 sont en cours d'élaboration, il faut signaler la présence de trois notions présentes dans IPv6 et pour lesquelles leur normalisation et admission définitives ne font aucun doute, à savoir : Authentication Header, Encapsulating Security Payload, Key Management.

L'utilisation des mécanismes de sécurité dans IPv6

Cet aspect sur la sécurité a pour principal objectif de donner un aperçu des différents mécanismes assurant la réduction des risques dans IPv6.

- Les Firewalls.

Les Firewalls, absents dans la version actuelle d'Internet mais utilisés dans IPv6, vont permettre de corriger les suites d'en-têtes et de déterminer le protocole de transport (UDP ou TCP) ainsi que le numéro de port de ce protocole. La performance des Firewalls dans IPv6 ne devrait pas en être trop affectée dans la mesure où le format des en-têtes IPv6 facilite la procédure de correction.

Les Firewalls utilisent le mécanisme de l'Authentication Header pour s'assurer l'authentification et la justesse des données utilisées pour les décisions de contrôle d'accès à savoir la source, la destination, le protocole de transport, le numéro de port. Cette authentification est impossible dans IPv4.

Les organisations disposant de plusieurs sites interconnectés utilisant les services commerciaux proposés par IP peuvent sélectionner un Firewall crypté. Par exemple, si un Firewall crypté est placé entre la Société A et le fournisseur du service commercial IP, le Firewall fournit alors un tunnel crypté au sein de tous les sites de la Société A. Il lui est ainsi possible de crypter tout le trafic entre elle et ses fournisseurs, ses clients ou des tiers. Une telle pratique permet de protéger facilement le trafic d'un grand nombre d'organisations de type gouvernemental par exemple qui peuvent même mettre en œuvre un mécanisme de fully encrypting Firewall autorisant aussi bien un filtrage du trafic décrypté qu'un cryptage des paquets IP.

- La protection de la Qualité de Service (QoS)

Le mécanisme de l'Authentication Header, utilisé avec la méthode de gestion des clés appropriée, permet d'authentifier les paquets. Le champ Flow Identifier dans IPv6 peut agir comme un Low-Level Identifier (LLID) ; par conséquent, la classification du paquet au sein des routeurs devient simple si le routeur est fourni avec la clé appropriée. Pour des raisons de performance, les routeurs authentifient des groupes de

paquets.

Ainsi, la qualité de service fournie est obtenue par l'utilisation du champ Flow ID conjointe à celle d'un protocole de réservation de ressources (tel que RSVP). Ainsi, la classification des paquets authentifiés s'obtient en s'assurant que chaque paquet reçoive bien la manipulation appropriée et correcte au sein des routeurs concernés.

- Des réseaux compartimentés ou à niveau multiple (Multi-level)

Un réseau multi-level secure (MLS) est un réseau unique utilisé pour communiquer des données selon différents degrés (non-classifié ou secret). De nombreux gouvernements trouvent beaucoup d'intérêt dans l'architecture réseau MLS. IPv6 devrait supporter ce type de structure. MLS nécessite l'utilisation des Mandatory Access Controls (MAC) que des utilisateurs normaux sont incapables de contrôler ou de violer.

Le mécanisme de l'Authentication Header peut être utilisé aussi bien pour authentifier plusieurs stations de travail dans un niveau unique du réseau que pour garantir les décisions MAC dans un réseau à niveau multiple. Si les étiquettes IP sont utilisées et la confidentialité considérée comme non obligatoire au sein d'un environnement opérationnel particulier, le mécanisme de l'Authentication Header permet l'authentification du paquet dans son intégralité, incluant un cryptage obligatoire du degré de sensibilité (non-classifié ou secret) de l'en-tête IPv6 et des données de l'utilisateur.

La technique ESP peut être combinée avec des politiques de clé appropriées pour garantir un réseau multi-level secure complet ainsi qu'un ensemble d'algorithmes appropriés. Dans ce cas, chaque clé doit être utilisée pour un degré de sensibilité et un compartiment précis. Par exemple, la clé A peut être utilisée pour des paquets non-classifiés ; la clé B, pour des paquets secrets pour un trafic sans compartiment, etc.

Le cryptage est une technique très pratique et souhaitable même dans un environnement bien protégé. L'algorithme de cryptage au standard Internet devrait être utilisable via une gestion des clés appropriée, afin de fournir de véritables Discretionary Access Controls (DAC) corrélés au degré de sensibilité des étiquettes, au-delà des seules possibilités MAC offertes pour le moment.

Le développement d'un mécanisme de cryptage complet devrait être disponible pour toutes les communications futures.

La prise en compte des autres éléments relatifs à la sécurité :

De manière générale, il faut retenir que la qualité de service fournie par les nouveaux mécanismes développés dans IPv6 dépend totalement de l'efficacité des algorithmes de cryptage implémentés, de la justesse de l'implémentation de ces algorithmes, des clés à utiliser, de la sécurité du protocole de gestion des clés, de l'implémentation d'IPv6 et particulièrement de ses mécanismes de sécurité.

En outre, certains aspects propres à la sécurité (comme la protection contre l'analyse du trafic) ne sont pas encore fournis par les mécaniques abordées précédemment. L'utilisateur doit donc faire preuve d'une extrême vigilance.

Enfin, quelques applications (comme le courrier électronique) nécessitent des applications de protections et de sécurités spécifiques qui ne sont pas du ressort des techniques de sécurité propres à IPv6 mais pour lesquels des RFC seront entièrement consacrées.

---

**IPv6 - L'Adressage :** L'adressage est de la toute première importance dans le réseau Internet. L'intérêt des utilisateurs est de pouvoir se connecter au réseau Internet pour avoir accès à des données ou pour pouvoir se connecter sur n'importe quelle machine. Les adresses IPng sont des identifiants de 128 bits pour des nœuds ou un ensemble de nœuds. Il y a trois types d'adresses:

Unicast: employé pour envoyer un datagramme à un unique nœud.

Cluster: employé pour identifier un groupe de nœuds qui ont en commun un préfixe d'adresse. Un datagramme envoyé à une adresse cluster sera délivré à un membre du groupe.

Multicast: employé pour envoyer un datagramme à tous les membres d'un groupe de nœuds.

Il n'y a pas d'adresses de broadcast dans la version d'IPv6, les adresses multicast assurent leurs fonctions.

Comme dans IPv4, un sous-réseau IPv6 est associé à une seule liaison. Mais IPng permet aussi d'associer plusieurs sous-réseaux à une même liaison.

Les champs des adresses ont des noms particuliers, prenons l'exemple de "subscriber". Lorsqu'il est utilisé avec le terme "ID" pour identifieur, après le nom ("subscriber ID"), on se réfère au contenu du champ nommé. Alors que s'il est utilisé avec "prefix" ("subscriber prefix"), le terme se rapporte à tous les bits de poids fort de l'adresse en incluant ce champ.

Représentation des adresses

Il y a trois formes conventionnelles de représentation d'adresses IPv6:

- La forme la plus appréciée est x:x:x:x:x:x:x:x, où les 'x' sont les valeurs hexadécimales des huit blocs de 2 octets chacun.

Exemples:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 1080:0:0:8:800:200C:417A

On remarquera qu'il n'est pas nécessaire d'écrire tous les zéros devant un chiffre hexadécimal dans un champ individuel, mais il doit y avoir au moins un chiffre dans chaque champ.

---

- La méthode d'allocation des adresses IPv6 montre qu'il est commode de "mettre" des bits à 0 dans le milieu des adresses. Pour avoir une écriture facilitée, une syntaxe adéquate sera de supprimer les zéros. L'expression de deux "::" indiquera un ou de multiple groupes de 16 bits à 0. Par exemple l'adresse multicast suivante:

FF01:0:0:0:0:0:43 sera représentée de la manière suivante: FF01::43

les "::" ne peuvent apparaître qu'une seule fois dans l'adresse.

- Une autre forme alternative est quelquefois plus commode lorsque l'on est dans un environnement mixte de nœuds IPv6 et IPv4. Elle est x:x:x:x:x:x:d.d.d.d, où les 'x' sont des valeurs hexadécimales (6 groupements de 16 bits) et les 'd' des valeurs décimales (4 groupements de 8 bits de la représentation standard d'IPv4). Exemples:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:1:129.144.52.38

ou dans le format compressé:

::13.1.68.3

::1:129.144.52.38

Les types d'adresses

Les types d'adresses d'IPng sont décrites par les bits de poids fort de l'adresse. Ce champ de longueur variable est appelé le préfixe du format (Format Prefix - FP) :

| Adresse | Préfixe | Fraction espace alloué |
|---|---|---|
| Réservé | 0000 0000 | 1/256 |
| Réservé | 0000 0001 | 1/256 |
| NSAP | 0000 001 | 1/128 |
| IPX | 0000 010 | 1/128 |
| Réservé | 0000 011 | 1/128 |
| Réservé | 0000 100 | 1/128 |
| Réservé | 0000 101 | 1/128 |
| Réservé | 0000 110 | 1/128 |
| Réservé | 0000 111 | 1/128 |
| Réservé | 0001 | 1/16 |
| Réservé | 001 | 1/8 |
| Adresse Unicast définie par fournisseur de service | 010 | 1/8 |
| Réservé | 011 | 1/8 |
| Réservé pour les adresses géographiques | 100 | 1/8 |
| Réservé | 101 | 1/8 |
| Réservé | 110 | 1/8 |
| Réservé | 1110 | 1/16 |
| Réservé | 1111 0 | 1/32 |
| Réservé | 1111 10 | 1/64 |
| Réservé | 1111 110 | 1/128 |
| Adresses locales | 1111 1110 | 1/256 |
| Adresses Multicast | 1111 1111 | 1/256 |

Pour les nœuds utilisant le protocole IPv4, les adresses unicast IPv6 ont pour préfixe 0000 0000.

Cette allocation supporte l'allocation directe des adresses fournisseurs (provider), adresses NSAP [NSAP-USE], adresses IPX, adresses d'usage local, et les adresses multicast. De l'espace est réservé pour les adresses géographiques. Les espaces adresses "Réservé" (85% du total adressable) seront attribués pour de futures utilisations. Elles pourront être utilisées pour étendre les adresses existantes (e.g. adresses de fournisseurs supplémentaires, adresses IPX, etc.) ou pour de nouveaux emplois.

On distingue les adresses unicast des adresses multicast par la valeur des octets de poids fort de ces adresses. Une valeur de FF (1111 1111) identifie une adresse multicast, toutes les autres sont des adresses unicast.

Les adresses individuelles ou adresses unicast :

L'adresse unicast d'IPv6 est basée sur le même principe de l'adresse de la version 4 d'IP sous le protocole de routage Internet sans classes (Classless Internet Domain Routing, CIDR). C'est-à-dire que les adresses sont allouées de manière contiguë et ont en commun les mêmes bits de poids fort, les mêmes préfixes.

Il existe plusieurs formes d'adresse unicast dans IPng : adresse unicast hiérarchique opérateur, adresse hiérarchique géographique, adresse hiérarchique NSAP, adresse hiérarchique IPX, adresse locale, et adresse unique de station.

Les nœuds peuvent avoir une connaissance plus ou moins étendue de la structure interne des adresses IPng, cela dépend du rôle "joué" par le nœud. Par exemple les fonctions d'une station sont différentes de celles d'un routeur. Au minimum, un nœud peut "voir" les adresses unicast (y compris la sienne) sans structure interne.

Une station légèrement plus perfectionnée (mais restant encore assez simple) peut avoir connaissance du ou des préfixes de sous-réseaux et donc des liaisons qui leur sont attachés.

Bien qu'un très simple routeur puisse n'avoir aucune connaissance de la structure interne des adresses unicast IPv6, les routeurs devront généralement avoir connaissance d'un ou de quelques niveaux hiérarchiques pour les protocoles de routage. La connaissance des domaines différera de chaque routeur, celle-ci dépendra des positions hiérarchiques des routeurs.

Exemples d'adresses unicast :

Les 48 bits du Node ID représentent l'adresse MAC. Dans d'autres environnements, où les adresses IEEE-802 ne sont pas disponibles, d'autres adresses de la couche liaison peuvent être utilisées, comme les adresses E.164.

L'utilisation d'un unique node identifier rend possible et de manière assez simple l'auto configuration des adresses. Un nœud peut ainsi relever le subnet ID en "écoutant" les messages "Advertisement" du routeur auquel il est rattaché, et donc fabriquer sa propre adresse IPv6 en y ajoutant son adresse IEEE MAC comme node ID dans ce sous-réseau.

Adresse unicast opérateur :

La partie haute de l'adresse est attribuée aux opérateurs (fournisseurs), qui attribuent des portions d'espace d'adresse aux souscripteurs (subscribers).

Le terme "préfixe opérateur" fait référence à la partie haute de l'adresse, provider ID compris. On est alors dans le même schéma que les adresses IP sous le protocole CIDR.

Le subscriber ID permet de distinguer un souscripteur (ou abonné) parmi d'autres attachés au même fournisseur repéré par le provider ID. Le terme de "préfixe du souscripteur" fait référence à la partie haute de l'adresse, subscriber compris.

Le subnet ID identifie une liaison physique spécifique. Il peut y avoir plusieurs sous-réseaux rattachés à la même liaison physique. Tandis qu'un sous-réseau ne peut pas être raccordé à de multiples liaisons physiques. Le terme de "préfixe sous-réseau" se rapporte à la partie haute de l'adresse, subnet ID compris. Le groupe de nœuds identifiés par un subnet ID doivent être attachés à la même liaison.

Le node ID identifie un unique nœud parmi le groupe de nœuds déterminé par un préfixe de sous-réseau.

Adresses NSAP :

La nouvelle version d'IP "supporte" les adresses NSAP (Network Service Access Point) d'une manière transparente (sans conversion) et celles-ci sont totalement compatibles avec l'en-tête étendu de nœud-par-nœud. IPng est totalement "compatible" avec le plan d'adressage NSAP existant qui a été défini par l'ISO et ITU-T, incluant des adresses utilisant la longueur totale maximale de 20 octets. Ceci est principalement adressé aux personnes qui ont déjà planifié ou déployé un plan d'adressage NSAP pour l'usage "du protocole réseau sans connexion" (Connectionless Network Protocol - CLNP) selon le plan d'adressage de la couche réseau OSI. On trouvera dans la draft "OSI NSA usage in IPv6" les recommandations pour continuer à dresser le plan d'adressage NSAP coexistant avec IPv6 et faire la transition pour IPv6.

Adresse unicast locale :

Les adresses "d'emploi local" sont des adresses utilisées à l'intérieur d'un site d'un souscripteur donné.

Les adresses locales sont employées pour des sites ou des organisations qui ne sont pas (encore) connectés au monde Internet. Pour accéder à ce dernier, il n'est pas besoin d'en faire la demande ou de "voler" un préfixe d'adresse depuis le monde Internet. L'adresse locale suffit, lorsque l'organisation veut se connecter au monde Internet, elle forme ses adresses globales en remplaçant le préfixe local par un préfixe souscripteur.

Adresse unspecified :

L'adresse 0:0:0:0:0:0:0:0 est appelée adresse unspecified. Elle ne doit être affectée à aucun nœud. Elle indique l'absence d'adresse. Par exemple, on peut la trouver dans le champ d'une adresse source de n'importe quels datagrammes envoyés par une station "initialisée" avant que cette dernière n'est réussie à constituer sa propre adresse.

L'adresse unspecified ne doit pas être employée comme adresse destination des datagrammes ou dans les en-têtes de routage d'IPv6.

Adresse de bouclage :

L'adresse unicast FE00:0:0:0:0:0:0:1 est appelée adresse de bouclage. Elle est utilisée par un nœud pour envoyer un datagramme à lui-même. Elle n'est affectée à aucune interface.

L'adresse de bouclage ne doit pas être utilisée comme adresse source de datagrammes envoyés à

l'extérieur du nœud.

Les adresses qui encapsulent les adresses IPv4 :

La transition simple à IPv6 (Simple IPv6 Transition - SIT) utilise deux formes d'adresses unicast IPv6, conçus spécialement pour faciliter l'évolution de l'Internet passant d'IPv4 à IPv6. Dans les deux cas, l'adresse IPv4 est inclue dans la partie basse de l'adresse IPv6 (32 derniers bits).

La première forme d'adresse est conçue pour représenter les adresses IPv4 des nœuds IPv4 (les nœuds ne peuvent pas comprendre le protocole IPv6) en adresses IPng.

La seconde forme d'adresse est conçue pour être utilisée par les nœuds IPv6 qui ont besoin de "dialoguer" avec des nœuds IPv4. On dira que ces adresses IPv4 sont compatibles IPv6.

Adresses cluster :

Les adresses cluster sont des adresses unicast, employées pour atteindre le "plus proche" nœud (selon une notion de routage unicast du plus proche nœud) d'un ensemble de routeurs "frontières" d'un groupe de nœuds, ces derniers étant identifiés par un préfixe commun. Un routeur frontière d'un groupe C possède au moins une adresse avec le préfixe C et au moins une liaison avec un autre nœud de préfixe différent de C.

Les adresses cluster ne doivent pas être utilisées comme adresses sources dans le datagramme IPv6.

Adresses multicast :

Une adresse multicast (de diffusion de groupe) IPv6 est un identifiant pour un groupe de nœuds. Un nœud peut appartenir à n'importe quel nombre de groupes multicast. Une adresse multicast commence toujours par : 11111111.

- Les drapeaux (flags) sont au nombre de 4 : Les trois bits de poids fort sont réservés, et doivent être positionnés à 0. T=0 indique que l'adresse est multicast de façon permanente, allouée par l'autorité d'adressage de l'Internet.
  T=1 indique que l'adresse est une adresse multicast provisoirement (de transition).
- Scope est une valeur de 4 bits, de portée du champ multicast. Elle est utilisée pour limitée l'étendue du groupe multicast. Les valeurs sont les suivantes : 0 reserved, 1 intra-node scope, 2 intra-link scope, 3 (unassigned), 4 (unassigned), 5 intra-site scope, 6 (unassigned), 7 (unassigned), 8 intra-organization scope, 9 (unassigned), A (unassigned), B intra-community scope, C (unassigned), D (unassigned), E global scope, F reserved.
- Group ID identifie le groupe multicast, qu'il soit permanent ou provisoire, à l'intérieur du domaine donné.

Exemple : Si le groupe de serveurs est assigné à une adresse permanente multicast avec un groupe ID de 43 en hexadécimal, alors :

FF01:0:0:0:0:0:0:43 signifie tous les serveurs NTP du même nœud que l'émetteur.

FF05:0:0:0:0:0:0:43 signifie tous les serveurs NTP du même site que l'émetteur.

FF0E:0:0:0:0:0:0:43 signifie tous les serveurs NTP du monde Internet.

Les adresses multicast provisoires ne sont significatives qu'à l'intérieur d'un domaine donné. Par exemple, un groupe identifié par une adresse multicast intra-site provisoire, FF15:0:0:0:0:0:0:43 d'un site donné, n'a aucun rapport avec un groupe utilisant la même adresse sur un site différent, ou un groupe provisoire utilisant le même group ID mais une valeur de scope différente, ou qu'un groupe permanent avec le même groupe ID.

Adresses multicast prédéfinies :

Reserved Multicast Address:

- FF0s:0:0:0:0:0:0:0.

Ces adresses multicast (avec une valeur de scope, s) sont réservées, et ne devront être assignées à aucun groupe multicast.

- FF01:0:0:0:0:0:0:1
- FF02:0:0:0:0:0:0:1

Ces adresses multicast identifient le groupe de tous les nœuds IPv6, à l'intérieur d'une étendue intra-nœud (scope=1) ou intra-liaison (scope=2).

- FF01:0:0:0:0:0:0:2
- FF02:0:0:0:0:0:0:2

Ces adresses multicast identifient le groupe de toutes les stations IPv6, à l'intérieur d'une étendue intra-nœud (scope=1) ou intra-liaison (scope=2).

- FF01:0:0:0:0:0:0:3
- FF02:0:0:0:0:0:0:3

Ces adresses multicast identifient le groupe de tous les routeurs IPv6, à l'intérieur d'une étendue intra-nœud (scope=1) ou intra-liaison (scope=2).

Les types d'adresses reconnus par les nœuds :

Pour une station:

- Adresses unicast allouées.
- Adresse de bouclage.
- Adresse multicast All Nodes.
- Adresse multicast All Hosts
- Toutes les autres adresses multicast auxquelles la station appartient.

Pour un routeur:

- Adresses unicast allouées.
- Adresses cluster de tous les groupements qui considèrent le routeur comme un routeur frontière.
- Adresse de bouclage.
- Adresse multicast All Nodes.
- Adresse multicast All Hosts
- Toutes les autres adresses multicast auxquelles le routeur appartient.

**IPv6 - L'auto configuration d'adresse - [RFC 1752]** - Les données des réseaux deviennent de plus en plus complexes, et le besoin de s'affranchir de certaines difficultés rend le "plug and play" (service immédiat) de plus en plus inévitable. L'utilisateur n'a pas à comprendre en détail l'architecture du réseau ou à savoir configurer le logiciel réseau de leur station de travail. Dans le cas idéal, un utilisateur quelconque doit être capable de déballer son nouvel ordinateur, le brancher au réseau local et le voir fonctionner sans devoir y introduire des informations de "spécialiste". Des soucis de sécurité peuvent limiter ce niveau de transparence d'auto configuration d'adresse dans certains environnements mais les mécanismes doivent être en place pour supporter n'importe quel niveau d'automatisation avec lequel l'environnement local serait en accord.

La première exigence de l'opération "plug and play" est qu'une station puisse être capable d'acquérir une adresse de manière dynamique, soit lorsqu'elle est attachée à un réseau pour la première fois, soit lorsque la station a besoin d'être reconfigurée parce que la station a bougé ou parce que l'identité du réseau a été modifiée. Il y a bien d'autres fonctions qui nécessitent un environnement de "plug and play". La plupart de celles-ci doivent se faire en-dehors du protocole IPv6, mais le protocole d'auto configuration d'adresse d'une station sera exécuté par IPv6.

Une station IPv6 peut auto configurer deux types d'adresses :

- Les adresses intra-liaison (intra-link scope address),
- Les adresses inter-liaison (inter-link scope address).

Une adresse d'environnement intra-liaison est auto configurable en l'absence de routeur, alors qu'une adresse inter-liaison est auto configurable lorsqu'un routeur est présent sur la liaison.

Il n'y a qu'une seule façon de former une adresse inter-liaison. A l'initialisation de l'interface, une station forme son adresse intra-liaison en concaténant un préfixe intra-liaison à un jeton ("token") qui est unique par liaison. Typiquement, la définition du jeton est dépendante de la couche liaison. Par exemple, dans le cas d'une station reliée à un réseau IEEE 802, le jeton est l'adresse IEEE 802 de l'interface.

Par contre, il y a deux manières pour former une adresse inter-liaison. Dans le premier mécanisme, une station obtient son adresse inter-liaison en concaténant un préfixe de réseau annoncé par un "Router Advertisement" [IPv6-DISC-PROC] à un jeton unique par liaison. L'autre mécanisme disponible pour les stations est d'utiliser le protocole de configuration dynamique des stations pour IPv6 [Dynamic Host Configuration Protocol - DHCPv6]. Le choix du protocole à utiliser est proposé par le routeur, et le choix est configurable par l'administrateur système.

Le premier processus de formation de l'adresse inter-liaison convient pour des environnements où aucune gestion administrative n'est désirée. Ce protocole est spécialement conçu dans le but particulier de faire de la configuration simple d'adresse. DHCPv6 est un protocole plus complexe permettant une affectation flexible des adresses; sous le contrôle de l'administrateur système. Ce protocole nécessite tout particulièrement un important gestionnaire de système (serveur et base de données).

Une station maintient une liste d'adresses par interface. Au minimum, la liste contient l'adresse intra-link scope que peut former automatiquement la station lorsqu'une interface est initialisée. Si un routeur est attaché à la liaison, la liste inclura aussi les adresses inter-link scope formées soit des préfixes de sous-réseau réclamés au router advertisements ou en faisant des appels à DHCPv6. Les adresses inter-link scope peuvent aussi être configurées manuellement.

Une station peut maintenir une liste de variables de configuration par interface :

- Adresse : une adresse unicast IPv6 valide pour cette interface. Par défaut : rien
- Durée de vie (LifeTime) : La durée pour laquelle l'adresse est valable en secondes. Par défaut : durée infinie.

Une adresse intra-link scope et toutes les adresses configurées manuellement ont leurs durées de vie positionnées à l'infini. Une station doit permettre à la variable suivante d'être configurée par un administrateur système par interface :

- Perform_Auto_Adress : Si sa valeur est vraie (TRUE), la station doit procéder à une configuration

d'adresse automatique, elle ne fait pas du tout d'auto configuration. Par défaut : TRUE.

Un routeur doit être configuré par un administrateur système, ainsi le choix du mécanisme utilisé pour la configuration des stations de leurs adresses inter-link scope peut être contrôlé. Par conséquent, un routeur peut voir sa variable suivante initialisée par un administrateur système par interface :

- Perform_Auto_Address : Si et seulement si cette variable est positionnée à TRUE, le routeur envoie une extension de préfixe d'adresse à tous les routeurs advertisement. Par défaut : TRUE

Une station doit suivre les procédures suivantes pour chaque interface lorsqu'elle "boot" ou quand une interface doit être initialisée.

Lorsqu'une station "boot" ou à n'importe quel moment où une station n'a pas d'adresse, la station produit une adresse intra-link scope et l'additionne à sa liste d'adresses.

La station doit envoyer une sollicitation au routeur (Router Solicitation) pour réaliser (ou vérifier) ses adresses inter-link scope le plus rapidement possible. Lorsqu'un Router Advertisement sollicité ou pas est reçu sur une interface, la station doit traiter la configuration d'adresse de la manière suivante :

Si une extension de préfixe d'adresse existe, la station forme ou vérifie ses adresses inter-link autonomes. Sinon, cela implique qu'elle doit se servir du protocole DHCPv6 pour l'auto configuration d'adresse. Si aucune adresse n'existe de l'interface, la station commence une requête au serveur DHCPv6 pour acquérir une nouvelle adresse. Pour quelque raison, si DHCPv6 ne réussit pas, la station revient à l'utilisation d'une adresse intra-link scope ou une adresse inter-link scope configurée manuellement jusqu'à ce que la requête au serveur DHCPv6 réussisse.

Formation d'une adresse IPv6 à partir de celle de l'IEEE 802. Une station peut former une adresse IPv6 pour une interface en concaténant un préfixe de sous-réseau de 80 bits avec une adresse IEEE 802 de 48 bits de l'interface. Dans le cas d'un préfixe intra-link scope, le préfixe de sous-réseau est bien défini (TBD). Alors que dans le cas d'un préfixe inter-link scope, le préfixe sous-réseau est configurable.

**IPv6 - e Protocole ICMP -** Le protocole ICMP (Internet Control Message Protocol) utilise l'encapsulation IP et sert à la gestion de l'Internet Protocol (IP). La nouvelle version IP emploie le protocole ICMP de la même manière que pour IPv4, avec quelques changements. Pour plus d'informations, se reporter aux documents [IPv6-DISC] et [RFC-1191].

Le protocole ICMP est utilisé par les nœuds IPv6, pour faire un compte-rendu des erreurs rencontrées dans le traitement des paquets, et pour assurer d'autres fonctions du monde Internet, telles que les diagnostics ("ping"), la découverte de voisins, ou donner les membres multicast.

Les messages ICMP sont regroupés en deux catégories :

- Destination Unreachable,
- Packet Too Big,
- Time Exceeded,
- Parameter Problem.

Les autres messages:

- Echo,
- Echo Reply,
- Group Membership Query,
- Group Membership Report,
- Group Membership Termination,
- Advertisement,
- Solicitation.

Tous les messages ICMP IPv6 sont précédés par un en-tête IPv6 et des en-têtes d'extension (ou pas). L'en-tête ICMP est identifié par une valeur de Next Header égale à 1, immédiatement dans l'en-tête précédent.

**IPv6 - Le Routage -** Le routage dans IPv6 est pratiquement identique au routage d'IPv4 sous CIDR à l'exception des adresses qui passent d'une longueur de 32 bits pour IPv4 à 128 bits pour la nouvelle version 6 d'IP. Avec de très simples extensions, tous les algorithmes de routage (OSPF, RIP, IDRP, IS-IS, etc.) peuvent être utilisés pour le routage IPv6.

IPv6 inclut aussi des extensions simples de routage qui lui confère une nouvelle fonctionnalité puissante. Ces possibilités permettent :

- La sélection de l'opérateur (basée sur une politique, des performances, des coûts financiers, etc.)
- La mobilité des terminaux (routage jusqu'à la position courante du terminal)
- Auto-ré adressage (routage à une nouvelle adresse)

La nouvelle fonctionnalité de routage est obtenue par la création d'une séquence d'adresses IPng, en employant l'option de routage IPng. L'option de routage est utilisée par un émetteur, et doit lister un ou plusieurs nœuds intermédiaires (ou groupes topologiques) que doit franchir en chemin un paquet, pour atteindre le destinataire. On peut retrouver une fonction similaire sur IPv4 en utilisant le champ option (enregistrement de la route, perte de la source).

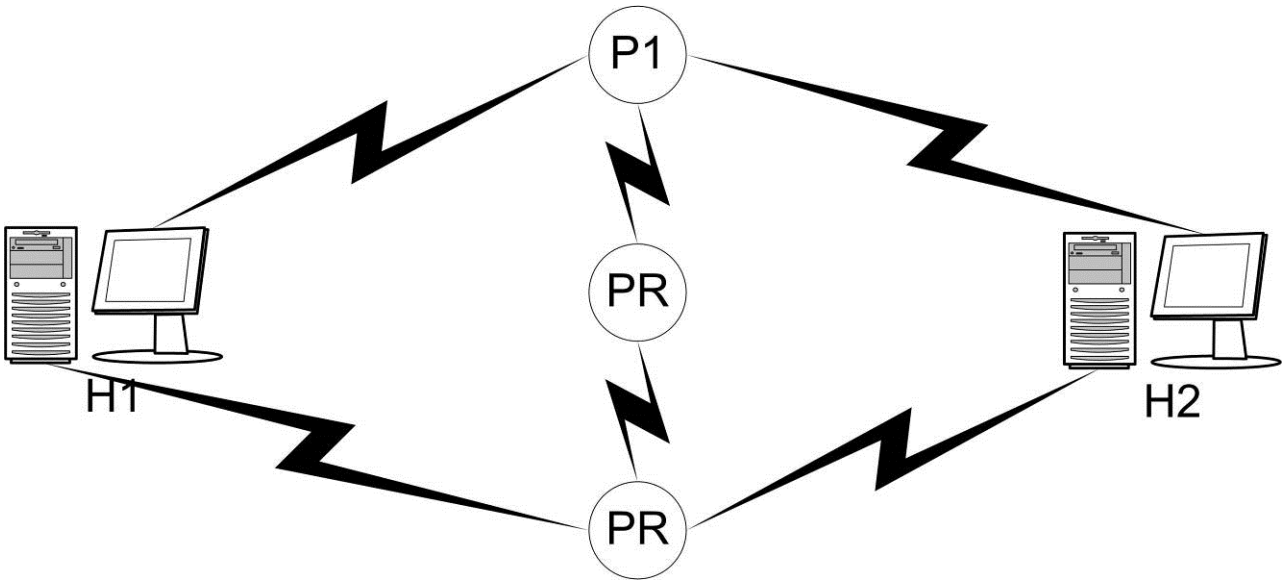
Pour le bon déroulement de cette fonctionnalité, les stations IPv6 qui reçoivent un paquet contenant la

séquence d'adresses doivent inverser la liste de ces dernières pour renvoyer un paquet à l'émetteur. Cette approche a été prise pour faire des implémentations sur des stations IPv6, depuis le support de départ, du traitement et de l'inversion des adresses déterminées par la source. C'est la solution pour permettre à ces implémentations de travailler avec des stations qui intègrent de nouvelles caractéristiques comme la sélection d'opérateur ou les adresses étendues.

La séquence d'adresse est désignée par une liste d'adresses individuelles séparées par des virgules. Par exemple :

SRC, I1, I2, I3, DST (la première adresse est l'adresse source, et la dernière est l'adresse destination, et les adresses du milieu sont des adresses intermédiaires).

Exemple : Les stations H1 et H2 veulent communiquer. Les deux sites de H1 et H2 sont tous les deux connectés aux opérateurs P1 et P2. Enfin, un troisième opérateur sans fil, PR, est connecté aux deux autres P1 et P2.




Le cas le plus simple (pas d'utilisation de liste d'adresses) a lieu lorsque H1 veut envoyer un paquet à H2 contenant les adresses : H1, H2

Quand H2 répondra, il devra inverser les adresses et construire un paquet contenant les adresses : H2, H1

Dans cet exemple n'importe quel opérateur peut être utilisé, et H1 et H2 ne peuvent pas diriger le trafic vers un opérateur précisément.

Si H1 décide de mener une politique telle que toutes les communications à destination ou d'origine H2 doivent uniquement utiliser l'opérateur P1, ce premier construira un paquet contenant la séquence d'adresses suivante : H1, P1, H2

Cela assure, lorsque H2 répondra à H1, que la route empruntée par le paquet passera par P1. La réponse de H2 contiendra donc les adresses : H2, P1, H1

Si H1 devient mobile et prend pour opérateur PR, il peut maintenir une communication avec H2, en envoyant des paquets qui contiennent la séquence d'adresses : H1, PR, P1, H2

La séquence d'adresses retournée par H2 sera donc : H2, P1, PR, H1

La facilité des séquences d'adresses d'IPv6 peut donc être utilisée pour de la sélection d'opérateur, pour la mobilité, et pour le ré adressage.

**IPv6 - Les mécanismes de transition de IPv4 vers IPv6 -** RFC 1752. Le principal objectif de la transition vers IPv6 est double, il doit permettre à des stations de travail implémentant IPv6 et/ou IPv4 de communiquer entre-elles ainsi qu'à des stations et des routeurs IPv6 d'être déployés sur l'Internet de manière incrémentale et à grande échelle. A ceci, un troisième objectif sous-jacent consiste à proposer une transition la plus simple possible pour tous les utilisateurs finaux, les administrateurs de réseaux et les opérateurs réseaux.

SIT (Simple IPv6 Transition) représente l'ensemble des mécanismes implémentés dans les stations de travail et les routeurs choisis afin d'assurer la transition d'IPv4 à IPv6.

La transition vers IPv6 se fera en deux temps :

- Seront d'abord introduites des stations supportant les deux versions, qui communiqueront en encapsulant les datagrammes IPv6 dans les datagrammes IPv4 (tunneling), de manière à traverser les routeurs en place implémentant IPv4.
- Puis de nouveaux routeurs (dotés d'un logiciel IPv6) assureront les fonctions d'encapsulation / de désencapsulation ou celles de traduction. Ainsi, ces deux modes de communication seront donc possibles : l'encapsulation des datagrammes et/ou la traduction de l'en-tête IP. Cette étape est particulièrement cruciale, puisqu'elle met en jeu la viabilité même d'Internet.

La modification de la taille des adresses a des conséquences sur l'usage des protocoles de l'IETF et de ceux qui sont associés à IP. Ainsi, ARP, RARP, BOOTP ou ICMP doivent être modifiés, tout comme les protocoles de routage RIP (version 2), IDRP, OSPF, BGP, IS-IS. Enfin, une grande partie des protocoles de niveau supérieur, FTP, DNS, SNMP devront prendre en compte cette migration.

Afin de faciliter la transition vers IPv6, un certain nombre de mécanismes obligatoires et optionnels sont définis comme ceux évoqués précédemment.

- L'utilisation conjointe d'adresses IPv4 et IPv6.
- La modernisation et, par conséquent, l'apparition de nouveaux routeurs et stations de travail.
- Le déploiement de serveurs DNS susceptibles de traiter des formats d'adresses de type IPv6.
- La mise en œuvre de plans permettant la transition des sites individuels Internet vers IPv6.
- La mise en œuvre de plans permettant la transition globale du monde de l'Internet à IPv6.

Cependant, ces objectifs ne pourront se réaliser aisément sans les caractéristiques suivantes définies dans SIT :

- Une adaptation facile. Les stations de travail et les routeurs actuels supportant IPv4 doivent s'adapter à IPv6 à tout moment sans recourir à d'autres stations ou routeurs intégrant déjà IPv6.
- Un nouveau déploiement aisé. Les nouveaux routeurs et stations IPv6 doivent être installés à tout moment sans pré requis particuliers.
- Un adressage facile. La structure d'adressage IPv4 actuelle doit pouvoir être réutilisée pour IPv6. Lorsque des stations de travail et des routeurs IPv4 sont adaptés au mode IPv6, ils ont la possibilité de continuer à utiliser leurs adresses initiales sans avoir recours à de nouvelles adresses.
- Une diminution des coûts de démarrage. Ce dernier aspect est une nécessité pour permettre une évolution d'IPv4 à IPv6 et surtout le déploiement croissant du nouvel IPv6.

Rappel : La notation utilisée pour représenter une adresse IPv6 est la suivante :

xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : ddd . ddd . ddd . ddd

où x représente un chiffre en hexadécimal et d, un chiffre décimal ; chaque groupe de nombres hexadécimaux séparé par ":" représente 16 bits de l'adresse ; chaque groupe de nombres décimaux séparé par "." représente 8 bits de l'adresse ; soit une adresse totale de 128 bits.

Les mécanismes de transition vers IPv6 introduisent un certain nombre de termes :

- Types de nœuds :
  - IPv4-only node : Un nœud IPv4-only (ou purement IPv4) ne comprend pas IPv6. Il a été installé avant la transition. Il se réfère à un routeur ou une station qui implémente seulement IPv4.
  - IPv4/IPv6 (dual) node : Un nœud IPv4/IPv6 (ou mixte) dual se réfère à un routeur ou une station qui reconnaît à la fois IPv4 et IPv6.
  - IPv6-only node : Un nœud IPv6-only (ou purement IPv6) se réfère à un routeur ou une station qui implémente IPv6 et pas IPv4. Il ne permet pas l'encapsulation des datagrammes IPv4 dans IPv6 et accepte uniquement des mécanismes intégrant IPv6.
  - IPv6 node : Tout routeur ou station qui utilise IPv6 y compris IPv4/IPv6 (dual) node et IPv6-only node.
  - IPv4 node : Tout routeur ou station qui utilise IPv4 y compris IPv4/IPv6 (dual) node et IPv4-only node.
  - IPv6/IPv4 header translating router : Un routeur IPv6/IPv4 qui réalise la traduction des en-têtes IPv6/IPv4.
- Types d'adresses IPv6 :
  - IPv4-compatible IPv6 address : Une adresse, se référant à un nœud IPv6, qui peut être utilisée à la fois pour des paquets IPv4 ou IPv6. Une adresse IPv4-compatible IPv6 inclut une adresse IPv4 contenue dans les 32 derniers bits. Les 96 premiers bits supportent le préfixe suivant <<0 : 0 : 0 : 0 : FFFF>>. Ainsi, la totalité des 128 bits de l'adresse peut être utilisée pour l'envoi de paquets IPv6 ; suivant le même raisonnement, les 32 derniers bits de l'adresse permettent l'envoi de paquets IPv4. Des adresses IPv4-compatible IPv6 identifient toujours des nœuds IPv6/IPv4 ou IPv6-only, mais jamais des nœuds IPv4-only.
  - IPv4-mapped IPv6 address : L'adresse d'un noeud IPv4-only est représentée comme une adresse IPv6. Une adresse IPv4-mapped IPv6 inclut une adresse IPv4 contenue dans les 32 derniers bits. Les 96 premiers bits supportent le préfixe suivant <<0 : 0 : 0 : 0 : 0 : 0>>. Ainsi, l'adresse d'un nœud IPv4-only peut être utilisée dans un espace d'adressage IPv6 en rajoutant le préfixe <<0 : 0 : 0 : 0 : 0 : 0>> à son adresse IPv4. Des adresses IPv4-mapped IPv6 identifient toujours des nœuds IPv4-only, mais jamais des nœuds IPv6/IPv4 ou IPv6-only.
  - IPv6-only address : Une adresse IPv6 n'intègre pas forcément une adresse IPv4 dans ses 32 derniers bits et peut avoir d'autres préfixes que ceux précédemment décrits. Des adresses IPv6-only identifient toujours des nœuds IPv6/IPv4 ou IPv6-only, mais jamais des nœuds IPv4-only.
- Types d'infrastructures de routage :

- IPv4-complete area : Un domaine d'infrastructure qui route entièrement IPv4.
- IPv6-complete area : Un domaine d'infrastructure qui route entièrement IPv6.

- Techniques utilisées pour la transition :
- IPv6-over-IPv4 tunneling : Une technique d'encapsulation des paquets IPv6 à l'intérieur de paquets IPv4 telle qu'ils puissent traverser un domaine IPv4-complete. IPv6-over-IPv4 tunneling est aussi appelée IPv6-in-IPv4 encapsulation.
- IPv6/IPv4 header translation : Une technique permettant la traduction des en-têtes Internet des paquets IPv6 dans des paquets IPv4 ou inversement, de telle sorte que les stations de travail IPv4-only et IPv6-only puissent communiquer.

Les étapes du modèle de transition SIT

Le modèle de transition vers IPv6 repose sur deux règles fondamentales. La première étant que l'Internet adoptera IPv6 de manière évolutive sur une période de temps échelonnée. La deuxième règle envisage une transition vers IPv6 à des niveaux et des moments différents selon les sites considérés.

Les techniques de transition ont pour objectif d'optimiser les deux phases de transition vers IPv6 :

- La première étape, le passage d'IPv4-only à Dual IPv6/IPv4, se réalise assez facilement.
- La seconde phase, la transition à une infrastructure IPv6-only qui maintient la possibilité de communiquer avec des nœuds IPv4, nécessite davantage d'efforts. En effet, les routeurs traducteurs (translating routers) doivent être déployés avant qu'une infrastructure IPv6-only ne puisse être construite.

La fin de la transition d'un site s'effectue lorsque ce dernier n'a plus besoin de communiquer avec l'environnement IPv4. L'arrêt de l'interconnexion avec IPv4 relève donc véritablement d'une décision propre au site lui-même.

Les principaux composants de SIT

La transition vers IPv6 accepte l'implémentation de trois différents types de stations de travail et routeurs : les nœuds IPv4-only, les nœuds IPv6/IPv4, les nœuds IPv6-only. En outre, à ces éléments, il faut aussi ajouter les routeurs de traduction d'en-têtes IPv6/IPv4, dont le rôle est particulièrement important afin d'assurer la transformation de paquets IPv4 en paquets IPv6 ou inversement.

Les nœuds IPv6/IPv4 dual sont des stations de travail ou des routeurs qui supportent les implémentations IPv4 et IPv6.

L'adressage dans SIT :

Exemple du format d'adresse IPv4-Compatible IPv6. Ce dernier est utilisé par les nœuds IPv6 qui désirent communiquer avec les nœuds IPv4. Dans DNS, ces adresses sont regroupées par enregistrement de type <<AAAA>> pour IPv6 et <<A>> pour IPv4. Ainsi, les enregistrements <<AAAA>> utilisent l'intégralité de l'adresse, à savoir 128 bits ; alors que les autres de type <<A>> ne travaillent que sur la portion d'adresse IPv4, c'est-à-dire 32 bits. Le raisonnement est identique pour l'autre format.

Le modèle de transition autorise une très grande flexibilité quant aux chemins que les formats d'adresse IPv6 peuvent utiliser. Ainsi, non seulement les nœuds IPv6 peuvent supporter les deux adresses IPv4-compatible et IPv6-only, mais ils sont aussi capables d'utiliser les deux types d'adresses simultanément. Ce qui signifie que les nœuds IPv6 pourront s'adapter à des environnements utilisant d'autres types d'adresses.

Les différentes topologies et les mécanismes utilisés dans SIT

Les topologies de routage se scindent en deux catégories.

- Les IPv4-complete areas sont des topologies entièrement connectées via le routage IPv4 où il existe au moins un routeur IPv4 rattaché à chaque sous-réseau du domaine IPv4-complete. Ces domaines peuvent cependant bénéficier d'un routage IPv6 partiel vers d'autres sous-réseaux sans pour autant nécessiter un routage IPv6. Les domaines IPv4-complete connaissent quelques limites ; ainsi, seules les stations de travail de type IPv4-only et IPv6/IPv4 peuvent être librement déployées au sein de ces domaines.
- Les IPv6-complete areas sont des topologies entièrement connectées via le routage IPv6 où il existe au moins un routeur IPv6 rattaché à chaque sous-réseau du domaine IPv6-complete. Ces domaines peuvent cependant bénéficier d'un routage IPv4 partiel vers d'autres sous-réseaux. Comme précédemment, seules les stations de type IPv6-only et IPv6/IPv4 peuvent être librement déployées au sein des domaines IPv6-complete.

Il est intéressant de noter qu'une topologie peut être à la fois IPv4-complete et IPv6-complete dans le cas d'un routage <<dual>> sur tous les sous-réseaux. Ces situations s'avèrent normalement plus simples à traiter.

En revanche, il est impossible de traiter un domaine constitué d'un mélange de routeurs IPv4-only et IPv6-only. Une telle topologie ne peut pas fonctionner dans la mesure où ces deux types de routeurs ne peuvent pas s'échanger leurs paquets sans un protocole commun.

Les tailles des domaines sont relativement flexibles : un seul nœud peut être traité comme un domaine voire comme l'Internet.

Première technique de transition : IPv6-over-IPv4 Tunneling :

Les paquets IPv6 ont la possibilité de traverser des segments reposant sur une typologie IPv4-complete grâce à la technique d'encapsulation (tunneling) IPv6-over-IPv4. Ainsi, concrètement et à titre d'exemple, un nœud IPv6/IPv4 cherchant à atteindre un autre nœud IPv6/IPv4 en passant par une typologie IPv4-complete peut voir ses paquets IPv6 arriver à destination en les encapsulant dans des en-têtes IPv4. Bien entendu, dans ce cas, les deux nœuds doivent disposer d'adresses IPv4 compatible IPv6. Les 32 derniers bits de ces adresses sont utilisés comme les adresses source et destination de l'en-tête d'encapsulation IPv4.

Deux types d'encapsulation se dégagent dans SIT.

- Les "Automatic tunnels" permettent de délivrer des paquets IPv6 à travers tous les chemins en direction des destinataires finaux.
- Les "Configured tunnels" sont utilisés pour délivrer des paquets IPv6 à un routeur intermédiaire IPv6/IPv4.

Ces deux types d'encapsulation utilisent néanmoins des adresses IPv4 intégrées dans des adresses IPv4-compatible IPv6. A la différence près que, lors de l'encapsulation automatique, l'adresse de "tunnel endpoint" considérée résulte d'une adresse IPv4 intégrée dans une adresse destination IPv6 sans informations de configuration préalables ; tandis que, lors de l'encapsulation configurée, l'adresse de "tunnel endpoint" considérée est celle du routeur IPv6/IPv4 intermédiaire, cette adresse doit donc posséder une information de routage issue soit de la table de routage d'une station de travail, soit de l'information de routage d'un routeur voisin.

Il est intéressant de remarquer que la technique de l'encapsulation automatique est une des caractéristiques propres aux mécanismes de transition vers IPv6.

- Automatic IPv6-over-IPv4 Tunneling

L'encapsulation automatique est généralement utilisée entre des stations de travail IPv6/IPv4 connectées sur un domaine IPv4-complete commun.

- Configured IPv6-over-IPv4 Tunneling

L'encapsulation peut aussi être utilisée entre deux routeurs IPv6/IPv4 ou bien entre une station et un routeur IPv6/IPv4. Dans ces situations, le paquet de destination final circule via un routeur intermédiaire.

- Le principe d'adressage utilisé

Excepté dans le cas des routeurs de traduction d'en-tête (header translating routers), lors de l'utilisation de routeurs intermédiaires, le routage des paquets repose entièrement sur les en-têtes IPv4. Le tableau suivant résume les situations suivant les deux techniques d'encapsulation.

- Les décisions d'envoi des paquets par les stations de travail

Lorsque des paquets IPv6 sont envoyés, la station IPv6/IPv4 doit décider de la technique à utiliser IPv6-over-IPv4 tunneling ou non. Dans la réalité, il est préférable d'envoyer des paquets IPv6 via des routeurs IPv6 plutôt qu'en utilisant la technique d'encapsulation (tunneling) pour plusieurs raisons :

- Les paquets IPv6 non encapsulés sont plus petits que les paquets IPv6-over-IPv4,
- Le trafic peut tirer profit des caractéristiques propres au routage IPv6.

En outre, une station de travail ne sait pas explicitement si elle est rattachée à un domaine IPv4-complete ou IPv6-complete. Dans le second cas (IPv6-complete area), il n'y aura pas de routeurs connectés à chaque sous-réseau et la station n'enverra jamais de paquets encapsulés à la différence de la première situation (IPv4-complete area).

Seconde technique de transition : Header Translation

La technique de traduction de l'en-tête est optionnelle, ce qui signifie que l'utilisateur peut y recourir quand il désire autoriser la communication entre des nœuds IPv6-only et des nœuds IPv4-only. La traduction de l'en-tête est assurée par les routeurs de traduction de l'en-tête (header translating routers), qui permettent d'interconnecter des domaines IPv4-complete et IPv6-complete. Le trafic écoulé entre ces domaines peut revêtir différentes formes :

- Terminating IPv4 traffic : les paquets IPv4 destinés à un nœud au sein d'un domaine IPv6-complete.
- Transit IPv4 traffic : les paquets IPv4 destinés à un nœud situé en dehors d'un domaine IPv6-complete, mais traversant un tel domaine.
- Terminating IPv6 traffic : les paquets IPv6 destinés à un nœud au sein d'un domaine IPv4-complete.
- Transit IPv6 traffic : les paquets IPv6 destinés à un nœud situé en dehors d'un domaine IPv4-complete, mais traversant un tel domaine.
- Encapsulated IPv6 traffic : les paquets IPv6 encapsulés dans des en-têtes IPv4 (cas particulier).

Les véritables traducteurs d'en-têtes sont les routeurs IPv6/IPv4. Ils opèrent en traduisant les en-têtes des paquets IPv4 en format IPv6 et/ou inversement. Pour agir de la sorte, ils ont besoin d'informations de configuration afin de connaître le type de paquets qu'ils ont à traduire.

- Traduction de paquets IPv4 : Les traducteurs d'en-têtes doivent traduire tous les paquets IPv4 destinés à des nœuds localisés dans les domaines IPv6-complete ou transitant à travers ceux-ci.
- Traduction de paquets IPv6 : Les traducteurs d'en-têtes doivent traduire tous les paquets IPv6

destinés à des nœuds localisés dans les domaines IPv4-complete ou transitant à travers ceux-ci.

Lors de la traduction des paquets IPv6 en mode IPv4, les routeurs traducteurs utilisent les 32 derniers bits des adresses IPv6 source et destination pour produire des adresses de paquets IPv4. Bien entendu, les adresses source et destination doivent être de type IPv4-compatible IPv6.

Lors de la traduction des paquets IPv4 en mode IPv6, les routeurs traducteurs ajoutent le préfixe <<0 : 0 : 0 : 0 : 0 : 0>> à l'adresse source IPv4 en vue de générer l'adresse source pour le paquet IPv6. Ils utilisent aussi les préfixes <<0 : 0 : 0 : 0 : 0 : 0>> ou <<0 : 0 : 0 : 0 : 0 : FFFF>> (destination au sein d'un domaine IPv6-complete) afin de générer l'adresse destination.

Lorsque les paquets de format IPv6-IPv4 arrivent au traducteur d'en-têtes, ils sont désencapsulés mais pas traduits.

Cette phase est nécessaire pour réaliser l'encapsulation d'un en-tête IPv4 d'un paquet IPv6-in-IPv4 pour être traduite au format d'en-tête IPv6.

Malgré la spécificité des techniques de transition vers IPv6, il est intéressant de noter que le processus vraisemblablement le plus important de SIT est le respect de la chronologie des étapes de la transition vers IPv6.

Le respect de la chronologie des étapes de la transition vers IPv6

Chaque étape de la transition vers IPv6 nécessite des pré requis tels que l'installation de nœuds IPv6/IPv4 avant le déploiement de nœuds IPv6-only. Il est important à ce stade de la migration d'avoir une vue précise des objectifs et délais de chaque étape.

**IPX -** Internetwork Packet Exchange - Protocole spécifique au logiciel d'exploitation de réseau Netware de Novell assurant la transmission des paquets de message sur ce type de réseau.

IPX est l'implémentation Novell de Internet Datagram Protocol (IDP) développé par Xerox. IPX est un protocole datagramme sans connexion qui transmet des paquets à travers Internet et fournit aux stations Netware et aux serveurs de fichiers des services d'adressage et de routage inter réseaux.

**IREST -** Institut de Recherches Economiques et Sociales sur les Télécommunications - S'intéresse particulièrement au rôle économique ou sociologique des télécommunications sur le plan national ou international.

**IRTF -** (Internet Research Task Force - Groupe de travail de l'IAB, responsable de la recherche à long terme et du développement de l'Internet.

**IS -** International Standard - Norme ISO dans son statut définitif.

**ISAKMP -** Internet Security Association and Key Management Protocol - Protocole de gestion de clés pour IPsec. Ce protocole, nécessaire à la mise en œuvre complète de IPsec, est également appelé IKE (Internet Key Management).

**iSCSI -** Interface réseau permettant de faire circuler des commandes SCSI sur un réseau IP. L'iSCSI est aujourd'hui considéré comme une alternative fiable et moins coûteuse que Fibre Channel.

**ISDB-T -** Integrated Broadcast Digital Broadcasting - Terrestrial - Norme de diffusion de télévision par voie terrestre similaire au DVB-T, cette norme a été retenue au Japon.

**ISDN -** Integrated Services Digital Network - Acronyme anglo-saxon équivalent de RNIS (Réseau numérique à intégration de services).

**IS-IS -** Intermediate System to Intermediate System - Procédé de routage normalisé dans le cadre de l'ISO.

**ISL -** Inter Switch Link - Le protocole ISL a été développé par CISCO afin d'étendre les réseaux virtuels sur plus d'un commutateur. Le principe du protocole ISL est de transporter les informations d'appartenance aux réseaux virtuels sur un backbone. L'identification des réseaux virtuels se fait par l'utilisation d'un marquage explicite (frame tagging) dans le protocole ISL. Ce marquage est réalisé lors de l'entrée de la trame dans un commutateur compatible ISL et non par la station émettrice de la trame. Lorsque la trame arrive au dernier commutateur, la trame est désencapsulée et livrée à la station. Le processus est ainsi totalement transparent pour les stations émettrices et réceptrices. Lorsqu'une trame arrive au premier commutateur, il identifie le VLAN d'appartenance de la trame et l'encapsule dans une trame ISL, puis la transmet uniquement aux commutateurs qui possèdent une station de ce VLAN sur un de leur port (ou si c'est un point de relais entre deux commutateurs possédant le VLAN en question). Cette technique a pour effet de réduire considérablement les broadcasts inutiles de commutateurs à commutateurs, et de commutateurs à routeurs.

**ISO -** International Standard Organization - Organisation Internationale de Normalisation - Fédération mondiale d'organismes nationaux de normalisation. Les travaux de l'ISO s'étendent à tous les domaines de la normalisation, à l'exception des normes concernant la technologie électrique et électrotechnique qui sont du ressort de la Commission Electrotechnique Internationale (CEI). Organisme international dépendant de l'ONU chargé de la normalisation. Il englobe les organismes nationaux de tous les pays Organisé en TC (Technical Comittees) ou en SC (Sous Comités), à leur tour subdivisés en Groupes de travail (Working Group). Les projets de normes passent par trois stades, DS (Draft Proposal) ou document de travail, Dis (Draft International Standard) ou proposition de norme, et enfin IS (International Standard) après l'adoption définitive.

L'expression ISO signifie également en français Interconnexion des systèmes Ouverts, pour désigner le modèle plus souvent mentionné sous son acronyme anglo-saxon d'OSI (Open System Interconnect).

**ISO 13406-2** - Norme publiée en 2001 - Cette norme s'applique aux écrans TFT et définit trois types de pixels défectueux (chaque pixel est compose de trois sous-pixels: un rouge, un vert, et un bleu) : le type 1 correspond à un pixel constamment allumé (blanc), le type 2 à un pixel toujours éteint (noir) et le type 3 a un défaut ne rentrant pas dans les deux catégories précédentes (pixel qui clignote par exemple). La norme définit également quatre classes de tolérance de pixels. Celle retenue par les constructeurs est généralement la classe II qui autorise au maximum deux (2) pixels défectueux de type 1, deux (2) pixels défectueux de type 2 et cinq (5) pixels défectueux de type 3. Ces valeurs s'entendent par millions de pixels effectifs de l'écran.

**ISO 8877 -** La prise ISO 8877 ou CCITT I.430 est légèrement différente au niveau des caractéristiques mécaniques à la prise RJ45. Le raccordement physique s'effectue au moyen d'un connecteur à 8 broches (bien que certaines prises RJ45 existent aussi en 9 points pour connecter l'écran) qui permet de connecter jusqu'à 8 fils.

**ISO IEC 11801 -** Norme internationale dédiée au précâblage système. La norme 11801 définit une installation complète (composants et liens) et valide les câbles 100 Ohm ou 120 Ohm , ainsi que le 150 Ohm. Cette norme reprend les catégories de l'EIA/TIA mais avec des valeurs d'impédance, de paradiaphonie et d'atténuation qui sont différentes suivant les types de câbles. La norme définit également des classes d'applications.

Différences entre ISO IEC 11801 et EIA/TIA 568 :

| Standard | Câbles | Prises | Brassage Défini** | Fibre Optique | Connecteur Optique | Classes d'application |
|---|---|---|---|---|---|---|
| EIA/TIA 568 TSB 36/40/53 | 100 Ohm<br>150 Ohm | RJ45 Data | CAd+<br>RJ45 | 50/125µ<br>62.5/125µ | ST et SC | |
| ISO IEC 11801 | 100 Ohm<br>120 Ohm<br>150 Ohm | RJ45 Data | CAd+<br>RJ45 | 50/125µ<br>62.5/125µ | ST et SC | A, B, C, D optique |

**Les modules et sucettes n'y sont pas définis.

Médias recommandés pour le précâblage :

- Horizontal : paire torsadée, fibre optique si nécessaire.
- Bâtiment (rocade) : paire torsadée pour la téléphonie et les données bas débit (RS 232, etc.), fibre optique pour les données moyens et hauts débits.
- Campus : fibre optique pour l'ensemble des applications, paire torsadée pour la téléphonie, GTB, etc.
- L'utilisation du connecteur RJ45 (ISO 8877) est définie par l'ISO IS11801 et l'EIA/TIA 568 TSB 40. Les 4 paires d'un câble doivent être connectées sur la même prise.

Précautions de mise en service :

L'affectation des paires par rapport aux pins du connecteur RJ45 fait l'objet de deux définitions : T568A et T568B. Un rayon de courbure au moins égal à 4 fois le diamètre du câble doit être maintenu pendant la pose. Une fois posé le rayon de courbure doit être d'au moins 8 fois le diamètre du câble. Les torsades doivent être maintenues jusqu'à 13 mm du point de raccordement pour une connexion Cat.5 .

**Isochrone -** Caractéristique d'une transmission où les deux extrémités travaillent au même rythme et ne supportent aucun retard. Attention, n'est pas synonyme de synchrone. L'isochronie suppose que la transmission peut être endommagée si le rythme de la transmission n'est pas conservé strictement. La téléphonie est un exemple d'application isochrone, puisqu'elle ne supporte pas que le rythme de transmission des échantillons de voix ne soit pas intégralement conservé, au contraire des transmissions de données qui admettent des décalages temporels entre les diverses parties du message sans que celui-ci soit affecté.

**Isonet Ace Line -** Système de câblage Alcatel Composants Télécom.

**ISP -** Internet Service Provider - Voir aussi Fournisseur d'accès à Internet (FAI) - Fournisseur de services Internet, et non fournisseur d'accès à Internet. Les ISP proposent généralement en effet l'accès à Internet, mais aussi l'hébergement de sites sur des serveurs Web, voire le développement de ces sites.

**ISRF -** Internet screenphones Reference Forum - ISRF est une association de quelque vingt-cinq entreprises des télécommunications, de l'électronique et du logiciel dont l'objectif est de définir une norme concernant les terminaux INTERNET (webphones…)

**ISTEL -** Société britannique spécialisée dans le domaine des échanges de documents informatisés (EDI). A été rachetée par l'exploitant américain AT&T qui s'en sert comme tête de pont pour déployer en Europe des services réseaux d'échanges de données.

**IT -** Information Technology - En français : Informatique.

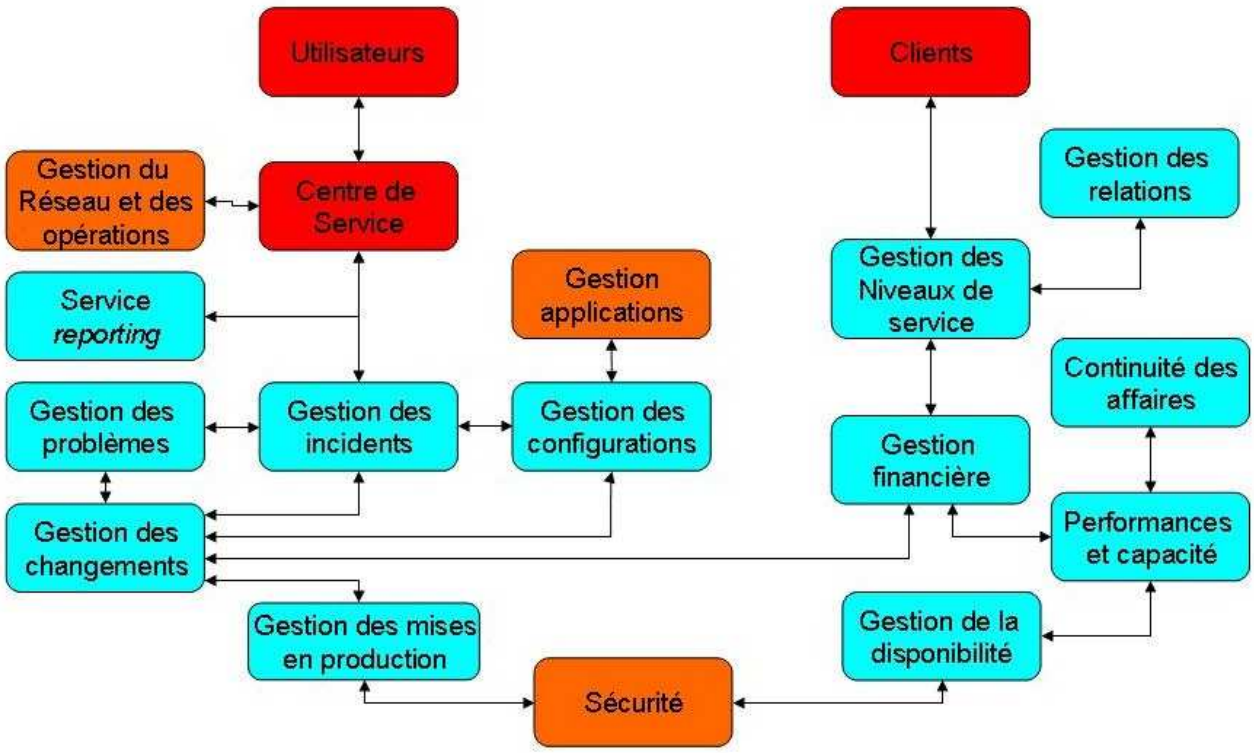
**IT Management -** Synonyme : Infogérance - Service consistant pour une SSII à prendre en charge la responsabilité complète de la gestion du service informatique de son client.

**ITA -** Information Technology Agreement - Accord-cadre adopté lors du Sommet de Singapour, dans le cadre des négociations de l'OMC, visant l'élimination totale des tarifs douaniers pour les produits des NTIC (Nouvelles Technologies de l'Information et de la Communication).

**ITAPAC -** Réseau de commutation de paquets italien.

**ITIL -** Information Technology Infrastructure Library **-** Méthode et outils permettant de faire de l'I.T. Management. ITIL est un recueil de normes dédiées à la bonne gestion des systèmes d'information, en 12 segments principaux.

Les douze principaux segments Itil :




**Itinérance** - (Roaming) - Capacité technique et informatique permettant à un client d'utiliser son téléphone à l'étranger sur le réseau d'un autre opérateur, comme s'il se trouvait dans son réseau d'appartenance.

En radiocommunication avec les mobiles, déplacement d'un client d'un opérateur en dehors de la zone de base correspondant à son abonnement, dans des zones où il peut bénéficier de certaines prestations, généralement fournies par un autre opérateur. Les opérateurs de radiocommunication mobile concluent entre eux des accords d'itinérance qui définissent les prestations que chacun d'eux s'engage à fournir aux clients des autres.

**ITSP -** Internet Telephony Service Provider - Fournisseur de services téléphoniques Internet - Un ITSP se connecte à Internet via un réseau téléphonique classique à l'aide d'une passerelle. Ceci permet aux abonnés qui ne disposent que d'un téléphone normal d'être contactés par un téléphone Internet.

**ITU -** International Telecommunication Union - Voir UIT, Union Internationale des Télécommunications.

**IXFR -** (voir DNS et AXFR) - Transfert de zone incrémental - Le transfert systématique de tout le fichier zone DNS pose de gros problèmes de surcharge sur le réseau. Il est en effet dommage de devoir transférer toutes les informations de la zone alors que simplement quelques enregistrements ont été modifiés, c'est pour cette raison qu'a été mise au point cette deuxième technique de mise à jour des zones DNS.

Cette technique de mise à jour permet de n'envoyer via des paquets UDP (s'il y a peu de modifications) ou TCP la liste des changements au niveau des enregistrements à effectuer sur le fichier zone. Le serveur secondaire envoie son numéro de version de fichier de zone dans sa requête IXFR, le serveur primaire de son coté, a conservé certains anciens fichiers de zone, s'il possède la version en question il la compare à la nouvelle et transmet les modifications. S'il ne possède pas l'ancienne version il doit faire un transfert total de la nouvelle zone. La problématique est de savoir alors quelle quantité d'anciennes versions de la zone il faut conserver. Une bonne stratégie de purge est de conserver les fichiers tant que le paquet IXFR contenant les modifications émis ne dépasse pas celui que l'on enverrait pour un transfert de zone total

# J

**J2EE -** Java 2 Enterprise Edition - Ensemble de standards permettant de créer des applications d'entreprise distribuées, ou services, en n'utilisant que le langage Java. Ces services définissent comment accéder à une base de données, quelle interface un composant doit avoir selon l'environnement, etc. L'ensemble de ces services techniques constitue l'architecture J2EE.

**Jabber -** Appélation simplifiée du protocole XMPP. Jabber est un protocole de messagerie normalisé. Une adresse de contact est appelé JID (Jabber Id) et est de la forme pseudo@serveur.domaine.

**Jack -** Terme anglais désignant une prise dans laquelle les deux contacts sont présentés de manière coaxiale : le contact extérieur est un cylindre entourant le contact intérieur, un isolant les séparant.

**Jarretière -** Cordon de courte longueur pour réaliser une connexion permanente, mais modifiable, dans un panneau de câblage ou de brassage, notamment sur les répartiteurs des systèmes de câblage modernes.

☺ Ruban ou galon de tissu élastique entourant la jambe au-dessus ou au-dessous du genou pour maintenir le bas. Attacher, détacher, nouer, dénouer ses jarretières. La jarretière de la mariée. L'ordre de la Jarretière, le plus ancien et le plus élevé en dignité des ordres de chevalerie anglais, institué par Édouard III en 1348.

**JavaScript -** Langage de programmation de scripts, créé et développé par Netscape. Contrairement à Java, JavaScript est un langage interprété.

**JavaT ou Technologie JavaT -** Java est un langage de programmation développé par Sun Microsystems. Certaines versions de Java sont susceptibles d'être utilisées dans la création de services mobiles. Certains téléphones supportent le téléchargement d'applications JavaT via la liaison WAP, de sorte que vous pouvez enrichir les fonctionnalités de votre téléphone d'applications intéressantes et utiles comme une horloge internationale, un convertisseur de devises ou des jeux.

**JCA -** J2EE Connector Architecture - Ensemble de spécifications Java, qui décrivent une interface "Java Connector Architecture". Elles visent à faciliter la mise au point d'interfaces de connexion et d'adaptateurs (ou connecteurs) standards, afin que les serveurs puissent invoquer des fonctions d'autres applicatifs mis à disposition par les adaptateurs.

**JEDI -** Joint Electronic Data Interchange - Comité international chargé sous l'égide de l'Onu de la mise en œuvre des normes d'Echanges de données informatisés (EDI) et de réaliser le rapprochement de ces normes avec les normes homologues américaines de l'Ansi.

**Jeton -** Suite de bits particulière utilisée dans la méthode d'accès dite "anneau à jeton" (en anglais: token-ring). Ce jeton circule en permanence d'une station à l'autre, toujours dans le même sens. Si la station n'a rien à émettre, elle retransmet le jeton à la station adjacente à l'état "libre" ; si elle a un message à émettre, elle fait précéder ce message du jeton à l'état occupé.

Message spécial utilisé sur les réseaux locaux pour demander l'autorisation d'émettre pour une station. Sur un réseau en anneau, le jeton circule en permanence. Sur un bus, il faut le solliciter.

Voir Token Ring.

**Jitter -** Gigue - Légère fluctuation de la phase d'un signal susceptible d'entraîner des erreurs de transmission.

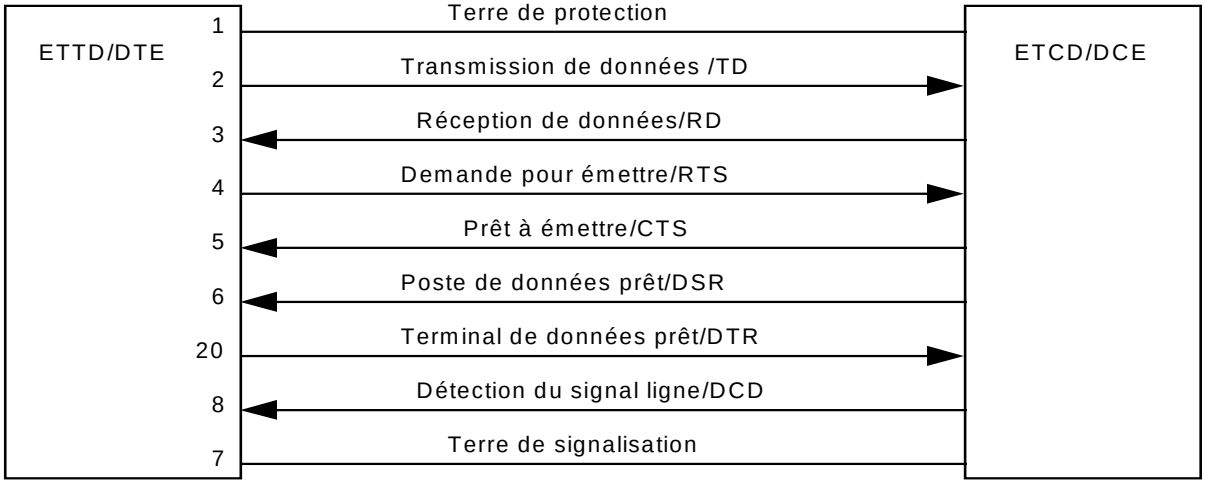
**Joncteur -** Interfacing Circuit - Situé à l'entrée ou à la sortie d'un commutateur, le joncteur permet le traitement d'une partie de la signalisation et la supervision des communications.

**Jonction -** Zone de communication définit par des caractéristiques physiques des points de connexion, les caractéristiques des signaux et les caractéristiques fonctionnelles des circuits d'échange.

La connexion d'un équipement informatique à un modem, par exemple, est réalisée par l'intermédiaire d'une jonction ou interface. L'étude de la jonction est une illustration intéressante des protocoles mis en œuvre au sein de la couche physique des architectures de communication. La jonction spécifie les caractéristiques mécaniques, électriques et fonctionnelles d'une connexion physique.

Il existe plusieurs types d'interfaces qui sont fonction de la vitesse de la liaison. La plus courante est l'interface V24/V28 ou RS232C qui peut être utilisée jusqu'à une vitesse maximale de 38 400 Kbit/s.

Les principaux signaux qui transitent sur une liaison asynchrone, entre un DTE/ETTD et un DCE/ETCD avec une interface RS 232C, sont les suivants (voir page suivante) :




Dans une liaison synchrone il faut ajouter les signaux d'horloge émission et réception.

Les autres types d'interfaces les plus courants sont : V35, V11 (RS422), RS 449 (V36).

**JPEG -** Joint Picture Expert Group - Groupe d'experts communs au CCITT et à l'ISO responsable de la normalisation dans le domaine de la compression d'images fixes. Par extension, désigne la méthode de compression normalisée par ce groupe.

La norme JPEG utilise l'ADCT (transformée en cosinus discrète).

**JTAPI -** Java Telephony Applications Programming Interface - Norme développée par Sun - Cette norme de Sun mise sur l'adoption de Java avec ses qualités intrinsèques comme l'indépendance vis-à-vis de la plateforme pour le serveur et le client.

JTAPI peut travailler selon une méthode client-PABX ou client-serveur. De plus, JTAPI se reposant sur Java est tout naturellement orienté vers le Web et TCP/IP, donc les nouvelles applications de la téléphonie comme la voix sur IP ou les Web Call Centers.

Voir CTI.

# K

**Kbps -** Kilobits par seconde, soit un millier de bits par seconde. Vitesse de transmission des données. Le kilobit est une unité d'information égale à 1024 bits. "Bit" est l'acronyme de binaire et digit.

**Kerberos -** Protocole d'authentification réseau à clé secrète développé par le MIT (Massachusetts Institute of Technology), basé sur l'utilisation de l'algorithme de cryptage DES pour le cryptage et une base de données de clés centralisée pour l'authentification.

Le protocole Kerberos repose sur un système de cryptographie à base de clés secrètes (clés symétriques ou clés privées), avec l'algorithme DES. Kerberos partage avec chaque client du réseau une clé secrète faisant office de preuve d'identité.

La version 5 du protocole Kerberos a été normalisée par l'IETF dans les RFC 1510 (septembre 1993) et 1964 (juin 1996). Le nom"Kerberos " provient provient de la mythologie grecque et correspond au nom du chien (en français"Cerbère ") protégeant l'accès aux portes d'Hadès.

Kerberos repose sur la mise en place de serveurs d'authentification (AS pour Authentication Server), permettant d'identifier des utilisateurs distants, et des serveurs de délivrement de tickets de service (TGS, pour Ticket Granting System), permettant de les autoriser à accéder à des services réseau. Les clients peuvent aussi bien être des utilisateurs que des machines. La plupart du temps, les deux types de services sont regroupés sur un même serveur, appelé Centre de Distribution des Clés (ou KDC, pour Key Distribution Center).

**Kermit -** Protocole de transmission de données en mode asynchrone très répandu dans les échanges entre micros et/ou mini-ordinateurs. Développé par l'université de Colombia, il est maintenant dans le domaine public.

**Killer Services -** Services nouveaux nécessitant une largeur de bande importante, ou proposés par Internet, dont le succès prévu sera immédiat et pour l'obtention desquels l'utilisateur est prêt à payer.

**Kiosque -** Service mise en place par France Télécom avec le système de vidéotex Télétel permettant de percevoir directement les paiements des services consultés en les imputant sur les factures téléphoniques des usagers et en reversant une partie de cette somme aux prestataires de services. Il existe plusieurs paliers de prix et de reversements selon les Accès (3614, 3615, 3617...).

**Kiosque téléphonique -** Service identique au précédent mais pour les prestations vocales (météo, messagerie, résultats des courses...) offertes sur le réseau téléphonique commuté.

**KVM -** Keyboard, Vidéo, Mouse - Les commutateurs KVM proposent une alternative qui permet d'utiliser plusieurs ordinateurs à l'aide d'un seul ensemble clavier, écran, souris. On trouvera ce type de commutateur dans les baies informatique regroupant plusieurs serveurs.

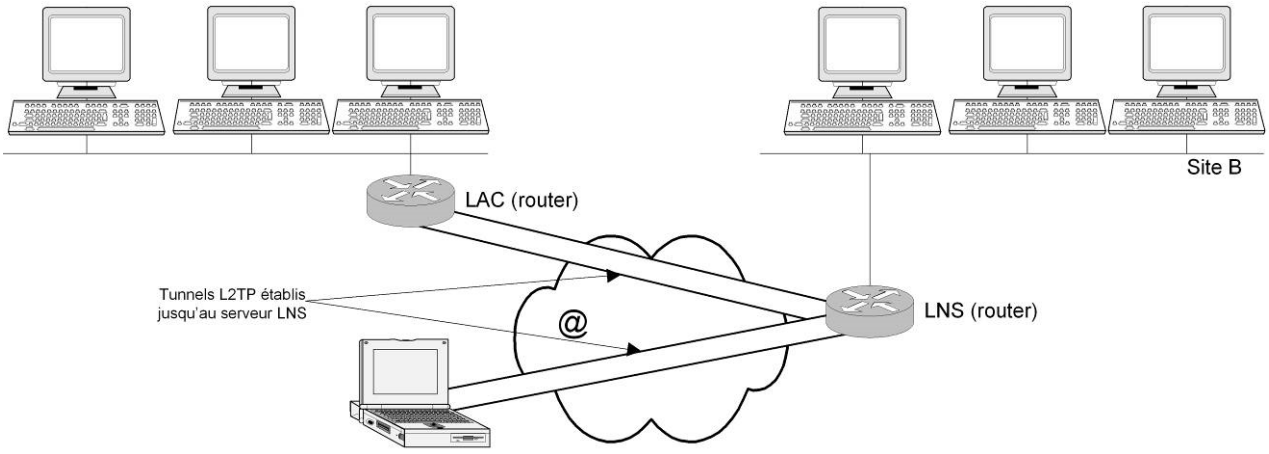
# L

**L2F -** Layer 2 Forwarding Protocol - Protocole gérant la mise en place de réseaux virtuels privés commutés via Internet. Protocole de tunneling propriétaire Cisco.

Protocole de niveau 2 qui permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer ces données jusqu'à un serveur L2F (routeur). Ce serveur L2F désencapsule les paquets et les envoie sur le réseau. Il faut noter que contrairement à PPTP et L2TP, L2F n'a pas besoin de client.

Ce protocole est progressivement remplacé par L2TP qui est plus souple.

**L2TP -** Layer 2 Tunneling Protocol - Protocole de réseau privé virtuel qui permet d'ouvrir des "tunnels" sur le réseau Internet en utilisant le protocole PPP. Il assure l'intégrité de la transmission des données quel que soit le protocole que l'on souhaite utiliser (IPX, SNA, Appletalk...). Il a été défini par l'IETF.




Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. Mais L2TP peut aussi être directement mis en œuvre sur des supports WAN (relais de trames) sans utiliser la couche de transport IP.
On utilise souvent ce protocole pour créer des VPN sur Internet. Dans ce cas, L2TP transporte des trames PPP dans des paquets IP. Il se sert d'une série de messages L2TP pour assurer la maintenance du tunnel et d'UDP pour envoyer les trames PPP dans du L2TP.

**L2TP/IPsec** - Layer 2 Tunneling Protocol over IPsec - Protocole VPN de Windows 2000 combinant accès distant (L2TP) et sécurité (IPsec).

**Label -** Identifiant de longueur fixe et réduite utilisé pour identifier une FEC (groupe de paquets IP subissnt le même traitement). Il a généralement une signification locale.

**Label Swap -** Opération d'acheminement de base qui consiste à examiner un label entrant afin de déterminer le label sortant, l'encapsulation, le port et d'autres informations de manipulation de données. (voir MPLS)

**Label Swapping -** Paradigme autorisant l'acheminement profilé des données en utilisant les labels pour identifier les classes de paquets qui sont traités de la même manière lors de l'acheminement.

**Label Switched Hop -** Saut entre deux nœuds MPLS sur lequel l'acheminement se fait en utilisant les labels.

**Label Switched Path -** Chemin traversant un ou plusieurs LSRs à un niveau de la hiérarchie, emprunté par un paquet d'une FEC donnée. (voir MPLS).

**LAC -** L2TP Access Concentrator - concentrateur d'accès L2TP - Le concentrateur d'accès LAC a la mission de transmettre les paquets entre le système distant et le serveur LNS, ce dernier se situant à la terminaison logique de la connexion L2TP. Le LAC peut très bien être un PC, un routeur ou tout autre équipement capable d'initialiser une connexion L2TP.

**LAN -** Local Area Network: expression anglo-saxonne équivalent du français Réseau local ou réseau local d'entreprise. Réseau d'entreprise de faible superficie (les équipements informatiques qui le composent sont géographiquement circonscrits à un étage, un bâtiment, voire un site).

Réseau de données à haute vitesse et à faible taux d'erreur couvrant une zone géographique relativement petite (jusqu'à quelques milliers de mètres). Les réseaux locaux interconnectent des stations de travail, des périphériques, des terminaux et d'autres équipements dans un seul immeuble ou autre zone géographique limitée. Les standards de réseaux locaux spécifient le câblage et la signalisation au niveau des couches physiques et liaison de données du modèle OSI. Ethernet, FDDI et Token Ring sont des technologies de réseau local largement utilisées.

**LAN Manager -** Progiciel gestionnaire de réseau local proposé par Microsoft. Il cherche à prendre une place centrale sur le marché dans la mesure où il a été conçu pour fonctionner avec le système d'exploitation pour micro-ordinateurs OS/2 et Unix, notamment.

**LANE 1.0 -** LAN Emulation 1.0 - Technique désignant des équipements de référence, dont un serveur de configuration, afin de véhiculer les trafics Ethernet ou Token-Ring en mode émulé sur un réseau ATM. Ensemble de services regroupés par groupes et protocoles nécessaire à l'allocation et au rattachement des postes de travail en environnement ATM.

Cette architecture proposée par l'ATM Forum est considérée comme un des premiers efforts pour véhiculer IP sur ATM. L'idée est de faire apparaître un LAN (Local Area Network) ATM comme un ensemble de LANs logiques interconnectés via des routeurs.

Un LAN partagé est émulé en configurant un groupe ATM multicast entre tous les nœuds qui appartiennent au même LAN logique. Pour le transfert de données entre les noeuds, un serveur de résolution d'adresses est utilisé pour traduire l' adresse MAC en adresse ATM.

Un canal virtuel point à point est alors établi entre les noeuds. L'inconvénient principal de cette solution est l'utilisation de routeurs pour transférer les données au sein du même LAN ATM physique. Les serveurs deviennent des points de faille.

**LAP -** Link Acces Protocol - Sous ensemble de protocoles servant à gérer une transmission, proches de la procédure HDLC. Les plus fréquemment employés sont les classes B (LAP-B), utilisé dans X25, et la classe D (LAP-D), utilisée pour la signalisation dans la norme du RNIS.

**LAPB -** Le protocole LAPB est un protocole de niveau 2 qui transporte les paquets X25.

**LAPD -** Link Access Protocol - channel D - Protocole de niveau 2 qui travaille avec l'Asynchronous Balanced Mode (ABM). Ce mode est complètement équilibré (ni maitre, ni esclave). Chaque station peut intialiser, superviser et envoyer des trame à tout moment.

**Large bande -** (Téléphonie mobile) - Expression utilisée pour exprimer la largeur de la bande de fréquence par rapport aux fréquences à bande étroite de 3 MHz. Les fréquences de large bande peuvent transmettre plus de données et à plus haut débit que les fréquences de bande étroite. Les services de recherche de personnes utilisent généralement la bande étroite, alors que les téléphones et appareils de communication mobiles utilisent la large bande. Voir également Fréquence.

**Large bande -** Désigne une liaison ou un réseau capable de véhiculer un très grand nombre de signaux à des fréquences élevées. Quoique l'expression ne soit pas très précise et varie selon les contextes, on l'utilise généralement aujourd'hui pour les réseaux capables de fournir des débits supérieurs au mégabit par seconde et de véhiculer, par exemple, des images ou des données de gros volumes entre ordinateurs.

**Largeur de bande -** Différence entre la plus basse et la plus haute fréquence que laisse passer convenablement une liaison. On dit aussi "bande passante".

**Largeur d'impulsion -** En Optique - Temps d'émission d'une source lumineuse. Rencontrée notamment dans le réglage des paramètres d'un réflectomètre optique. Plus la largeur de l'impulsion est grande, plus l'énergie produite est importante.

**Largeur Spectrale** - En Optique - Ecart entre les valeurs de longueurs d'onde harmoniques émises par une source lumineuse autour de sa valeur centrale.

Typiquement quelques dizaines de nanomètre pour une diode électroluminescente et de < 1 à 2 nm pour les Lasers.

**Laser -** Onde lumineuse utilisée pour transporter des données dans des réseaux sans fil en mode point à point. Ce type de support émet sur une longueur d'onde comprise entre 900 et 950 nm. Les liaisons point à point en raison de la forte puissance concentrée sur une très faible surface rendent dangereux pour l'homme une diffusion de cette lumière.

En raison de la très forte puissance fournie et de sa concentration, ce type de support est très fiable en extérieur pour les liasions sans fil. Le rapport signal/bruit est assez constant. La liaison est cependant souvent sujette aux aléas des conditions climatiques.

La vitesse de propagation de ce type d'onde est très grande ($3.10^8$ m/s - 300 000 000 km / seconde).

Utilisé sur les réseaux optiques, et mobilisant plusieurs longueur d'ondes, le laser est utilisé comme source dans des nombreux équipements réseaux longue distance.

**LAT -** Local Area Transport - Protocole développé par Digital Equipement permettant de relier des terminaux et imprimantes aux serveurs VAX en environnement Decnet.

**LATA -** Local Access Transport Area - Aire géographique dans laquelle la réglementation permet à un exploitant local américain d'offrir ses services d'Accès à des réseaux longue distance.

**LCIE -** Laboratoire Central des Industries Electriques, en charge de la définition de normes sur la sécurité d'équipements télécoms ou radioélectriques. Bureau français de test et certification.

**LCP -** Link Control Protocol - Ce protocole de contrôle de liens est chargé de gérer les options et les liens créés. LCP est utilisé pour établir, maintenir, et fermer la liaison physique.

Dans l'optique d'être transportable sur un grand nombre d'environnements, PPP comprend un protocole de contrôle de liens pour établir, configurer, tester, et terminer le lien. LCP est utilisé pour manipuler les tailles variables des paquets, en effet selon le protocole d'encapsulation sélectionné dans le champ protocole, la taille du champ options/données n'est pas la même. Ces fonctions de test permettent de détecter un lien bouclé sur lui même ou toute autre erreur classique de configuration. D'autres fonctionnalités optionnelles comme l'authentification d'identité des extrémités, et la détermination de l'état du lien peuvent s'avérer intéressantes.

L'en-tête est le suivant :

| Code<br>1 octet | Identifiant<br>1 octet | Longueur<br>2 octets | Options |
|---|---|---|---|

Code = Définit, sur un octet, le type de paquet LCP:

1 : Configure request - 2 : Configure Ack - 3 : Configure NAK - 4 : Configure Reject - 5 : Terminate Request - 6 : Terminate Ack - 7 : Code Reject - 8 : Protocol Reject - 9 : Echo Request - 10 : Echo Reply - 11 : Discard Request - 12 : Link quality report.

Identifiant = Ce champ contient une valeur numérique qui sert à la gestion des requêtes et des réponses.

Longueur = Longueur totale du paquet LCP. Ce paquet comprend le code, l'identifiant, la longueur et les données.

Options = Ce champ de taille variable peut contenir une ou plusieurs configuration d'options. Le format d'une configuration d'options LCP possède 3 champs : type, longueur et données.

**LDAP -** Lightweight Directory Access Protocol - Protocole utilisé à l'origine pour transporter les informations entre serveurs d'annuaires. Son évolution actuelle tend à le transformer à court terme en un service d'annuaire à part entière. Il est utilisé dans le concept DEN pour permettre la communication entre les équipements réseaux et le service d'annuaire.

Il s'agit d'une version allégée de DAP (Directory Application Protocol), le protocole utilisé pour l'interrogation des serveurs X.500.

LDAP est un protocole d'accès à des annuaires (qu'ils soient compatibles X.500 ou non) qui fonctionne suivant le mode client/serveur. Il est basé sur TCP/IP et utilise en standard le port 389. On peut alors facilement faire un parallèle entre X.500 qui nécessite le modèle ISO de l'OSI et LDAP qui est basé sur TCP/IP de l'IETF (Internet Engineering Task Force).

LDAP est un protocole et non une spécification d'annuaire. Même si certains distributeurs préfèrent stocker les informations dans le format natif de LDAP pour des gains de performances, ce n'est en rien une obligation puisque LDAP ne définit que la façon dont les données sont échangées et non pas stockées.

Il n'y a donc pas d'annuaire LDAP, mais des annuaires supportant le protocole LDAP ou encore annuaires compatibles LDAP. C'est donc par abus de langage que l'on trouvera le terme d'annuaire LDAP.

Comme LDAP est élaboré par l'IETF, il est définit dans des RFC (Request For Comments) :

• LDAP v1 - juillet 1993

RFC 1487 : X.500 Lightweight Directory Access Protocol

RFC 1488 : The X.500 String Representation of Standard Attribute Syntaxes

• LDAP v2 - mars 1995

RFC 1777 : Lightweight Directory Access Protocol

RFC 1778 : The String Representation of Standard Attribute Syntaxes

RFC 1779 : A String Representation of Distinguished Names

• LDAP v3 - décembre 1997

RFC 2251 : Lightweight Directory Access Protocol v3

RFC 2252 : LDAP v3 Attribute Syntax Definitions

RFC 2253 : LDAP v3 UTF-8 String Representation of Distinguished Names

RFC 2254 : The String Representation of LDAP Search Filters

RFC 2255 : The LDAP URL Format

RFC 2256 : A Summary of the X.500 (96) User Schema for use with LDAP v3

**LEA -** Laboratoire d'Essais et d'Agrément.

**LEAP -** Lightweight EAP - Protocole d'authentification concurrent de PEAP proposé par Cisco.

**Least Cost Routing -** Routage optimal correspondant à un système d'acheminement des appels permettant de choisir systématiquement les liaisons les moins chères en fonction des destinations et de l'heure d'appel.

**LECAM -** Lecteur de cartes à mémoire (Marque déposée).

**LED -** LIGHT EMITTING DIODE - Source lumineuse à semi-conducteurs qui convertit les signaux électriques en une lumière visible ou en des rayonnements infrarouges.

**LEO -** Low Earth Orbit - Orbite basse de la terre. Un satellite LEO est en orbite basse, entre 700 et 1500km d'altitude. Le temps de réponse est ultra-rapide (5 à 15 millièmes de seconde) mais il faut plusieurs dizaines ou centaines de satellites pour quadriller la terre.

**Level 6 -** Aussi connu sous l'appellation Catégorie 5+ ou Catégorie 5 améliorée, le câble " Catégorie 5+ " offre de meilleures performances que le câble standard Catégorie 5. Il doit se conformer à des caractéristiques plus strictes, comme le rapport atténuation/diaphonie (ACR) de 10 dB à 155 Mhz et le test de la paradiaphonie (NEXT) sur 4 paires

**Liaison -** Ensemble des ressources nécessaires pour mettre en communication deux équipements.

**Liaison commutée et liaison permanente** - Un canal de transmission pourra être établi de manière permanente ou au contraire de manière limitée dans le temps. Dans ce dernier cas, on parle de commutation. Cette notion est donc inséparable de la notion de réseau. Commuter c'est sélectionner puis libérer un canal et le laisser ensuite disponible pour d'autres utilisateurs potentiels.

**Liaison de données -** Data Link - Liaison affectée à une transmission numérique. L'expression désigne surtout la deuxième couche du modèle OSI (Open Systems Interconnect) de l'ISO (International Standard Organisation).

**Liaison louée -** Sur le plan technique, une liaison louée se définit comme une liaison permanente constituée par un ou plusieurs tronçons d'un réseau ouvert au public et réservée à l'usage exclusif d'un utilisateur. Elle s'oppose ainsi à la liaison commutée, qui est temporaire. Au plan juridique, la ligne louée, encore appelée liaison louée ou liaison spécialisée, est ainsi définie par le code des postes et télécommunications : "la mise à disposition par l'exploitant public dans le cadre d'un contrat de location d'une capacité de transmission entre des points de terminaison déterminés du réseau public, au profit d'un utilisateur, à l'exclusion de toute commutation contrôlée par cet utilisateur". Ce type de service est utilisé par les entreprises pour leurs réseaux internes, ainsi que par les fournisseurs de services de télécommunications qui ne disposent pas d'infrastructures propres ou souhaitent les compléter.

**Liaison Multipoint -** Multipoint Connection - Liaison établie entre une entité et plusieurs autres.

**Liaison numérique -** Liaison sur laquelle la transmission des information s'effectue en mode numérique. Le terme "numérique" s'oppose à "analogique" et qualifie toute information de base (son, texte, image) qui a été codée et transformée en une suite de nombres.

**Liaison par faisceaux hertziens -** Liaison de radiocommunications de terre entre points fixes

**Liaisons duplex, simplex, semi-duplex -** Si un canal de transmission ne véhicule qu'un seul signal à la fois et dans un seul sens, on parlera de transmission simplex. Mais en transmission de données, on cherche à faire dialoguer deux équipements et donc à transporter un signal dans les deux sens. Il est intéressant que les deux transmissions utilisent le même canal. On parlera alors de liaison duplex. Cela pourra se faire soit en inversant périodiquement le sens du signal, c'est la méthode dite à l'alternat ou semi-duplex (ou encore half-duplex), soit en transportant simultanément les deux signaux de direction inverse, c'est le full-duplex. C'est cette dernière méthode que tendent à employer aujourd'hui beaucoup d'équipements de transmissions de données.

**Licences -** (France) - La loi du 26 juillet 1996 dispose que les activités de télécommunications s'exercent librement. Elle a toutefois prévu que certaines de ces activités s'exercent dans le cadre d'une autorisation, encore appelée licence. Ainsi l'établissement et l'exploitation d'un réseau ouvert au public, la fourniture du service téléphonique au public ainsi que la fourniture au public de services de télécommunications utilisant des fréquences hertziennes sont soumis à une autorisation délivrée par le ministre chargé des télécommunications, après instruction de l'Autorité. Les autorisations d'établissement et d'exploitation des réseaux indépendants sont délivrées par l'Autorité.

**LIDIC -** Association regroupant les grossistes en matériel électrique autour d'un projet d'Echanges de données informatisés (EDI).

**Lien hypertexte -** Zone interactive insérée dans une page web et permettant à l'utilisateur d'accéder directement à une autre ressource web quelle que soit sa localisation physique sur Internet.

**LIFO -** Last in First out - Mode d'organisation des files d'attente en "pile" où le dernier élément reçu est le premier utilisé.

**Lignes de communications électroniques à très haut débit en fibre optique -** Terminologie FTTH - Liaison passive d'un réseau de boucle locale à très haut débit constituée d'un ou plusieurs chemins continus en fibres optiques et permettant de desservir un utilisateur final.

**Ligne spécialisée -** Liaison permanente constituée d'un ou de plusieurs tronçons d'un réseau public mis bout à bout et affectée à un utilisateur particulier. On dit aussi ligne ou liaison "louée". En France, les lignes spécialisées numériques sont commercialisées sous le nom de Transfix.

Les liaisons spécialisées sont des lignes affectées en permanence à travers un réseau. La tarification est fixe, composée uniquement d'une taxe de raccordement et d'une redevance mensuelle dépendant des caractéristiques et surtout de la longueur de la ligne.

**Lignes spécialisées analogiques -** Elles peuvent être louées pour le transport de la voix (pour relier deux autocommutateurs téléphoniques) ou pour celui des données: dans ce dernier cas, un modem, identique aux modems réseau commuté ou plus perfectionné est bien entendu nécessaire. On peut louer des lignes à deux fils ou des lignes à 4 fils de qualité normale ou supérieure. Mais les débits ne permettent guère de dépasser 28,8 kbit/s en ligne.

**Li-Ion -** Type de batterie Lithium-Ion alimentant les appareils de communication mobile. Les piles (ou batteries) Li-Ion sont plus légères que les autres types de batterie, ont une durée de vie relativement longue et ne souffrent généralement pas de l'effet de mémoire. Voir également Batterie, NiCd et NiMH.

**Listes noires/blanches -** listes d'adresses d'expéditeurs systématiquement interdites par un filtre anti pourriel (liste noire) ou autorisées (liste blanche). Il peut s'agir également de listes de mots-clés.

**Livre vert -** Publication de la Commission des communautés européennes datant de 1988 et fixant des grands principes d'action pour préparer le Marché unique de 1993 dans le domaine des télécommunications. Ces principes d'inspiration libérale prônent l'ouverture du marché (assimilation des services de télécommunications à des services marchands) tout en accordant aux Etats la possibilité de conserver des monopoles pour les "services de base" (essentiellement le téléphone). Autres principes recommandés : claire séparation des instances réglementaires par rapport aux organismes d'exploitation des réseaux publics, reconnaissance automatique d'une homologation d'équipements si un seul pays de la CEE l'a délivrée, Accès à tous services ou réseaux à des conditions financières et techniques identiques pour tous.

**LLC -** Logical Link Control - Sous-couche faisant partie de la couche OSI 2 (Liaison de données) pour les réseaux locaux. Elle définit un protocole d'échange par paquets non fixes identique pour tous les réseaux locaux.

**LLC1 -** Logical Link Control 1 - Couche liaison de données dans les réseaux locaux en mode non connecté, dérivée d'HDLC.

**LMDS -** Local Multipoint Distribution Services - Technologie permettant de bénéficier de débits élevés, qui utilise des ondes radio pour accéder notamment au service téléphonique, à Internet et aux émissions de télévision. L'utilisation de ce mode de transmission peut notamment convenir aux zones peu peuplées non desservies par le câble. Toutefois, son développement se heurte encore à des obstacles techniques liés à l'atténuation du signal, d'une part en cas de perturbations atmosphériques et notamment de pluie, d'autre part dans les "zones d'ombres" (immeubles, reliefs, feuillages) qui perturbent la propagation des ondes radio.

Accès sans fil asymétrique fondé sur antenne parabolique qui agit à la fois comme receveur et émetteur avec une "hub station ". Ce système d'accès radio à haut débit (fréquences comprises entre 28 et 400 gHz) offre des services de Télévision comparables à ceux fournis par le câble.

**LMI -** Local Management Interface - Voir Relais de Trame et Frame Relay - Le protocole LMI sert à contrôler et commander la connexion entre l'utilisateur et le réseau. Il s'assure que le lien entre le réseau et l'utilisateur est actif. Il enregistre l'ajout et la suppression des PVC (Permanent Virtual Circuit ). Enfin il délivre des messages d'état sur la disponibilité des circuits à intervalle régulier.

**LNS -** L2TP Network Server - Serveur de réseau L2TP - A la mission de recevoir les paquets entre le système distant (LAC), ce dernier se situant au commencement logique de la connexion L2TP

**Local -** Désigne habituellement des dispositifs reliés à la station de travail de l'utilisateur, par opposition aux ressources distantes, accessibles par le biais d'un serveur.

**LocalTalk -** Système de câblage utilisé en standard dans le réseau bas débit d'Apple (230 Kbps) avec le protocole Appletalk.

**Logement abonné -** Terminologie FTTH - Logement dont l'occupant a souscrit un abonnement à une offre d'un opérateur commercial basé sur un réseau en fibre optique jusqu'à l'abonné

**Logment éligible -** Terminologie FTTH - Logement pour lequel au moins au moins un opérateur (qui peut être l'opérateur d'immeuble) a relié le point de mutualisation (PM) à son nœud de raccordement optique (NRO), et pour lequel il manque il manque seulement le raccordement final et un éventuel brassage au PM pour avoir une continuité optique entre le NRO de l'opérateur et la prise terminale optique.

**Logement éligible mutualisé -** Terminologie FTTH - logement éligible pour le quel plusieurs opérateurs ont relié le point de mutualisation à leur noeude de raccordement optique.

**Logement programmé -** Terminologie FTTH - Logement situé dans la zone arrière d'un point de mutualisation pour lequel le point de mutualisation a été installé et mis à disposition des opérateurs tiers, au sens de l'annexe II dela décision n°2009-1106.

**Logement raccordable -** Terminologie FTTH - Logement pour lequel il existe une continuité optique entre le point de mutualisation et le point de branchement optique, ou entre le point de mutualisation et la prise terminale optique si le point de branchement optique est absent. (dans le second cas, le logement est raccordé).

**Logement raccordé -** Terminologie FTTH - Logement pour le quel il existe une continuité optique entre le point de mutualisation et la prise terminale optique.

**Logiciel -** Ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données.

**Logon -** Commande d'ouverture d'une session de communication qui permet d'identifier l'utilisateur et de lui affecter les ressources auxquelles il a droit. On dit aussi parfois "login".

**Loi de Réflexion -** En Optique - Loi par laquelle tout rayon lumineux, à la frontière de deux matériaux d'indices de réfraction différents se réfléchit symétriquement par rapport à la perpendiculaire au plan formé par la surface de séparation de ces deux matériaux.

**Longueur d'onde** - en Optique - Mesure de l'oscillation d'une onde. Définie comme: Vitesse de l'onde divisée par sa fréquence. Elle est représentée par le symbole À (Lambda) et exprimée en unité de longueur (µm ou nm).

**Longueur d'onde de coupure -** En optique - Longueur d'onde à partir de laquelle une fibre se comporte en propagation unimodale en «coupant» tout autre mode hors le mode fondamental.

**Lot -** Regroupement de tâches ou d'informations à transmettre pour effectuer x traitements en une seule séquence. Surtout employé dans l'expression "traitement par lots" (ou batch), par opposition à l'interactif ou au temps réel, dans lesquels une tâche ou une information sont traitées dés qu'elles sont disponibles.

**Love -** Sur Longueur - Longueur de fibre optique enroulée, laissée en surplus afin d'effectuer des opérations ultérieures (soudure, manipulation de boîtiers d'étage, demande de déplacement de prise, etc.).

**LR -** Liaison de Raccordement. (voir "colocalisation").

**LRC -** Longitudinal Redundancy Check - Contrôle longitudinal de redondance - Système de détection d'erreurs par parité où celle-ci s'applique à la totalité des mots d'un bloc, par opposition à la parité "verticale" qui s'applique à chaque mot de ce bloc. Les deux types de parité sont fréquemment associés.

**LRT -** (France) - Loi de réglementation des télécommunications - Loi du 26 juillet 1996 préparant la libéralisation totale des télécommunications au 1er janvier 1998. Elle organise, avec le code des postes et télécommunications, le secteur des télécommunications.

**LS -** Ligne Spécialisée - Liaison permanente entre deux points, numérique ou analogique. En principe cette liaison est louée à une entreprise de télécommunications pour établir une liaison d'un débit supérieur à des lignes téléphoniques standard.

**LSOH -** Low Smoke Zéro Halogène. Caratéristique d'un cable attendus au cours d'un sinistre par le feu. Caractérise la gaine d'un câble, ou un plastique qui ne dégage pas de fumées toxiques en brûlant.

**LSR -** Label Switching Router - Nœud MPLS capable d'acheminer un paquet IP natif.

**LTE -** Evolution de HSPA - Les réseaux 3G LTE pourront reposer sur une architecture dotée de deux antennes par station de base et par terminal, qui permettront d'atteindre 144 Mbit/s en débit descendant et 50 Mbit/s en débit ascendant, en utilisant des porteuses de 20 MHz, contre 5 MHz en UMTS aujourd'hui.

En parallèle, le temps de latence du réseau ne devrait pas dépasser 10 ms. Parmi les évolutions attendues, outre le débit, la 3G LTE devrait passer au tout IP, assurer l'interopérabilité avec les autres infrastructures radio (Wi-Fi et Wimax) et permettre une plus grande intégration des réseaux fixe et mobile. Autant de caractéristiques qui permettront aux réseaux LTE de diminuer les coûts de déploiement et d'exploitation, tout comme l'intégration des concepts de plug and play et d'autoconfiguration dans leur conception. Par ailleurs, les réseaux LTE pourront fonctionner sur différentes bandes de fréquences (y compris les bandes GSM).

**LU -** Logical Unit - Unité logique. Dans le vocabulaire de l'architecture de communication d'IBM SNA, désigne une entité de haut niveau définissant des droits et des règles d'interconnexion et de communications avec les autres entités d'un réseau SNA. Les interactions entre utilisateurs se font ainsi par l'intermédiaire des LU qui les représentent et leur sont affectées.

**LU 6.2 -** Type particulier de LU pour permettre des échanges symétriques de programme à programme.

**Lumière -** En Optique - Rayonnement optique susceptible de produire directement une sensation visuelle chez l'être humain. Attention, tous les rayonnements utilisés dans les fibres optiques ne sont pas nécessairement visibles.

**Luminance -** Partie du signal vidéo qui contient les informations concernant l'intensité lumineuse, ou brillance, de chaque point.

**LWAPP -** Lightweight Access Point Protocole - Protocole proposé par Cisco pour servir de base à un standard permettant de construire un réseau WLAN à partir de composants réseaux de constructeurs différents.

Cisco a développé LWAPP en réponse à Slapp, solution plus basique d'Aruba et Trapeze, concurrents d'Airespace (Slapp écartait l'idée d'un standard de contrôle commun des points d'accès WLAN et suggérait un simple protocole qui permettait aux différents constructeurs de télécharger les firmwares de différents points (l'accès).

Le principe de fonctionnement repose sur l'établissement d'un tunnel du point d'accès jusqu'au contrôleur. C'est le préalable à l'établissement de la communication entre ces deux entités.

Le protocole peut opérer à deux niveaux : au niveau 2 et au niveau 3. Le tunnel est encapsulé dans un datagramme IP utilisant UDP comme protocole de transport. Le fonctionnement en mode niveau 2 n'est pas routable (impossible de répartir les points d'accès sur plusieurs réseaux différents) et il oblige à une visibilité directe du contrôleur et des points d'accès (même VLAN).

Le trafic, encapsulé dans un datagrappe UDP, se répartit en deux types distincts :

- Les flux de contrôles, entre contrôleur et point d'accès. Les flux de contrôle utilisent le port destination UDP 12223. Les données sont chiffrées par une clé symétrique à l'aide de l'algorithme AES-CCM. L'échange des clés de session est réalisé au travers d'un tunnel établi suite à l'échange de certificats X.509 générés par la PKI de Cisco.
- Les flux de données des utilisateurs. Les flux véhiculant les données des clients (en clair), utilisent le port UDP 12222. La totalité de la trame 802.11 reçue par le point d'accès est recopiée dans le datagramme en clair, et envoyée au contrôleur en unicast.

# M

**M&S -** Maintenance and Support - En Français = TMA - Voir TMA

**MAC -** (Média Access Control) Partie la plus basse du modèle OSI régissant les accès physiques aux câbles de communication. Dans l'architecture des réseaux locaux, couche chargée de contrôler l'accès au support. Sous-couches de la couche 2 de l'OSI (Liaison de données) qui contiennent le protocole de partage du canal de communication dans un réseau local. Les plus connues sont 802.3 (Ethernet), 802.4 (bus à jeton) et 802.5 (anneau à jeton).

**Maillage -** Architecture d'un réseau permettant d'une part à tous les nœuds d'avoir accès (directement ou indirectement) à n'importe quel autre nœud, d'autre part de disposer pour atteindre un autre nœud de plusieurs chemins d'Accès. Avantages du maillage : sécurité de fonctionnement en cas de rupture d'une liaison et possibilité de répartir les charges.

**MAN -** Metropolitan Area Network - Réseau métropolitain - Désigne un réseau dont l'étendue peut varier entre celle d'un campus, d'une ville et d'une region.

**Manager (snmp) -** C'est le logiciel d'administration de réseau - Il est hébergé sur un terminal qui lui est dédié (ou tout cas c'est largement conseillé). Son rôle est de faire remonter et de centraliser toutes les informations de gestion de réseau issues des objets situés sur les équipements.

**Manchester** - Codage Manchester - Norme de codage dans laquelle chaque bit provoque une transition du signal.

Ville Anglaise connue pour son équipe de football (aussi).

**Manchon -** Pièce de protection mécanique. Les manchons peuvent protéger des épissures ou des soudures effectuées sur des câbles en fibre optique. Certains de ces boîtiers de forme cylindrique ne permettent pas de réintervention ultérieure sur leur contenu, typiquement lorsque le manchon posé est termorétractable.

Les câbles laissés en attente doivent aussi être manchonnés de telle sorte qu'

**Map -** Manufacturing Automation Protocol - Réseau local normalisé pour l'environnement industriel. Conçu à l'origine par General Motors, il fonctionne selon la méthode d'Accès du "bus à jeton" (norme IEEE 802.4 et ISO 8802/4), en principe sur un câble de type télévision.

**Map Factory -** Abréviation de Mapping Factory, usine de réalisation de la cartographie du Système d'Information. Plateforme de développement mutualisé de schémas de description des liens entre les données et des règles de gestion des données.

**Mapi -** Mail Application Programmer Interface. Interface permettant d'accéder aux applications destinées à la gestion du courrier électronique.

**Masque jetable -** Procédé cryptographique utilisant une très longue suite non répétitive et aléatoire de lettres, écrite sur des pages reliées ensemble pour former un bloc. L'émetteur utilise chaque lettre du masque à son tour pour chiffrer exactement un caractère du texte clair. Le destinataire dispose d'un bloc identique et utilise le masque de la même manière pour déchiffrer les lettres du texte chiffré une à une.

**Mass-mailer -** Terme utilisé, entre autres, pour désigner un virus se servant de la messagerie électronique pour se propager. Contrairement aux "virus mailers", qui envoient un e-mail à chaque activation, les mass-mailers en envoient plusieurs à la fois, par exemple à tout un carnet d'adresses. Leur dangerosité est très relative, puisque l'effet majeur est de saturer les serveurs de messagerie.

**MAU -** Multistation Access Unit - Equipement de connexion concentrant plusieurs voies (8 en général) dans un réseau local de type anneau à jeton d'IBM. Il s'agit d'un équipement actif ou passif ne modifiant aucun signal, mais assurant une connexion refermant automatiquement l'anneau lorsqu'une prise est enfoncée ou retirée.

**MBGP -** Multicast Border Gateway Protocol ou Multiprotocol extension for BGP4 **-** RFC 2283 - MBGP permet de router les réseaux des sources Multicast au sein d'un domaine PIM (iMBP) ou entre domaines PIM distincts (eMBGP). Il fonctionne en établissant des "peerings" MBGP (comme en BGP4). Il permet de récupérer les routes annoncées par d'autres protocoles Multicast et de les réinjecter vers d'autres protocoles de routage Multicast. Voir Multicast.

**MBMS -** Multimédia Broadcast Multicast Services - Evolution du réseau mobile UMTS (validé par le 3GPP) offrant une bande passante de 5 MHz, un débit de 384 Kbit/seconde. Il n'existe pas encore de terminal, ni d'expérimentation prévue à la date de rédaction de cette définition (décembre 2005).

**Mbps -** Méga bits par seconde - Unité de débit d'un réseau de données.

**MD5** - Message Digest 5 - Algorithme de hachage utilisé pour l'authentification de données et la vérification de l'intégrité des communications.

Algorithme de chiffrement créé en 1991 par Ronald Rivest. Ce générateur de clés utilise, entre autres, une somme de contrôle d'intégrité du fichier, sa taille et son nom pour créer une clé sur 128 bits.

**Mégahertz -** Fréquence d'un million de cycles par seconde. Voir MHz.

**Mesh Network -** Réseaux maillés - Le principe des réseaux maillés est la base même d'Internet. Il suscite un regain d'intérêt dans les réseaux sans fils, parce que plus filable et moins coûteux à déployer. Contrairement à l'architecture traditionnelle d'un réseau sans fil dans laquelle les "îlots" Wi-Fi ne sont qu'une extension de l'infrastructure réseau filaire, un réseau sans-fil de type Mesh constitue le cœur du réseau à partir des matériels sans-fils eux-mêmes : Ces derniers dialoguent entre eux selon une architecture multipoint à multipoint, tout en desservant les postes clients.

Il n'existe pas encore de standard (voir 802.11s) pour définir le ou les protocoles mis en œuvre dans les réseaux Wi-Fi maillés, les implémentations actuelles sont par conséquent propriétaires.

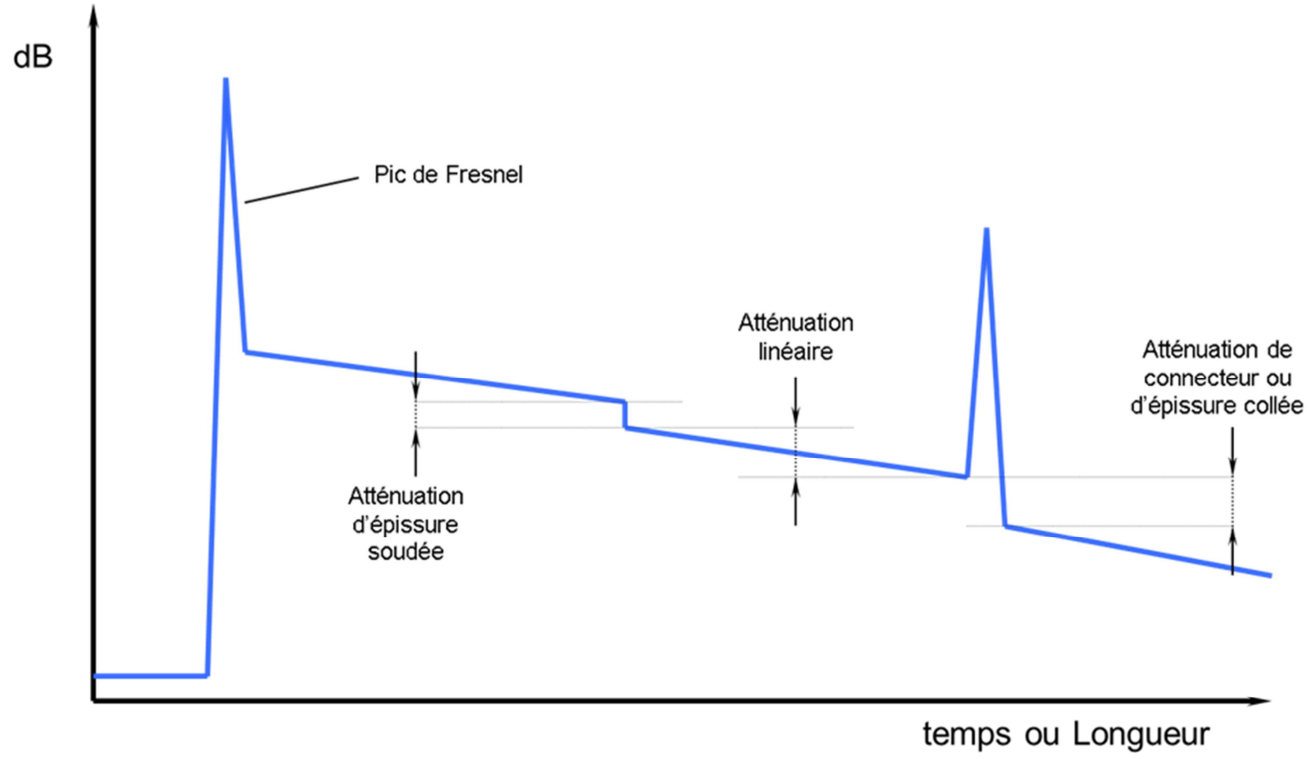
**Message -** Entité logique constituée par une suite cohérente d'informations.

**Messagerie électronique -** Technique d'échange de messages utilisant un ou plusieurs réseaux de télécommunications.

**Messagerie Vocale Instantanée - Push To Talk -** Service qui permet aux utilisateurs d'un téléphone cellulaire d'appuyer simplement sur une touche de fonction ou sur une icône, pour transmettre instantanément des messages vocaux à une ou plusieurs personnes qu'ils ont préalablement choisies, l'appareil se transformant alors en walkie-talkie, puisqu'une fois la communication établie, les correspondants ne peuvent parler qu'à tour de rôle.

**Messages courts - ou SMS - Short Message Service -** Ces messages, qui sont transmis via les canaux de signalisation du réseau mobile GSM, ont une longueur maximale de 160 caractères. La transmission de ces messages sur le réseau GSM est normalisée. Un serveur de messages courts intégré au réseau mobile assure l'interface entre environnement mobile et fixe.

**Mesures Optiques -**



**Méthode d'accès -** Mécanisme logique permettant aux différents utilisateurs d'une liaison ou d'un réseau de disposer des ressources de ce réseau sans perturber les autres utilisateurs. Selon le contexte, cette expression peut désigner un logiciel complet à la disposition des programmes d'applications (exemple: VTAM dans les systèmes IBM), ou des protocoles assurant le fonctionnement de base d'un réseau (exemple: méthode d'accès par jeton ou par détection de collision dans un réseau local, voir MAC).

Pour "mettre de l'ordre" dans un réseau local, ou toutes les stations peuvent prendre l'initiative des envois de messages, il faut une règle respectée par tout le monde. C'est la méthode d'accès. On distingue deux méthodes principales, la contention et le jeton. Elles distinguent les deux principales familles de réseaux locaux : Ethernet, qui utilise la contention, et l'anneau à jeton (Token-Ring), méthode déterministe (non aléatoire).

Dans la contention, tout le monde peut prendre la parole quand il le souhaite. Mais alors il faut une règle pour le cas où deux stations se mettraient à "parler" au même moment. Dans le jeton, on devra attendre son tour, matérialisé par le passage d'une configuration particulière de bit appelé jeton.

La principale méthode de contention en réseaux locaux est le CSMA/CD (Carrier Sense Multiple Acces), avec détection de collision (CD). C'est celle d'Ethernet. Elle consiste pour une station, au moment où elle émet, à écouter si une autre station n'est pas aussi en train d'émettre. Si c'est le cas, la station diffèrera son émission et attendra que le média soit libre pour émettre son message. Cette méthode est aléatoire, en ce sens qu'on ne peut prévoir le temps nécessaire à un message pour être émis, transmis et reçu.

L'autre méthode, celle du jeton (matérialisé par un ensemble de données, ou trame, affecté à cet usage), est dite déterministe puisqu'en fonction des caractéristiques du réseau (nombre de stations et longueur du câble), on peut déterminer le temps maximal que prendra un message pour atteindre son destinataire.

Les deux méthodes sont normalisées dans le cadre de l'association IEEE américaine, normalisation reprise dans le cadre de l'ISO. La méthode Ethernet CSMA/CD est normalisée en IEEE sous l'appellation 802.3 et l'anneau à jeton sous 802.5.

**MGCF -** Media Gateway Control Function - Passerelle permettant d'assurer la conversion entre des flux d'origines différentes. Aussi appelé MGW. Voir IMS.

**MHS -** Message Handling System - Désigne parfois un système de messagerie en général, mais le plus souvent fait référence à un sous-ensemble de la norme de messagerie électronique X400 comportant l'ensemble des mécanismes de gestion des messages.

**MHz -** Un million de Hertz ou de cycles par seconde. Mesure d'une fréquence radio.

**MHz et Mbps -** Il n'y a pas de relation directe entre Mbs et MHz car l'information peut être codée suivant différents modèles (Manchester, NRZI, MLT 3, etc.). Ethernet 10 Mbs et Token Ring utilisent le codage Manchester : le nombre de MHz est voisin du nombre de Mbps. Ethernet 100 Mbs et ATM utilisent un codage MLT3 : le nombre de MHz est environ 3 fois moins élevé que le nombre de Mbps.

MHz = millions de cycles par seconde

Mbps = millions de bits par seconde

**MIB (snmp) -** Management Information Base - Il s'agit d'une base de données située au sein de chaque agent. Cette base contient des informations de gestion sur l'équipement en question (concentrateur, hub...). La MIB n'est autre qu'un fichier détaillé qui sert de base au dialogue entre l'agent SNMP et la station du Manager SNMP

**MIC -** Modulation par Impulsions Codées - Technique de transmission utilisée pour véhiculer un signal analogique sous une forme numérique. Elle consiste à "échantillonner" ce signal et à transmettre le résultat codé des valeurs obtenues.

Procédé de transmission consistant à convertir le signal téléphonique en impulsions suivant un certain code. Le procédé consiste d'abord en un échantillonnage du signal, puis à exprimer l'amplitude de chaque échantillon par un nombre, représenté par un train d'impulsions en numération binaire.

Par extension, désigne des lignes à 2 048 mégabits par seconde commercialisées par France Télécom et qui utilisent cette technique. Ces lignes, utilisées notamment pour connecter au réseau téléphonique des autocommutateurs numériques, peuvent être divisées par multiplexage en 32 canaux de 64 Kbps.

**MICDA -** ADPCM - Modulation par Impulsions et Codage Différentiel Adaptatif - Méthode de compression utilisée pour réduire le volume de données. Cette méthode se base sur le codage des différences d'un échantillon à l'autre.

La MICDA est une technique utilisée en particulier pour les disques compacts (CD) et dans la norme DECT.

**Micro-ondes -** Un rayonnement est qualifié de "micro-ondes "dans la gamme qui s'étend entre 300 MHz et 300 GHz. Les fours à micro-ondes domestiques fonctionnent en Europe à une fréquence de 2,45 GHz, correspondant à une longueur d'onde de 12 centimètres.

**Microprocesseur -** Calculateur de très petites dimensions, constitué par un seul circuit intégré, permettant d'effectuer des opérations arithmétiques ou logiques suivant un programme enregistré en mémoire.

**Mime -** Multipurpose Internet Mail Extensions - Protocole de communication élargissant le champ d'applications du protocole SMTP, limité à l'envoi de fichiers textes, pour l'étendre aux pièces attachées et aux fichiers multimédias, en convertissant les éléments non textuels à un format reconnaissable par toutes les passerelles de messagerie.

**MIMO -** Multiple Input / Multiple Output - Technologie d'antennes multiples permettant d'augmenter les débits sur des technologies type WLAN ou UMTS, et à tirer partie des réflexions du signal radio sur les murs et les plafonds, souvent considérés comme perturbateurs, en améliorant l'efficacité spectrale.

La technique de modulation consiste à utiliser plusieurs antennes et diviser les données en autant de flux que d'antennes émettrices, transmis sur une même fréquence. Chaque antenne réceptrice reçoit une combinaison linéaire de ces flux, qui sont reconstitués par des fonctions de traitement de signal, et recollées pour constituer les données.

Utilisé dans les réseaux 802.11n, MIMO est un concept qui spécifie que l'on utilise plusieurs antennes pour le trafic sortant et entrant, mais ce n'est en aucun cas une norme ou une spécification. Donc, contrairement à ce que l'on peut croire de prime abord, le MIMO n'est absolument pas lié au Wifi, même si c'est lui qui le démocratise (d'ailleurs, le concept et les premières implémentations du MIMO remontent à bien avant les premiers drafts Wifi).

**Mini DVD -** C'est l'adéquation du VCD et du SVCD. Et c'est là tout le génie de l'idée, de mixer Vidéo CD "non standard" et mini-DVD. En deux mots, on va faire du Vidocq non "Toast-Ready", en tirant le data rate au maximum, et puisque celui-ci ne pourra pas être gravé en Vidocq, et bien, on va le graver en mini-DVD ! Il offre 18 minutes de Vidéo sur un CD-R 700 en qualité optimale. De plus il faut que le codage ait été effectué avec des valeurs proches de 4500000 Bits/s en VBR (bitrate variable) afin d'éviter toutes saccades lors de la lecture. (réglages conseilles : PAL en 352*288).

**Minitel -** Nom commercial des terminaux conçus par France Télécom pour le vidéotex français (programme Télétel).

Internet n'étant pas considéré comme sûr, les autorités françaises ont préféré développer, dès le début des années 80 le système Minitel, fondé sur le protocole V23.

**Mirroring -** Méthode consistant à répliquer les mêmes données sur deux espaces de stockage distincts afin de les sécuriser. En éloignant les deux pools de données, on diminue le risque d'accident et de perte.

**MISO -** Multiple In - Single Out. Comparable au MIMO sur le principe et c'est précisément cette technologie qui est utilisé pour l'interconnexion sans fils entre les freebox v5 et vHD.

**MMDS -** Multichannel Multipoint Distribution System - Système d'accès radio à haut débit dont les fréquences se situent entre 2 et 10 gHz. voir LMDS.

**MMJ -** Modified Modular Jack - Connecteur RJ 6 points décalé utilisé essentiellement dans l'environnement DEC.

**MMS -** Service de Messagerie MultiMedia - Les services liés au MMS sont dépendants du réseau, de la compatibilité du réseau utilisé et des formats de contenus supportés.

Un des derniers développements en matière de messagerie mobile est le service de messagerie multimédia ou MMS. Tout comme le traditionnel SMS (Short Message Service), la messagerie multimédia assure la transmission automatique et immédiate de messages personnels. Cependant, le MMS permet également aux utilisateurs de téléphones mobiles d'enrichir leurs messages en y intégrant du son, des images et d'autres éléments pour en faire de véritables messages vidéo et audio personnalisés.

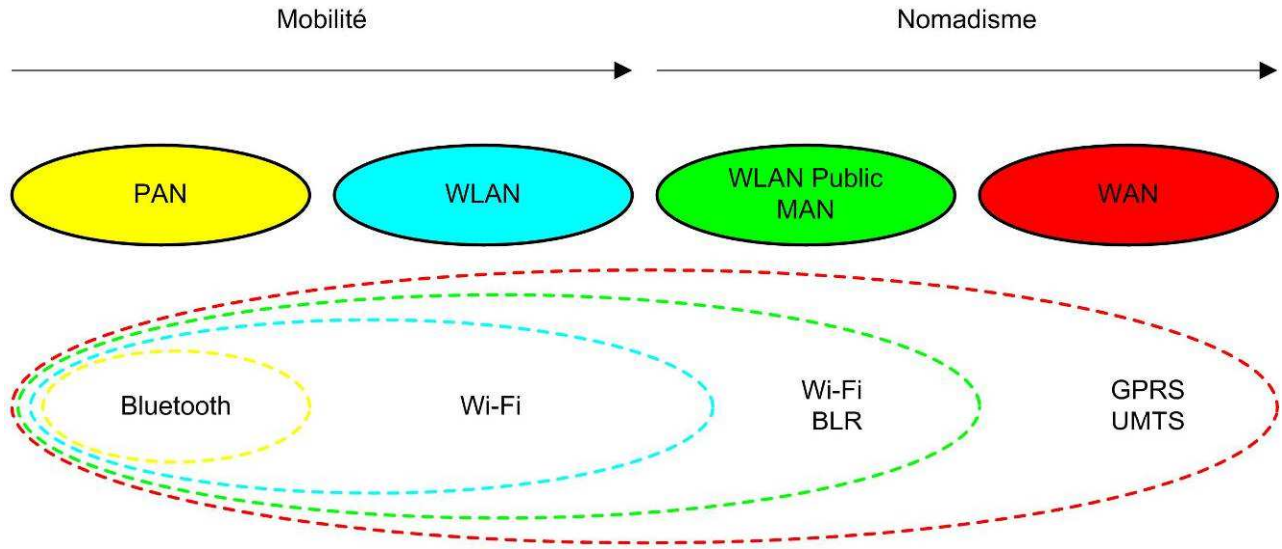
Outre les contenus textuels habituels des messages courts, les messages multimédias peuvent aussi contenir des photos, des graphiques, des clips audio et vocaux. Un message MMS à la forme d'une présentation en une seule entrée - ce n'est pas un fichier texte avec des pièces jointes. De plus, il sera possible d'envoyer des clips vidéo via MMS. Même si le MMS supporte des contenus multiples, il représente le prolongement logique du SMS.

La norme MMS recommande l'emploi de formats JPEG, GIF, texte, ARM et quelques autres formats moins importants. Le MMS supporte également l'envoi de messages à des adresses email. Comme le SMS, le MMS est une norme industrielle ouverte. Les messages MMS peuvent être transmis via des réseaux et des protocoles déjà existants. Par ailleurs, le MMS est indépendant du support. Il ne se limite donc pas aux réseaux GSM ou WCDMA.

**MOA -** Maitrise d'OuvrAge - C'est un rôle de "commanditaire" de travaux. Il s'agit de spécifier, organiser et planifier le projet lors de la phase de conception, et jusqu'au lancement du projet, en s'appuyant sur la ou les maitrises d'œuvre (voir MOE). La Maitrise d'Ouvrage est responsable du contenu fonctionnel du projet, et en gère la conduite.
Dotée d'une réelle connaissance de la société, elle sait exprimer clairement les demandes des utilisateurs, de façon à les traduire en exigences précises et exploitables. Son rôle est principalement fonctionnel, sa mission consiste aussi à fournir des outils méthodologiques essentiels à la réussite du projet.
Principales tâches :

- Responsable du contenu fonctionnel du Projet
  - Définition des besoins métier et établissement des spécifications fonctionnelles.
  - Rédaction du cahier des charges.
  - Choix des solutions.
  - Prévision des moyens à mettre en œuvre (humains, outils, techniques, financiers,…)
  - Définition et supervision de la réalisation des prototypes et des tests fonctionnels.
  - Recette fonctionnelles.
- Préparation, déploiement du projet, mise en œuvre des actions d'accompagnement des utilisateurs
  - Définition de la méthode et des moyens pédagogiques de formations des utilisateurs.
- Conduite de projet
  - Organisation, coordination et animation de l'équipe de maitrise d'ouvrage du projet.
  - Supervision du déroulement du projet.
  - Coordination et synthèse des validations, assurance de la qualité des validations prononcées.
  - Responsabilité des évènements survenant dans le projet.
- Garantie de la meilleure adéquation qualité/coûts/délais
  - Recette des réalisations et appréciation de leur conformité au cahier des charges de l'ouvrage.
  - Respect des délais et des coûts.
  - Définition et gestion du planning d'avancée du projet.
  - Arbitrage des choix à opérer en fonction du risque et du résultat.
  - Mise en place des indicateurs nécessaires au suivi et à la gestion du projet.

**Mobilité -** Mobilité et Nomadisme - Une technologie pour chaque application. Du réseau personnel (PAN pour Personnal Area network) au réseau large (WAN pour Wide Area Network), chaque standard, chaque technologie de la mobilité trouve un usage à sa taille :




| | | | |
|---|---|---|---|
| Quelques mètres | Jusqu'à 50 m | Jusqu'à 3 km | Couverture nationale |
| Faible coût | Faible coût | Coût moyen | Coût élevé |
| < 1 Mbit/s | De 11 à 54 Mbit/s | De 1 à 54 Mbit/s | De 10 à 100 kbit/s |
| Interface PC/PDA/ Téléphone | De PC à PC, de PC à Internet ou de PC à réseau d'entreprise | De PC à Internet, de PC à VPN IP d'entreprise | De PC ou PDA à internet ou à VPN IP d'entreprise |

**Mode -** Caractérise en général les principes physiques ou logiques d'une liaison. Il peut concerner les paramètres temporels (mode asynchrone ou synchrone), le découpage logique du contenu (mode bit, mode caractère, mode bloc) ou l'aspect général (mode interactif ou mode batch).

**Modes** - En Optique - Solutions physiques satisfaisant, pour le guide d'onde considéré, aux équations de Maxwell. Plus simplement: trajet que peuvent effectuer certains rayons lumineux à l'intérieur d'une fibre.

**Mode fondamental -** En Optique - Noté HE 11 ou LP 01 pour Linéairement Polarisé. Seul mode guidé dans une fibre satisfaisant à l'équation dans laquelle la fréquence normalisée V devient inférieure à une valeur de 2,405.

**Mode d'ordre bas** - En Optique - Mode qui se propage dans la fibre suivant un angle plat avec l'axe de la fibre.La longueur d'onde est importante (angle plat).

**Mode d'ordre élevé** - En Optique - Mode qui se propage dans la fibre suivant un angle aigu avec l'axe de la fibre. La longueur d'onde est courte (angle fermé).

**Mode de coeur** - En Optique - Partie d'énergie qui se propage dans le coeur d'une fibre.

**Mode de gaine** - En Optique - Partie d'énergie qui se propage dans la gaine optique d'une fibre.

**Mode guidé à fuite** - En Optique - Ondes qui se trouvent à la limite des modes guidés, et dont la propagation est limitée à cause d'un affaiblissement élevé.

**Mode bit -** Technique de communication dans laquelle un ensemble de données (bloc ou trame) est considéré comme une suite de bits sans référence au contenu (caractères, mots ou type de codage). L'avantage de ce mode, outre son efficacité (la synchronisation n'est nécessaire que pour l'ensemble du bloc et non pas à chaque mot), est de pouvoir être utilisé avec différents codes. C'est ce mode qui est employé dans les procédures dites HDLC.

**Mode bloc -** Technique de communications dans laquelle les informations sont regroupées par ensembles de longueur fixe.

**Mode caractère -** Technique de communication dans laquelle l'élément de base est le caractère ou le mot de longueur fixe. La synchronisation peut se faire soit à chaque caractère (mode asynchrone), soit par une séquence spéciale de caractères.

**Mode connecté et mode non connecté -** Comparaison

| Comparaison entre mode connecté et mode non connecté | | |
|---|---|---|
| Critères | Mode connecté | Monde non connecté |
| Mise en relation nécessaire | Obligatoire | Non |
| Délai de connexion | Oui, pouvant être important. | Non, puisque pas de connexion |
| Type de circuit offert | Permanent durant l'échange | Pas de circuit réservé, mode datagramme |
| Contrôle de flux possible | Oui | Non |
| Séquencement des informations | Oui (garanti par le réseau) | Non (à charge du destinataire) |
| Reprise sur incident | Oui | Non |
| Optimisation des réseaux | Non, circuits et ressources réservés durant toute la relation. | Oui, pas de ressource réservée, optimisation lors du routage. |
| Adressage | Peut être simplifié voir absent | Complet, chaque bloc de données (paquet) contient l'adresse du destinataire |
| Exemple de réseau | Transpac (X25) | Internet (TCP/IP) |

**Mode de transmission** - Une transmission de données, plus que tout autre transmission, devra se définir avant tout par rapport au facteur temps. Aussi, quel que soit le type de modulation utilisé, elle devra toujours se référer à un signal d'horloge qui indiquera à chaque équipement l'instant précis où il doit prendre en compte une donnée.

Dans les transmissions en série, qui constituent l'immense majorité des transmissions de données, il faut qu'émetteur et récepteur utilisent des horloges travaillant à la même cadence. Deux méthodes sont utilisées pour cela:

Méthode asynchrone, l'horloge du récepteur est inactive au repos et est déclenchée au début puis stoppée à la fin de chaque caractère par des bits de démarrage et de fin.

C'est pourquoi on la désigne aussi par l'expression de start stop. On dit également que l'on travaille en mode caractère.

Méthode synchrone, émettrice et réceptrice sont calés sur le même rythme pendant la transmission, des signaux d'horloge étant émis avant la transmission des données pour caler les deux horloges. On dit que l'on travaille en mode bit.

En mode asynchrone, l'horloge du récepteur est arrêtée à l'état de repos entre deux caractères. Elle est activée par le premier bit envoyé par l'émetteur. Ce bit est appelé le bit start. Elle rythme ensuite la réception des sept ou huit bits suivants et éventuellement d'un bit de vérification dit de parité. L'horloge s'interrompt ensuite lors de la réception d'un ou deux bits d'arrêt ou stop bit et attend le caractère suivant. Son principal avantage réside dans son prix car il ne nécessite pas une électronique très complexe. Le mode asynchrone oblige à envoyer les informations caractère par caractère et surtout perd 20 à 30% du débit total, sans parler des temps perdus entre les caractères.

Les transmissions en mode synchrone sont nettement plus efficaces, puisqu'il n'est plus nécessaire d'ajouter des bits au début et à la fin de chaque mot, et surtout il n'y a plus de temps perdu entre les mots. Le gros avantage du mode synchrone est d'envoyer les données par blocs d'information, généralement fixes, correspondant souvent à la taille d'un élément du terminal (par exemple le contenu d'un écran entier). Au début de chaque bloc, on enverra deux mots (ou plus) de synchronisation, puis tous les autres mots du bloc seront envoyés à la suite sans interruption ni séparateurs. En mode synchrone, l'unité de transmission n'est donc plus le mot, mais un bloc de données logique que l'on appelle une trame.

**Mode de transmission asynchrone -** Mode de transmission dans lequel l'horloge du récepteur est indépendante de celle de l'émetteur. L'horloge de réception est resynchronisée au début de chaque caractère transmis.

Technique de multiplexage et d'acheminement de données numériques par paquets de longueur fixe, destinée aux réseaux multiservices à haut débit. L'abréviation usuelle ATM est le sigle de l'expression asynchronous transfer mode

**Mode de transmission synchrone -** Mode de transmission dans lequel l'horloge du récepteur est liée à celle de l'émetteur La synchronisation des horloges est permanente et assurée à chaque bit transmis.

**Mode non connecté -** ConnectionLess Network Service - En mode non connecté, les paquets d'informations transitent dans le réseau indépendamment les uns des autres. Le routage de chaque paquet appartenant à un même message est alors décidé de façon instantanée par les routeurs sans itinéraire préétabli. Cette simplicité de fonctionnement a ses revers: le séquencement des informations ne peut être garanti. En revanche, le mode non connecté optimise l'utilisation du réseau en permettant une meilleure répartition de ses charges. De même, les mécanismes réseaux sont allégés (le réseau se limite à commuter) et ce sont les équipements terminaux qui mettent en œuvre les procédures liées à la communication pour remettre dans le bon ordre les différents blocs d'information. Chaque bloc étant routé indépendamment du précédent, il doit, par conséquent, contenir l'adresse complète du destinataire. Mais. en cas de surcharge du réseau, des blocs d'information peuvent être perdus. Ce mode de mise en relation ne permet pas d'envoyer des accusés de réception et l'arrivée à destination des paquets ne peut donc être assurée.

Le mode non connecté est aussi souvent référé sous l'expression de mode datagramme". Et, depuis l'avènement d'internet. on parle aussi de best effort. Ce qui signifie que le réseau "fait pour le mieux". Les premiers réseaux à commutation de paquets, comme le réseau Arpanet de la Défense Américaine ont lancé le principe de communication en mode non connecté. Le protocole IP (Internet Protocol) l'a repris avec force. Il est mis en œuvre dans les réseaux locaux et sur Internet.

Pour pallier les inconvénients liés au mode non connecté (absence de garantie dans le séquencement des données, problèmes de congestion et risques de perte de paquets - les opérateurs publics se sont orientés vers des technologies qui simulent la commutation de circuits en émulant entre les équipements Communicants un circuit logique, avant tout échange de données (donc en mode connecté), c'est le cas des réseaux Frame-Relay et ATM.

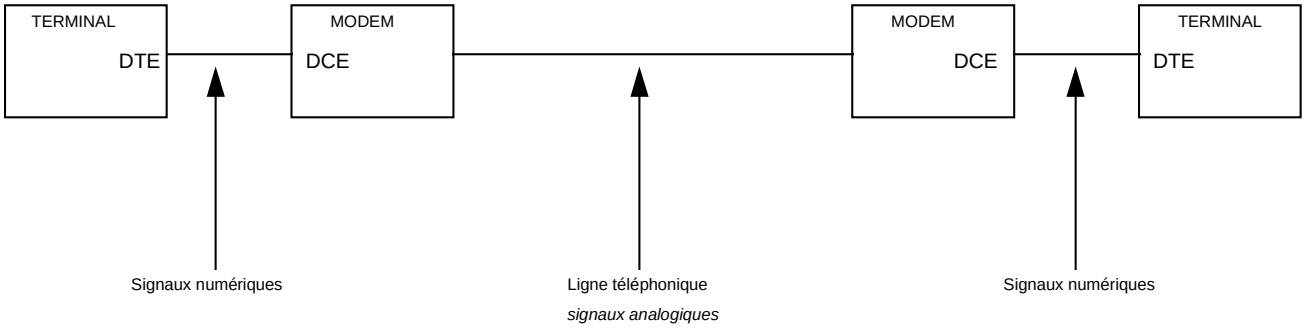
**Mode NT -** Network Termination - Terminaison de réseau - Le mode NT est une fonction des cartes ISDN particulières qui permet à des périphériques traditionnels ISDN (comme des téléphones, des systèmes téléphoniques ISDN) d'être utilisés pour la Voix sur IP. La Terminaison de réseau identifie à la base le point sur lequel le terminal a accès à un réseau de communication.

**Mode orienté connexion -** Mode selon lequel les paquets d'informations sont envoyés sur le réseau selon une route bien définie (à fa différence du mode non connecté, dit encore "mode datagramme").

**Modèle OSI -** Ensemble cohérent de normes défini par l'ISO (International Standard Organisation) pour servir de cadre de référence aux communications entre systèmes de marques différentes (hétérogènes). D'où son nom d'OSI: Open System Interconnect, ou Interconnexion de systèmes ouverts (en français les sigles OSI et ISO sont inversés). Il est divisé en 7 couches séparées, chacune assurant une fonction de communication.

**Modem -** Contraction pour "modulateur/démodulateur", utilisable quand les deux fonctions sont regroupées dans un même équipement de conversion de signaux. Appareil d'adaptation servant à transformer des signaux numériques pour les transmettre sur un canal de transmission analogique et inversement. Il assure également les fonctions de synchronisation de la communication et, souvent, d'autres fonctions additionnelles (mise en concordance des débits, numérotation automatique, correction d'erreurs, tests de la liaison). Les modems peuvent être contenus dans un coffret ou intégré à un équipement (micro-ordinateur par exemple). Il existe d'autres types particuliers d'équipement d'adaptation, que l'on désigne, parfois à tort, par le vocable de modem. Le modem acoustique, par exemple, sert à acheminer les données à travers un combiné téléphonique. Le modem "bande de base" n'est pas à proprement parler un modem, puisqu'une ligne "bande de base" ne nécessite pas de modulation, les données à transmettre étant directement injectées sur la ligne. Un modem se caractérise par son débit exprimé en bit par seconde, souvent accompagné ou confondu avec sa fréquence de modulation sur la liaison analogique exprimée elle en Baud, ainsi que par sa capacité à répondre à un ou plusieurs avis (Vxx) du CCITT.

Bien que l'évolution de fond des télécommunications soit le passage à la numérisation, les réseaux publics, en particulier le réseau téléphonique, restent en partie analogique. Il faut donc encore, pour transmettre des données à travers une liaison analogique, par exemple, une liaison téléphonique, faire appel à une paire d'adaptateurs: ceux-ci vont traduire les signaux numériques issus d'un équipement informatique en signaux analogiques dans un sens et réaliser l'adaptation inverse dans l'autre. C'est le rôle du modem ou modulateur-démodulateur.




Le modem doit exploiter au mieux la bande passante (BP) disponible sur une liaison analogique. Aussi utilise-t-on une gamme de techniques de modulations et de codage très variée, allant de la modulation d'amplitude à la modulation de fréquence, en passant par la modulation de phase ou des combinaisons souvent complexes des trois dans les modèles les plus récents.

Leurs modes de fonctionnement et leurs vitesses (débits) sont fixés par des avis rendus régulièrement par l'UIT (ex CCITT). Le choix d'un modem se fait donc en fonction de l'avis désigné par la lettre V suivie de 2 chiffres. Pour communiquer, 2 modems doivent respecter le même avis ou tout du moins deux avis compatibles. La miniaturisation des circuits permet aujourd'hui à la plupart des modems de gérer plusieurs avis différents et de s'apparier avec une gamme plus large de modems partenaires.

Les modems fonctionnent soit en transmission synchrone, soit en asynchrone, selon l'équipement auquel ils doivent se connecter. Certains assurent d'ailleurs les deux modes.

**Modem Câble -** Expression qui se réfère aux équipements des réseaux mixtes composés de fibre optique et de petits coaxiaux (HFC, Hybrid Fibre Coaxial) utilisés dans les réseaux de diffusion de programmes télévisuels. Les nouvelles normes de ce domaine permettent aujourd'hui la distribution de services numériques interactifs (télévision, accès Internet, accès téléphoniques, visiophonie, etc.).

**Modulation -** Modification des caractéristiques d'un signal par rapport à un autre signal. Variation dans le temps d'une caractéristique physique d'une liaison en fonction du message à transmettre. En général, la modulation consiste à modifier les caractéristiques d'une onde de base dite "onde porteuse", qui en l'absence d'informations à transmettre est constante et régulière. On peut modifier son amplitude (modulation d'amplitude), sa fréquence d'oscillation (modulation de fréquence), sa périodicité (modulation de phase)...

Modification d'une des caractéristiques d'une onde dite porteuse, par le signal qui contient l'information :

- Dans la modulation d'amplitude, on fait varier l'amplitude, c'est-à-dire la grandeur de l'onde porteuse, au rythme des variations du signal à transmettre.
- Dans la modulation de fréquence, ou la modulation de phase, c'est la fréquence ou la phase de l'onde porteuse qu'on fait varier dans les mêmes conditions.

**Modulation d'amplitude -** Modulation dans laquelle la caractéristique sur laquelle porte la variation est l'amplitude d'un courant alternatif.

**Module -** En FTTH - Terme utilisé dans le domaine de la fibre optique pour désigner un ensemble cohérent (tube, gaine, micro-module, micro-gaine). Le cas le plus fréquent est le module de 12, dans lequel les sous ensembles sont composés de 12 éléments. On rencontre aussi usuellement des modules de 6, et depuis les recommandations ARCEP sur les installations en zone dense des modules de 4.

Par exemple, un câble de 144 fibres peut contenir 12 modules comprenant chacun 12 fibres optiques, les cassettes seront alors en module 12 pour y épanouir les câbles de manière organisée et logique.

**MOE -** Maîtrise d'œuvre - Le rôle du maitre d'œuvre est d'animer une équipe, il est responsable au quotidien de l'avancement du projet ainsi que de la satisfaction des clients. Il doit parvenir à un résultat qui s'avère conforme au référentiel établi par (ou pour) la maîtrise d'ouvrage sur les plans de la qualité, des performances, des coûts et des délais.

Principales tâches :

- Responsable du contenu technique du Projet
  - Définition de la conception technique du projet.
  - Spécifications techniques détaillées
  - Participation au choix de solution techniques en liaison avec la maîtrise d'ouvrage
  - Réalisation (développements, spécificités, intégration, déploiement,…)
  - Définition des tests
  - Recettes
- Conduite de projet sur le terrain
  - Organisation et coordination de l'équipe de maîtrise d'œuvre
  - Arbitrage des différents entre l'équipe et les autres intervenants
  - Supervision du déroulement du projet
  - Coordination et synthèse des validations, garantie de leur qualité
  - Circulation et diffusion de l'information côté maître d'ouvrage
- Déploiement technique, mise en œuvre du suivi des utilisateurs
  - Déploiement de la nouvelle application et/ou du nouveau service
  - Organisation de la maintenance
  - Formation des utilisateurs
  - Organisation du support utilisateur
- Garant d'une adéquation qualité/délais/coûts optimale
  - Respect du cahier des charges
  - Respect des délais
  - Respect des coûts
  - En cours de projet, proposition au maître d'ouvrage de modifications d'objectifs éventuels (qualités, coûts, délais, technologies…) liées à des contraintes de réalisation.

**MOM -** Middleware Orienté Messages - Mécanisme de routage des messages. C'est lui qui redirigera, par exemple, une commande passée par le web vers les applications concernées en ne fournissant à chacune que les informations dont elle a besoin. Le MOM se comporte à la manière du bus de données d'un processeur.

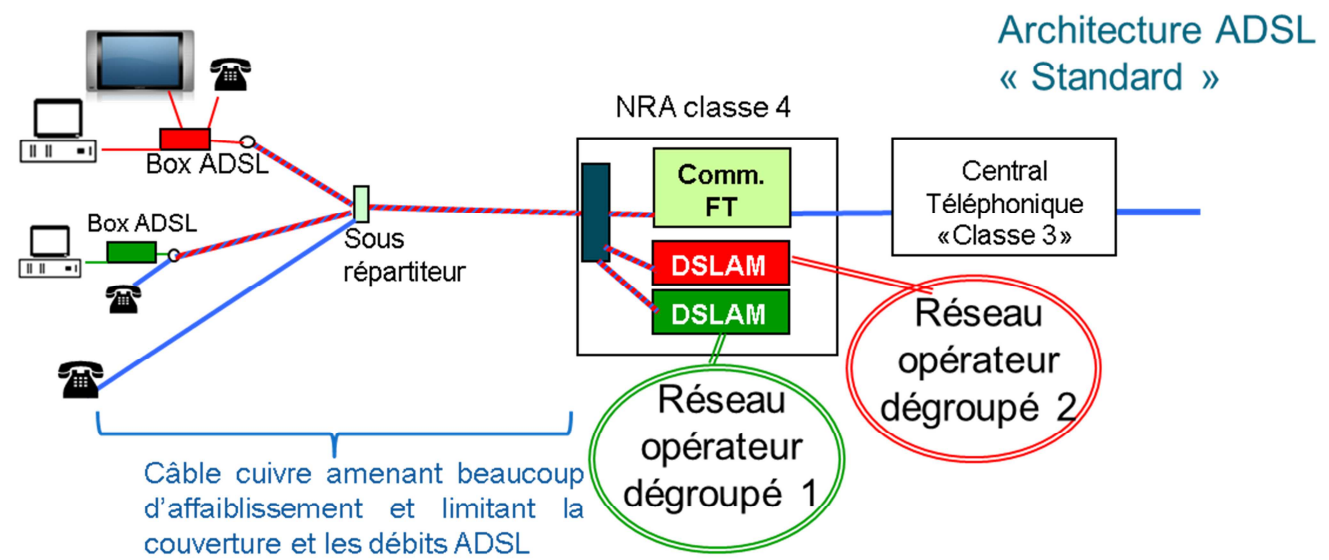
**Moniteur -** Logiciel assurant le contrôle de plusieurs autres logiciels pour coordonner des tâches particulières répétitives. Il intervient entre les applications et le système d'exploitation. Par exemple, un moniteur de télétraitement coordonne toutes les tâches servant à gérer des ressources à distance. Désigne aussi un "moniteur de visualisation", c'est-à- dire un écran.

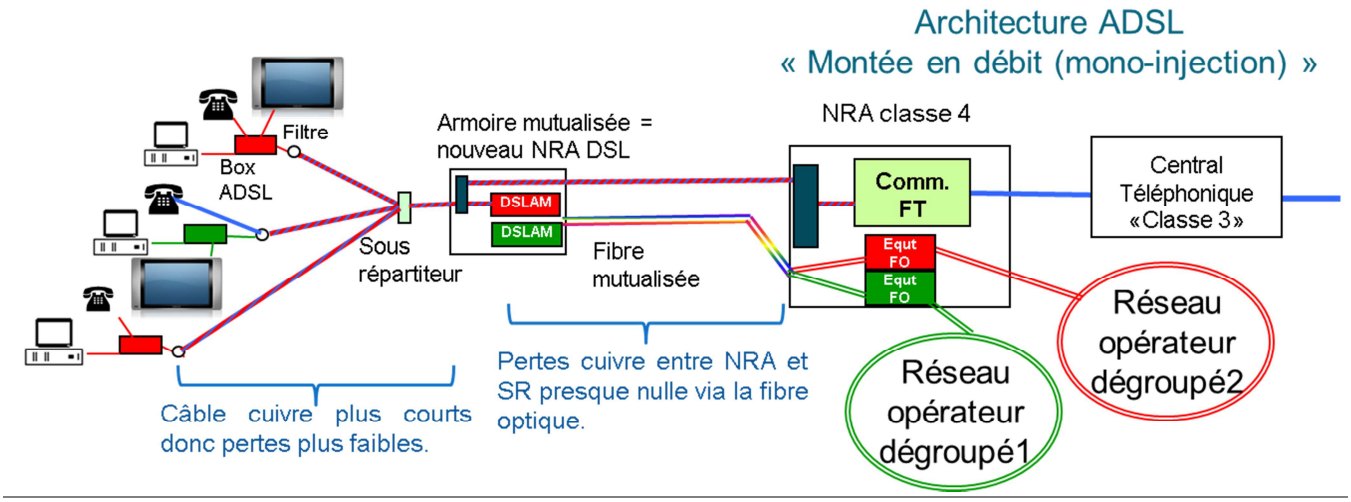
**Monomode -** ou **Unimodale -** Se dit d'une fibre optique dans laquelle ne peut être entretenu qu'un seul faisceau de rayons lumineux. Cette qualification de "seul faisceau lumineux" est sujette depuis à caution avec des équipement DWDM. Idéal pour les longues distances.

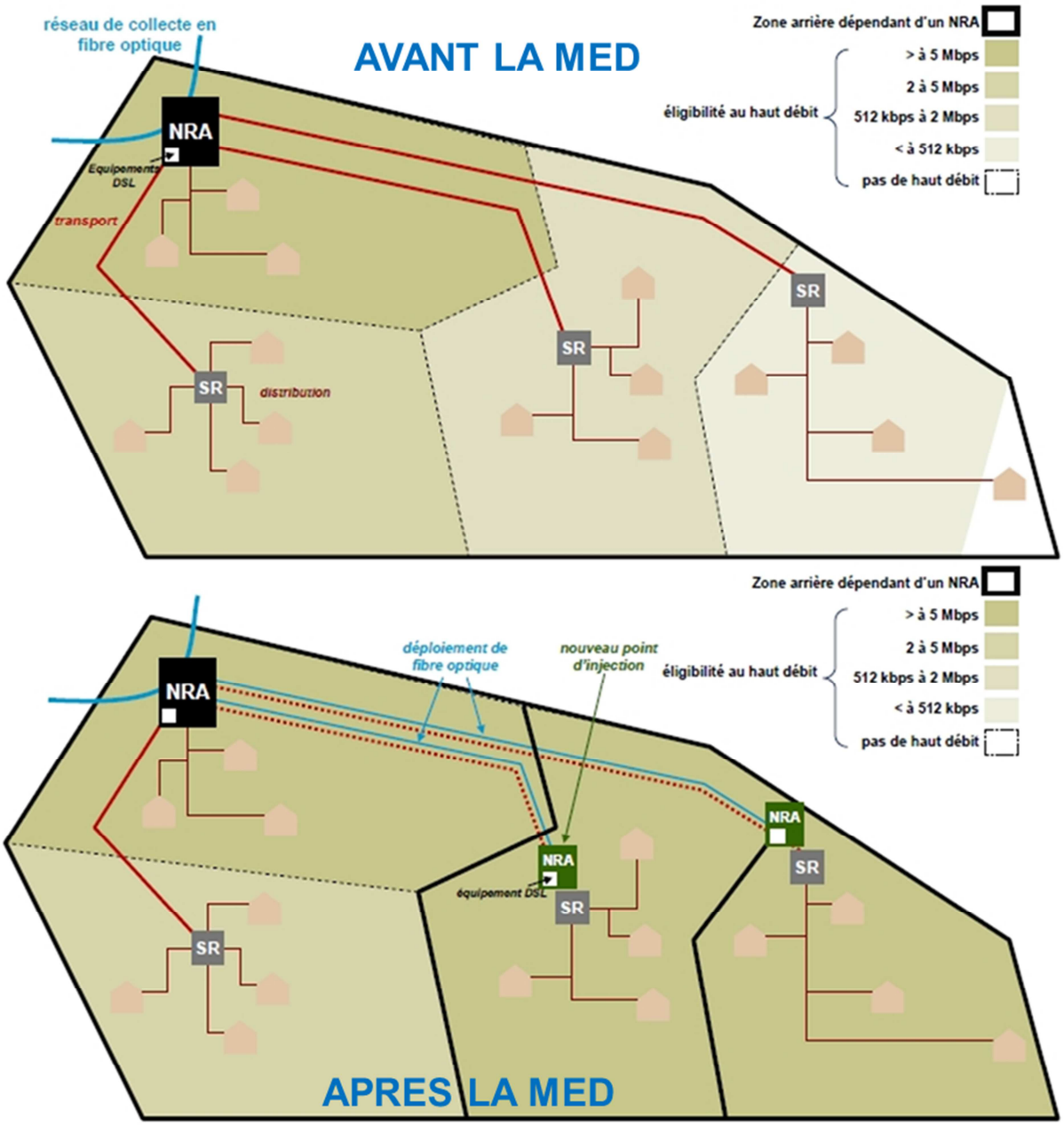
Fibre optique dans laquelle un seul mode, le mode fondamental, est capable de se propager à la longueur d'onde de fonctionnement.

Fibre optique dans laquelle un seul mode de propagation peut être entretenu à la longueur d'onde considérée. Diamètre de gaine identique au standard multimode 125 µm et valeur de coeur située autour de 9 µm

**Montée en Débit (MED) -** Terminologie désigant des projets visant à améliorer la couverture ADSL d'une emprise géographique en y installant des répéteur de NRA dans des sous répartiteurs de zone.






**Moore -** Loi de Gordon Moore - "Le nombre de transistors intégré dans une puce doublera tous les deux ans. "C'est la loi de Gordon Moore, l'un des fondateurs d'Intel, qui a eu raison jusqu'en 1992, alors qu'il avait énoncé sa loi dans les années 1960. Depuis la courbe s'est infléchie. Ce que la loi ne dit pas, c'est que le volume des investissements nécessaires pour une telle croissance suit la même courbe.

**MOSPF -** Multicast extension Open Shortest Path First - RFC 1584 (voir Multicast). Extension du protocole de routage OSPF (voir OSPF) MOSPF inclut une information Multicast dans l'annonce de l'état de lien OSPF pour construire les arbres de distribution Multicast.

Les LSAs d'appartenance à un groupe sont propagés dans l'ensemble du domaine de routage OSPF, afin que les routeurs MOSPF puissent calculer les listes des interfaces de sortie.

MOSPF utilise l'algorithme Dijkstra pour calculer l'arbre du plus court chemin. Un calcul séparé est requit pour chaque couple "source/groupe".

MOSPF ne propage pas partout le trafic Multicast pour créer les états, ce protocole utilise les LSAs et la base de données d'états des liens. Par conséquent, ce protocole ne peut fonctionner qu'en présence du protocole de routage OSPF sur un réseau. L'algorithme Dijkstra tourne pour tous les couples multicast (S, G), ce qui génère des problèmes significatifs d'échelle, comme le fait que ce protocole ne supporte pas les arbres partagés.

MOSPF est inapproprié pour les grandes interconnexions de réseaux avec beaucoup de sources et de récepteurs.

**Moteur de recherche -** Un moteur de recherche est un logiciel permettant de trouver sur Internet des ressources (pages web, forums, images, vidéo, fichiers, etc.) associées à des mots quelconques. Google, yahoo, sont des exemples de moteurs de recherche.

Des « robots », encore appelés bots, spiders, crawlers ou agents, parcourent les sites à intervalles réguliers et de façon automatique (sans intervention humaine, ce qui les distingue des annuaires) pour découvrir de nouvelles adresses (URL). Ils suivent les liens hypertextes (qui relient les pages les unes aux autres) rencontrés sur chaque page atteinte. Chaque page identifiée est alors indexée dans une base de données (organisée comme l'index d'un livre), accessible ensuite par les internautes à partir de mots-clés. Les mots-clés sont associés à une valeur de « poids » qui correspond à la probabilité d'apparition dans un document. Cette valeur permet de présenter les résultats des recherches par ordre de pertinence supposée. Les algorithmes de recherche font l'objet de très nombreuses investigations scientifiques. Les moteurs de recherche les plus simples se contentent de requêtes booléennes pour comparer les mots d'une requête avec ceux des documents. Les moteurs plus évoluées utilisent la formule TF-IDF pour mettre en perspective le poids des mots dans une requête avec ceux contenus dans les documents. Pour améliorer encore les performances d'un moteur, il existe de nombreuses techniques, la plus connue étant celle du PageRank de Google qui utilise un indice de notoriété de pages. Les recherches les plus récentes utilisent la méthode dîtes d'analyse sémantique latente qui tente d'introduire l'idée de co-occurrences dans la recherche de résultats (le terme "voiture" est automatiquement associé à ses mots proches tels que "garage" ou un nom de marque dans le critère de recherche) Elle permet d'établir des relations entre un ensemble de documents et les termes qu'ils contiennent, en construisant des « concepts » liés aux documents et aux termes.

On trouve également des métamoteurs, c'est-à-dire des sites web où une même recherche est lancée simultanément sur plusieurs moteurs de recherche (les résultats étant ensuite fusionnés pour être présentés à l'internaute).

**MOV -** Mode de compression d'un fichier vidéo compresse par Adobe et qui est utilisé pour Quicktime. Il est très utilisé notamment pour les bandes annonce de films sur internet ou les CD de magazine. C'est une compression de fichier vidéo qui ne permet qu'une faible définition vidéo mais qui est en contre partie évolutive: il y a par exemple le mode Quicktime VR qui est un mode vidéo 3d virtuelle.

**MP3 -** MPEG 1 Audio Layer 3 - Le MP3 est un format de compression numérique du son, sans perte de qualité perceptible à l'oreille. Extension du MPEG audio. Format de compression de fichiers audio qui permet de supprimer toutes les informations superflues, non perçues par l'oreille humaine et de regrouper les répétitions de sons.

**MPEG -** Motion Pictures Experts Group - Norme de compression d'animation Par rapport à la compression M-JPEG, elle offre une réduction de 75-80% des données avec la même qualité visuelle.

**MPEG 1 -** Motion Pictures Experts Group 1 - Standard de compression des vidéos avec leurs informations sonores, sur le principe que l'arrière-plan reste statique dans une succession d'images (pour gagner en stockage et rapidité).

Le MPEG-1 est utilisé pour une bande passante de 1 à 1,5 Mbps, offrant une qualité VHS pour une résolution 352x288 et 30 images/secondes. MPEG-1 nécessite beaucoup de puissance CPU pour de l'encodage temps réel. C'est pourquoi il est bien souvent nécessaire d'avoir un équipement hardware dédié à l'encodage. De plus, MPEG-1 n'offre pas de résolution dimensionnable et la qualité de la vidéo est fortement dépendante de la perte de paquets, liée au principe d'encodage des transitions et des images par prédiction.

**MPEG 2 -** Evolution du format Mpeg 1, incluant un support pour des résolutions plus élevées et en augmentant les capacités audio, il offre une qualité d'image supérieure à celle des cassettes VHS. Pour être visualisée, une séquence de ce format doit être décodée par un outil spécifique (logiciel ou matériel), c'est pourquoi les lecteurs de DVD sont vendus avec une carte de décompression. de MPEG1. Le débit visé par MPEG-2 est de 4 à 15

Mbps, offrant une vidéo plein écran de qualité. Il nécessite aussi du matériel plus coûteux pour l'encodage et le décodage temps réel. Il a les même problèmes que MPEG-1 en ce qui concerne les pertes de paquets.

**MPEG 4 -** Evolution du format Mpeg II, il offre une qualité d'image supérieure à celui-ci à taille équivalente. Pour être visualisée, une séquence de ce format doit être décodée par un outil spécifique (logiciel ou matériel), c'est pourquoi les lecteurs de salon sont vendus avec une carte de décompression. Le MPEG 4 est a la vidéo ce qu'est le MP3 à l'audio.

**MPLS -** MultiProtocole Label Switching - Protocole qui améliore le trafic dans les infrastructures des opérateurs. Il intervient également dans les procédés d'optimisation de bande passante, et est capable de mieux rééquilibrer les flux de d'informations. Il offre la possibilité de bâtir des réseaux privés Virtuels (VPN).

Le protocole MPLS consiste à marquer les trames (Label = réseau privé et Classe de Service). MPLS est utilisé au dessus d'un réseau niveau 2 ou d'un réseau ATM. Sur un réseau stabilisé, les équipements internes commutent les trames en examinant le label comme un swich.

MPLS ne fournit pas d'encryption des paquets, en ce sens il n'est pas plus sur qu'un réseau X.25 ou Frame Relais, mais on peut chiffrer les trames en utilisant IPSEC. MPLS permet d'assurer la qualité de service de bout en bout au travers d'un backbone IP.

MPLS est normalisé par l'IETF (Internet Engineering Task Force). Il assure les fonctions suivantes :

- Il spécifie les mécanismes pour administrer les flux de trafic des plusieurs types, comme les flux entre des matériels différents, des machines différentes ou même entre des applications différentes,
- Il est indépendant des protocoles des couches 2 et 3,
- Il interagit avec des protocoles de routage existant, comme RSVP et OSPF,
- Il supporte les couches de niveau 2 des réseaux IP, ATM, et Frame Relay.

Dans MPLS, la transmission de données se fait sur des Label-Switched Paths (LSP - Chemin à commutation de label). Les LSP sont une séquence de labels (ou étiquettes) à chaque nœud du chemin allant de la source à la destination. Les LSP sont établis en fonction du type de transmission des données (control-driven) ou après détection d'un certain type de données (data-driven). Les labels, qui sont des identifiants spécifiques au protocole des couches basses, sont distribués suivant le protocole LDP (Label Distribution Protocol), RSVP ou parfois par les protocoles de routage comme BGP (Border Gateway Protocol) ou OSPF. Chaque paquet de données encapsule et transporte les labels pendant leur acheminement. La commutation haut débit est possible puisque les labels de longueur fixe sont insérés au tout début du paquet ou de la cellule et peuvent être utilisés par le hardware pour commuter plus rapidement les paquets.

LSR et LER :

Les éléments qui participent aux mécanismes du protocole MPLS peuvent être séparés en Label Edge Routers (LER, Routeur d'extrémité supportant les labels) et Label Switching Routers (LSR, routeur de commutation des labels).

- Un LSR est un routeur haut débit au cœur d'un réseau MPLS qui participe à l'établissement des LSP.
- Un LER est un élément à l'extrémité du réseau d'accès ou du réseau MPLS. Les LER peuvent supporter plusieurs ports connectés à des réseaux différents (ATM, Frame Relay ou Ethernet) et qui fait suivre le trafic sur le réseau MPLS après établissement des LSP. Le LER joue un rôle fondamental dans l'assignation et la suppression des labels, au fur et à mesure que le trafic entre et sort du réseau MPLS.

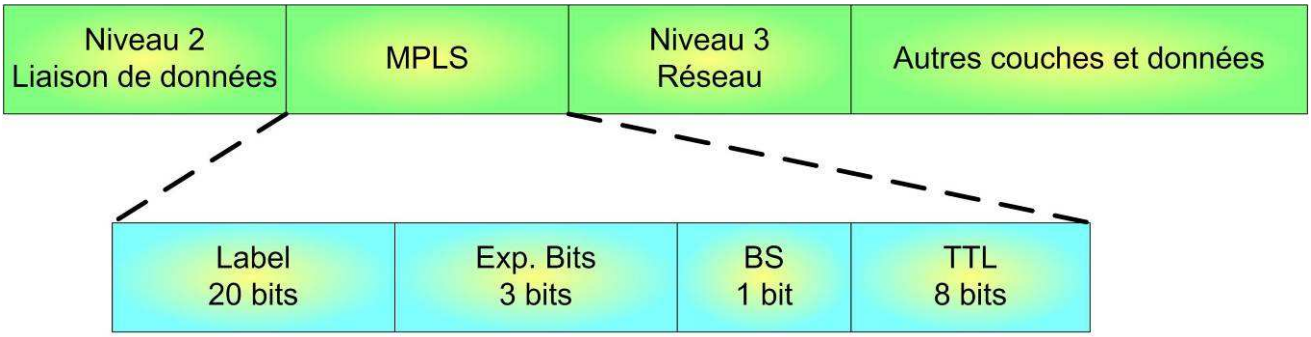
FEC :

La Forward Equivalence Class (FEC) est la représentation d'un groupe de paquets qui ont en commun les mêmes besoins quant à leur transport. Tous les paquets d'un tel groupe reçoivent le même traitement au cours de leur acheminement. Contrairement aux transmissions IP classiques, dans MPLS, un paquet est assigné à une FEC une seule fois, lors de son entrée sur le réseau. Les FEC sont basés sur les besoins en terme de service pour certains groupes de paquets, ou même un certain préfixe d'adresses. Chaque LSR se construit une table pour savoir comment un paquet doit être transmis. Cette table est appelée Label Information Base (LIB, Base d'information sur les labels).

Labels et association de labels :

Un label, dans sa forme la plus simple, identifie le chemin que le paquet doit suivre. Un label est transporté ou encapsulé dans l'en-tête de niveau 2 du paquet. Le routeur qui le reçoit examine le paquet pour déterminer le saut suivant selon son label. Une fois qu'un paquet est labellisé, le reste de son voyage est basé sur la commutation de labels. Les valeurs du label ont simplement une signification locale. Ces valeurs peuvent d'ailleurs directement déterminer un chemin virtuel (DLCI en Frame Relay ou VCI et VPI en ATM).

Les labels sont associés à un FEC suivant une logique ou une politique déterminant cette association. Cette décision peut se faire sur les critères suivants : Routage unicast vers la destination, gestion du trafic, multicast, Virtual Private Network (VPN) ou QoS.




Format de base des labels MPLS

Le format générique d'un label est illustré par la figure. Le label peut aussi se situer dans l'entête de la couche 2, ou entre les couches 2 et 3.

Label-Switched Paths (LSP) :

Un ensemble d'éléments compatibles avec MPLS représente un domaine MPLS. Au sein d'un domaine MPLS, un chemin est défini pour un paquet donné à partir d'une FEC. MPLS propose les deux solutions suivantes pour

implémenter un LSP :

- Routage saut-par-saut : chaque LSP choisit indépendamment le saut suivant pour un FEC donné. Cette méthodologie est similaire à celle utilisé dans les réseaux IP courants. Le LSR utilise les protocoles de routage disponibles, comme OSPF, PNNI (ATM Private Network-to-Network Interface), etc…
- Routage explicite : similaire au source routing. Le premier LSR détermine la liste des nœuds à suivre. Le chemin spécifié peut être non-optimal. Le long de ce chemin, les ressources peuvent être réservées pour assurer la Qos voulue au trafic.

Un LSP est unidirectionnel et le trafic de retour doit donc prendre un autre LSP.

Label Distribution Protocol (LDP) :

LDP est un nouveau protocole permettant d'apporter aux LSR les informations d'association des labels dans un réseau MPLS. Il est utilisé pour associer les labels aux FEC, ce qui crée des LSP. Les sessions LDP sont établies entre deux éléments du réseau MPLS, qui ne sont pas nécessairement adjacents.

Ces éléments échanges les types suivants de messages LDP :

- Messages de découverte : annoncent et maintiennent la présence d'un LSR dans le réseau.
- Messages de session : Etablissent, maintiennent et terminent les sessions LDP.
- Messages d'avertissement : Créent, changent et effacent des associations entre FEC et labels
- Messages de notification : Permettent d'apporter d'autres informations comme signaler une erreur.

**MPLS edge node -** Nœud de Bordure - Equipement constitutif d'un réseau MPLS qui connecte un domaine MPLS avec un nœud se trouvant hors du domaine, soit parce qu'il ne supporte mas le MPLS, soit parce qu'il appartient à un autre domaine.

**MPLS egress node -** Nœud de Bordure - Equipement constitutif d'un réseau qui se charge de manipuler le trafic qui sort du domaine MPLS.

**MPLS ingress node -** nœud de bordure - Equipement constitutif d'un réseau qui se charge de manipuler le trafic qui rentre dans le domaine MPLS.

**MPOA -** Standard de l'ATM Forum (approuvé en juillet 1997). Il permet à une entreprise ou à un campus universitaire de bénéficier des avantages de l'ATM (vitesse de commutation et garantie de qualité de service) sans nécessiter de modification aux applications existantes. Ceci est un point de première importance car ces applications ont souvent été l'objet d'investissements lourds et se révèlent toujours indispensables aujourd'hui.

D'autre part, MPOA permet de s'affranchir du goulot d'étranglement que constitue de plus en plus souvent le routeur qui permet de passer d'un réseau local à un autre. En effet, les deux fonctions antinomiques d'un routeur classique que sont le calcul de la meilleure route à suivre et la commutation des paquets IP sont, dans une architecture MPOA, séparées l'une de l'autre et effectuées dans deux équipements différents et spécialisés: le serveur de routes et le "edge device" ou équipement de périphérie, ce qui leur permet à chacun d'être beaucoup plus efficace. Un système MPOA peut ainsi servir plusieurs milliers de PC ou stations de travail raccordées en leur offrant des performances très supérieures à celles d'un routeur classique.

Le serveur de routes effectue le travail du calcul de la meilleure route à suivre en appliquant un protocole de routage tel que RIP ou OSPF. Il est interrogé peu souvent et à bon escient par les équipements de périphérie.

Les équipements de périphérie effectuent une commutation Ethernet rapide, fondée sur un processus hardware, de la même façon que les commutateurs du réseau de campus effectuent leur commutation ATM. Ils conservent en mémoire cache les correspondances entre adresses ATM et adresses IP qu'ils ont demandées au serveur de route et sont ainsi capables d'établir des circuits ATM directs appelés "short cuts" ou "raccourcis" au travers du réseau ATM de campus, ce qui donne d'excellentes performances au système.

Enfin, MPOA permet d'établir des réseaux locaux virtuels ou VLANs qui permettent de regrouper les utilisateurs selon la structure logique de leur entreprise ou de leur université et non plus selon leur position géographique dans les différents bâtiments et étages comme c'est le cas dans un système à routeurs classiques. Les restructurations, si fréquentes aujourd'hui, sont ainsi grandement simplifiées et la flexibilité de la structure des réseaux permet de suivre parfaitement celle de l'organisation humaine.

**MRC -** Milestone Review Committee - Groupe consultatif établi conjointement par l'ECTRA et l'ERC au sein de la CEPT pour s'assurer que les différents systèmes réglementaires remplissent les conditions requises.

**MRFC -** Media Resource Function Controler - Passerelle qui détecte et oriente les différents en function de le source, de leur distination, de leur priorité, de leur type, de leur urgence… Voir IMS

**MRT -** Multiplexage à Répartition dans le Temps. Voir Multiplexage temporel.

**MSC -** Mobile Switching Center ou Main Switch Center - Centre de commutation des systèmes mobiles. C'est la partie commutation des infrastructures des mobiles.

Un MSC gère l'établissement des communications, la transmission des messages courts et l'exécution du handover. Le MSC est en communication avec le VLR pour gérer la mobilité des usagers.

Le GMSC est une fonction passerelle d'un MSC. Cela permet la communication entre un poste fixe et un mobile. Cette fonction est un détournement de l'usage du MSC mais elle permet de limiter l'impact sur le RTC. Il existe aussi une passerelle pour les messages courts.

**MS-CHAP -** Microsoft Challenge Handshake Authentication Protocol version 1 - MS-CHAP-v1- Protocole d'authentification développé par Microsoft s'inspirant de CHAP et améliorant globalement la sécurité. Le protocole CHAP implique que l'ensemble des mots de passe des utilisateurs soient stockés en clair sur le serveur, ce qui constitue une vulnérabilité potentielle. MS-CHAP propose une fonction de hachage propriétaire permettant de stocker un hash intermédiaire du mot de passe sur le serveur. Lorsque la machine distante répond au défi, elle doit ainsi préalablement hacher le mot de passe à l'aide de l'algorithme propriétaire. Ce protocole souffre de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire.

**MS-CHAP v2** - Microsoft Challenge Handshake Authentication Protocol version 2 - La version 2 a été définie en Janvier 2000 dans la RFC 2759. Cette nouvelle version définit une méthode dite"d'authentification mutuelle ", permettant au serveur d'authentification et à la machine distante de vérifier leurs identités respectives.

Le processus d'authentification mutuelle de MS-CHAP v2 fonctionne de la manière suivante :

- Le serveur d'authentification envoie à l'utilisateur distant une demande de vérification composée d'un identifiant de session ainsi que d'une chaîne aléatoire.
- Le client distant répond avec :
  - o son nom d'utilisateur,
  - o un haché contenant la chaîne arbitraire fournie par le serveur d'authentification, l'identifiant de session ainsi que son mot de passe,
  - o une chaîne aléatoire.
- Le serveur d'authentification vérifie la réponse de l'utilisateur distant et renvoie &agave; son tour les éléments suivants :
  - o la notification de succès ou d'échec de l'authentification
  - o une réponse chiffrée sur la base de la chaîne aléatoire fournie par le client distant, la réponse chiffrée fournie et le mot de passe de l'utilisateur distant.
- Le client distant vérifie enfin à son tour la réponse et, en cas de réussite, établit la connexion.

**MSDP -** Multicast Source Discovery Protocol - Internet Draft msdp-06.txt - MSDP permet d'échanger la connaissance des sources entre plusieurs RP, en établissant des "peerings" MSDP. Voir Multicast

**MSISDN -** Mobile station ISDN number - Numéro de téléphone international d'un abonné mobile, c'est-à-dire son numéro de téléphone courant.

**MTA -** Message Transfer Agent - Dans la norme de messagerie électronique X400, désigne l'entité (logiciel) qui assure l'acheminement des messages en provenance de et vers les "agents utilisateurs".

**MTBF -** Mean Time Between Failure - Temps Moyen Entre Panne - Valeur, souvent exprimée en heures, qui détermine, pour un équipement, le temps moyen estimé entre 2 pannes. Cette valeur théorique est déterminée par le constructeur en fonction de la qualité des composants choisis et des règles d'assemblage. Il est à noter que le MTBF d'un équipement est donné à titre indicatif, pour un fonctionnement sans surcharge, dans un environnement sain, protégé, et à une température de fonctionnement optimale.

**MTS -** Message Transfer System - Dans la norme X400, désigne l'ensemble des MTA appartenant à un même domaine.

**MTU de chemin (path MTU) -** Le plus petit MTU de liaison de toutes les liaisons que compose un chemin entre un nœud source et un nœud de destination.

**MTU de liaison (link MTU) -** L'unité de transmission maximale (Maximum Transmission Unit - MTU), c'est à dire la taille maximale du paquet en octets, qui peut être acheminé en un seul "morceau" sur une liaison (un paquet étant composé d'un en-tête et de son "payload").

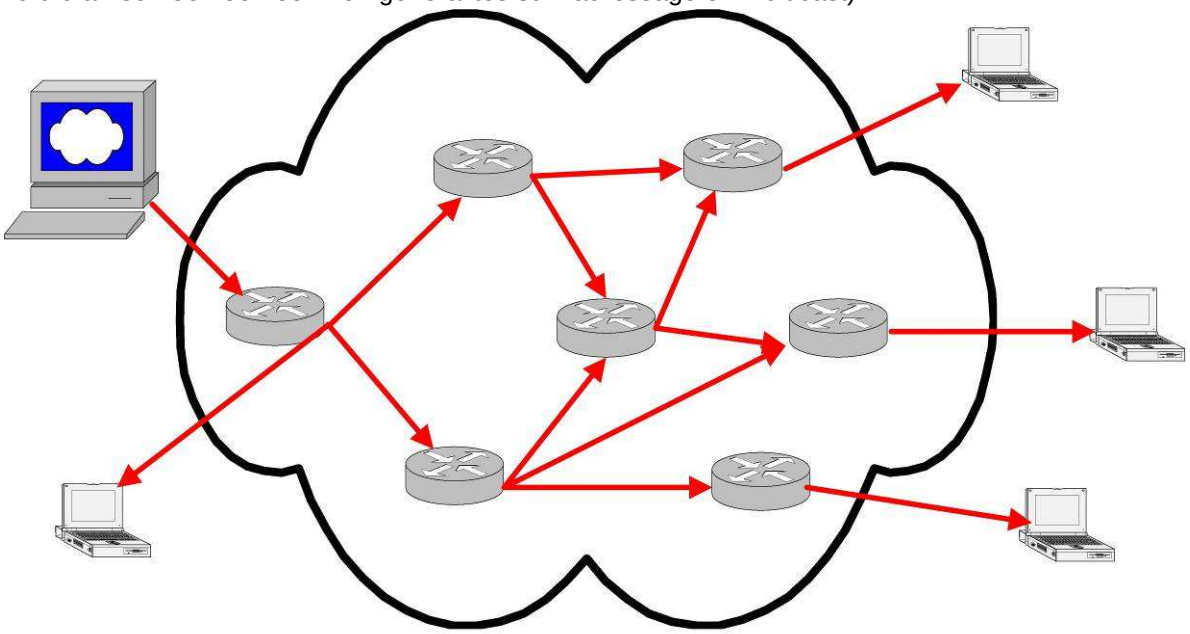
**Multicast** - Le Multicast est un mode de fonctionnement particulier de l'Internet, en mode diffusion. Il optimise les flux à travers le réseau lorsque plusieurs utilisateurs doivent partager, en temps réel, des données qui circulent dans le réseau. C'est le cas, par exemple, pour l'image et la voix d'une session de visioconférence : tous les participants doivent les recevoir simultanément.

En Multicast (ou diffusion), le réseau fonctionne de point à multipoint. Le poste émetteur envoie des paquets avec une adresse de destination Multicast qui est en fait un identifieur de session Multicast, ou groupe Multicast (l'équivalent d'un numéro de canal en diffusion télévision hertzienne). Au niveau de ses routeurs IP, le réseau réplique les paquets de telle sorte que tous les postes récepteurs abonnés à cet instant à ce groupe Multicast, et uniquement eux, en reçoivent chacun une copie (chaque paquet sera répliqué le plus tard possible en fonction de la topologie du réseau) : vu sous cet angle, le Multicast IP est bien plus évolué qu'une diffusion de télévision (câble, hertzien ou satellite), qui "inonde" tout le monde sans distinction.

Il s'agit en fait d'applications entre une source et plusieurs destinataires, à la différence suivante : En multipoint "classique", le nombre de connexions est égal au nombre de récepteurs, en Multicast le nombre de connexions est inférieur au nombre de récepteurs.

Cela peut sembler une banalité, mais il est à noter que la réception de paquets Multicast par une station du réseau est conditionnée par sa capacité à écouter. Par défaut, le coupleur réseau d'une station écoute (en réception) son adresse Ethernet (fixée en PROM) et l'adresse de Broadcast (FF…FF). Pour le Multicast, il lui

faut aussi écouter au minimum l'équivalent Ethernet de 224.0.0.1 (tous les hôtes Multicast du LAN) et la classe D (224.0.0.0 à 239.255.255.255 - voir généralités sur l'adressage en multicast).

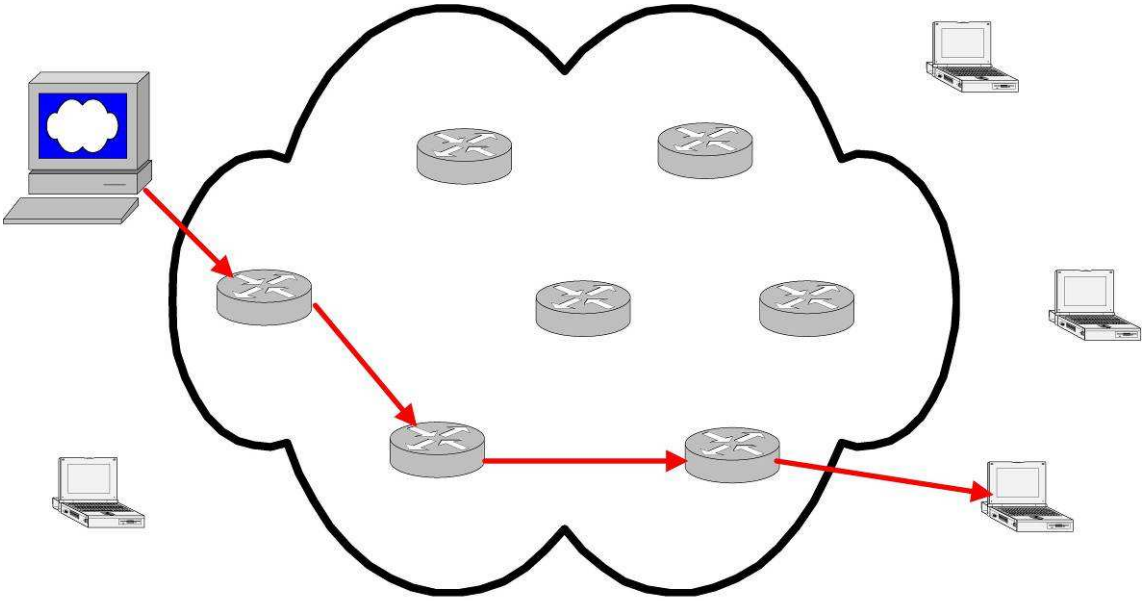


Multicast

En terme de bande passante, l'envoi en unicast vers tous les clients devant recevoir l'émission multimédia n'est pas ce qu'il y a de mieux. Le Multicast offre une meilleure solution, surtout si tous les clients sont localisés hors du sous-réseau qui est à l'origine de l'émission. Le Multicast permet d'économiser la bande passante, les ressources des routeurs, les ressources de la source,…

Par opposition, l'utilisation la plus commune de IP est dite unicast. Elle fonctionne en point à point : le poste émetteur envoie des paquets IP dont chacun porte une adresse de destination explicite. Le réseau transporte le paquet vers ce destinataire, et uniquement vers lui.

Le choix des identifieurs de groupe Multicast est généralement automatique au niveau des applications lorsqu'elles démarrent une nouvelle session. La mise en place d'une nouvelle session, ainsi que le raccordement d'un nouvel abonné à une session préexistante, sont fait automatiquement par le réseau en quelques secondes. Il n'y a pas de limite (autre que la capacité du réseau) au nombre de sessions simultanées. Dans chaque session, chaque abonné peut à son tour devenir émetteur, et tous les autres abonnés de la même session reçoivent alors les données qu'il émet.



Unicast

Détails sur le Multicast IP :

Généralités sur l'adressage :

L'espace des adresses IP est distribué en trois groupes de classes d'adresses. Les classes d'adresses A, B et C. Il en existe une quatrième (Classe D) réservée pour les adresses Multicast. Les adresses IPv4 entre 224.0.0.0 et 239.255.255.255 appartiennent à cette classe.

Adressage de groupe :

- Unicast :

Classes A, B, C

Classe A : 127 réseaux, 16 millions hôtes/réseau

Classe B : 16384 réseaux, 65534 hôtes/réseau

Classe C : 2 millions de réseaux, 254 hôtes/réseau

- Multicast :

Une adresse IPmc de la couche 3 correspond à une seule adresse fonctionnelle où à l'adresse de diffusion)

Classe D : Adresses Multicast : Ce type d'adresse permet d'appeler un groupe spécifique d'hôtes (interfaces) dans un sous réseau. Une adresse Multicast ne peut être que destinataire. Les sources (émetteurs) sont connues par leur adresse Unicast. Etre membre d'un groupe est indépendant d'envoyer à ce groupe (une source n'est pas obligatoirement membre du groupe Multicast auquel elle envoie des données).

Adresse commençant par les 4 bits 1110 - Les 4 bits les plus significatifs de l'adresse IP autorisent des valeurs comprises entre 224 et 239. Les autres 28 bits, moins significatifs, sont réservés à l'identificateur du groupe Multicast.

Plage d'adresses de 224.0.0.0 à 239.255.255.255 28 bits d'adresses utiles soit 250 millions d'adresses disponibles

Au niveau du réseau, les adresses Multicast IPv4 doivent être "mappées" sur des adresses physiques du type de réseau utilisé. Dans le cas d'une session unicast, l'obtention des adresses physiques associées est réalisée en utilisant le protocole ARP. Dans le cas des adresses Multicast, ARP ne peut pas être utilisé et les adresses physiques doivent être obtenues d'une autre manière. Une RFC décrit la correspondance des adresses Multicast IPv4 (RFC 1112 - Host Extension for IP Multicasting).

Dans les réseaux Ethernet et FDDI les plus étendus, le "mappage" est effectué en fixant les 24 bits les plus significatifs de l'adresse Ethernet à 01: 00 : 5E. Le bit suivant est fixé à 0 et les 23 bits les moins significatifs utilisent les 23 bits les moins significatifs de l'adresse Multicast IPv4. En Token-Ring, c'est l'adresse de diffusion qui sera utilisé (ff.ff.ff.ff.ff.ff). Par exemple, l'adresse Multicast IPv4 224.0.0.5 correspondra à l'adresse physique Ethernet 01:00:5E:00:00:05.

Il existe quelques adresses Multicast IPv4 particulières :

L'adresse 224.0.0.1 identifie tous les hôtes Multicast d'un LAN (un groupe). Tous les hôtes ayant des capacités Multicast dans un sous réseau doivent faire partie de ce groupe.

L'adresse 224.0.0.2 identifie tout routeur Multicast dans un réseau (LAN).

L'adresse 224.0.0.4 identifie tous les routeurs DVMRP d'un réseau (LAN).

L'adresse 224.0.0.9 identifie tous les routeurs RIPv2 d'un réseau (LAN).

L'adresse 224.0.0.13 identifie tous les routeurs PIM d'un réseau (LAN).

Le champ d'adresse 224.0.0.0 - 224.0.0.255 est alloué pour les protocoles bas niveau. Les datagrammes envoyés dans cette plage d'adresse ne seront pas routés par des routeurs Multicast.

La plage d'adresse 232.0.0.0 - 232.255.255.255 est réservée pour PIMSSM utilisant IGMPv3

La plage d'adresse 233.0.0.0 - 233.255.255.255 est réservée pour GLOP (allocation dynamique d'adresses de groupe).

La plage d'adresse 239.0.0.0 - 239.255.255.255 est allouée à des fins administratives. Les adresses sont allouées localement pour chaque organisation mais elles ne peuvent exister à l'extérieur de celle-ci. Les routeurs de l'organisation ne doivent pas pouvoir router ces adresses à l'extérieur du réseau de l'entreprise.

Portée des adresses Multicast :

- Global scope : 224.0.1.0 - 238.255.255.255
- Limited scope : 239.0.0.0 - 239.255.255.255
- Site-local scope : 239.253.0.0 /16
- Organisation local scope : 239.192.0.0 /14

Avec le Multicast IPv4, le TTL a une double signification. Il contrôle la durée de vie d'un datagramme dans le réseau pour éviter toute boucle infinie dans le cas de tables de routage mal configurées. En travaillant avec le Multicast, la valeur TTL définit aussi le champ d'activité du datagramme, par exemple, jusqu'où il circulera au sein du réseau. Ceci permet une définition de champ d'activité basée sur la catégorie du datagramme.

Il existe plusieurs systèmes d'allocation d'adresse de groupe :

- Dynamique
  - Session Annoucement Protocol, (SAP), ID,
  - MADCAP, RFC 2730 (Multicast Address Dynamic Client Allocation Protocol).
- Manuelle
  - GLOP, RFC 2770

- RFC 2365 (Administratively Scoped IP Multicast)

Enfin, il est aussi possible d'adresser un réseau Multicast en utilisant des tunnels pour définir une structure logique faisant abstraction de la topologie sous-jacente du réseau (on encapsule les paquets Multicast dans des paquets Unicast). Voir RFC 1075.

Protocoles Multicast :

Les protocoles Stations - Routeurs

Adresses Multicast de la couche MAC (liaison)

Adresses IP de groupe comprises entre 224.0.0.0 et 239.255.255.255

Adresses de classe D (bits de poids forts à 1110)

Inconvénient de l'adressage Multicast au niveau MAC : Les systèmes non destinataires recevront quand même les messages. Des algorithmes spécifiques permettent de limiter les impacts sur les commutateurs et routeurs centraux, notamment certaines fonctions propriétaires liées au Multicast).

Pour limiter la diffusion la diffusion Multicast au niveau 2, il existe les solutions suivantes (liste non exhaustive) :

- 802.1 GMRP (Garp Multicast Registration Protocol) - Standard du comité IEEE 802.1, il requiert le changement de la longueur maximale de la trame Ethernet IEEE 802.3 (1518 octets étendus à 1522 octets). Les ordinateurs et les commutateurs doivent être mis à jour pour GMRP, IGMP est toujours requis sur l'ordinateur.
- IGMP Snooping - Ce mécanisme donne au commutateur une capacité de niveau 3, il examine chaque paquet pour savoir si c'est un message IGMP (rejoindre ou quitter), découvre dynamiquement les routeurs et les sources Multicast, inter opère avec les commutateurs utilisant CGMP. IGMP Snooping peut être traité par le hardware de certains commutateurs (moindre altération des performances).
- CGMP (Cisco Group Management Protocol) - Utilise les adresses Multicast de la couche standard MAC pour limiter le trafic Multicast, transparent pour les ordinateurs, CGMP programme dynamiquement les commutateurs en fonction des messages IGMP, il économise les ressources (bande passante du réseau, charge CPU) et offre les performances de la commutation de niveau 2. CGMP est destiné aux communications inter équipements du LAN, RGMP est destiné aux routeurs connectés à un commutateur.
- IGMP v1 (Internet Group Management Protocol v1 - RFC 1112). Adresse de groupe abstraite : pas de notion de machine ni de réseau. Le groupe est dynamique : de 0 à une quasi-infinité de membres. Les membres d'un groupe sont indépendants d'une localisation physique. Un membre doit envoyer un rapport à l'adresse 224.1.1.1 pour rejoindre le groupe. Le routeur envoie périodiquement des requêtes générales à l'adresse 224.0.0.1 pour déterminer l'appartenance aux groupes. Pour maintenir le groupe, un membre (par groupe et par sous réseau) rapporte au routeur, les autres membres annulent leur rapport. Les ordinateurs quittent le groupe sans en référer au routeur. Si pas de réponse aux requêtes périodiques du routeur, le groupe disparaît sur temporisation.
- IGMP v2 (Internet Group Management Protocol v2 - RFC 2236). Compatibilité descendante avec IGMP v1 + Requête spécifique à un groupe - Le routeur vérifie que le dernier récepteur intéressé a quitté un groupe avant de cesser l'envoi de ses données sur un sous réseau. Message pour quitter explicitement un groupe - Un ordinateur envoie un message de résiliation s'il quitte le groupe et s'il est le dernier membre (réduit le temps de latence de disparition d'un groupe par rapport au IGMP v1). Mécanisme d'élection du routeur requérant - Sur les réseaux multi accès, un routeur requérant IGMP est élu sur la base de la plus petite adresse IP. Seul le routeur requérant envoie des requêtes générales. Requêtes Générales - Intervalle de temps de réponse - Les requêtes générales spécifient le temps de réponse maximum imparti aux ordinateurs pour répondre (amélioration de la réactivité des ordinateurs).
- IGMP v3 & 4 (Internet Group Management Protocol v3 & 4 - en cours d'élaboration). Autoriseront l'écoute d'un sous-ensemble de participants au groupe Multicast.

Les protocoles Routeurs - Routeurs :

Préambule : l'adresse de destination IP dans un datagramme Multicast est l'adresse du groupe Multicast (mais on ne peut pas router d'une source vers une destination virtuelle). Le routage Multicast est à l'envers du routage unicast : le routage unicast détermine où le paquet va (on route en fonction de la destination), le routage Multicast détermine d'où le paquet vient (on route en fonction de la source).

Le rôle du protocole de routage Multicast est de construire et maintenir les arbres de distribution et de fournir un mécanisme pour informer les routeurs des sources actives et des groupes.

Le routage Multicast est basé sur la source, ce qui implique une connaissance des sources dans chaque routeur ou un mécanisme pour fournir cette connaissance sur demande.

Le routage Multicast utilise le "Reverse Path Forwarding" (RPF = diffuser dans le sens inverse de la source) pour construire les arbres de distribution et s'assurer que les paquets arrivent par la bonne interface. Les arbres de distribution Multicast sont de deux types : arbre source (Source -> Groupe = S, G) et arbre distribué (tous -> Groupe = *,G). Un protocole de routage unicast est utilisé pour déterminer ce "chemin inverse" qui est le meilleur chemin unicast du récepteur vers la source.

Les arbres de distribution sont construits de proche en proche, en déterminant le meilleur chemin vers la source

unicast émettant sur un groupe particulier. Dans un arbre de diffusion, la source (l'émetteur) est la racine de l'arbre de diffusion, toutes les branches correspondent aux diverses chemins où sont connectées les membres du groupe Multicast. L'arbre est en constante évolution, chaque branche pouvant être coupé (élaguée), puisque ne sont maintenues que les branches utiles.

Après que le meilleur chemin soit déterminé, les informations sont envoyées vers l'interface RPF, ou l'interface avec la plus courte distance administrative vers la source, ce qui construit l'arbre du récepteur vers la source. Le contrôle RPF consiste à chercher l'adresse source du datagramme Multicast dans la table de routage utilisé pour le Multicast. Si le datagramme est arrivé sur l'interface spécifiée dans la table de routage pour l'adresse source, le contrôle RPF réussit. Un paquet n'est jamais renvoyé vers l'interface RPF.

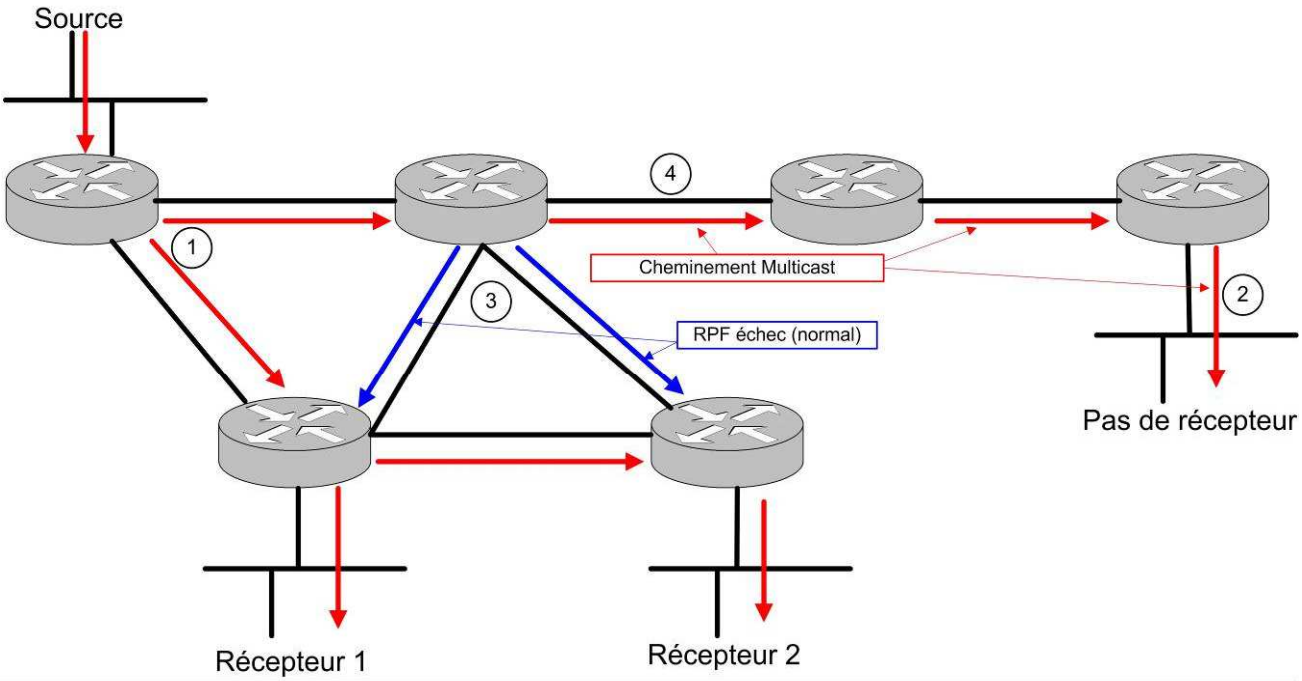
Il existe deux types de protocoles de routage Multicast :

- Dense : On diffuse tant qu'on ne nous demande pas d'arrêter. Un état est crée en permanence pour chaque source sur tous les routeurs. Le mode Dense offre le support pour les arbres dont la racine est la source (ou arbre du court chemin).
- Sparse : (clairsemé) : On diffuse quand on le demande explicitement. Le mode Sparse offre le support pour les arbres partagés et les arbres sources.

Les caractéristiques nécessaires d'un protocole de routage Multicast sont d'être indépendant du routage unicast, supporter une distribution dense de participants, être extensible au routage Multicast inter domaine, et enfin être largement déployé (maturité) et correctement définit (RFC).

Les Protocoles en mode Dense :

- DVMRP (Distance Vector Multicast Routing Protocol v1, v2 & v3) - RFC 1075. Echange des informations de routage entre routeurs voisins (inspiré de RIP). Dépendant d'un protocole de routage Unicast, il requiert son propre protocole de routage unicast intégré (similaire à RIP). DVMRP construit un arbre de distribution séparé pour chaque source / Groupe. Il utilise le Reverse Path Forwarding pour propager et élaguer (propagation = diffuser les paquets sur toutes les interfaces de sortie de l'arbre de diffusion, en supposant au départ que chaque branche mène à des membres du groupe) (élaguer = Eliminer les branches de l'arbre sans membre du groupe multicast, coupant la transmission sur les LANs sans récepteur intéressé, élague aussi les chemins redondants non optimaux de chaque récepteur vers la source). Tous les routeurs ont la même vue de la topologie Multicast. Il est possible de paramétrer certains paramètres en DVMRP : Le nombre de sauts (hops), les métriques et les seuils (threshold). Le seuil indique si un datagramme Multicast peut être réémis. Il y a échange des tables de routage entre routeurs DVMRP : Destination : ce sont les adresses Unicast des sources (émetteurs des datagrammes Multicast), masque : c'est le masque associé de la destination, métrique : c'est le nombre de routeurs Multicast à franchir pour atteindre la source (distance). DVMRP est plus efficace pour les distributions denses de récepteurs Multicast, a été largement utilisé sur le MBONE (réseau Multicast Européen // Internet), mais induit des facteurs significatifs de facteur d'échelle (convergence lente comme RIP dont il s'inspire), beaucoup d'informations d'état sur le routage Multicast maintenues sur les routeurs, partout (Sources, Groupe), ne supporte pas les arbres partagés, n'est pas adapté sur des architectures avec un nombre de saut supérieur à 32. DVMRP est inapproprié pour les grands réseaux avec peu de récepteurs intéressés due au mécanisme propager et élaguer et/ou dans le cas de groupes faiblement représentés sur un WAN.
- PIM Mode Dense (Protocol Independent Multicast) - Ce protocole n'a jamais été standardisé par l'IETF. Protocole développé par CISCO, mode dense (DM) - Indépendant de tout protocole, il supporte tous les protocoles de routage Unicast : Statique, RIP, IGRP, EIGRP, IS-IS, BGP et OSPF. PIM utilise le Reverse Path Forwarding pour la propagation dans le réseau et l'élagage basé sur l'information d'appartenance à un groupe. C'est un protocole de routage Multicast plutôt approprié aux petites implémentations et aux réseaux pilotes. Le protocole de routage PIM Dense Mode est plus efficace pour les distributions denses de récepteurs Multicast, facile à configurer (2 commandes), il utilise un mécanisme simple de propagation et d'élagage, ce qui induit une certaine facilité à le comprendre et à le debugger. Ce protocole génère un faible overhead pour les groupes denses. Problèmes potentiels : Propagation et élagage sur le WAN, pas de support pour les arbres partagés.

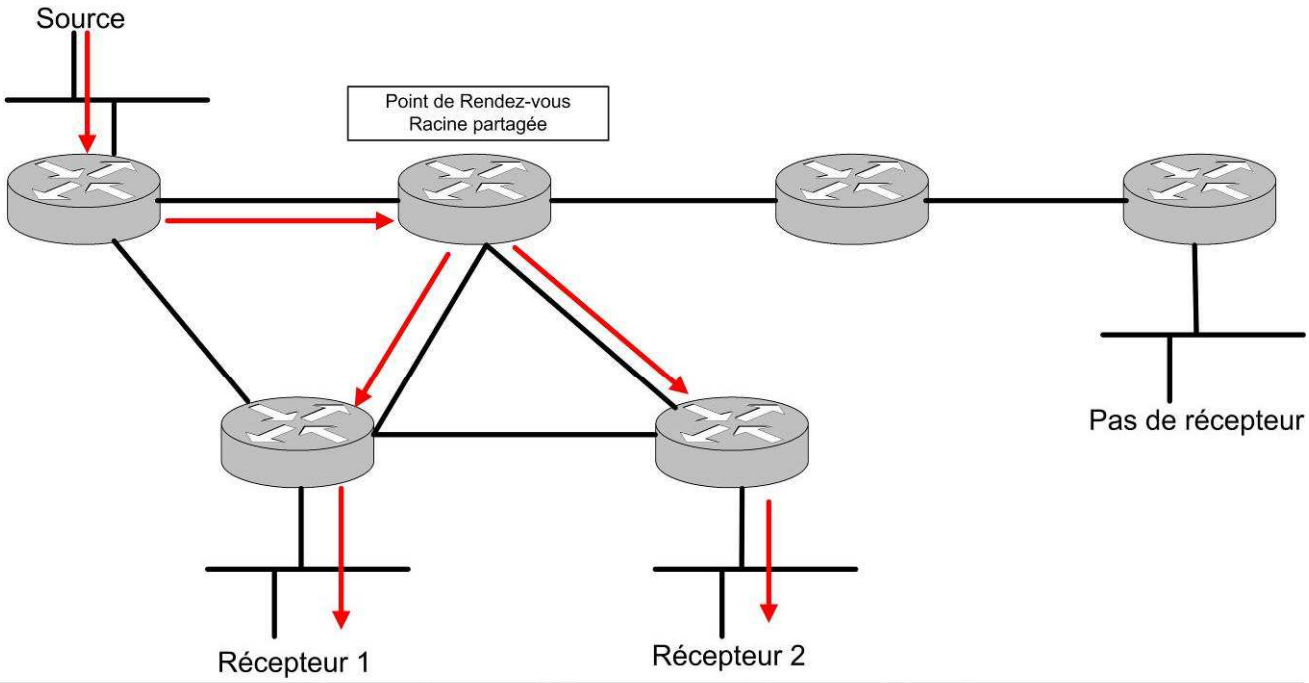



**Mode Dense - Arbre du chemin le plus court - La méthode « Propager et Elaguer » :**
1 - Propager partout au départ / 2 - Elaguer quand il n'y a pas de membre du groupe / 3 - Elaguer les chemins redondants / 4 - Reprise des propagations périodiquement.

- MOSPF (Multicast extension Open Shortest Path First) - RFC 1584. Extension du protocole de routage OSPF (OSPF = Protocole de routage Unicast - Les routeurs utilisent des annonces d'état de lien (Link Stat Advertisement - LSA) pour connaître toutes les liaisons disponibles du réseau (route et chemin au moindre coût)). MOSPF inclut une information Multicast dans l'annonce de l'état de lien OSPF pour construire les arbres de distribution Multicast. Les LSAs d'appartenance à un groupe sont propagés dans l'ensemble du domaine de routage OSPF, afin que les routeurs MOSPF puissent calculer les listes des interfaces de sortie. MOSPF utilise l'algorithme Dijkstra pour calculer l'arbre du plus court chemin. Un calcul séparé est requit pour chaque couple "source/groupe". MOSPF ne propage pas partout le trafic Multicast pour créer les états, ce protocole utilise les LSAs et la base de données d'états des liens. Par conséquent, ce protocole ne peut fonctionner qu'en présence du protocole de routage OSPF sur un réseau. L'algorithme Dijkstra tourne pour tous les couples multicast (S, G), ce qui génère des problèmes significatifs d'échelle, comme le fait que ce protocole ne supporte pas les arbres partagés. MOSPF est inapproprié pour les grandes interconnexions de réseaux avec beaucoup de sources et de récepteurs.

Les protocoles en mode Sparse (clairsemé) :

Ces protocoles fonctionnent pour les groupes clairsemés ou denses. Ils sont optimisés pour les groupes à faible densité de membres. Basés sur une demande explicite (suppose que personne ne veut les paquets à moins qu'il ne le demande explicitement) les protocoles en mode clairsemé utilisent des arbres de distribution source ou partagés. Les demandes (JOIN) sont propagées du récepteur vers le Point de Rendez-vous (RP) ou vers les sources. Les sources sont connues par une propagation au préalable par l'arbre partagé.




**Mode Sparse - Arbre partagé - Peut commuter sur l'arbre source si nécessaire:**
1 - Personne ne reçoit le trafic d'un groupe sans le demander / 2 - Enregistrement d'appartenance à un groupe auprès du Point de rendez-vous / 3 - Des sites élagués en permanence si nécessaire / 4 - Pas de propagation systématique comme en mode Dense.

- PIM SM (Protocol Independent Multicast Sparse mode). Protocole développé par CISCO, mode clairsemé (RFC 2362 - v2) - Supporte les arbres sources et partagés, utilise un Point de Rendez-vous (RP). Les sources s'enregistrent auprès du RP et envoient les données aux récepteurs connus via ce RP. Le RP est la racine de l'arbre de diffusion Multicast partagé, il est configuré statiquement ou connu dynamiquement par Auto-RP ou "candidate RP" (PIMv2). Sur un même réseau, il peut y avoir plusieurs RP, mais un groupe n'est enregistré qu'auprès d'un seul RP. PIM SM est approprié pour les déploiements à large échelle pour groupe à faible ou forte densité, où il est très efficace. C'est le choix optimal pour les groupes clairsemés avec peu de récepteurs, surtout si les récepteurs sont séparés par des liaisons WAN coûteuses. Le trafic n'est envoyé que sur les branches depuis lesquelles on a reçu une demande (Join), on peut commuter dynamiquement sur les arbres source optimaux pour les sources à fort trafic. Indépendant de tout protocole, il supporte tous les protocoles de routage Unicast : Statique, RIP, IGRP, EIGRP, IS-IS, BGP et OSPF, il offre aussi de bonnes bases pour les protocoles de routage Multicast inter domaine.
- PIM Sparse Dense (Protocol Independent Multicast Sparse Dense) - Non standardisé IETF. Protocole développé par CISCO, mode Clairsemé Dense - PIM utilise le Reverse Path Forwarding pour la propagation dans le réseau et l'élagage basé sur l'information d'appartenance à un groupe, il supporte les arbres sources et partagés, utilise un Point de Rendez-vous (RP). Les sources s'enregistrent auprès du RP et envoient les données aux récepteurs connus via ce RP. PIM Sparse Dense fonctionne en mode Dense pour les groupes Multicast sans Point de rendez-vous actif et en mode Sparse pour les groupes avec Point de Rendez-vous actif. Ce mixte est recommandé pour les déploiements initiaux, à utiliser d'abord sans RP (mode Dense), il suffit ensuite d'ajouter des RPs pour basculer en mode Sparse.
- Mixage PIM <-> DVMRP. En utilisant PIM SDM (Sparse Dense Mode), il est possible d'interconnecter des nuages DVMRP à des domaines PIM. Le routage vers la source (RPF) peut être extrait des tables DVMRP ou PIM, voire des mroutes statiques. Il est plutôt conseillé d'utiliser sur les LANs sans récepteur de groupe des tunnels. La commande ip dvmrp unicast routing permet de forcer l'échange des tables de routage DVMRP.

Recommandations :

Comme avec les protocoles de routages Unicast, un mixage de protocoles en Multicast peut générer des problèmes de routage (boucles, …).

Les règles d'ingénierie et d'architecture doivent être respectées à la lettre. Par exemple ne jamais mettre en œuvre deux protocoles Multicast PIM sur une même interface de routeur, utiliser à cette fin PIM SDM. Toujours chercher à déployer un protocole de routage Multicast unique (PIM SDM détermine automatiquement le mode approprié au groupe Multicast) et auto RP discovery protocol (évite les configurations manuelles et statiques du RP).

Créer des îlots de protocoles homogènes et les étendre progressivement, interconnecter ces îlots par un routeur frontière, et pour des situations complexes en cas d'interconnexion lourde (dans le cas d'un ISP par exemple) utiliser MBGP (description ci-après).

Pour simplifier la gestion, il faut limiter la mise en œuvre de tunnels pour interconnecter les domaines de Multicast.

L'implication de l'équipe technique en charge du réseau à l'initiative du projet Multicast est impérative. Cette équipe doit participer aux différents réglages sur le réseau et les applications (réglages des débits et seuils) et surveiller les équipements.

Les protocoles de routage inter domaine (PIM):

Un domaine Multicast est un (ou un ensemble) de Point de Rendez-vous (RP), ou une frontière vis-à-vis des autres domaines (notamment en PIM).

On utilise le routage inter domaine dans le cas où l'on souhaite administrer ses propres ressources (RP) ou confiner le trafic des sources locales à un seul domaine.

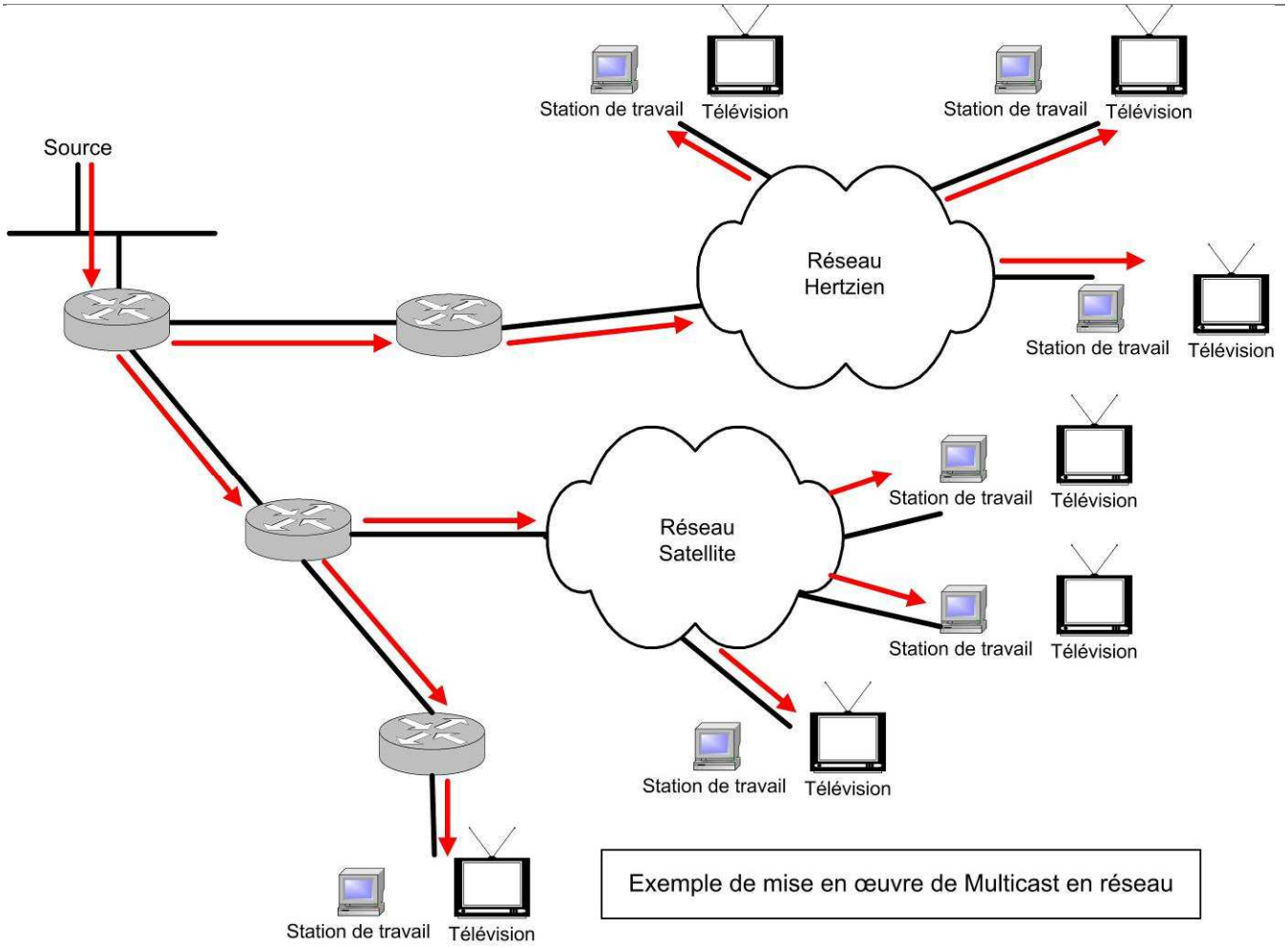
- MBGP (Multicast Border Gateway Protocol ou Multiprotocol extension for BGP4) - RFC 2283. MBGP permet de router les réseaux des sources Multicast au sein d'un domaine PIM (iMBP) ou entre domaines PIM distincts (eMBGP). Il fonctionne en établissant des "peerings" MBGP (comme en BGP4). Il permet de récupérer les routes annoncées par d'autres protocoles Multicast et de les réinjecter vers d'autres protocoles de routage Multicast.
- MSDP (Multicast Source Discovery Protocol) - Internet Draft msdp-06.txt. MSDP permet d'échanger la connaissance des sources entre plusieurs RP, en établissant des "peerings" MSDP.
- Le protocole de routage PIM SSM. Devant la trop grande complexité dans la mise en œuvre des réseaux Multicast, les difficultés de maîtrise de la supervision de ces réseaux, et pour pouvoir mettre en œuvre simplement Internet TV pour tous les usagers, un protocole de routage dénommé PIM SSM (PIM Source Specific Multicast) a été élaboré selon les caractéristiques suivantes :
  - S'appuyer sur IGMPv3 pour sélectionner la source dont on veut récupérer les données,
  - Sur le routage de PIM pour accéder directement à la source,
  - Sans avoir besoin de passer par un RP,
  - Adapté à la diffusion Multicast 1 -> n (mais inadapté à la diffusion m -> n (interactivité)).

Des expériences sont en cours avec des implantations d'IGMP3 (FreeBSD, Cisco) et des applications adaptées à IGMPv3, ainsi que des applications de vidéoconférence pour IPv6.

Exemples d'utilisation du Multicast :

Le Multicast est un excellent support pour :

- Le routage Dynamique en IPv4 (OSPF utilise des adresses Multicast pour diffuser les "hello packet"),
- La visioconférence,
- Le travail collaboratif,
- Le téléenseignement et le télé séminaire,
- Les transferts de données (miroirs, cache,…).
- La découverte de ressources réseau au niveau local…




La visioconférence sur IP se prête fort bien au téléenseignement interactif, et le Multicast IP est à la base de plusieurs réalisations de pointe en France dans ce secteur : cours partagés entre DESS à travers la France, conférences et séminaires virtuels ...

Les services Multicast ou leurs utilisations ont évolués au cours des années. Utilisé à l'origine au sein de groupes fermés, dans des applications très spécifiques telles que le téléenseignement et le routage dynamique, ces services nécessitaient une bande passante importante pour pouvoir fonctionner correctement (les raccordements hauts débit étaient encore très chers il y a 5 ans).

La démocratisation du haut débit, mais aussi les baisses de prix des équipements d'interconnexion (routeurs puissants), cumulées à l'intégration native des fonctionnalités Multicast dans les équipements de commutation permettent de proposer des services Multicast à moindre coût aujourd'hui.

Mbone / TEN-155 / FMbone-2 :

A la fin des années 80 a été installée la première expérimentation Multicast sur le réseau DARTnet. Cette expérimentation deviendra par la suite le réseau Mbone, qui dans sa dernière version offrait le routage Multicast sur plusieurs Points de Présence dans le monde (environ 20 pays, environ 901 routeurs, de 1 à plusieurs points de présence par pays).

En 1992 a eu lieu la première implémentation Unix sur un routeur IP Multicast.

En 1992 toujours la première diffusion audio Multicast d'une réunion de l'IETF.

En 1993 la première diffusion vidéo Multicast depuis l'IETF.

A ce jour, le réseau Mbone est en perte de vitesse, le Multicast étant maintenant installé en mode natif au niveau mondial, et le service Multicast est proposé par la majorité des ISP.

Au niveau Européen, il existe une réseau Multicast : TEN-155. Basé sur des routeurs Cisco et Juniper, il fournit un service Multicast vers et de Internet. TEN-155 est basé sur les protocoles PIM SM, MBGP et MSDP.

En France, Le réseau Renater FMbone en est à la version 2 (FMbone-2). Ce réseau est basé sur un modèle hiérarchisé clairsemé (Sparse Mode). Il utilise des routeurs Cisco, les protocoles MBGP et MSDP. Ce réseau est connecté au réseau TEN-155.

Il est à noter que les expérimentations de diffusions vidéo nécessitent une bande passante comprise entre 1 Mbits par seconde en Streaming (avec une compression idoine…) et 3,5 Mbits par seconde (et plus) en codage de type MPEG2.

**Multiligne -** Qui regroupe plusieurs liaisons dans une même entité. En téléphonie, regroupe sous un seul numéro un ensemble de lignes. En transmission de données, regroupe plusieurs canaux à faible vitesse pour les combiner dans un réseau haute vitesse.

**Multimode - ou Multimodal -** Se dit d'une fibre optique dans laquelle peuvent être entretenus plusieurs faisceaux de rayons lumineux. Idéal pour le câblage d'immeuble.

Fibre pour laquelle le guide d'onde formé, notamment avec une taille importante du coeur comparée à la longueur d'onde, permet la propagation de plusieurs modes. Le nombre de modes est plus important pour des fibres à saut d'indice (plusieurs centaines) que pour des fibres à gradients d'indice (deux fois moins) ce qui explique les performances meilleures des fibres à gradients d'indice en bande passante.

Fibre optique dans le coeur de laquelle plusieurs modes de propagation peuvent être entretenus à la longueur d'onde considérée. Standard: 50/ 125, 62,5/ 125, 100/ 140 (diamètre decoeur (µm) sur diamètre de gaine).

**Multiplex -** Désigne une liaison multiplexée. Se dit d'un système dans lequel une voie de transmission commune permet de transmettre dans le même sens des signaux indépendants assemblés en un seul signal composite à partir duquel ils peuvent être restitués.

**Multiplexage -** Opération consistant à assembler des signaux issus de plusieurs sources distinctes en un seul signal composite destiné à être transmis sur une voie de transmission commune.

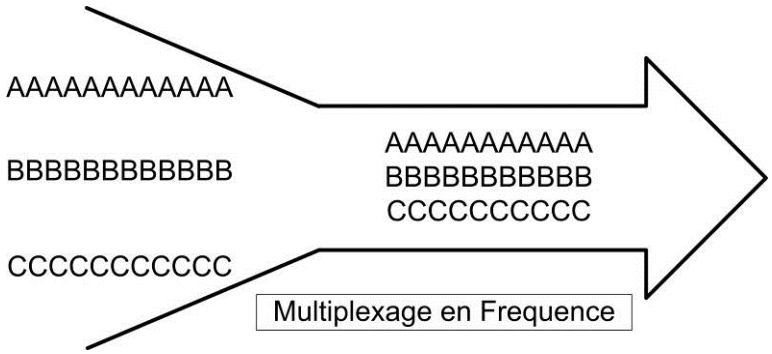
Le Multiplexage est avant tout effectué par des équipements (les multiplexeurs) qui permettent de prendre en charge sur une voie haute vitesse plusieurs voies basses vitesses simultanément. Pour augmenter la capacité des grands réseaux sur fibre optique, il existe deux méthodes :

1 - accroître le débit du train numérique (155 Mbits/s, 622 Mbits/s, 2,5 Gbits/s, puis 10, puis 40) avec l'utilisation du multiplexage temporel (TDM),

2 - faire passer plusieurs trains (canaux) dans la même fibre optique, chacun étant caractérisé par une longueur d'onde. Cette seconde méthode se nomme le multiplexage en longueur d'onde ou WDM (Wavelength Division Multiplexing) ou encore DWDM (Dense Wavelength Division Multiplexing).

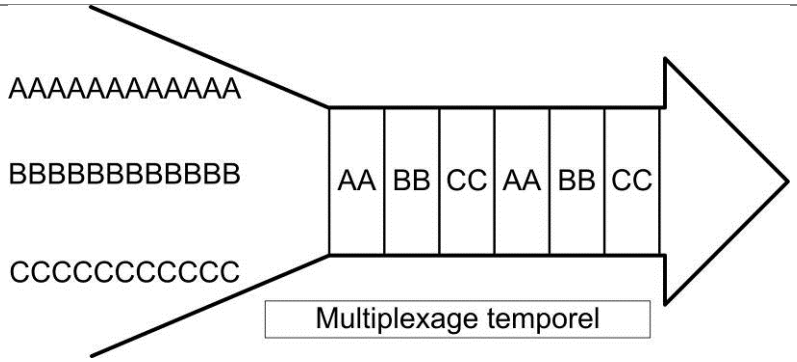
Les télécommunications n'ont qu'une obsession, faire passer le maximum de signaux sur le minimum de canaux. Pour y parvenir, le multiplexage est depuis longtemps une méthode favorite surtout depuis que les progrès du numérique ont permis de l'appliquer aussi bien au transport de la voix qu'à celui des données.

Techniquement, le multiplexeur, ou "mux", assure une tâche de concentration - déconcentration. Elle consiste à assembler des signaux émanant de plusieurs sources pour les transporter sur un seul canal, sous la forme d'un signal composite. Le multiplexeur permet de concentrer sur une seule liaison le trafic d'un grand nombre de canaux (terminaux) et donc d'additionner sur une voie à haut débit plusieurs voies à bas ou moyen débit. Trois techniques cohabitent: le multiplexage en fréquence, le multiplexage temporel (TDM) et le multiplexage statistique.




Le multiplexage en fréquence consiste à découper la Bande Passante d'un canal en plusieurs sous- bandes, chacune étant affectée à une voie. Technique qui consiste à diviser la bande passante haut débit en autant de sous-bandes qu'il y a de canaux ou de terminaux bas débit à raccorder. Dit "de fréquence", ce type de multiplexage concerne la transmission des ondes de fréquence et donc les voies de type analogique. Cette technique est peu utilisée aujourd'hui.

Le multiplexage temporel est au contraire une technique numérique. Elle consiste à imbriquer des bits ou des octets, prélevés successivement sur les différentes voies à bas débit pour construire un train de bits ou de caractères transmis sur la ligne à haut débit. Technique numérique qui a pour effet de diviser la bande passante selon un cycle bien défini d'intervalles de temps. Il s'agit d'un multiplexage statique et égalitaire. chaque terminal ayant son créneau de temps réservé, même s'il n'a rien à émettre. Bien entendu, dans le sens inverse, le multiplexeur "démultiplexe" et restitue chaque bit à la ligne bas débit de son destinataire.




Dans le multiplexeur statistique, au contraire, le prélèvement des voies n'est plus forcément cyclique ou plutôt le cycle de construction du train composite est modifié dynamiquement en permanence selon l'activité réelle des différents terminaux. Technique numérique fondée sur le postulat que, statistiquement, certaines voies à bas débit émettent des données plus souvent que d'autres, si bien que la liaison à haut débit peut avoir un débit nominal inférieur à la somme des débits des voies de basse vitesse.

**Multiplexage en Fréquence -** Méthode de multiplexage consistant en une modulation, par chacun des signaux à transmettre, d'une onde de fréquence différente et en une combinaison de ces ondes sur un même support. Pour la téléphonie, l'espacement entre ondes porteuses est de 4000 Hz, la largeur de bande de fréquences pour une communication téléphonique étant de 3100 Hz (de 300 à 3400). On dit aussi multiplexage à répartition en fréquence (MRF).

**Multiplexage par Répartition en Code -** Multiplexage dans lequel chaque signal indépendant est caractérisé par une séquence codée qui permet de le restituer à partir du signal composite.

**Multiplexage par répartition en longueur d'onde -** (Voir aussi WDM) - Multiplexage dans lequel des signaux indépendants utilisent des ondes porteuses à des longueurs d'onde différents dans le domaine optique.

Le principe est d'injecter simultanément dans une fibre optique plusieurs trains de signaux numériques sur des longueurs d'ondes distinctes. Le multiplexage en longueur d'onde (désigné souvent par le sigle WDM pour Wavelength Division Multiplexing) est une technique largement employée pour mettre à profit la bande passante des fibres unimodale. Un multiplexeur est un composant qui permet d'injecter sur la même ligne deux (ou plusieurs) signaux de différentes longueurs d'onde. La séparation des signaux est effectuée à l'autre extrémité de la ligne par un démultiplexeur.

La variation quasi-sinusoïdale de la transmission spectrale d'un coupleur est à la base de la plupart des multiplexeurs. Comme ce sont des composants réversibles, le même coupleur peut être utilisé en multiplexeur ou en démultiplexeur bien que ce dernier requière, en général, un meilleure performance d'isolation que le premier.

Le plus courant est conçu pour les longueurs d'onde 1300/1550 nm, ce qui permet de doubler la capacité des lignes en place, mais la réponse spectrale d'un coupleur peut aussi être manipulée pour d'autres applications : par exemple, les lasers et les amplificateurs à fibre dopée à l'erbium nécessitent aussi des multiplexeurs. Le multiplexage dense met en jeu une séparation des longueurs d'onde de l'ordre du nanomètre.

La fibre optique du fait de sa bande passante élevée présente donc un fort potentiel au multiplexage de très nombreux canaux sur de longues distances.

**Multiplexage Temporel -** Méthode de multiplexage consistant en une modulation par impulsions et codage (MIC), et en une transmission sur un même support, pendant des intervalles de temps distincts, des impulsions codées correspondant à chaque signal. On dit aussi multiplexage à répartition dans le temps (MRT).

Le multiplexage TDM (Time Division Multiplexing) ou MRT (Multiplexage à répartition dans le temps) consiste à affecter à un utilisateur unique la totalité de la bande passante pendant un court instant et à tour de rôle pour chaque utilisateur. Lorsqu'une trame se présentera à l'entrée du multiplexeur, et que la tranche de temps ne lui sera pas affectée, il faudra qu'elle soit mémorisée.

Le multiplexage TDM permet de regrouper plusieurs canaux de communications à bas débit sur un seul canal à débit plus élevé.

On retrouve ce type d'utilisation sur les canaux aux Etats-Unis qui regroupent par multiplexage temporel 24 voies à 64 Kbits/s en une voie à 1,544 Mbits/s ou sur les canaux E1 en Europe qui regroupent 30 voies analogiques en une voie à 2,048 Mbits/s.

Le multiplexage TDM peut être utilisé indifféremment sur paire torsadée ou fibre optique, il est indépendant du média de transmission.

**Multiplexer -** Assembler des signaux indépendants en un seul signal composite à partir duquel ils peuvent être restitués.

**Multipoint -** Canal de transmission reliant plus de deux équipements et où tout message émis par un équipement est reçu par tous les autres. Une telle liaison suppose donc un mécanisme d'adressage qui fait que seul l'équipement concerné prend en compte le message. Les liaisons multipoints sont généralement hiérarchisées, l'un des équipements dirigeant la séquence des communications.

Une autre notion de base distingue les liaisons point à point des liaisons multipoints. Une transmission de données point-à-point ne met en relation à un moment donné qu'un seul émetteur et un seul récepteur. Au contraire, une liaison multipoint permet au même instant à un émetteur de transmettre vers plusieurs récepteurs. Il y a ainsi partage d'une partie des liaisons entre émetteurs et récepteurs. Si, dans une liaison multipoint, la transmission est unidirectionnelle, on parlera de diffusion (en anglais: broadcast).

**Mux -** Abréviation familière de multiplexeur.

**MVNO -** Mobile Virtual Network Operator - Opérateur Virtuel Mobile - Opérateur Mobile qui sous-traite la gestion et le déploiement du réseau mobile à un opérateur, le MVNO se différenciant sur la région, le secteur économique, l'offre commerciale.

Techniquement, l'opérateur virtuel peut détenir une partie des éléments du réseau, ou alors se limiter à la diffusion des cartes SIM ou USIM.

# N

**NAC -** Network Access Control - Solution de contrôle d'accès au réseau. Cette solution s'assure de la conformité des postes par rapport aux exigences de l'entreprise. Un contrôle préalable des outils de sécurité (antivirus, antispyware, pare-feu,…) présents sur ces PC est effectué avant qu'ils ne soient admis dans le réseau. Dans le cas contraire, la demande de connexion au réseau de l'entreprise est rejettée (rejet ou mise en quarantaine).

En cas de mise en quarantaine, une procédure de remédiation est alors déclenchée, requérant des mises à jour ou correctifs logiciels sur le poste client non conforme.

Les systèmes NAC reposent sur les éléments suivants :

- un serveur qui prend les décisions d'accès et délivre l'adresse IP,
- un serveur qui gère la quarantaine et la remédiation,
- un agent logiciel sur PC**.**

La solution NAC est par nature intimmement liée au service DHCP du réseau, le complétant ou le suppléant.

**Named pipes -** Canal virtuel de communication, affecté d'un nom, qui permet à des applications de communiquer entre elles. Correspond à une interface de programmation rendue populaire par Microsoft.

**NAPLPS -** North American Presentation Level Protocol Syntax - Système vidéotex développé par ATT aux Etats-Unis à partir du système canadien Telidon.

**NAS -** Network Access Server - Equipements utilisés par les opérateurs et les ISP dans le cadre des services d'accès à Internet par le réseau téléphonique commuté. Ils servent à transformer les communications téléphoniques en flux de données IP en assurant l'interface entre le réseau téléphonique commuté et le réseau de transport de données IP.

Composés de modems analogiques et numériques, ils assurent la terminaison de l'appel et la gestion du maintien de la communication pendant toute la durée de la session de l'utilisateur. Les NAS doivent aussi, lorsque le service le nécessite, assurer des fonctions de réassemblage de paquet localement (si les sessions sont multilink) et aussi assurer le routage desdits paquets IP.

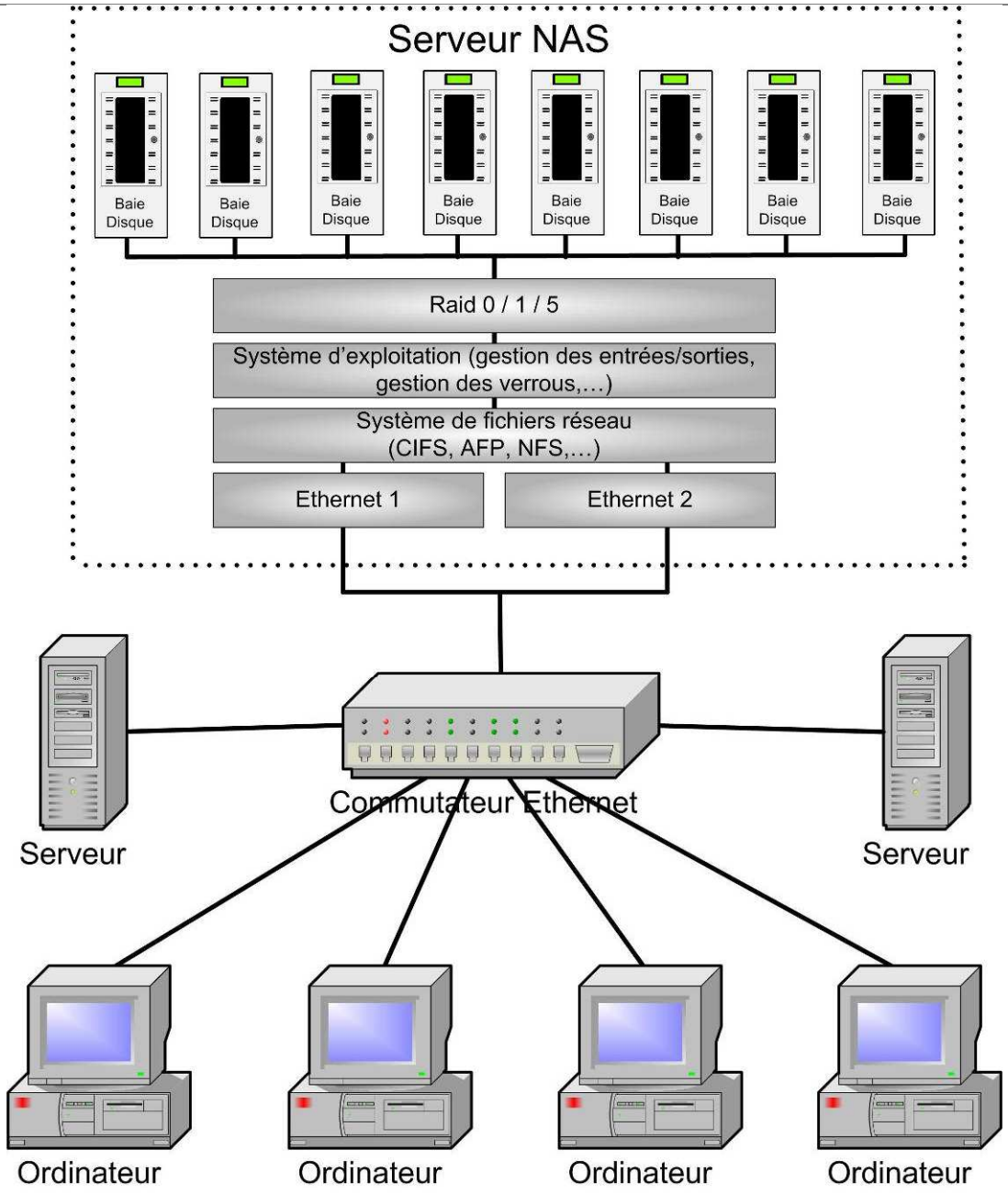
Ce terme tend à disparaître parce que remplacé par RAS - Remote Access Server.

**NAS -** Network Attached Storage - Littéralement Stockage Attaché au Réseau - Un NAS n'est rien d'autre qu'un serveur de fichiers très largement dopé. Il se compose en général d'une carte mère redondante avec une ou plusieurs cartes réseau Ethernet et de multiples unités de disques configurées en Raid logiciel ou matériel selon le prix du serveur.

Le principal avantage d'un serveur NAS est sa simplicité de mise en œuvre. En fait, il se configure comme un serveur de fichiers. L'administrateur définit des volumes logiques sur la baie et les autorisations de partage. Puis il décide quels systèmes de fichiers seront disponibles. Ceci fait, les volumes du NAS apparaissent sur le réseau comme tout volume réseau partagé. Un PC voit ainsi les volumes CIFS comme des volumes de serveur Windows dans son voisinage réseau.

Sa limitation à un mode fichier dote le NAS de plusieurs atouts. Un volume logique peut ainsi être configuré pour être accessible via plusieurs systèmes de fichiers réseau (par exemple SMB/CIFS, AFP et NFS). Il peut alors être partagé en natif par des PC sous Windows, des Mac et des stations Unix/Linux pour s'échanger des fichiers. Ce genre de fonctionnalités explique le succès du NAS en environnement PME/PMI.

Selon le constructeur, le système d'exploitation utilisé est soit spécifique (Snap OS de Quantum, Data Ontap de Network Appliance), soit banalisé (Linux, BSD ou Windows). L'OS gère les disques Raid du serveur, fournit les systèmes de fichiers réseau adaptés (SMB/CIFS, NFS, AFP, HTTP...) et gère les authentifications. Pour simplifier la configuration, le dispositif peut s'intégrer dans une architecture de gestion de droits d'utilisateurs préexistante (NIS, Active Directory, NDS, etc.). Quelques NAS incorporent enfin des fonctions simplifiant les sauvegardes. Certains fabricants dotent l'outil d'un agent de sauvegarde (Legato, CA, Veritas...), ce qui permet de l'intégrer dans les procédures standard de backup de l'entreprise. Chez d'autres, ceux utilisant Windows ou Linux, le logiciel de sauvegarde est embarqué dans le serveur pour piloter en direct une librairie ou un lecteur de bandes externe. Les PME bénéficient ainsi d'un serveur NAS et d'un backup asservi. Voir SAN.




Fonctionnement d'un serveur NAS

**NAT -** Network Address Translation - Traduction d'adresse réseau - Mécanisme consistant à convertir une adresse IP en une autre. Le NAT est essentiellement utilisé pour connecter un espace d'adressage interne utilisant un protocole différent d'un autre réseau, tel qu'Internet. La translation d'adresse permet de cacher les adresses des utilisateurs d'un réseau local et de créer une séparation entre les adresses "privées" et les adresses "publiques". La translation d'adresse est également un moyen de répondre au manque d'adresse disponible.

Processus destiné à augmenter le nombre d'adresses IP au sein d'un réseau privé. NAT enregistre les adresses IP d'un réseau privé et les attribue à une adresse IP publiquement enregistrée. L'avantage de ce processus est que les ordinateurs qui ne peuvent que communiquent entre eux au sein du réseau de la société ne requièrent pas d'adresses IP publiques. Les ordinateurs qui communiquent avec d'autres ordinateurs externes recoivent un numéro de référence lors du routage.

**NAT- PT -** Network Address Translation-Protocol Translator - Mécanisme permettant de traduire des adresses IPv6 en adresses IPv4. Indispensable tant que les deux protocoles cohabiteront.

**NAU -** Network Adressable Units - Unité adressable dans l'architecture SNA d'IBM. Trois types de NAU: LU, PU et SSCP.

**NBS -** National Bureau of Standards - Ancien organisme fédéral de normalisation aux USA, représentant ce pays à l'ISO (International Standard Organisation). S'est transformé en Nist : National Institute of Standards and Technology.

**NCP -** Novell Netware Core Protocol - Protocole de la famille Novell Netware en charge de l'accès ressources du serveur primaire Netware. Il fait des appels de procédures au NFSP (Netware File Sharing Protocol) .

**NDI -** Numéro de Désignation Inactif - Désigne un type d'offre qui permet de s'abonner chez un FAI lorsque l'on emménage dans un appartement et que l'ancien occupant a résilié sa ligne FT depuis moins de 3 mois. Avantage : pas besoin de payer des frais d'ouverture de ligne FT. Inconvénients : connaitre le n° de l'occupant précédent, qui doit donc avoir résilié depuis moins de 3 mois.

**NDS -** Netware Directory Services - Service d'annuaire de Novell qui s'étend de plus en plus hors du seul milieu Netware pour devenir un service global et compatible avec X500 et la norme LDAP.

**Net/Master -** Logiciel commercialisé par la société Systems Center destiné, à l'origine, à l'administration centralisée d'un réseau SNA d'IBM.

**NetBEUI -** Network Bios Extended User Interface - Protocole de transport de l'environnement NetBios (Network Basic Input/Output System) d'IBM.

**Netbios -** Network Basic Input Output System - Progiciel d'interface entre le système d'exploitation MS-DOS d'un micro-ordinateur et les applications permettant de gérer les échanges entre plusieurs micros en réseau local. Comme cette interface est utilisée par la plupart des logiciels de gestion de réseau, elle fait aujourd'hui figure de standard de fait.

**Nétiquette ou netiquette -** Ensemble informel de règles de savoir-vivre et de bonne conduite sur Internet et dans l'usage du courrier électronique. Le terme (pratiquement identique en anglais et en français) est une contraction de « net » (réseau en anglais) et d'étiquette (au sens où on l'entendait à la cour du Roi Soleil). Il existe sur Internet quelques documents qui essayent de rassembler en un corpus « législatif » homogène ce qui n'est souvent que la formalisation d'un consensus social par définition imprècis et mouvant. Mais le non-respect de ces règles - comme dans toute société - expose les contrevenants à l'ire de leurs pairs et à l'opprobre sociale. Si les infractions à la nétiquette sont aujourd'hui plus tolérées que dans les jeunes années d'Internet, elles constituent maintenant davantage un moyen de reconnaissance sociale pour des groupes qui se distinguent par leurs pratiques et leurs tolérances différentes en matière d'usages et de règles de vie autour du courrier électronique (les vieux hackers, les jeunes hackers, les internautes récents, etc.)

**Netscape Directory Service -** Service d'annuaire de Netscape compatible avec la norme LDAP version 3.

**Netview -** Ensemble de logiciels proposé par IBM permettant l'administration centralisée d'un réseau organisé autour de son architecture de communication SNA.

**Netware -** Ensemble de logiciels de gestion de réseau local proposé par la société Novell. Aujourd'hui le plus répandu des gestionnaires de réseaux locaux.

**NetWare For SAA -** Le logiciel NetWare pour SAA permet aux utilisateurs d'un réseau NetWare de communiquer de manière très souple avec un site central IBM et les mini-ordinateurs IBM AS400 via TokenRing, SDLC et QLLC tout en tirant profit des fonctionnalités de sécurité et administration du système d'exploitation NetWare. La plate-forme NetWare pour SAA permet une intégration totalement transparente de l'environnement site central dans NetWare. Les utilisateurs tirent profit des applications comme la distribution des logiciels, l'accès aux bases de données site central, les passerelles de messageries.

**NFC -** Near Field Communication - Communication sans contact mobile qui utilise une technologie radio à très courte portée. Cette technologie permet l'échange de données à une distance de quelques centimètres.

Les équipements intégrant la technologie NFC vont simplifier les interractions des uns avec les autres et de la sorte simplifier l'accessibilité des services pour les clients.

L'une des première application connue du grand public est le micro paiement via les terminaux téléphoniques.

**NFS -** Network File System - Architecture logicielle développée par Sun Microsystems pour permettre l'utilisation de ressources partagées (notamment des fichiers) sur un réseau de stations de travail fonctionnant sous le système d'exploitation Unix. Il est devenu un des grands standards de fait du marché.

**NGA -** New Generation Access - Réseau d'accès de nouvelle génération - La stratégie numérique lancée par la Commission européenne en mai 2010 introduit la notion de NGA au niveau européen. Le NGA doit permettre d'accéder au haut débit d'ici à 2013 et au débit ultra-rapide d'ici à 2020. La règlementation de l'accès aux réseaux de nouvelle génération (NGA) constitue une première étape pour atteindre l'objectif. La recommandation définit une approche règlementaire en ce qui concerne l'accès aux nouveaux réseaux à très haut débit en fibre optique en offrant un équilibre entre encouragement des investissements et préservation de la concurrence. Voir Recommandation 2010/572/UE

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:251:0035:0048:FR:PDF

**NGN -** Next Generation Networks ou New Generation Network - Evolution des réseaux de télécommunications s'appuyant sur le protocole Internet. Autrement appelé effectivement Réseau Convergent Multiservice mais c'est un peu un abus de traduction... En fait, il s'agit d'un concept assez vaste d'évolution des plates formes de services de coeur de réseau destinées au routages des appels voix incluant dans un réseau global mais pas forcément dans une même baie des équipements tels que les média gateway, les serveurs, le back bone d'interconnexion des différents serveurs...

La grande évolutivité de ce concept autorise effectivement telle ou telle orientation en fonction des besoins, chaque composante du système étant enfin dissociée.

- Les serveurs - Ils sont en charge de la gestion de la signalisation, du contrôle et du routage. Leur dimensionnement est donc lié au type de trafic, pas vraiment au volume, ils ne sont pas chargé de la commutation. C'est un peu "l'intelligence" du réseau, les contrôles IN se font sur cet équipement.
- Les Média Gateway - Ces équipements là ont 2 fonctions principales (simplifiées à l'extrême) = Convertir le média et servir de passerelle entre les média. c'est aussi sur la média Gateway que se traite la commutation (mais pas le routage). En fait, c'est là dessus que l'on connecte la voix en TDM (ligne fixes, interconnexion opérateur, SS7..., les BSS (radio GSM 2G), l'ATM (pour la radio 3G) ou les baies d'abonnées pour raccorder des abonnées du filaire. En fait, ces machines doivent être dimensionnées aussi en fonction des besoins de connexion et du volume de trafic à traiter. On peut bien sûr les utiliser aussi pour de la VOiP, mais je ne l'ai jamais fait... j'ai fait le reste ;-)
- Le back bone d'interconnexion - IP - Il faut y distinguer les liens utilisés pour le trafic de signalisation (SIGTRAN) et les liens d'interconnexion utilisés pour le trafic voix et "user", on parle plus précisément de contrôle plane et de user plane. le back bone est lui aussi dimensionné en fonction des besoins, mais là on tient compte des besoins liés au contrôle plane (donc du trafic de signalisation) et du trafic sur le user plane (donc du volume d'appels à véhiculer simultanément en interconnexion média gateway).

C'est extrêmement simplifié comme présentation technique, je l'avoue. En fait, ce qui semble avoir motivé les concepteurs, ce sont les séparations de fonctions de commutation des fonctions de signalisation, en apportant une très forte souplesse de configuration. Il suffit de changer, modifier, updater la média Gateway pour traiter une autre type de client sur le réseau voix, sans modifier les systèmes de signalisation, donc les tickets de taxation, donc le billing... certains champs supplémentaires devront être pris en compte dans les tickets de taxation. on peut dédier une média gateway à une fonction ou la mutualiser, on peut utiliser un seul serveur de signalisation et lui ajouter plusieurs média Gateway, on peut déployer des média Gateway en Province mais conserver les serveur de signalisation en région parisienne... etc etc... Le protocole majoritaire pour ceux que cela intéresse est IMS en cœur de réseau NGN (a terme).

Les principaux concernés sont les opérateurs et les fournisseurs de service des opérateurs. Les principaux avantages du concept n'apparaissent que dans des configurations "musclées" et/ou multi environnement. Il s'agit d'une évolution des cœurs de réseau TDM vers l'IP. A terme, il est envisageable de voir apparaitre des offres d'interconnexion entre plates forme VOiP en environnement SIP avec du NGN en environnement IMS, mais ce n'est pas encore acquis, les porteurs des deux technologies étant assez éloignés :

- SIP = Cisco, Thomson, Avaya, Matra...
- IMS = Alcatel, Nortel, Ericsson,...

**NGSO -** Non Geostationary Satellite Orbit - Orbite d'un satellite qui n'est pas géostationnaire.

**NHRP -** Next Hop Resolution Protocol - Protocole proposé par l'IETF pour résoudre le problème de traversée des routeurs entre les sous réseaux logiques. Le but est ici de localiser un point de sortie du nuage ATM le plus proche de la destination et d'obtenir son adresse ATM. On a ici des serveurs NHRP qui fournissent le next hop vers la destination. Ces serveurs NHRP interagissent entre eux pour trouver le point de sortie le plus proche de la destination.

**NIAG -** NATO Industry Advisory Group - Groupe Consultatif Industriel de l'OTAN.

**NIC -** Network Information Center - Organisation responsable du maintien et de la cohérence du serveur DNS de la zone racine (". "le root) et de son équivalent binaire. En plus, il est responsable de l'administration des domaines de premier niveau, ou encore Top Level Domain Name (TLDN, ex : ARPA, COM, EDU, ORG, GOV, MIL, etc.) au nom du DCA et DARPA jusqu'à ce qu'il soit possible pour les organisations appropriées de s'en charger.

**NiCd -** Une batterie Nickel Cadmium (ou NiCd) est "longue durée", rechargeable, et supporte environ 700 cycles de charge et décharge. Si elle n'est pas totalement déchargée avant d'être remise en charge, la batterie NiCd risque de souffrir de l'effet mémoire, qui réduira sa durée de vie. Voir également Effet de mémoire.

**NiMH** - Une batterie à hydrure métallique de nickel, également appelée batterie Ni-MH ou NiMH, est une batterie rechargeable capable de conserver davantage d'énergie qu'une batterie NiCd et souffrant moins de l'effet de mémoire. Elle est d'ailleurs généralement plus chère. Voir également Effet de mémoire.

**NIS -** Network Information Services - Propriétaire SUN - Ensemble de fonctions et de programmes qui permettent de diffuser des informations communes de configuration sur différentes machines UNIX. Ce protocole était anciennement appelé Yellow Pages (YP), mais pour des raisons de copyright avec British Télécoms, le nom à du être changé, même si les deux termes sont couramment employés aujourd'hui.

NIS est un système d'accès à l'information distribué, chaque machine implémentant NIS, accède à un serveur central qui se base sur le protocole RPC (Remote Procedure Call) pour transmettre les fichiers de mots de passe, groupes et d'hôtes (et bien d'autres). De cette façon, toutes les machines possèdent les informations de configuration sans qu'il soit besoin d'intervenir sur chacune à la fois. Les modifications sont appliquées uniquement sur le serveur maître, et le système se charge de les répercuter sur toutes les machines du réseau. Il faut signaler que depuis sa création NIS a subi un certain nombre d'évolutions. La première version, NIS v1 a été rapidement remplacé à cause d'un certain nombre de bugs, c'est donc la version 2 de NIS qui est la plus couramment utilisée. Mais Sun ne s'est pas arrêté là, face aux problèmes de sécurité de son produit, une nouvelle version de NIS a vu le jour : NIS+, qui est donc la version 4 du "Network Information Services ". Cette version n'est pas qu'une simple mise à jour, mais une refonte totale du système. Enfin, une dernière version : NYS, pour NIS, YP et "Switching System ", qui est encore une autre librairie de fonctions beaucoup moins utilisée que le NIS "standard ".

Les domaines de NIS

Comme pour le DNS, NIS utilise la notion de domaine et de nom de domaine. Chaque domaine est géré par un serveur primaire, qui peut être aidé par un ou plusieurs serveurs secondaires. La connaissance ou plutôt la "non connaissance "du nom d'un domaine NIS est un élément primordial pour assurer la sécurité dans le réseau. En effet, une machine n'aurait aucune difficulté à se faire passer pour un serveur du domaine si elle en connaît le nom. La librairie standard de NIS n'offre pas suffisamment de mécanisme de sécurité donc il faut éviter de divulguer le nom du domaine NIS.

Les différentes entités du réseau

- Le serveur primaire - Le serveur primaire a la charge d'un domaine NIS. Il est possible pour une même machine d'être le serveur primaire sur plus d'un domaine. C'est le primaire qui va posséder les informations à partager, c'est sur cette machine que les informations vont être modifiées localement. Tous les serveurs primaires ou secondaires, doivent faire tourner sans interruption le programme ypserv, si ce processus venait à tomber le serveur ne serait plus en fonction et ne répondrait plus aux requêtes des clients.
- Les serveurs secondaires - Les serveurs secondaires ou esclaves contiennent une copie des informations du serveur primaire. Cela permet d'assurer la redondance en cas de panne, et de répartir la charge du réseau sur plusieurs machines, évitant ainsi la saturation. Dans un domaine NIS les serveurs sont vraiment des pièces maîtresses du réseau. A la différence d'autres architectures où un serveur tombant en panne, le service assuré n'est plus disponible, dans un domaine NIS, si les serveurs ne sont plus en fonction c'est tout le réseau qui est paralysé, car si aucun client ne peut récupérer les informations sur les mots de passe, plus personne ne peut se connecter. Il est donc primordial de s'assurer du bon fonctionnement des serveurs et surtout de ne pas se contenter d'une seule machine assurant ce rôle.
- Les clients - Les clients du domaine NIS, sont les différentes machines qui se servent de NIS pour récupérer leurs informations de mot de passe, groupes ou encore annuaire. Ils doivent se lier lors de leur mise en fonction à un serveur NIS du domaine. Pour cela, ils utilisent un programme nommé ypbind. Celui ci, broadcast sur le réseau une demande d'attachement à un serveur, en spécifiant le nom du domaine NIS auquel il veut être rattaché. Le serveur qui répond le plus rapidement deviendra son serveur NIS et c'est à lui que les requêtes seront envoyées par la suite.
- La base de données - Les fichiers de données de NIS sont appelés maps. Ils sont contenus dan le répertoire /var/yp. Ces maps sont générées d'après les fichiers de configuration situés dans le répertoire /etc du serveur maître, à l'exception du fichier /etc/master.passwd. La raison est simple, on ne voudrait pas voir les mots de passe du root et autres comptes importants se propager sur tout le réseau. Pour générer ces fichiers maps on utilise le programme ypininit.

**NIST** - National Institute of Standards and Technology - Agence gouvernementale américaine établissant des normes techniques à l'échelle nationale.

**NLSP -** Netware Link Services Protocol - Protocole de routage à état des liens (link state) crée par la société Novell et fonctionne sur ses réseaux propriétaires IPX. Ce protocole a été définit pour pallier les limitations du protocoles de routage RIP IPX et du protocole SAP (Service Advertisement Protocol) qui sont des protocoles de type Distance Vector. NLSP est basé sur le protocole OSI IS-IS et permet l'échange d'informations entre les routeurs et peut interopérer avec les protocoles originaux de Novell : RIP IPX et SAP.

NLSP s'occupe des communications inter-routeurs, mais pour les communications utilisateurs / routeurs, c'est RIP IPX qui est utilisé.

NLSP est un protocole de routage à état des liens de type « Link State » qui est similaire à L'OSPF.

**NMS -** Network Management System - Système de gestion de Réseau est un système conçu pour contrôler le fonctionnement d'un réseau d'ordinateur ou un système de réseaux d'ordinateur. Les fonctions possibles d'un NMS incluent la détection des erreurs (détection et correction d'erreur), le suivi de configuration, le suivi de changement, le suivi système, comptabilisation (accounting) des utilisations système, l'exécution (performance) du système dans le temps (over the time) et sa sécurité.

Traditionnellement, les produits (logiciel pour la gestion de réseau) ont été divisés en deux camps :

D'abord, il y a la solution "Framework". C'est caractérisé par des produits comme Tivoli d'IBM et de Computer Associates Unicenter. Ces produits essayent d'exécuter toutes les fonctions d'un NMS avec un système simple : Faute, Configuration, Comptabilité, Exécution (performance) et Sécurité. À cause de la portée (étendue) de solutions de "Framework", ils ont tendance à être longs à mettre en œuvre (et à configurer) et peuvent être très chers.

Deuxièmement, il y a la solution "Best of Breed", où des produits de vendeurs divers se concentrent sur un ou deux aspects de gestion de réseau, et sont intégrés ensembles pour couvrir toutes les fonctions d'un NMS. Parce que chaque vendeur de produit se concentre sur une tâche spécifique, des solutions "Best of Breed" ont tendance à répondre plus rapidement aux changements dans les exigences des utilisateurs que des solutions "Framework". Cependant, gérer un grand nombre de vendeurs peut influer sur les coûts en ce qui concerne la formation de produit, des mises à niveau et des dépenses de support technique.

Dans presque tous les cas, les produits sont développés en langage propriétaire (code de marque déposée). Autrement dit, l'utilisateur final n'a aucun accès au code source qui compose ces produits. Ainsi il faut attendre que le vendeur de produit mette en œuvre des particularités ou spécifications ou bien changer l'orientation de gestion (Network Management stratégie and/or architecture) du réseau pour adapter leur technologie. La majorité des éditeurs de produits NMS en langage propriétaire ont un droit acquis dans la fabrication de leur code inaccessible aux concurrents, puisque leur affaire est basée sur la vente du logiciel, ce qui crée des barrages à l'intégration.

**NMT -** Nordic Mobile Telephone - Norme de radiotéléphonie cellulaire analogique fonctionnant dans des bases de fréquences de 450 et 900 mhz.

**NNI -** Network to Network Interface - Protocole d'interface de communication de réseau de relais de trame à réseau à relais de trame. Le NNI est désigné pour faire office d'interface entre 2 sous-réseaux Relais de Trames. Le protocole NNI autorise le transfert de données à haute vitesse, la gestion de la congestion, et le transfert d'informations de circuit.

**NNTP -** Network News transfert Protocol - Protocole gérant les transferts de messages des groupes de discussion Internet.

**Nœud -** Node - Dans un réseau, point où des commutateurs mettent en communication des voies de transmission.

**Nœud de Transit International -** NTI - Commutateur qui permet la connexion de Transpac aux réseaux étrangers de transmission par paquets conformes à la norme X 25.

**Non-répudiation -** Caractéristique d'un système cryptographique permettant d'empêcher qu'un expéditeur puisse nier ultérieurement avoir envoyé un message ou effectué une action spécifique.

**Normalisation** - Activité qui a pour objet d'établir des documents de référence : les normes. La normalisation est définie par l'article premier du décret n° 84-74 du 8 janvier 1983. Elle a pour objet de fournir des documents techniques de référence contenant les solutions de problèmes techniques et commerciaux posés par les produits, les biens et les services, de façon répétée, dans les relations entre partenaires économiques, scientifiques, techniques et sociaux.

En France, l'État confie à l'Afnor (Association française de normalisation) la mission de coordination de la normalisation et contribue à son financement. L'Afnor conduit le processus de normalisation et produit essentiellement des normes dont l'application est volontaire, pouvant occasionnellement être rendu obligatoire par une réglementation. Au plan européen, c'est le CEN qui a cette responsabilité. Au plan international, ce sont l'ISO (International Standardization Organization) et l'IUT (International Union Telecommunications).

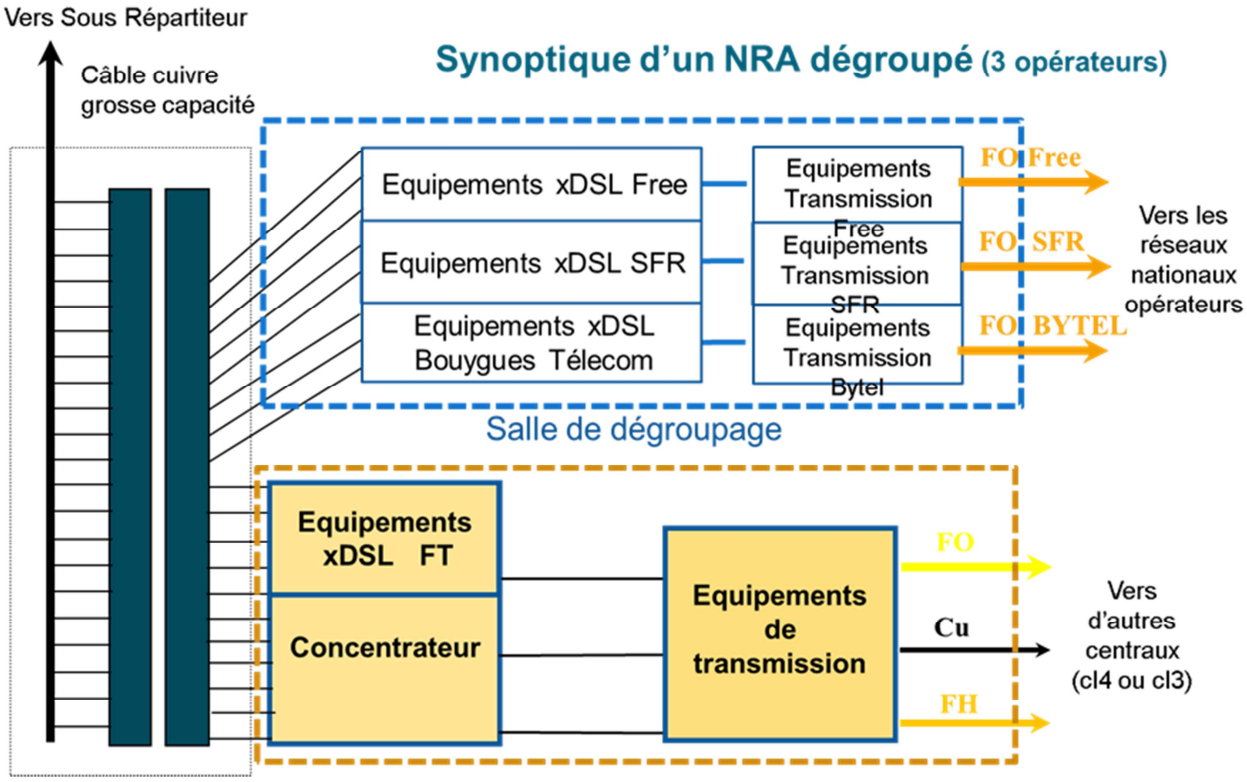
**Norme -** Standard - Document établi par consensus et approuvé par un organisme de normalisation reconnu (ISO, CEI, UIT-T, ETSI ...). Ne pas confondre avec standard.

**Novell -** (Protocoles) - L'ensemble des protocoles Novell Netware a été grandement influencée par le design et l'implémentation de l'architecture de protocoles du Xerox Network System (XNS). Il fournit un support compréhensible par DOS, Windows, Macintosh, OS/2 et UNIX. De plus, Novell fournit un large support aux réseaux locaux et aux communications asynchrones de large zone. Novell comprend les protocoles suivants :

- IPX - Internetwork Packet Exchange
- RIPX - Routing Information Protocol
- BCAST - Broadcast DIAG - Diagnostic Responder
- SER - Serialization WDOG - Watchdog
- SPX - Sequenced Packet Exchange
- SAP - Service Advertising Protocol NovelNetBios
- BMP - Burst Mode Protocol
- NCP - Netware Core Protocol
- NDS - Netware Directory Services

...

**NRA -** Noeud de Raccordement Abonné - Central téléphonique ou encore répartiteur. C'est de là que partent toutes les lignes d'abonnés d'une zone géographique définie. On y trouve les équipements de liaison, DSLAMs pour l'adsl par exemple, mais aussi les commutateurs E10B3 de la téléphonie RTC. C'est aussi là qu'on "cable" les abonnés en adsl en ajoutant des jarretières.




**NRO -** Noeud de Raccordement Optique - Terminologie FTTH - Désigne les locaux où sont concentrés les arrivées des fibres optiques des abonnés. Point de concentration d'un réseau en fibre optique où sont installés les équipements actifs permettant à un opérateur d'acheminer le signal depuis son réseau vers les abonnés.

On peut définir un NRO en le comparant à un local informatique dans lequel sont installés :

- Les tableaux d'arrivée des liaisons optiques (TDO)
- Les tableaux de départ les liaisons optiques (TDO)
- Les équipements télécoms des opérateurs
- Les équipements d'infrastructure (climatiseurs, onduleurs, Routeurs, OLT / ONT,…)

**NRZ, NRZI -** Non-Retour à Zéro, Non-Retour à Zéro Indirect. Désignent des méthodes de codages du signal binaire dans lesquelles deux bits successifs ne sont pas séparés par une plage de séparation.

**NSA -** National Security Agency - Agence gouvernementale américaine chargée de contrôler et de décoder toutes les communications émanant de pays étrangers et susceptibles de concerner la sécurité des Etats-Unis.

Service secret américain qui n'est pas tenu au secret défense (donc qui n'a pas à révéler ses secrets au bout d'un certain temps) et qui détient selon la rumeur l'un des plus grands fichiers nominatifs du monde (plusieurs dizaines de millions de fiches indiscrètes). On l'accuse (sans preuve objective) de lire tous les messages de l'Internet pour y déceler les activités plus ou moins subversives, à l'aide de programmes de recherche de mots-clés, les NSA Line Eaters. C'est pourquoi on trouve régulièrement dans les signatures des messages électroniques des mots-clés ("bombes ", "attentat ", "drogue "...) sans rapport avec le message évidemment, ils sont uniquement présents pour que la NSA tilte pour rien.

**NSAP -** Network Service Access Point - Standard OSI définissant une adresse de 20 octets pour les réseaux ATM privés.

**NSS -** Network Sub System - Sous système d'acheminement des données d'un réseau GSM composé des HLR, MSC et VLR.

**NTI -** Nœud de Transit International - Système assurant la connexion du réseau à commutation de paquets Transpac vers les réseaux à commutation de paquets d'autres pays.

**NTSC -** Television Standards Committee - Norme de TV couleur créée par ce groupe en 1951 avec 525 lignes et 60 trames par seconde. Le standard NTSC est utilisé en Amérique du Nord et en Amérique Centrale ainsi que dans d'autres pays. NTSC 4,43; Norme vidéo NTSC avec porteuse de couleurs PAL.

**NUI -** Numéro d'Utilisateur International. Adresse affectée à tout utilisateur de Transpac désirant une connexion internationale.

**Numérique -** Désigne un signal ne pouvant prendre qu'un nombre limité de valeurs discontinues (deux valeurs si le signal est binaire).

Se dit, par opposition à "analogique" de la représentation discrète de données ou de grandeurs physiques au moyen de caractères (des chiffres généralement) ; se dit aussi des systèmes, dispositifs ou procédés employant ce mode de représentation.

**Numeris -** Nom commercial du RNIS commercialisé par France Télécom.

L'infrastructure nationale de télécommunications est en train de s'unifier pour devenir peu à peu totalement numérique. Une offre de nouveaux services est donc disponible.Cette offre porte le nom de Numéris, nom commercial du RNIS (*Réseau Numérique à Intégration de Services*) en anglais ISDN. Derrière cette offre, il faut considérer plusieurs composantes majeures : d'abord, l'accès à un service de commutation de circuits numériques, ensuite la possibilité de bénéficier sur le même accès de plusieurs services, une interface normalisée universelle pour tout type de service, et enfin un accès à une signalisation riche soit entre un usager et le réseau, soit entre deux usagers. La normalisation du RNIS est parfaitement définie pour les 3 couches basses du modèle OSI. La couche Physique (couche 1) décrit les interfaces dites S côté usager et T côté réseau, ainsi qu'une prise universelle à huit contacts (RJ45) prévue pour raccorder n'importe quel type de terminal. La couche Liaison de données (couche 2) utilise une procédure HDLC similaire à celle des réseaux à commutation de paquets X25. La couche Réseau (couche 3) est également identique à X25 avec en plus un protocole de signalisation spécial.

Sont ainsi définis, pour l'utilisateur, deux types d'accès:

- L'accès de base prévoit un débit total de 144 Kbit/s découpé par multiplexage en deux canaux de 64 kbit/s, dits canaux B, et un canal de signalisation de 16kbit/s, dit canal D. L'interface est identifiée par la norme S0.
- L'accès primaire, sous le nom d'interface T2 (ou S2), correspond à un débit global de 1 984 kbit/s, composé de trente canaux B de 64 kbit/s et d'un canal D à 64 kbit/s. Le nom de primaire provient du fait qu'il correspond à l'unité de concentration primaire dans la hiérarchie de multiplexage des réseaux publics.

Les configurations de câblage sont de 4 types:

- Bus court : 130m 10 prises max
- Bus étendu : 130 à 500m (4 prises regroupées sur 30m)
- Point à point : 800m
- Distribution en Y : 2 branches de 90m (10 prises).

**Numérisation -** Digitizing - Conversion (transformation) d'un signal analogique en un signal numérique. La numérisation comporte deux activités parallèles : l'échantillonnage (sampling) et la quantification. L'échantillonnage consiste à prélever périodiquement des échantillons d'un signal analogique. La quantification consiste à affecter une valeur numérique à chaque échantillon prélevé.

La qualité du signal numérique dépendra de deux facteurs :

- la fréquence d'échantillonnage (appelé taux d'échantillonnage) : plus celle-ci est grande (c'est-à-dire que les échantillons sont relevés à de petits intervalles de temps) plus le signal numérique sera fidèle à l'original ;
- le nombre de bits sur lequel on code les valeurs (appelé résolution) : il s'agit en fait du nombre de valeurs différentes qu'un échantillon peut prendre. Plus celui-ci est grand, meilleure est la qualité.

Ainsi, grâce à la numérisation on peut garantir la qualité d'un signal, ou bien la réduire volontairement pour :

- diminuer le coût de stockage
- diminuer le coût de la numérisation
- diminuer les temps de traitement
- tenir compte du nombre de valeurs nécessaires selon l'application
- tenir compte des limitations matérielles

**Numéro Pastel -** Service commercial proposé par France Télécom permettant à un abonné de prendre en charge une partie des coûts des appels téléphoniques qui lui parviennent. L'émetteur ne paye lui qu'une communication locale.

**Numéro Vert -** Service commercial proposé par France Télécom permettant à une entreprise de prendre à sa charge les appels téléphoniques qu'elle reçoit.

**Numéros libre appel (France) -** Couramment appelés "numéros verts" par France Télécom, ces numéros sont gratuits pour l'appelant car ils sont financés intégralement par les personnes, sociétés ou organismes qui ont demandé l'attribution d'un tel numéro pour pouvoir être appelés. Les numéros "libre appel" commencent par 0800 et 0805.

**Numéros non géographiques (France) -** Numéros commençant par 08, parmi lesquels on distingue les services par nature, services de mobilité généralisée et services de réseaux privés virtuels, et par niveau tarifaire, services de libre appel, services à coût partagés et services à revenus partagés.

**Numérotation -** Le réseau téléphonique Français utilise une numérotation dite à "10" chiffres. Sur 10 chiffres, 9 sont utilisés pour désigner l'installation de l'abonné (Z ABPQ MCDU) et un - le préfixe "E" pour indiquer, dans un contexte d'interconnexion des réseaux, à l'opérateur de boucle locale (OBL), l'opérateur longue distance (OLD) chargé d'acheminer la communication.

Dans le plan de désignation des 9 chiffres (Z ABPQ MCDU), on a:

• Z = zone (1 à 9).

• ABPQ = commutateur de rattachement.

• MCDU = numéro de ligne.

Le préfixe Z peut avoir les valeurs:

| Z | Description | Choix OLD | Tarification type |
|---|---|---|---|
| 1 | Ile de France | Oui | Dépend distance |
| 2 | Nord-ouest | Oui | Dépend distance |
| 3 | Nord-est | Oui | Dépend distance |
| 4 | Sud-est | Oui | Dépend distance |
| 5 | Sud-ouest | Oui | Dépend distance |
| 6 | N° non géographiques - mobiles (GSM, pagers) | Non | Forfaitaire |
| 7 | N° non géographiques - Portables ?? ?? | ?? | ?? |
| 8 | N° non géographiques - non mobiles | Non | Forfaitaire |
| 9 | N° non géographiques - VOIP | Non | Forfaitaire - Local |
| 080B | Numéros Verts | Non | Gratuit ou forfaitaire |
| 081B | Numéros Azur | Non | Forfaitaire |
| 082B | Numéros Indigo | Non | Forfaitaire |
| 0860 et 0868 | Accès Internet | Non | Gratuit à local |
| 089B | Kiosque et passerelles Transpac | Non | Supérieur à local |

**Numérotation abrégée -** Numéro court (4 chiffres au maximum) raccourcissant une séquence d'appel téléphonique.

Service assuré par les autocommutateurs électroniques, permettant à un abonné d'enregistrer un certain nombre de numéros d'abonnés nationaux ou internationaux sous forme de numéros courts (un ou deux chiffres). Il suffit ensuite à l'abonné de composer ces numéros courts pour obtenir son correspondant.

**NVP -** Nominal Velocity of Propagation - Vitesse Nominale de Propagation. Vitesse de propagation des électrons dans un câble. Vitesse à laquelle les signaux électriques circulent sur un support de transmismission. S'exprime normalement sous forme d'une fraction de la vitesse de la lumière (C = 3.108 m/s).

# O

**OADM -** Optical Add Drop Multiplexing - Nouvelles techniques en cours de développement permettant de multiplier encore plus les capacités des systèmes optiques avec l'introduction des multiplexeurs à insertion/extraction optiques reconfigurable et de brasseurs optiques (Optical Cross-Connect : OXC).

Un multiplexeur OADM est un élément de réseau qui permet à une liaison de transmission en WDM d'ajouter ou d'extraire des signaux optiques sans convertir le train photonique en un signal électrique.

Des filtres optiques ou des démultiplexeurs effectuent l'insertion et l'extraction. Un OADM est ou non reconfigurable. Dans le premier cas, il faut recourir à des commutateurs optiques.

**OBL -** Opérateur de Boucle Locale (voir opérateur local). Opérateur qui déploie des infrastructures de télécommunication permettant le raccordement physique d'un abonné aux réseaux commutés de télécommunication.

Ses infrastructures sont constituées d'une ligne d'abonné (qui peut être une ligne hertzienne) et d'équipements de commutation (Commutateur à autonomie d'acheminement).

Ses activités sont l'écoulement des appels locaux, la facturation de l'abonnement de la ligne au client, la facturation des appels locaux au client (selon des tarifs qui lui sont spécifiques).

**Octet -** Groupe de 8 bits représentant une donnée. Ensemble de données de 8 éléments binaires traités comme un tout. Un octet est souvent utilisé pour représenter un caractère alphanumérique.

**ODA -** Office Document Architecture - Norme d'échange de documents entre systèmes hétérogènes. Elle permet de prendre en compte des documents textuels, des données ou des graphiques.

La norme ODA est une norme de l'ISO (IS 8613) et du CCITT (recommandations T.401 à T.408).

**ODIF -** Office Document Interchange Format - Format d'échange de documents Oda.

**OEM -** Original Equipment Manufacturer - Intégrateurs intermédiaires qui incorporent dans leurs produits, des sous-systèmes, appareils ou machines fournis par un fabricant en amont.

**OFDM -** Orthogonal Frequency Division Multiplexing - Cette technologie pourrait à terme remplacer les technologies actuelles (avril 2005) de modulation utilisées en UMTS. Divise les canaux de 20 MHz en 52 sous-canaux de 0,3125 MHz (sur 64 sous-canaux possibles) pour obtenir au choix des débits de 6, 9, 12, 18, 24, 36, 48 ou 54 Mbps. Seuls les débits de 6, 12 et 24 Mbps doivent être impérativement implémentés sur tous les produits. (voir 802.11a).

26 térabits/seconde = record mondial de vitesse de transmission de données réalisé en 2011 avec un seul faisceau laser utilisant le procédé de modulation OFDM sur une distance de 50 kilomètres. Ce record a été établit oas une équipe de l'institut de technologie de Karlsruhe (Allemagne). Les données ont été codées, transmises sur 50 kms puis décodées. C'est l'équivalent de 700 DVD tranférés en 1 seconde.

**Off-line -** Littéralement "hors ligne" - Mode de fonctionnement d'un équipement assurant une tâche de façon autonome sans être relié à un réseau.

**OfTel -** Office of Telecommunications - Organisme britannique chargé de la réglementation et de la surveillance des télécommunications.

**OFTP -** Odette File Transfer Protocole - Protocole de transfert de fichiers mis au point dans le cadre de l'organisation Odette.

**OGG -** Format de compression audio environ 30 % plus compact que le MP3 , pour une qualité équivalente ou supérieure. L'objectif affiché des développeurs de ce format comme Vorbis, est d'en faire un remplaçant libre du MP3.

**OHM -** Unité de mesure de la résistance électrique ou d'impédance. Résistance électrique mesurée entre deux points d'un conducteur lorsqu'une différence de potentiel constante de 1 volt, appliquée entre ces deux points, produit dans ce conducteur un courant de 1 ampère, le dit conducteur n'étant le siège d'aucune force électromotrice.

**OLD -** Opérateur longue distance - Opérateur qui ne déploie pas d'infrastructure de raccordement des abonnés et se borne à transporter des communications entre commutateurs raccordant des abonnés. Il dispose d'infrastructures de transport.

Ses activités sont l'écoulement des appels longue distance, la facturation de l'abonnement à ses services au client, la facturation des appels longue distance au client (selon des tarifs qui lui sont spécifiques).

**OLE -** Object Linking and Embedding - Technologie qui définit un ensemble d'interfaces afin d'accéder à de nouveaux services à partir d'applications Windows.

**OLT -** Optical Line Terminaison, ou terminal de ligne optique dans le centre d'accès.

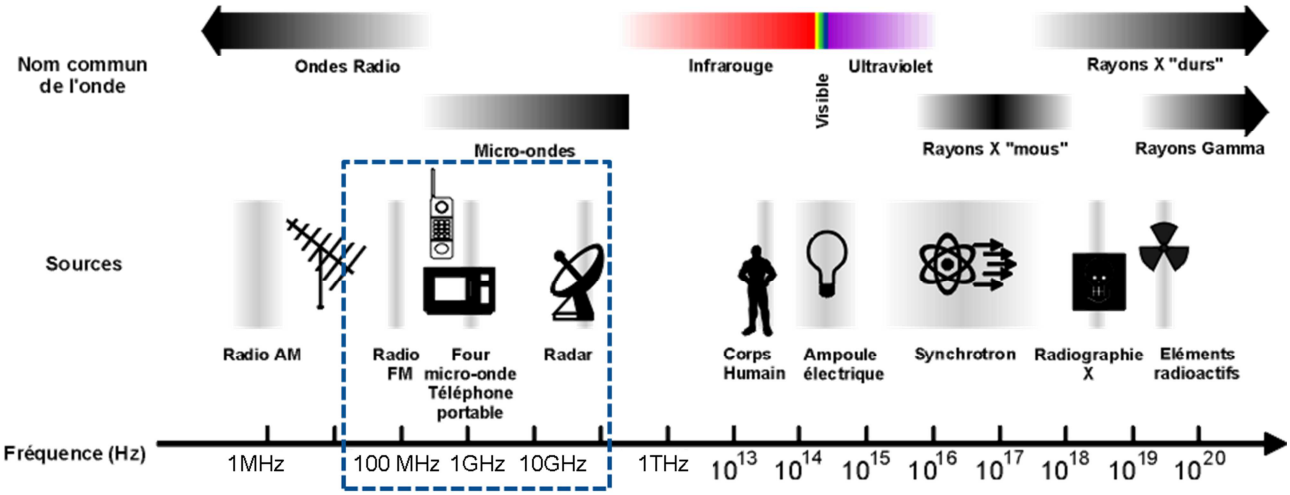
**OLTP -** On Line Transaction Processing - Transactionnel en ligne.

**OMG -** Object Management Group - Organisation internationale dont les membres sont des éditeurs, des intégrateurs et des utilisateurs. Elle a pour mission de standardiser les technologies objet. On lui doit notamment la norme Corba, les ORB (Object Request Broker) et la méthode d'analyse et de conception objet UML.

**OMS -** Organisation Mondiale de la Santé (Institution relevant des Nations Unies).

**Onde Radio -** Champ électromagnétique variable, souvent périodique, produit par une antenne.

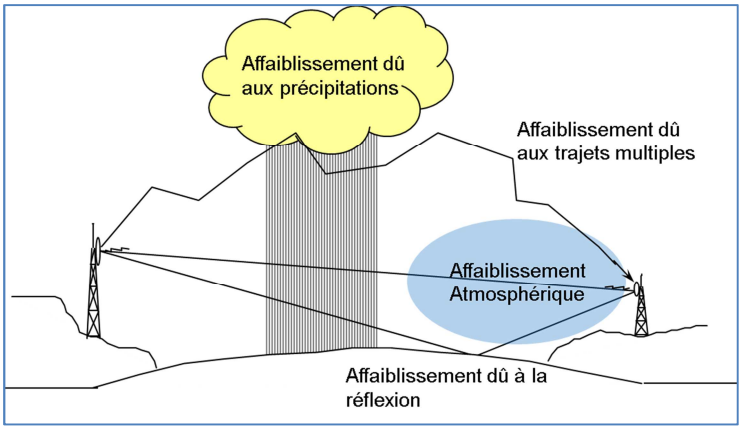
**Ondes Radioélectriques -** Les télécoms utilisent des ondes radio entre 100 MHz (FM) et 40 GHz (FH) en fonction des utilisations et des services attendu :




- Radio FM: 88.8 à 107.7 MHz
- Radio Tetra : 400Mhz à 800MHz (police, pompier…etc)
- Téléphone mobile: 900MHz / 1800MHz / 2100MHz (GSM/DCS/UMTS ou 3G)
- Wifi : 2.4GHz
- 4G : 800 Mhz, 2.4 Ghz
- Wimax : 3.5GHz
- WifiMax, Hiperlan : 5.4GHz
- - Faisceaux Hertziens: 8GHz à 38GHz

Les ondes radioélectriques n'étant pas transportées par un support guidé, elles sont soumises aux contraintes physiques du milieu extérieur. Les ondes radios à toutes les fréquences subissent un affaiblissement dû :

- A sa propagation (proportionnel à la distance ²)
- Aux précipitations (pluie, neige, brouillard…)
- A ses propres réflexions (sur le sol, les bâtiments, les nuages…)
- A l'absorption de l'air (dépend des fréquences utilisées)




**On-line -** Littéralement "en ligne" - Désigne tout équipement fonctionnant en liaison avec un autre équipement.

**ONP -** Open Network Provision ou fourniture d'un réseau ouvert - Le principe de fourniture d'un réseau ouvert permet la mise à disposition du réseau de l'opérateur historique aux nouveaux opérateurs, en dissociant la propriété du réseau et la fourniture du service ayant comme support ce réseau ; il permet ainsi de distinguer la disposition de l'infrastructure de son exploitation commerciale. Les directives européennes dites "ONP" sont des directives d'harmonisation qui ont pour objet l'application aux différents services de télécommunications des conditions de fourniture d'un réseau ouvert, c'est-à-dire les conditions harmonisées d'un accès ouvert et efficace aux réseaux de télécommunications.

**ONU -** Optical Network Unit, ou unité optique de réseau

**Openview -** Système d'administration de réseau décentralisé proposé par Hewlett-Packard.

**Opérateur -** Désigne une société ou un organisme exploitant un grand réseau de télécommunications. Exemple : AT&T, France Télécom, Mercury...

**Opérateur Alternatif -** En France, cette expression désigne les opérateurs privés qui, à partir d'infrastructures de télécommunications construites par de grandes entreprises de services (EDF, SNCF, Sociétés d'autoroutes), proposent leurs capacités venant ainsi concurrencer FRANCE TELECOM.

**Opérateur booléen ou opérateurs logiques** - Il y a quatre opérateurs booléens (relatifs à la logique booléenne) permettant d'effectuer des opérations sur des valeurs binaires. Ces opérateurs sont utilisés pour lier plusieurs mots d'une requête. Il s'agit de : ET, SOIT (ou OU inclusif), OU exclusif (aussi désigné par XOR qui signifie l'un ou l'autre mais pas les deux à la fois) et SAUF (en logique c'est NON).

**Opérateur de transport -** (ou transporteur longue distance) - Entreprise de télécommunications assurant l'acheminement des communications longue distance nationales et / ou internationales.

**Opérateur d'immeuble -** Terminologie FTTH - Désigne toute personne chargée de l'établissement ou de la gestion d'une ou plusieurs lignes dans un immeuble bâti, notamment dans le cadre d'une convention d'installation, d'entretien, de remplacement ou de gestion des lignes signée avec le propriétaire ou le syndicat de copropriétaires, en application de l'article l33-6 du code des postes et des communications électroniques. L'opérateur d'immeuble n'est pas nécessairement un opérateur au sens de l'article L33-1 du même code.

**Opérateur de point de mutualisation -** Terminologie FTTH - Opérateur d'immeuble qui exploite un point de mutualisation.

**Opérateur d'opérateurs -** L'opérateur connu du grand public est un opérateur de service ou de détail (FAI). L'opérateur d'opérateurs exploite un réseau qui est loué aux opérateurs de services pour assurer la connectivité vers les clients finaux.

**Opérateur local -** (ou opérateur de boucle locale) - Entreprise de télécommunications ayant installé la ligne de l'abonné.

**Opérateur puissant (France) -** La loi prévoit que l'Autorité arrête chaque année la liste des opérateurs considérés comme puissants (c'est à dire qui exercent une influence significative sur un marché pertinent du secteur des télécommunications). Ils sont soumis à l'obligation de publier un catalogue d'interconnexion. Est présumé puissant tout opérateur qui détient une part supérieure à 25% d'un marché pertinent de télécommunications. Pour établir cette liste, l'Autorité tient également compte du chiffre d'affaires de l'opérateur par rapport à la taille du marché, de son contrôle des moyens d'accès à l'utilisateur final, de son accès aux ressources financières et de son expérience du marché.

**Operator -** Système de radiomessagerie unilatérale (la personne peut être jointe pour recevoir un message ou un numéro à rappeler) proposé en France par TDF.

**OPEX -** Opération Expandures - Terme anglophone désignant les dépenses de fonctionnement, les frais de personnels non amortissable, les charges.

**Optoélectronique -** Discipline commune à l'électronique et à la photonique qui traite de la transformation de signaux électriques en signaux optiques et vice versa. Par exemple, les composants optoélectroniques sont les lasers à semi-conducteurs, les diodes électroluminescentes, les photodiodes. Il convient de ne pas confondre l'optoélectronique avec l'optique électronique ou l'électro-optique.

**Orbites -** Communication par satellite - Les caractéristiques d'une communication via satellite sont directement liées au choix de l'orbite sur laquelle est positionnée le satellite. Les délais de transmission, la durée de vie,… ne seront pas les mêmes si l'on se place à 36 000 km ou à 700 km.

On peut distinguer trois catégories d'orbites :

Orbite géostationnaire ou GEO (Geosynchronous Earth Orbit), altitude à 36 000 Km. Un satellite en orbite géostationnaire réalise une révolution en 24 heures, ce qui correspond à la période de rotation de la Terre. Comme il se déplace dans la même direction de rotation que la Terre, il reste à une position fixe au-dessus d'un point situé à l'équateur, et assure de ce fait un contact ininterrompu entre les stations terrestres situées dans son champ de vision. De part sa haute altitude, cette orbite a l'avantage d'offrir une couverture importante de la terre (42%), ainsi avec seulement trois satellites il est possible de couvrir l'ensemble de la planète. L'application principale des satellites GEO est la diffusion unidirectionnelle. Cette orbite a cependant des inconvénients. Le principal étant le délai de transmission. En effet un aller-retour Terre->satellite->Terre peut durer de 0.25 à 0.50 s. => Cette orbite est mal adaptée aux applications téléphoniques. Le deuxième inconvénient, dû à la distance, est que les satellites doivent être de forte puissance (donc de grosse dimension). Cela implique que l'on ne pourra pas utiliser n'importe quel type de lanceurs, cela reviendra donc plus cher.

- Orbite moyenne ou MEO (Medium Earth Orbit), altitude 10 000 à 20 000 Km
- Orbite basse ou LEO (Low Earth Orbite), altitude 700 à 1 500 Km Les satellites LEO sont séparés en trois catégories, selon leur fréquence :"Little LEO " (800 Mhz),"Big LEO " (2 Ghz) et"Broadband LEO " (large bande, de 20 à 30 Ghz). Les"little LEO " délivreront des messages, feront du pagging et de

la localisation de véhicule (similaire au GPS). Les"Big LEO ", quant à eux, transmettront la voix dans les régions qui ne sont pas couvertes par des réseaux cellulaires ou terrestres. Ils délivreront également des données à faibles débits. A l'inverse, les"Broadband LEO " (LEO à large bande) pourront transmettre des données jusqu'à 155 Mbits/s

Le principal inconvénient des GEO et le temps de transmission. Les satellites en orbites LEO et MEO ne souffrent pas de ces ralentissements. Comme ces satellites sont plus près de la terre, les temps de propagation sont plus courts : respectivement 0,05 seconde et 0,1 seconde. Le deuxième avantage de ces orbites est que le signal reçu est plus fort. Cela signifie que les terminaux de réception sont de plus en plus petits. Ces satellites sont également de plus petite taille, ils coûtent donc moins cher à lancer. Le principal inconvénient de cet orbite est qu'il faut placer beaucoup plus de satellites afin de couvrir l'ensemble de la planète. La durée de vie de ces satellites est également beaucoup plus faible (4 à 5 ans contre 7 à 10 ans pour les GEO).

Tableau récapitulatif :

| | GEO | MEO | LEO |
|---|---|---|---|
| Altitude (Km) | 36 000 | 10 000 à 20 000 | 700 à 1 500 |
| Délai (sec) | 0,25 à 0,50 | 0,1 | 0,05 |
| Vitesse | > 155 Mbits/s | 9,6 Kbits/s à 38,4 Kbits/s | 2,4 Kbits/s à 9,6 Kbits/s (Little LEO)<br>2,4 Kbits/s à 300 Kbits/s (Big LEO)<br>16 Kbits/s à 155 Mbits/s (Broadband LEO) |
| Avantages | - Couverture importante<br>- Haut débit | - Temps de propagation faible<br>- Adapté à tout type de service<br>- Coût des satellites plus faible | |
| Inconvénient | - Temps de propagation Importants<br>- Nécessite une forte puissance d'émission | - Nécessite de nombreux satellites (couverture)<br>- Durée de vie plus faible que GEO | |

**Ordonnanceur de paquets -** Fonction du contrôle de trafic qui assure la qualité de service pour chaque flot de données conformément à des modèles de services préalablement définis.

**OSI -** (Open System Interconnection = Interconnexion de systèmes ouverts) - Modèle de référence en couches destiné à fournir un cadre conceptuel et normatif aux échanges entre systèmes hétérogènes. Ensemble de normes permettant la communication entre systèmes hétérogènes. Le modèle OSI s'appuie sur sept couches : physique, liaison de données, réseau, transport, session, présentation et application. Chaque couche assure une fonction à l'aide de protocoles. Elle ne communique qu'avec la couche homologue d'un autre système et fournit à la couche supérieure des "services" à travers une interface. Il peut exister à l'intérieur d'une couche plusieurs "classes" de services selon les besoins. Le modèle comporte 7 couches allant du niveau le plus proche du niveau physique au niveau le plus logique.

Les 7 couches sont les suivantes:

Couche 1. Physique : elle comporte tout ce qui concerne l'établissement de la liaison : caractéristiques mécaniques, électriques et fonctionnelles (*signaux*).Elle ne s'occupe que de faire passer un train de bits sur le média. L'interface est un exemple typique du contenu de la couche physique.

Couche 2. Liaison de données : elle permet le transfert sans erreur entre deux éléments de réseaux directement connectés. Elle ne considère donc plus la transmission comme un signal électrique, mais comme un train organisé de données.

Couche 3. Réseau : elle concerne l'acheminement des informations au travers du réseau, y compris éventuellement au travers des nœuds intermédiaires. Elle est donc inséparable de la notion de routage.

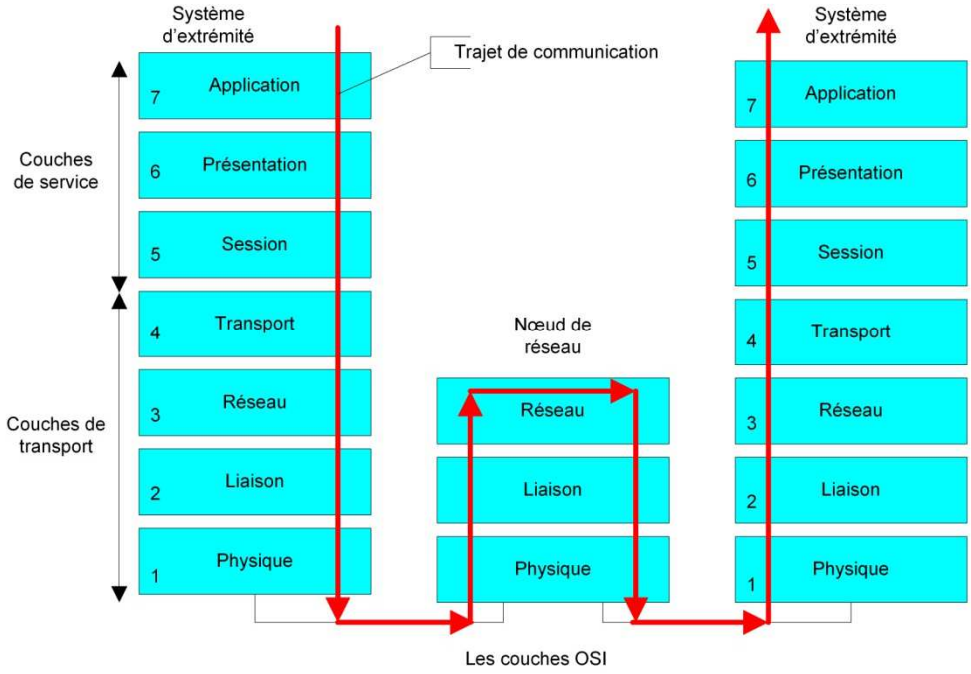
Couche 4. Transport : elle met en œuvre les règles pour qu'une communication de bout en bout s'établisse. Autrement dit, elle gère la reconnaissance mutuelle des extrémités.

Couche 5. Session : elle définit l'organisation des échanges et la structure du dialogue. Elle traite donc surtout de la synchronisation et des séquences de l'échange.

Couche 6. Présentation : elle définit la présentation des informations, en fonction d'une syntaxe et d'un

vocabulaire effectivement communs à l'émetteur et au récepteur. Elle se préoccupe en particulier de la compatibilité des codes (*ASCII, EBCDIC*).

Couche 7. Application : elle définit des mécanismes communs aux deux processus utilisateurs. Elle joue le rôle d'interface entre l'utilisateur et le monde ISO. La couche 7 ne contient pas les applications ou les programmes de l'utilisateur, mais seulement quelques processus et règles en général nécessaires pour faciliter le travail communicant de ces applications. Elle sert donc plutôt d'intermédiaire entre les autres couches et les applications de l'utilisateur.




OSI est "le" modèle de communication de référence universel qui définit les règles d'un langage commun pour que deux machines puissent s'échanger des données.

Mis au point dans les années 80 par l'organisme de standardisation international, l'ISO, et approuvé par l'IUT -TU (qui s'appelait à l'époque le CCITT), le modèle OSI continue de faire figure de référence en tant que modèle d'interconnexion, mérite s'il est quelque peu éclipsé aujourd'hui par le modèle TCP/IP à deux couches.

Le modèle OSI découpe la communication entre deux équipements informatiques en sept couches indépendantes depuis la couche physique jusqu'à celle réservée à l'application. Entre les deux, en remontant vers la couche application, on trouve, dans l'ordre, les couches liaison, réseau, transport, session et présentation.

Le principe de fonctionnement de ce modèle est le suivant: la communication est initiée à partir de la couche application d'un équipement par le lancement d'une application en direction d'un équipement distant. Il peut s'agir, par exemple, de lancer un transfert de fichier, d'envoyer un message électronique, voire d'accéder à une base de données distantes. Quel que soit l'applicatif, la communication traverse alors les couches du premier équipement en descendant jusqu'à la couche physique de celui-ci. Là, de nœud en nœud, elle suit son chemin jusqu'au support de liaison connecté au deuxième équipement dont elle remonte les sept couches en sens inverse. Il s'agit d'une relation biunivoque entre les deux équipements, la communication de l'équipement A vers B se faisant de façon identique dans le sens inverse.

Lorsque la communication descend les couches du premier équipement et remonte celles du deuxième, chaque couche joue le rôle de prestataire de services pour la couche qui lui est directement supérieure. et seulement celle-là. Elle fournit ces services à travers des SAP (Service Access Point). Ainsi, la couche présentation, immédiatement en dessous de la couche application, joue pour celle-ci le rôle de traducteur. En clair, elle s'occupe de mettre en ordre les données reçues de l'application selon une syntaxe et un vocabulaire bien définis et communs à l'émetteur et au récepteur. Outre cette mise en forme des données, la couche présentation offre aussi des services de sécurité tels que l'encryptage.

Une fois l'opération de présentation terminée, la communication descend d'un cran au niveau de la couche session. C'est là, que le dialogue entre les deux équipements est véritablement initialisé. Les mécanismes de synchronisation sont activés à ce niveau ainsi que les séquences de l'échange (détection et reprise en cas d'erreurs, règlement des conflits de priorité, etc.). Cette étape franchie, la communication est prête pour le transport, la couche transport se situant juste avant l'infrastructure de réseau. C'est à ce niveau que tout est mis en œuvre, par le biais de cinq classes de services, pour veiller à établir la communication de bout en bout. Les opérations de multiplexage, de démultiplexage, de récupération des erreurs, de contrôle de flux, de séquencement des messages, par exemple, se font à ce niveau. Tout est alors prêt pour passer aux

opérations d'adressage et de routage réalisées au niveau de la couche réseau. C'est au niveau de la couche réseau que l'on trouve les références nécessaires pour organiser une interconnexion de réseaux locaux ou la mise en place d'une infrastructure de réseau local virtuel. C'est aussi au niveau de cette couche réseau que sont mis en œuvre les protocoles de type X25 et relais de trames.

À ce stade, la descente en cascade des couches est presque terminée. Deux couches restent à franchir avant d'atteindre le câble physique de télécommunication. La couche liaison d'abord, puis la couche physique.

La couche liaison propose trois services à la couche 3 (réseau) qui lui est immédiatement supérieure: un service de datagramme sans acquittement, un service orienté connexion et un service datagramme avec acquittement. Cette couche est aussi appelée LLC (pour Logical Link Control). Elle permet le transfert de données sans erreur entre les deux équipements en réalisant des opérations telles que la mise en paquets ou trames, la détection des erreurs et la réémission éventuelle de la communication.

Une lois ces opérations terminées, les données sont prêtes pour être transmises à l'équipement destinataire, ce que se charge de faire la couche physique en fournissant les moyens mécaniques, électriques et fonctionnels pour déclencher, maintenir et désactiver les connexions physiques.

Au fond, la mécanique du modèle de communication OSI est relativement simple: chaque couche fournit des services à la couche supérieure. Elle ne peut dialoguer qu'avec une couche strictement équivalente. En d'autres termes, entre deux équipements A et B, la couche session de A ne peut dialoguer qu'avec la couche session de B. Et pour cela, l'information doit descendre la chaîne jusqu'au niveau physique de A, les niveaux équivalents de B décodant les trames qui les concernent au fur et à mesure de leur remontée dans les sept couches.

**OSITOP -** Open Systems Interconnection Technical and Office Protocol - Association formée à l'origine d'utilisateurs européens de Top, aujourd'hui consacrée à la promotion d'une architecture complète, et opérationnelle et à son évolution dans le cadre officiel du modèle OSI (Open System Interconnect).

**OSPF -** Open Shortest Path First - Protocole de routage du chemin le plus court. OSPF est un protocole de routage d'état de liaison. Grâce à l'algorithme SPF (Shortest Path First), chaque routeur calcule les informations de routage de façon autonome, sans utiliser les calculs des autres machines. Présenté comme le successeur de RIP, OSPF est plus avancé et mieux adapté aux réseaux de grande taille. C'est un protocole ouvert dont les spécifications sont publiques. OSPF utilise des datagrammes de petite taille. Ils n'ont donc pas besoin d'être fragmentés. Seul l'élément qui n'arrive pas à destination est retransmis (au contraire, lorsqu'on utilise des datagrammes fragmentés, en cas de perte, tous les fragments sont renvoyés). Le protocole permet le routage par type de service, ce qui signifie qu'il est possible d'imposer des routes différentes en fonction de la nature des données transmises. Pour permettre ce routage particulier, l'en-tête des datagrammes comprend des informations sur le type de service.

Malgré ses qualités, OSPF ne peut assurer le routage si l'on souhaite faire de la multi diffusion. C'est pour cette raison qu'a été développé MOSPF (Multicast Open Shortest Path First), une extension d'OSPF qui permet le multicasting. MOSPF fonctionne à l'intérieur d'un système autonome. Pour l'utiliser sur Internet, il faut également un protocole de roulage Multicast autonome. Avec MOSPF, le routage ne se fait plus uniquement en fonction de la destination, mais également en fonction de la source. II s'agit de ce que l'on appelle du source-destination routing. MOSPF choisit toujours la route qui offre le coût le plus faible. Si deux chemins présentent des coûts identiques, un seul sera choisi, alors qu'OSPF, dans ce cas, répartit les données sur les différentes routes.

Dans le contexte de la multi diffusion, MOSPF utilise le "tronc commun" du réseau le plus longtemps possible, puis duplique le datagramme lorsque les membres du groupe de discussion sont sur des réseaux différents. Comme OSPF, MOSPF peut déterminer le chemin en fonction du type de données transmises. MOSPF possède quelques limites: il ne fonctionne que dans un seul système autonome, on ne peut pas l'utiliser dans de très grands réseaux et il consomme beaucoup de puissance processeur, et ce, d'autant plus que le réseau est important. Des rouleurs OSPF et MOSPF peuvent cohabiter dans un même système autonome, bien que certaines configurations puissent occasionner des erreurs.

**OSS -** Operation System and Service - Sous-système d'exploitation et de maintenance - Réseaux Mobiles - L'administration du réseau consiste à contrôler les ressources du réseau afin de maintenir le niveau de service de façon optimale.

Les différentes fonctions d'administration sont définies par la norme GSM :

- Administration commerciale (déclaration des abonnés, mobiles, facturation).
- Gestion de la sécurité.
- Gestion de la charge du réseau.
- Contrôle de configuration du système (mises à jour).
- Maintenance.

Le système d'administration du GSM est proche du TMN ( Telecommunication Management Network)

**OTA -** Téléchargement en liaison radio (OTA = Over The Air).

**OTAN -** Organisation du Traité de l'Atlantique Nord

**Outsourcing -** Externalisation - Forme raccourcie de BPO - Externalisation d'une des fonctions de l'entreprise.

**Ouverture Numérique** - En Optique - Valeur qui correspond à la propriété d'une fibre à collecter la lumière pour la propager. Définie comme étant le sinus du demi angle du cône d'acceptance (appelé angle d'acceptance ou angle critique).

**OXC -** Optical Cross-Connect - Brasseurs Optiques - Les brasseurs sont des éléments primordiaux des réseaux de télécommunication actuels, qui permettent aux opérateurs de gérer leurs réseaux et d'atteindre une qualité de service (QoS) aux critères très rigoureux.

Dans le cas de réseaux optiques, la fonctionnalité de brasseur optique est indispensable. A la différence des OADM, un brasseur a plusieurs fibres d'entrée. Chaque entrée transportant des canaux WDM, et plusieurs fibres de sortie, transportant également des canaux WDM. Le brasseur doit connecter des signaux d'entrée et de sortie dans les domaines spatio-temporels. (voir Star Wars - Episodes I à VI)

# P

**PABX -** Private Automatic Branch Exchange - Expression anglo-saxonne pour désigner un autocommutateur privé d'entreprise, qu'on appelle plus couramment standard ou central téléphonique privé. Equipement de télécommunication effectuant de façon automatique l'aiguillage des communications.

**PAD -** Packet Assembler-Disassembler - Assembleur-Désassembleur de paquets. Equipement d'Accès aux réseaux de commutation de paquets, il adapte les terminaux fonctionnant en mode "caractère par caractère" pour les rendre compatibles à la norme X25.

**Pager -** Petit terminal portatif muni d'un écran à cristaux liquides pouvant recevoir de courts messages émis par un service de radiomessagerie (comme Alphapage ou Operator en France).

**Paging -** Désigne en anglais les systèmes de radiomessagerie par voie hertzienne.

**Paire téléphonique -** Ensemble de deux fils de cuivre utilisé pour une liaison téléphonique. Equivalent de paire torsadée.

**Paire torsadée -** Canal de transmission formé de deux fils de cuivre gainés et torsadés l'un avec l'autre (pour éviter qu'un des deux fils soit plus exposé que l'autre à d'éventuelles perturbations électromagnétiques). Utilisée pour le câblage du téléphone dans les entreprises, la paire torsadée est devenue un médium très utilisé pour les réseaux locaux informatiques.

**PAL -** Phase Alternation Line - Norme de couleur, développée en Allemagne, à 625 lignes et 50 champs d'image par seconde. C'est le standard TV européen le plus répandu.

**PAN -** Personnal Area Network - Réseau Personnel - Réseau local sans fil créé par divers dispositifs sans fil et qui s'étend sur la zone de travail au bureau ou au domicile.

**Panier de consommation -** Outil statistique d'observation du marché qui permet de déterminer, à consommation constante, l'évolution de la facture moyenne des utilisateurs. L'Autorité a établi deux paniers de consommation pour observer l'évolution moyenne annuelle des tarifs téléphoniques.

**Panneau de Brassage -** Panneau permettant de réunir et brasser les paires torsadées et les fils optiques (format standard 19").

**PAP -** Password Authentication Protocol - Protocole d'authentification permettant à des postes PPP de s'authentifier les uns auprès des autres. Le routeur distant qui effectue une tentative de connexion sur le routeur local doit envoyer une requête d'authentification. Contrairement à CHAP, PAP ne crypte pas le mot de passe et le nom d'hôte ou d'utilisateur. PAP détermine si un mot de passe est valide ou non.

Protocole d'authentification par mot de passe. Le principe du protocole PAP consiste à envoyer l'identifiant et le mot de passe en clair à travers le réseau. Si le mot de passe correspond, alors l'accès est autorisé. Ainsi, le protocole PAP n'est utilisé en pratique qu'à travers un réseau sécurisé.

**Paquet -** Ensemble d'informations de taille généralement fixe véhiculé comme une entité minimale dans un réseau à commutation de paquets ou un réseau local. Le paquet comporte les informations à transmettre encadrées par des messages de service (identification, adresses de l'expéditeur et du destinataire...). Ensemble de données qui représente l'unité de base des données sur un réseau. Exemple: un paquet IP.

**Paquet par paquet -** Packet by Packet - Technique de commutation qui à chaque fois qu'elle reçoit un paquet l'analyse afin d'en tirer son adresse de destination avant de le transmettre. Avec cette technique un commutateur de niveau 3 utilise les protocoles de routage standard exactement comme le fait un rouleur classique.

**Paradiaphonie ou Diaphonie -** Précise l'affaiblissement d'un signal parasite transmis d'une paire vers les autres paires d'un même câble (se mesure en dB), Near End Cross Talk. Voir Diaphonie

**Parallèle -** Mode de transmission où l'on dispose d'autant de canaux que de bits à transmettre (par opposition à série, où les bits sont transmis successivement sur un seul canal). S'utilise dans les équipements informatiques et les périphériques, rarement dans les télécommunications.

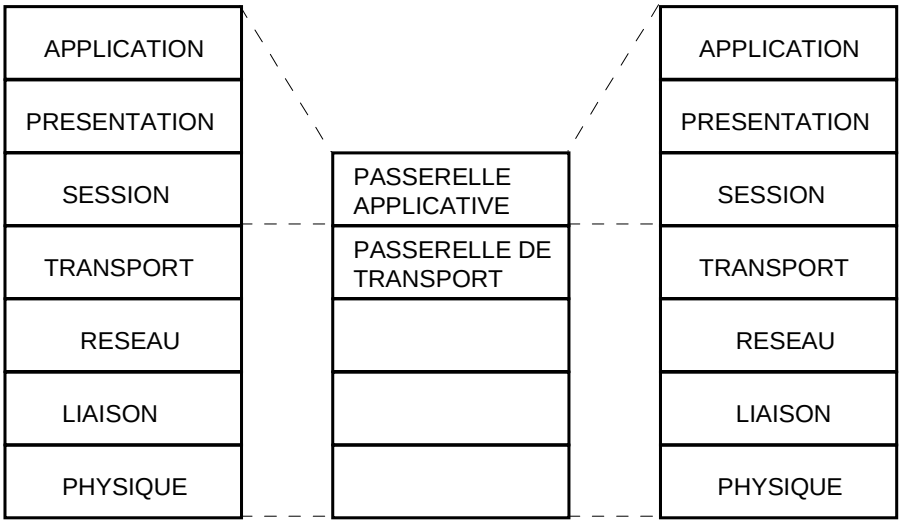
Mode de transmission généralement unidirectionnelle dans lequel les données sont émises simultanément sur des lignes séparées.

**Pare-feu -** Un pare-feu est un logiciel de protection ou un matériel qui protège un réseau interne sécurisé connecté à un réseau public (par exemple, à Internet) contre les virus, les pirates et autres données dangereuses. Voir FireWall.

**Parité -** Technique de détection d'erreurs, consistant à mettre à 1 (ou à 0 selon la convention adoptée) un bit supplémentaire dit de parité, selon que la somme des bits du message est paire ou non. On distingue la parité "verticale", qui s'ajoute à chaque mot ou octet, de la parité "longitudinale", qui concerne tous les bits de même position dans un bloc de données.

**Partie terminale -** Terminologie FTTH - Partie du réseau comprise entre le point de mutualisation et la prise terminale optique. La partie terminale est constituée par un ensemble de lignes.

**Passerelle -** Gateway - Une passerelle est un équipement très complexe et difficile à mettre en œuvre. On distingue deux types de passerelles : les passerelles de transport et les passerelles applicatives.




Equipement (logiciel et/ou matériel) permettant de transformer les conventions d'un réseau dans celles d'un autre réseau différent pour leur permettre de communiquer. Par comparaison avec le pont, qui ne fait que faire passer des informations d'un réseau vers un autre sans les adapter, la passerelle est un dispositif assez complexe qui doit adapter la syntaxe des informations. Dans le modèle OSI, une passerelle agit jusqu'au niveau 6 (Présentation), à la différence du pont, qui agit au niveau 2, et du routeur, qui agit au niveau 3.

Serveur relais utilisé par exemple pour protéger un serveur de messagerie (passerelle SMTP).

Une passerelle est une interface d'échange de données entre deux réseaux différents. La fonction de passerelle d'un système téléphonique sur IP, par exemple, traduit le protocole SIP en protocole ISDN et forme ainsi l'interface entre la Voix sur IP et la téléphonie classique.

**PAV -** Point d'Accès vidéotex - Variante de PAD (Assembleur-Désassembleur de paquets) spécialisée pour le réseau vidéotex français Télétel. Il concentre les communications des Minitel et sert de point d'entrée dans Transpac, réseau utilisé comme infrastructure de base de Télétel.

**PAVI -** Point d'Accès vidéotex Intermédiaire - Variante de PAD (Assembleur-Désassembleur de paquets) dérivée des autocommutateurs publics pour concentrer le trafic des Minitel vers le réseau de support Transpac. Ils sont progressivement remplacés par les PAV plus performants.

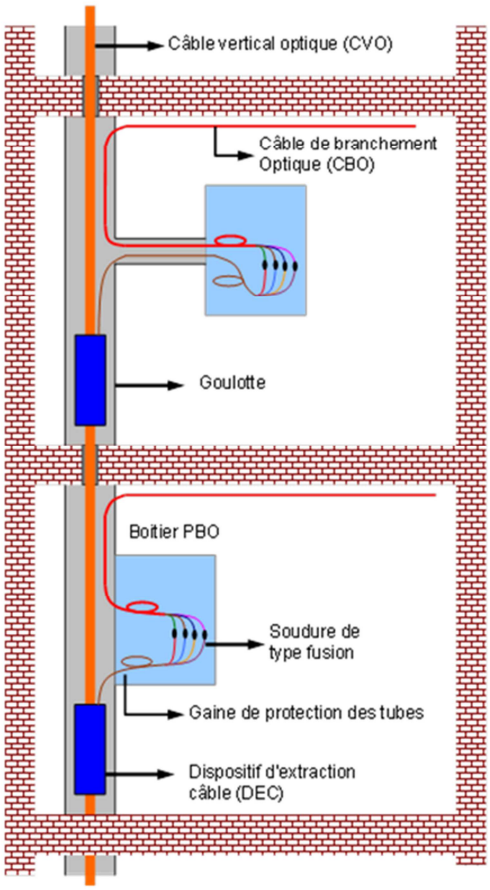
**Payload -** Charge utile - Partie utile d'un message, par opposition à la partie servant pour assurer la transmission.

**PBE -** Terminologie FTTH - voir PBO - Point de Brachement d'Etage.

**PBO - Terminologie FTTH -** Point de Branchement Optique - Appelé aussi PBE (Point de Branchement Etage) - Boitier dans le lequel sont raccordé(s) le ou les câbles en fibre optique venant du point de mutualisation et les câbles en fibre optique du raccordement client.

Ce terme désigne, dans les immeubles de plusieurs logements ou locaux à usage professionnel comprenant une colonne montante, un équipement généralement situé dans les boitiers d'étage de la colonne montante qui permet de raccorder le câblage vertical avec le câble de branchement.

Un PBO peut être situé dans les étages d'un immeuble ou à l'extérieur pour desservir plusieurs maisons ou petits immeubles.




Les raccordements des PTO sur le PBO

**PBX -** Private Branch Exchange - Désigne l'autocommutateur privé de l'entreprise utilisé pour la téléphonie analogique. Souvent confondu avec PABX (Private Automatic Branch Exchange), terme utilisé quand les PBX n'étaient pas automatiques.

**PC -** Point de concentration (dans le réseau de distribution).

**PCF -** Point Coordination Function - Applicable en WLAN, et complémentaire à la fonction de base de coordination distribuée (DCF), il y a la fonction optimale de coordination par point (PCF) qui peut être utilisée pour implémenter des services temps réel, comme la transmission de voix ou de vidéo. Cette PCF fait qu'on utilise des priorités supérieures que le Point d'Accès peut gagner en utilisant des temps inter-trames plus petit (PIFS).

En utilisant un accès par priorité supérieure, le Point d'Accès peut envoyer des données aux stations en réponse à un Polling Request, tout en contrôlant l'accès au support. Pour permettre aux stations classiques d'avoir accès au support, il y a une condition qui est que le Point d'Accès doit laisser suffisamment de temps DCF par rapport au PCF.

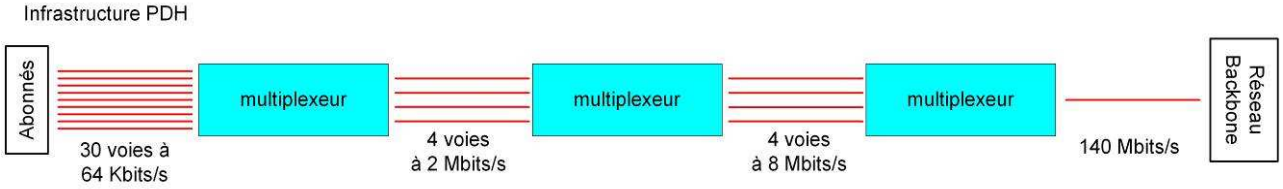
**PCN -** Personnal Communication Network - Réseau de radiotéléphonie conçu pour des terminaux légers, portables et capables d'émettre et de recevoir des appels. Un projet de norme sur ce concept plus léger que le GSM a été lancé en Grande-Bretagne pour compléter ce dernier. Il cherche à marier les avantages du CT2 et du GSM.

**PCS -** Personnal Communications Services - Un système de téléphonie mobile numérique principalement utilisé aux Etats-Unis et au Canada. La bande de fréquence utilisée par le PCS est le 1900 MHz.

**P-CSCF -** Proxy Call Session Control Fonction - Serveur permettant d'identifier les types d'appel entrants dans une architecture IMS. Voir IMS

**PCV -** Appel téléphonique payable à l'arrivée après autorisation de l'appelé (la signification du sigle a été perdue). Abandonné en France, mais encore utilisé aux Etats-Unis et dans de nombreux pays.

**PDH -** Plesiochronous Digital Hierarchy - Hiérarchie numérique plésiochrone - Système de transmission numérique presque synchrone.




C'est dans les années 70 que la transmission numérique a fait son apparition avec l'utilisation, sur les premières infrastructures de fibre optique, de la technologie PDH. Il s'agit d'un système de multiplexage hiérarchique et numérique à haut débit (140 Mbits/s) plésiochrone, du grec "plesiochronos ", c'est à dire "presque synchrone". Ce système est relativement complexe, en tout cas trop rigide pour permettre d'injecter et d'extraire du réseau des flux de très hauts débits (au dessus de 140 Mbits/s) tels que ceux associés à l'ATM.

Un réseau PDH fonctionne au travers de toute une batterie de multiplexeurs et démultiplexeurs disposés sur le réseau de façon hiérarchique en cascade, pour regrouper (multiplexer) puis dégrouper (démultiplexer) les canaux (terminaux) d'abonnés en respectant les intervalles de temps propres à chaque utilisateur.

Ainsi, le premier multiplexeur concentre trente voies d'abonnés à 64 Kbits/s sur un circuit à 2 Mbits/s, le deuxième réunit quatre de ces canaux sur une ligne de 8 Mbits/s, et ainsi de suite jusqu'à l'artère de 140 Mbits/s. (voir tableau ci-dessous). Et inversement pour restituer les flux à l'arrivée. En raison du nombre d'équipements requis pour le faire fonctionner, le système PDH est non seulement rigide, mais aussi coûteux. Son remplacement par le système SDH est en cours, mais les réseaux PDH restent pour l'instant majoritaires sur la carte mondiale des réseaux de transmission.

| Désignation des Multiplex | Ordre | Nombre de Voies Utiles | Nombre de Voies Totales | Débit Utile (Kbit/sec.) | Débit Total (Kbit/sec.) | Gamme |
|---|---|---|---|---|---|---|
| Débit de base | | 1 | 1 | 64 | 64 | X |
| TN1 | 1er | 30 | 32 | 1920 | 2048 | 2 Mbit/sec. |
| TN2 = 4TN1 | 2ème | 120 | 128 | 7680 | 8162 | 8 Mbit/sec. |
| TN3 = 4TN2 | 3ème | 480 | 512 | 30720 | 32768 | 34 Mbit/sec. |
| TN4 = 4TN3 | 4ème | 1920 | 2048 | 122880 | 131072 | 140 Mbit/sec. |

Le PDH trouve son origine dans le transport de signaux téléphoniques vocaux, convertis en canaux numériques à 64 Kbits/s suivant le théorème de Shannon qui souhaitait restituer la bande passante analogique de 3400 Hz de l'époque. Le signal numérique, défini sur 8 bits et échantillonné à une fréquence de 2 x 4000 Hz par seconde, se représente ainsi par un octet tous les 125 µs.

Pour transporter simultanément plusieurs voies téléphoniques les canaux à 64 Kbits/s sont regroupés. Le premier regroupement s'appelle multiplex de base, il est réalise en multiplexant temporellement les blocs de 8 bits de chacun des canaux considères, ce qui revient à les entrelacer.

On distingue deux grandes familles issues des multiplex de base. Il est réalise en Europe avec un débit de 2,048 Mbits/s qui réalise un groupement de 32 canaux (recommandation G.732) dont 30 utiles (plus 1 pour la synchronisation et 1 pour la signalisation quand il y en a). L'autre utilisé aux USA et au Japon, avec un débit de 1,544 Mbits par secondes qui regroupe 24 canaux (recommandation G.733).

Pour extraire un canal inférieur d'un multiplex, ou en injecter un, il faut démultiplexer, parfois plusieurs niveaux afin de retrouver le niveau hiérarchique du canal à extraire ; il est donc nécessaire de multiplexer de nouveaux plusieurs fois pour revenir au groupement d'origine.

**PDN -** Public Data Network - Désigne en anglais les réseaux publics de transmission de données.

**PDS -** Premises Distribution System - Système de précâblage mis au point par AT&T, principalement à base de paires torsadées.

**PEAP -** Protected EAP - Authentification à base de certificat pouvant être utilisée avec EAP.

**Peering -** Désigne un type d'accord d'interconnexion entre deux réseaux backbone IP qui s'échangent le trafic Internet à destination de leur réseau respectif. Ces échanges ont lieu au sein de nœuds d'échange publics ou privés.

Internet est composé de milliers de réseaux. Ce n'est pas un gros nuage, comme on se le représente généralement, mais en fait une multitude de "petits" nuages interconnectés. Tout fournisseur d'accès est ainsi à son tour connecté à un ou plusieurs de ces réseaux. Un peering est l'une de ces interconnexions entre réseaux, permettant aux opérateurs de s'échanger des droits de parcours.

Un grand nombre de points de peering est censé optimiser la connectivité d'un réseau en permettant à l'échange de s'effectuer au plus près de l'origine et de la destination, réduisant donc le nombre de "hops" et ainsi l'efficacité des connexions.

Le protocole standardisé BGP4 permet aux routeurs de chacun des opérateurs impliqués dans ces accords de peering, d'échanger les informations techniques nécessaires, avec gestion des AS (Autonomous Systems).

La gestion du peering et d'un protocole BGP est tout Sauf simple ! "Un grand nombre d'accords de peering n'est pas en soit ou encore une assurance de performances. En plus de backbones d'excellente qualité, il faut également s'assurer que les points de passage entre ces différents backbones sont d'une performance au moins équivalente, ce qui n'est pas toujours le cas. Il finit savoir que les accords de peering, qui sont de simples accords commerciaux entre les opérateurs. ne contiennent aucun engagement en terme de qualité.

La gestion de BGP requiert de solides compétences, réservées à un nombre limité de spécialistes réseau. Les conséquences d'une manipulation humaine erronée peuvent ainsi être lourdes de conséquences et impacter une partie importante du réseau Internet.

Equilibrer la charge entre les peering est délicat et totalement statique. Il faut retenir que la charge de gestion d'un peering croît en fonction du carré du nombre de participants. A titre d'exemple, passer de 2 à 4 échanges multipliera par 4 (et non par deux) la charge de travail.

**Périmètre de sécurité -** Périmètre dans lequel des contrôles de sécurité sont effectués afin de protéger les équipements réseau.

**Périmètre de prestation :** Description des composantes qui seront l'objet de prestations, et capacité d'évolutions mineures. Proposé par le fournisseur, le périmètre de prestation va permettre de mesurer la compréhension de la problématique"client " de la part du fournisseur, mais aussi d'estimer la corrélation entre besoin exprimé et réponse proposée. C'est une synthèse des besoins repris par le fournisseur.

La pertinence de la réponse du fournisseur est aussi directement liée à l'expression de besoins initiale.

Couverture :

- Les utilisateurs : Utilisateurs par typologie, Administrateurs,
- La volulétrie : Capacité initiale, Evolutivité
- Architecture proposée : Schéma général de l'architecture proposée incluant les différentes zones de sécurité et les serveurs, Environnements à héberger (production + si demandé l'environnement de pré production), Description et dimensionnement des flux de données (issues du dossier d'architecture transmis), Architectures des liaisons inter et intra (Normes et protocoles retenus, Réseaux locaux, Réseaux étendus, Filtrage / sécurité / isolation, Equilibrage de charge, Maintenance, Redondance)
- Dispositifs de sécurité : FireWall, Détection d'intrusion, Détection de virus
- Maintenance : Description des applications supportées par le fournisseur, Criticité retenue, Complexité, Maintenance
- Base de données : Type, Capacité, Evolutivité, Maintenance
- Volumétrie estimée des travaux d'exploitation : Reprise du dossier client et/ou dossier d'architecture, Architecture technique des systèmes applicatifs
- Type et nombre de serveurs (marque, modèle, OS, capacité processeurs, mémoire, disques, redondance partielle d'éléments ou redondance complète) détaillée par application. Type de sauvegardes et fréquence. Mutualisation des espaces disques en baie externe ou pas. (NAS, SAN ?) Si oui présentation.
- Description précise des équipements de sécurité : Marque, modèle, type, maintenance associée au matériel, maintenance associée au logiciel, redondance, capacité, fréquence des mises à jour.
- Description de l'accès Internet proposé : Mutualisé, Dédié, Opérateur interne et/ou externe, Routage associé, Capacité réservée, Adressage, Protocole de transport
- Description de l'accès au réseau du client,
- Respect des contraintes de raccordement au réseau d'entreprise du client : Forcément dédié, Opérateur interne et/ou externe, Routage associé, Capacité retenue, Protocole

Environnement de pré production :

- Si l'environnement de pré production doit différer de l'environnement de production, il devra faire l'objet d'une présentation complète et exhaustive. Dans le cas contraire, (environnement de pré production identique à environnement de production, seule la sécurisation des accès sera indiquée et qualifiée)
- Capacité d'hébergement d'équipements"client "
- Capacité du fournisseur à héberger des équipements clients (serveurs) dans des zones isolées et sécurisées.
- Description des paramètres d'infrastructure associés à l'hébergement de machines (résistance mécanique des planchers, capacité électrique fournie, capacité de refroidissement des climatiseurs ou échangeurs thermiques, isolement (grillage, cloison, murs béton vibré ?), sécurité physique, logique.) limites d'environnement, Redondance des différentes fournitures, dimension des ouvertures et quai de chargement/déchargement, monte charge direct, etc etc…

Outils et méthodes de l'entreprise

- Capacité du fournisseur à s'adapter aux référentiels du client
- Langue de travail pour les documentations liées aux prestations.
- Evolutions prévues
- Calendrier prévisionnel des mises en productions

…

**Période -** Temps entre deux événements dans un processus cyclique (onde).

**Perte** - Voir Affaiblissement - Perte d'amplitude du signal à travers les lignes et les équipements de transmission. Valeur exprimée en décibels. Terme quantitatif qualifiant l'affaiblissement d'une ligne.

**Pertes -** En Optique - En transmission optique, on mesure les pertes selon leur origine :

- Pertes par par absorption (voir Absorption)
- Pertes par courbures ( Bending Losses) - Phénomène induit par les courbures des câbles prises pour franchir des obstacles mais également par le positionnement de la fibre elle-même à l'intérieur du câble. Typiquement: Rmin courbure = 45 mm pour une multimode et 20 mm pour une monomode. **-**
- Pertes par diffusion: voir Diffusion de Rayleigh.
- Pertes par micro courbures - dans le cas où une fibre est câblée, il peut y avoir contrainte physique entre la fibre et les éléments constitutifs du câble, qui peut entraîner des micro courbures. Par micro courbures, on entend une perturbation géométrique de faible amplitude mais qui se répète le long de la fibre avec une période de quelques millimètres. Cette perturbation change l'angle de propagation de la lumière et provoque des couplages de modes c'est-à-dire des transferts d'énergie entre modes qui peuvent alors induire des pertes d'énergie pour les modes d'ordre élevé. La sensibilité d'une fibre aux micro courbures est principalement fonction des diamètres de coeur et de gaine ainsi que de son profil d'indice.
- Pertes de Fresnel - Dans un connecteur, une épissure mécanique, certains coupleurs, et d'une façon générale lors de tout passage d'un dioptre se produit non seulement un phénomène de réfraction de la lumière mais également un phénomène de réflexion sur le dioptre entraînant la perte pour la transmission de l'énergie correspondante.

**PGI -** Progiciel de Gestion Intégré - En Anglais = ERP - Logiciel global visant à couvrir l'ensemble du système d'information d'une société.

**PGP -** Pretty Good Privacy - Implantation du système de chiffrement RSA mise sur l'Internet par Philip Zimerman, ce qui a valu à ce dernier pas mal de problème, car PGP est de qualité militaire, or le gouvernement interdit l'exportation de ce genre de système. Qui plus est, RSA, qui a été développé sur des fonds publics, est breveté, et la licence exclusive appartient à une société privée.

**Phase -** Un des trois éléments définissant une onde, avec son amplitude (grandeur des variations), sa fréquence (nombre de variations par seconde). Elle tient compte du décalage dans le temps par rapport à une origine ou à événement extérieur.

**Photon -** Particule élémentaire, quantum d'énergie d'un champ électromagnétique.

**Photonique -** Discipline regroupant les techniques qui utilisent des photons comme support de l'information.

**Phreaker -** Celui qui pirate les lignes téléphoniques (GSM, cabines) pour téléphoner à moindre frais.

**Physique -** Niveau I du modèle OSI où se trouvent tous les mécanismes physiques (mécaniques, électriques, de codage) pour établir la connexion.

**Physique (ATM) -** La couche physique, définie dans la recommandation I. 432, est applicable à l'interface UNI ( User-Network Interface ). Le support souhaité est la fibre optique bien que depuis les supports électriques ont également été normalisés.

La couche physique est responsable du transport correct de cellules et de la remise, aux couches supérieures, d'information de synchronisation afin de permettre des services tels que l'émulation de circuit.

La couche physique est divisée en deux sous-couches afin de supporter plusieurs médias différents tout en offrant toujours le même service à la couche ATM :

- La sous-couche PM (Physical Medium) dépend du support de transmission utilisé. Elle assure principalement les fonctions de synchronisation de bit et d'accès au support. L'unité de données échangée entre les deux sous-couches est constituée d'un flot d'octets associé à des information de synchronisation. Cette sous-couche est responsable de la transmission et de la réception correcte des bits sur le support. Elle assure principalement la synchronisation en réception ainsi que les fonctions dépendantes du support (support de type optique ou électrique). L'émetteur est tenu d'insérer des bits de synchronisation et d'assurer le bon codage de l'information.
- La sous-couche TC (Transmission Convergence) présente à la couche ATM un service uniforme indépendamment du support de transmission utilisé. Elle assure les fonctions d'adaptation du débit, de génération de la séquence utilisée. Elle assure les fonctions d'adaptation du débit, de génération de la séquence de contrôle HEC portant sur l'en-tête, de délimitation des cellules, l'adaptation de trame et de génération/réception des trames. A ce niveau, les bits sont déjà reconnus puisqu'ils proviennent de la couche PM. La sous-couche TC réalise cinq fonctions:

- La génération/réception de la trame de transmission,
- L'adaptation du flux ATM au système de transmission,
- La délimitation (ou cadrage) des cellules,
- La génération/vérification de HEC (Header Error Control),
- L'adaptation du débit cellule.

Les deux première fonctions permettent d'adapter le flux de cellules ATM au format utilisé par le système de transmission utilisé dans le réseau de transmission (PDH, SDH, mode cellule). Les autres fonctions sont identiques quel que soit le système de transmission.

**PictBridge -** Technologie adoptée par de nombreux constructeurs permettant d'imprimer des images directement depuis un appareil photo numérique sans passer par un ordinateur, en reliant l'appareil photo à l'imprimante en direct, au travers d'une liaison de type USB. Le port USB sur l'imprimante est "dédié", le câble USB pouvant pour sa part être spécifique.

**Piggyback -** Littéralement "sur le dos du cochon" - Désigne une procédure dans laquelle l'acquittement (avis de bonne réception) d'un bloc de données est transmis en même temps que le bloc de données suivant dans une liaison duplex. Données et acquittement font ainsi partie du même bloc. Cela évite d'avoir à envoyer des blocs utilisés uniquement pour l'acquittement, et optimise le débit global.

**Pigtail -** Câble en fibre optique servant pour les raccords optiques dont l'une des deux extrémités est munie de connecteurs (voir fibre pré connectorisé). Un pigtail est une demi-jarretière.

**PIM - Protocol Indépendant Multicast -** Protocole capable de fonctionner avec n'importe quel protocole de routage standard afin de faire transiter un flux IP multicast (vidéo, multimédia. . .). voir Multicast.

- PIM DM (Protocol Independent Multicast Dense Mode) -

Protocole développé par CISCO - Indépendant de tout protocole, il supporte tous les protocoles de routage Unicast : Statique, RIP, IGRP, EIGRP, IS-IS, BGP et OSPF. PIM utilise le Reverse Path Forwarding pour la propagation dans le réseau et l'élagage basé sur l'information d'appartenance à un groupe.

C'est un protocole de routage Multicast plutôt approprié aux petites implémentations et aux réseaux pilotes.

Le protocole de routage PIM Dense Mode est plus efficace pour les distributions denses de récepteurs Multicast, facile à configurer (2 commandes), il utilise un mécanisme simple de propagation et d'élagage, ce qui induit une certaine facilité à le comprendre et à le debugger.

Problèmes potentiels : Propagation et élagage sur le WAN, pas de support pour les arbres partagés.

- PIM SM (Protocol Independent Multicast Sparse mode)

Protocole développé par CISCO, mode clairsemé (RFC 2362 - v2) - Supporte les arbres sources et partagés, utilise un Point de Rendez-vous (RP). Les sources s'enregistrent auprès du RP et envoient les données aux récepteurs connus via ce RP.

PIM SM est approprié pour les déploiements à large échelle pour groupe à faible ou forte densité, où il est très efficace. C'est le choix optimal pour les groupes clairsemés avec peu de récepteurs, surtout si les récepteurs sont séparés par des liaisons WAN coûteuses. Le trafic n'est envoyé que sur les branches depuis lesquelles on a reçu une demande (Join), on peut commuter dynamiquement sur les arbres source optimaux pour les sources à fort trafic. Indépendant de tout protocole, il supporte tous les protocoles de routage Unicast : Statique, RIP, IGRP, EIGRP, IS-IS, BGP et OSPF, il offre aussi de bonnes bases pour les protocoles de routage Multicast inter-domaine.

- PIM SDM (Protocol Independent Multicast Sparse Dense Mode)

Protocole développé par CISCO, mode clairsemé Dense - PIM utilise le Reverse Path Forwarding pour la propagation dans le réseau et l'élagage basé sur l'information d'appartenance à un groupe, il supporte les arbres sources et partagés, utilise un Point de Rendez-vous (RP). Les sources s'enregistrent auprès du RP et envoient les données aux récepteurs connus via ce RP.

PIM Sparse Dense fonctionne en mode Dense pour les groupes Multicast sans Point de rendez-vous actif et en mode Sparse pour les groupes avec Point de Rendez-vous actif.

Ce mixte est recommandé pour les déploiements initiaux, à utiliser d'abord sans RP (mode Dense), il suffit ensuite d'ajouter des RPs pour basculer en mode Sparse.

**PIMF -** Terme allemand servant à définir les câbles multipaires avec écran par paire et blindage général.

**PIN -** Personnal Identification Number - Code d'accès, de 4 à 8 chiffres, qui verrouille l'accès et l'utilisation du téléphone mobile. Dans le contexte des appareils mobiles, le PIN est un code d'identification personnelle utilisé avec une carte SIM afin de pouvoir effectuer un appel ou une transmission de données. Le fournisseur de service peut également avoir besoin du code PIN pour les appels sortants dans un souci de protection contre la fraude. Voir également SIM.

**Ping -** Commande permettant de déterminer la présence et l'état de fonctionnement d'un autre système.

**Ping of Death -** Ping de la mort - Attaque par interruption de service (DoS) consistant en l'envoi d'un paquet Ping de taille surdimensionnée, dans le but d'entraîner le blocage de la machine réceptrice lors de la tentative de réassemblage du paquet de données surdimensionné.

**Pivot -** Nœud concentrateur, hub, hub station - Station qui assure la coordination d'un groupe de stations ou de sous-réseaux, ainsi que leurs accès éventuels à d'autres réseaux.

**Pixel -** Contraction de l'anglais picture element. Désigne un point élémentaire dans une image numérisée. Un pixel peut être représenté par un seul bit (noir ou blanc) mais plus souvent par 8, 16, voire même parfois 32 bits (couleur, texture, transparence, ...).

Désigne le plus petit élément d'une surface de détection, d'une image échantillonnée ou d'une surface de visualisation, auquel on puisse affecter individuellement des caractéristiques visuelles.

**PKI -** Public Key Infrastructure - Infrastructure de gestion de clés offrant un environnement sûr et fiable - Architecture globale de sécurité permettant d'intégrer et de gérer les technologies de chiffrement et de signature électronique dans le système d'information.

Les PKI, aussi appelées infrastructures à clés publiques (ou encore ICP) sont un ensemble d'éléments nécessaires pour pouvoir émettre des certificats numériques à une population et permettre leur administration (révocation, renouvellement, suspension,…). Cette infrastructure gère la production et la distribution des paires de clés publiques et privées, diffuse les clés publiques et protège les clés privées.

Une infrastructure comprend :

- une autorité de certification
- un annuaire de certificats
- un système de révocation de certificats
- un système de sauvegarde et de récupération de clés
- un soutien à la non répudiation
- une mise à jour automatique des clés
- une gestion de l'historique des clés
- un logiciel client interagissant de manière fiable et continue avec tout ce qui est présenté ci-dessus

Il existe plusieurs types de PKI, la plupart développées par un groupe de travail de l'IETF :

- PKIX (Public Key Infrastructure X509), groupe de travail IETF crée en 1995. Le but de ce groupe de travail est de mettre en place une PKI basée sur les certificats X509 utilisable sur Internet. L'infrastructure développée par ce groupe de travail est nommée IPKI (Internet Public Key Infrastructure).
- SPKI (Simple Key Infrastructure), groupe de travail IETF crée en 1996. Le but de ce groupe est de définir une infrastructure à clé publique et un format de certificat propre à l'IETF, qui soit simple et adapté à l'ensemble des applications Internet.
- DNSSEC (Domain Name System Security) est l'extension du DNS pour fournir des services de sécurité. Ce projet est réalisé par un groupe de travail de l'IETF, et transforme un DNS en PKI.
- PKCS (Public Key Cryptography Standard) est une syntaxe développée par RSA qui est devenue un standard de facto. Il existe de nombreux documents PKCS (PKCS # [09]+) définissant les méthodes de cryptage, le format des certificats…

Les PKI peuvent être utilisées dans différents types d'applications, comme les courriers électroniques sécurisés, le Web, les VPN, et bien sûr le commerce électronique. Une PKI ne s'achète pas mais se construit, avec des composants logiciels et matériels, et des services.

**Plan Câble (France) -** Ce terme désigne le plan gouvernemental introduit par la loi n°82-652 du 29 juillet 1982 sur la communication audiovisuelle qui visait au développement des réseaux câblés audiovisuels en France.

**Plan de numérotation -** Numbering Plan - Ensemble des règles permettant d'attribuer à chaque abonné d'un réseau un numéro d'appel.

**Planification des Réseaux de Télécommunications** - Télécommunication Network Planning - Ensemble des moyens mis en œuvre pour prévoir l'évolution de la demande en raccordement d'abonnés, le volume du trafic induit par catégorie d'abonnés, les équipements nécessaires à son acheminement dans des conditions de sécurité et avec une qualité de service défini.

**Plaque ADSL -** Ensemble des DSLAM et des BAS d'une même région.

**PLMN -** Public Land Mobile Network. Réseau GSM d'un opérateur.

**PLRP -** Adaptation propriétaire du standard de CPL domestique (Home-Plug) permettant d'augmenter significativement le débit théorique de 14 Mbit/seconde à 85 Mbit/seconde, de tripler la portée (de 200 mètres à 600 mètres) et de réaliser des réseaux locaux de 225 connexions (au lieu de 16) moyennant la mise en œuvre de répéteurs.

**PLT -** Power Line Telecommunications - Cette technologie existe soit en réseau d'Accès (pour couvrir les dernières centaines mètres entre le transformateur basse tension - moyenne tension de 220 V et les différents domiciles), soit au niveau résidentiel, où l'on effectue des transferts à l'intérieur d'une habitation entre une prise de courant et une autre.

Cette dernière solution intéresse particulièrement les industriels. En moyenne, les habitations sont équipées de 30 prises de courant. Il s'agit de faire communiquer entre eux des ordinateurs, où n'importe quel appareil ménager. Techniquement, on superpose un signal radio très haut en fréquence (entre 1,6 et 30 MHz) sur la ligne électrique. En prenant un modem autonome, on entre d'un côté en USB ou 10baseT, puis on ressort sur une autre prise de courant, ailleurs dans la maison, sur un autre modem du même type. Cette solution est très simple : le modem est acheté en grande surface, cela évite d'ajouter un câble supplémentaire, de faire des travaux ou de faire intervenir du personnel qualifié.

Le problème qui existe actuellement est purement réglementaire : les normes européennes ne sont pas encore finies et sont en cours de discussion au sein de l'ETSI et du PLT Forum. La tâche est difficile car beaucoup d'acteurs demandent des précautions. Les militaires et radioamateurs sont contre l'utilisation de la bande de fréquence proposée actuellement. De plus, les bandes de services diffèrent d'un pays à un autre entre les différents réseaux de secours ou autre. Les câbles électriques ne sont pas blindés et rayonnent, ce qui pose un problème de CEM et radio. Une norme doit donner une énergie pas trop réduite pour faire passer l'information, et pas trop haute pour éviter de rayonner. Actuellement, il y a des négociations en cours.

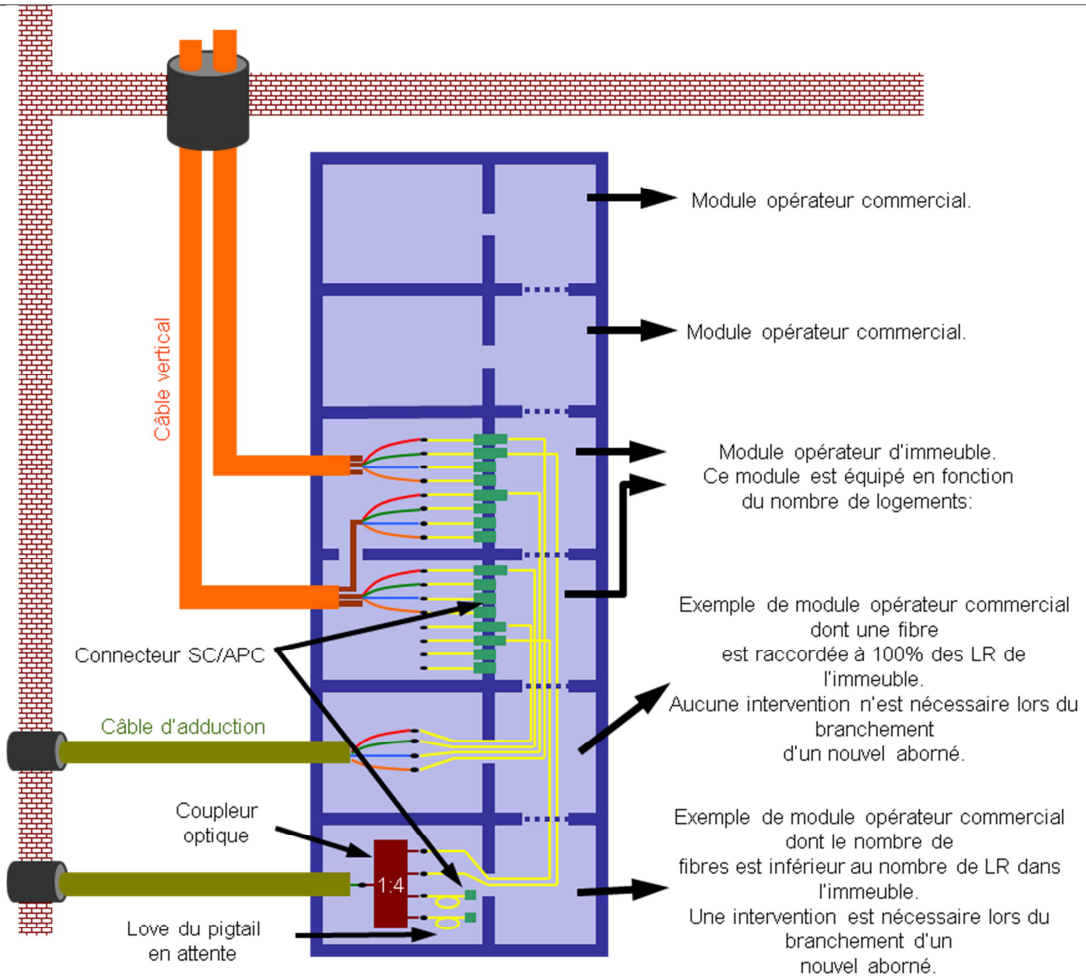
Les distances peuvent sembler courtes, mais dans une maison, les 50 mètres sont facilement atteints. Pour aller d'une chambre à une autre, dans les nouvelles maisons, les deux chambres sont généralement sur des fusibles différents et il faut donc faire 2 fois l'aller-retour, sans compter les quantités de tours de portes.

Dans ce domaine, on commence tout juste à éclaircir le problème de la qualité de service. Certains tests atteignent des débits de 7,5 Mbps net en IP (soit 13 Mbps en débit brut). Cependant, le débit chute parfois brutalement lorsque la ligne électrique n'est pas parfaite.

**Plug to plug -** Littéralement "prise à prise" - Désigne en anglais la parfaite interchangeabilité de deux équipements. Synonyme de compatible.

**PM -** Point de mutualisation - Terminologie FTTH - Endroit typique d'un réseau dans lequel il est possible de mutualiser tout ou partie du réseau de la zone arrière.

Um PM se présente très souvent sous la forme d'un boitier d'interconnexion dans lequel ou trouve tous les départs optiques vers les logements.




Les raccordements des Opérateurs dans le PM

Point d'extrémité d'une ou plusieurs lignes au niveau duquel la personne établissant ou ayant établi dans un immeuble bâti ou exploitant une ligne de communication électronique à très haut débit en fibre optique donne accès à des opérateurs à ces lignes en vue de fournir des services de communications électroniques aux utilisateurs finals correspondants, conformément à l'article L34-8-3 du code des postes et des communications électroniques.

**PMR - Professional Mobile Radio** - Réseaux radio mobiles professionnels (également appelés RRI) parmi lesquels on distingue notamment :

- 3RP : réseaux radioélectriques à ressources partagées.
- 3RPC : réseaux commerciaux mettant en œuvre la technologie 3RP
- RPN (radiocommunications mobiles professionnelles numériques) : réseaux fonctionnant en technologie numérique à la norme Tetra ou Tetrapol.
- 2RC : réseaux à usage partagé à relais commun.
- 3R2P : réseaux exploités pour les besoins propres de l'utilisateur mettant en œuvre la technologie 3RP.
- RPX : réseaux locaux à usage partagé (nouvelle catégorie de réseaux).

**PNNI -** Private Network Network Interface (ATM) - Protocole de routage qui introduit un support de la qualité de service, un routage à la source, le support de plusieurs niveaux hiérarchiques, la découverte automatique de la topologie du réseau.

Protocole de routage et de signalisation adapté aux réseaux ATM. Il définit les mécanismes de routage et signalisation entre noeuds du réseau (établissement, maintien et libération des circuits virtuels). Celui-ci simplifie les tâches relatives à la configuration de connexion selon des critères de qualité de service (QoS, Quality of Service).

Ce protocole intègre un jeu de métriques pour rendre compte des disponibilités et des capacités des liens.

Le protocole de signalisation PNNI est une extension de l'UNI V3.1 avec quelques fonctionnalités supplémentaires de l'UNI 4.0. qui sont incorporées (Extended QOS, VP Switching, classe de service ABR).

Le protocole de signalisation PNNI utilise l'information rassemblée par le protocole de routage PNNI (Métriques / Attributs ). La détermination du chemin à suivre pour relier un point à un autre se fait grâce aux informations d'accessibilité, de connectivité et de ressources disponibles.

Un réseau ATM PNNI est un ensemble de commutateurs ATM interconnectés. La structure hiérarchique des adresses ATM permet d'associer à une entité donnée un préfixe ATM reflétant l'organisation administrative des entités.

PNNI décrit comment chaque niveau opère, comment les noeuds d'un niveau sont vus du niveau supérieur, comment l'information est échangée entre les niveaux. C'est ainsi que chaque commutateur possède des informations détaillées sur son réseau local, et des informations abrégées sur les réseaux distants.

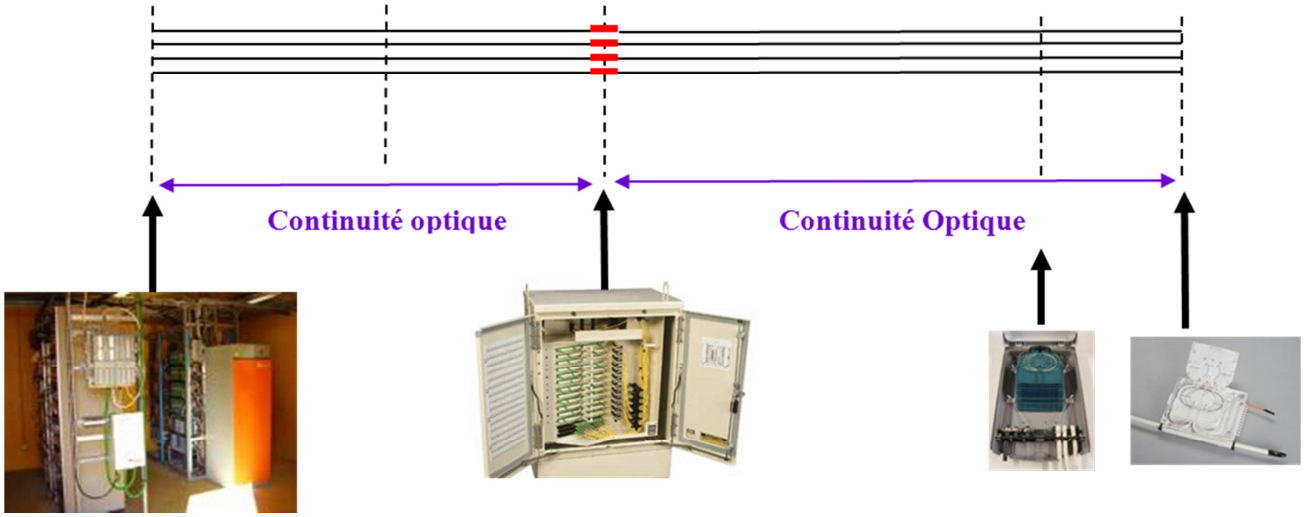
Les commutateurs du plus bas niveau hiérarchique sont identifiés par un préfixe de 13 octets. La définition des niveaux hiérarchiques génère une arborescence logique. Cette arborescence est en fait la structure de données manipulée par l'algorithme réparti qui implémente le protocole de routage PNNI qui propose une gestion hiérarchique.

PNNI est un protocole de routage à la source (Source Routing). Le routage par la source signifie que le chemin est défini par le premier noeud qui insère le chemin de routage dans la requête de signalisation. La détermination de la route est basée sur la connaissance de l'état du réseau et sur la QoS demandée. Les nœuds intermédiaires se contentent de faire du contrôle d'admission (CAC, Connection Admission Control) avant d'expédier la requête. Ce choix de routage par la source est fait car le routage de proche en proche type IP n'est pas acceptable car le commutateur courant devrait connaître l'ensemble de la QoS sur le réseau.

**Point d'accès -** Composant d'un réseau sans fil (ou Wi-Fi) qui assure l'interface entre le réseau et les clients sans fil qui s'y connectent. Il s'agit en fait de l'équipement électronique qui convertit le signal électrique du câble réseau en signal radio.

**Point à point -** Désigne une liaison ne connectant que deux équipements.

En FTTH, désigne une architecture en continuité optique de bout en bout par opposition à l'architecture en Arbre PON.




Une autre notion de base distingue les liaisons point à point des liaisons multipoints. Une transmission de données point-à-point ne met en relation à un moment donné qu'un seul émetteur et un seul récepteur. Au contraire, une liaison multipoint permet au même instant à un émetteur de transmettre vers plusieurs récepteurs. Il y a ainsi partage d'une partie des liaisons entre émetteurs et récepteurs. Si, dans une liaison multipoint, la transmission est unidirectionnelle, on parlera de diffusion (en anglais : Broadcast).

**Point de flexibilité -** Endroit (localisation, par construction, d'un point sur le réseau) sur le réseau sur lequel un opérateur peut effectuer une mise en correspondance entre les fibres de son réseau amont et celles situées en aval, par exemple pour des besoins d'adaptation (nouveaux bâtiments), d'optimisation de réseau (par l'allumage progressif de ses équipements actifs par exemple), ou des modifications d'architecture physique de câblage (point à point ou pooints à multipoint).

Le point de flexibilité peut être « en chambre de tirage » ou en armoire de rue. Il peut être connectorisé ou non.

**Polarisation orthogonale -** Technique qui permet d'isoler les cellules et de faciliter leur chevauchement en utilisant une polarisation horizontale sur une cellule et une polarisation verticale sur la cellule voisine.

**Politique de sécurité -** Ensemble de directives de haut niveau permettant de contrôler le déploiement des services réseau. La maintenance et l'audit du réseau font également partie de la politique de sécurité.

**Polling -** Scrutation - Désigne en général une méthode de transmission de données dans laquelle un équipement contrôle un certain nombre de terminaux par des "invitations à émettre" et des "invitations à recevoir".

**Polychlorure de vinyle - PVC -** Isolant issu de mélange de résines synthétiques, de charge et de plastifiant. Bonne résistance mécanique. Propriété électrique limitée en haute fréquence mais moyenne en haute tension. Ne propage pas la flamme.

**Polytethylène - PE -** Isolant primaire ayant d'excellentes propriétés électriques en haute fréquence et haute tension. Limité en température et transmet la flamme.

**PON -** Passive Optical Network. On distingue aujourd'hui plusieurs modes de distribution passive sur les réseaux de distribution optique :

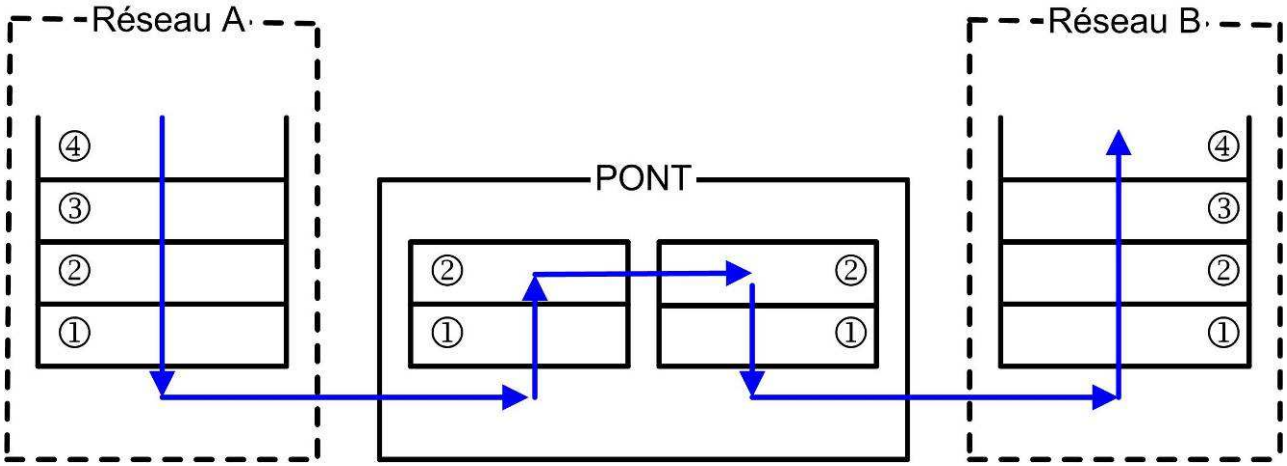
- Le mode APON (en .ATM),
- Le mode EPON (sous protocole Ethernet)
- Le mode BPON (large bande)
- Le Mode GPON (sous protocole GigaBit Ethernet)

Les industriels recherchent avec les exploitants à définir les meilleures solutions technico-économiques compte tenu des paramètres de débits et de distance.

Technologie de déploiement d'un réseau en fibre optique selon laquelle une fibre unique partant du NRO permet de desservir plusieurs logements (par exemple jusqu'à 64), par réplication du signal au niveau de coupleurs.

**Pont -** Le pont est le plus simple des dispositifs d'interconnexion, sa fonction n'étant que de faire passer des trames d'un réseau dans un autre. Intervenant au niveau 2 de l'OSI, il n'a donc qu'à lire l'adresse des trames qui lui parviennent et, en fonction des tables dont il dispose, décider soit de faire passer les trames qui doivent aller sur le second réseau, soit de les abandonner lorsqu'elles y sont déjà. Sa fonction est donc de filtrer ou de répéter. Le pont est indépendant des protocoles de réseaux locaux (*puisque tous les protocoles sont identiques à ce niveau et conforme à la norme OSI 802.2*). Il peut donc servir à interconnecter des réseaux locaux hétérogènes (*par exemple, un Ethernet avec un anneau à jeton*).

Ses principales utilisations : relier des réseaux locaux de type différent ou lier un réseau local à un site éloigné. Mais on y recourt aussi pour segmenter un réseau local, si l'on constate un trafic important entre certaines stations sur un réseau.




Les ponts font partie des équipements d'interconnexion de niveau 2 et possèdent au minimum 2 ports munis de Tranceivers ou de connecteurs AUI ayant une adresse physique chacun.

Ce type d'équipement, logiciel et matériel, assure une segmentation physique du réseau. Seul les paquets destinés à un équipement situé de l'autre côté du pont le traversent. Cela signifie que le trafic local entre 2 noeuds situés sur un segment "à gauche "d'un pont ne le traverse pas et n'encombre ainsi pas le segment

"de droite ". Le trafic est filtré, les collisions ne sont pas propagées.

Les ponts sont des équipements uniquement utilisés dans un environnement de réseaux locaux. Le pont est l'équipement d'interconnexion le plus ancien et le plus facile à mettre en oeuvre. La standardisation du pontage a été effectuée par l'IEEE (comité 802.1D) en 1990.

L'ISO a apporté en 1993 des ajouts à ce document en y ajoutant les différents modes de pontage. Le rôle principal d'un pont est de subdiviser un réseau unique en sous-réseaux afin d'accroître les performances, et de construire des architectures plus étendues. Le pont agit au niveau MAC. Ainsi, il n'a pas connaissance et ignore les protocoles de niveau supérieur (réseau, transport,…) utilisés. Son utilisation s'applique donc à tous les protocoles de manière unique, son action étant indépendante du champ de données de la trame MAC.

Par défaut, le pont relie entre-eux des réseaux de même type (ethernet, token-ring, …), puisque les couches MAC doivent être compatibles, mais les débits peuvent être différents de part et d'autre du pont . Il existe cependant des ponts dit "hybrides "qui relient des réseaux hétérogènes entre eux.

Les ponts peuvent être groupés en plusieurs catégories. Une façon de les classer est établie suivant que leur opération est "locale" ou "distante". Un pont local fournit une connexion directe entre les segments de LAN dans le même domaine. Un pont distant connecte différents segments de différents domaines géographiques, habituellement à travers le réseau public.

Cependant, la plupart des ponts aujourd'hui sont à la fois distants et locaux. En fait, la différence se fait d'avantage sur la technique de routage supportée par les ponts. On distingue des ponts dits transparents associés à l'algorithme du Spanning Tree intégrés dans des environnements Ethernet et les ponts dits Source Routing associés à l'algorithme du même nom et intégrés dans les environnements Token Ring.

**PoP -** Point of Presence - Point de Présence - C'est dans ce local technique situé sur le réseau d'un opérateur que se trouvent les équipements actifs du réseau.

**POP3 -** Post Office Protocol version 3 - Protocole de gestion du courrier électronique lu par n'importe quel logiciel de messagerie (Outlook Express, Netscape Messenger, etc.).

**Port -** Interface physique d'une ligne dans un équipement.

**Portabilité -** Possibilité pour l'abonné de conserver son numéro actuel en cas de changement de fournisseur.

**Portabilité des numéros -** Possibilité, pour un abonné, de conserver son numéro de téléphone lorsqu'il change d'opérateur de boucle locale (service accessible depuis le 1er janvier 1998 si l'abonné ne change pas d'adresse) ou lorsqu'il change de localisation géographique ou d'opérateur de boucle locale ou les deux (service accessible à partir du 1er janvier 2001).

Pour les portables, la décision a été prise en 2002 d'offrir son numéro de téléphone portable quel que soit l'opérateur. L'application de la décision de l'ART devant avoir lieu dans le courant de 2003

**Portabilité du Numéro -** Complément de service qui permet à un utilisateur de déplacer un terminal d'une prise à une autre au sein d'un même accès de base, pendant la phase active de la communication, ou, dans les mêmes conditions, de transférer la communication d'un terminal à un autre.

**Porteuse -** Onde, régulière en l'absence de transmission, que l'on modifie légèrement (modulation) en fonction des informations à transmettre, l'ensemble porteuse et modulation constituant le "signal".

Onde dont une grandeur caractéristique est destinée à suivre les variations d'un signal dans une modulation.

**Ports -** Les ports sur un ordinateur sont des entrées qui permettent d'échanger des informations dans un sens ou dans un autre avec une autre machine.

En TCP/IP, lorsque vous échangez des données, la communication s'effectue par plusieurs ports différents à une ou plusieurs machines. Chaque port à ses caractéristiques, l'un permet de lire le courrier, l'autre permet de communiquer par des logiciels de messagerie, un autre permet de télécharger des fichiers... Il existe en tout et pour tout plus de 65000 ports sur une machine. Ainsi, les ports sont indispensables à l'échange d'informations par TCP/IP (donc sur Internet).

Les ports constituent les seules entrées existantes vers une station, c'est aussi par là que les surfeurs malveillants pénètrent dans votre machine. Pour communiquer avec un autre ordinateur du réseau internet, une adresse IP (Internet Protocol) et un numéro de port sont nécessaires. Leur numéro spécifie le type de communication qui va s'établir entre deux machines. Par exemple, le port 80 est utilisé par un serveur web lorsqu'il vous délivre des pages web.

Un détail des numéros de ports est joint en annexe au présent document ainsi que les RFC de référence.

**POS -** Point of Sale - Expression anglaise pour désigner un Terminal point de vente (TPV).

**POSI -** Promotion for Open Systems Interconnection - Groupement japonais cherchant à promouvoir et à influencer le passage des normes OSI dans des systèmes fonctionnels.

**PPP -** Point to Point Protocol - Protocole standard de mise en trames et d'authentification qui garantit l'interopérabilité avec des logiciels d'accès distant. PPP négocie les paramètres de configuration pour les différentes couches du modèle OSI. Il assure la délimitation des trames, la détection des erreurs.

PPP fut développé pour transférer des données sur des liens synchrones ou asynchrones entre deux points en utilisant HDLC comme base d'encapsulation et un Frame Check Sequence (FCS) HDLC pour la détection des erreurs. Cette liaison permet le full duplex et garantit l'ordre d'arrivée des paquets. Une fonctionnalité intéressante de ce protocole est le multiplexage simultané de plusieurs protocoles de niveau 3 du modèle OSI.

Ce protocole encapsule des paquets IP, IPX et Netbeui, dans des trames PPP, puis transmet ces paquets PPP encapsulés à travers la liaison point à point. PPP est donc utilisé entre un client distant et un serveur d'accès distant.

Le protocole PPP est décrit dans la RFC 1331.

Format de la trame PPP

| Fanion<br>01111110 | Adresse<br>11111111 | Contrôle<br>00000011 | Protocole<br>16 bits | Données | FCS<br>16 bits | Fanion<br>01111110 |
|---|---|---|---|---|---|---|

- Fanion = séparateur de trame. Un seul drapeau est nécessaire entre 2 trames.
- Adresse = Le champ adresse correspond à une adresse HDLC, or PPP ne permet pas un adressage individuel des stations donc ce champ doit être à 0xFF (toutes les stations), toute adresse non reconnue fera que la trame sera détruite.
- contrôle = Le champ contrôle doit être à 0x03, ce qui correspond à une trame HDLC non numérotée. Toute autre valeur fera que la trame sera détruite.
- Protocole = La valeur contenue dans ce champ doit être impaire, l'octet de poids fort étant pair. Ce champ identifie le protocole encapsulé dans le champ informations de la trame. Les différentes valeurs utilisables sont définies dans la RFC "assign number "et représentent les différents protocoles supportés par PPP (OSI, IP, Decnet IV, IPX, etc.), les NCP associés ainsi que les LCP.
- Informations = De longueur comprise entre 0 et 1500 octets, ce champ contient le datagramme du protocole supérieur indiqué dans le champ "protocole". Sa longueur est détectée par le drapeau de fin de trame, moins 2 octets de contrôle
- FCS (Frame Check Sequence) = Ce champ contient la valeur du checksum de la trame. PPP vérifie le contenu du FCS lorsqu'il reçoit un paquet. Le contrôle d'erreur appliqué par PPP est conforme à X25.

**PPTP -** Point-to-Point Tunneling Protocol - Norme IETF soutenue par Microsoft pour la mise en œuvre des VPN à partir du système d'exploitation Windows 95/98 vers une passerelle VPN.

Protocole de niveau 2 qui encapsule des trames PPP dans des datagrammes IP afin de les transférer sur un réseau IP. PPTP permet le cryptage des données PPP encapsulées mais aussi leur compression. Ainsi, dans ce mode de connexion, les machines distantes des deux réseaux locaux sont connectés par une connexion point à point (comprenant un système de chiffrement et d'authentification, et le paquet transite au sein d'un datagramme IP. De cette façon, les données du réseau local (ainsi que les adresses des machines présentes dans l'en-tête du message) sont encapsulées dans un message PPP, qui est lui-même encapsulé dans un message IP.

**PRDM -** Point de Raccordement Distant Mutualisé - Terminologie FTTH - Lorsque le point de mutualisation regroupe moins de 1000 lignes, le PRDM désigne le point de livraison de l'offre de raccordement distant prévu par la décision n°2010-1312 et regroupant au moins 1000 lignes. En pratique, ce point peut être confondu avec le nœud de raccordement optique de l'opérateur.

**Précâblage -** Installation dans un bâtiment neuf ou ancien, d'une infrastructure de câble a priori, relativement indépendante des usages et des connexions qui seront effectivement mis en œuvre par les équipements. La plupart des systèmes de précâblage prévoient simultanément la téléphonie et les connexions informatiques.

**Présentation -** Règles de structuration de données en fonction des équipements (écrans, imprimantes...) qui les recevront. Le mot "présentation" désigne également la sixième couche du modèle OSI. Elle fournit à la couche supérieure (Application) les moyens de représenter l'information de telle manière que sa signification soit conservée : elle concerne donc son codage et sa syntaxe.

**Pression acoustique -** Audio - On mesure la capacité d'une l'enceinte à restituer des niveaux sonores importants sans risques pour elle ni pour l'amplificateur.

**Prestel -** Système de vidéotex britannique.

**PRI -** Primary Rate Interface - Interface de raccordement au réseau numérique (appelée accès primaire ou T2 en France) d'une capacité de 30 canaux 64 Kbits seconde avec 2 canaux de signalisation.

**PRI -** Point de Raccordement Immeuble - Dispositif de brassage installé dans un immeuble comprenant des compartiments dédiés aux opérateurs commerciaux en vue de la mutualisation des liaisons vers les logements.

**PRMD -** Private Management Domain - Dans la norme de messagerie X400, désigne un ensemble d'utilisateurs qui possède ses propres ressources de gestion et d'acheminement des messages.

**PRO -** Point de Raccordement Opérateur.

**Procédure -** Séquence de règles pour accomplir un processus. Souvent équivalent de protocole.

**Procédure de commande d'appel -** Ensemble des signaux interactifs nécessaires pour l'établissement, la maintenance et la libération d'une communication.

**Profil -** Ensemble cohérent d'options choisies pour chacune des couches du modèle OSI (Open System Interconnection) en vue d'un type d'application déterminé.

**Protocole -** Séquence de règles à suivre dans un échange d'informations - Un protocole est une description formelle de règles et de conventions à suivre dans un échange d'informations, que ce soit pour acheminer les données jusqu'au destinataire ou pour que le destinataire comprenne comment il doit utiliser les données qu'il a reçues. C'est l'ensemble des règles de dialogue qui permettent à deux niveaux équivalents du modèle OSI de communiquer.

Pour qu'une transmission de données puisse se dérouler convenablement jusqu'au bout entre deux équipements ETTD (DTE) ou entre deux adaptateurs de circuits ETCD (DCE), il faut que tous les maillons de la chaîne suivent des procédures ou des conventions préalables parfaitement définies qui constitueront la grammaire du dialogue. Ce sont ces conventions que d'une manière générale on désigne par le nom de protocole. Cette notion, désignant toute convention de dialogue, est très large, mais elle est indispensable en télécommunications. On peut dire qu'une grande partie des décisions en matière de réseaux porte en dernier sur des choix de protocoles. Un protocole définira, par exemple, la structure et l'ordre dans lesquels les informations seront transmises (organisation par bits, par mots, par blocs...), la synchronisation entre émetteur et récepteur, les règles de priorité, la façon dont seront détectées, et éventuellement corrigées, les erreurs de transmission, les procédures à suivre en cas d'incident, l'adaptation des flux de données aux débits des canaux...

Les protocoles peuvent être implantés dans n'importe quel type d'équipement soit sous forme matérielle dans des circuits électroniques, soit sous forme logicielle, un protocole se présentant alors comme un programme d'ordinateur. Une transmission nécessite en général le recours à plusieurs protocoles, souvent imbriqués les uns dans les autres. Par exemple, dans une transmission simple, on aura au minimum un protocole de dialogue entre ETTD et ETCD et entre les deux ETTD's. Cette hiérarchie imbriquée des protocoles sera à la base du modèle d'interconnexion de systèmes ouverts en "couches" OSI.

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines). Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (le FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (c'est le cas du protocole ICMP), ...

Sur Internet, les protocoles utilisés font partie d'une suite de protocoles, c'est-à-dire un ensemble de protocoles reliés entre-eux. Cette suite de protocole s'appelle TCP/IP :

Elle contient, entre autres, les protocoles suivants: http, FTP, ARP, ICMP, IP, TCP, UDP, SMTP, Telnet, NNTP

On classe généralement les protocoles en deux catégories selon le niveau de contrôle des données que l'on désire:

- Les protocoles orientés connexion: Il s'agit des protocoles opérant un contrôle de transmission des données pendant une communication établie entre deux machines. dans un tel schéma, la machine réceptrice envoie des accusés de réception lors de la communication, ainsi la machine émettrice est garante de la validité des données qu'elle envoie. Les données sont ainsi envoyées sous forme de flot. TCP est un protocole orienté connexion
- Les protocoles non orientés connexion: Il s'agit d'un mode de communication dans lequel la machine émettrice envoie des données sans prévenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyer d'avis de réception à la première. Les données sont ainsi envoyées sous forme de blocs (datagrammes). UDP est un protocole non orienté connexion

Un protocole définit uniquement la façon par laquelle les machines doivent communiquer, c'est-à-dire la forme et la séquence des données à échanger. Un protocole ne définit par contre pas la manière de programmer un logiciel de telle manière à ce qu'il soit compatible avec le protocole. On appelle ainsi implémentation la traduction d'un protocole en langage informatique.

Les spécifications des protocoles ne sont jamais exhaustives, aussi il est courant que les implémentations soient l'objet d'une certaine interprétation des spécifications, ce qui conduit parfois à des spécificités de certaines implémentations ou pire à des incompatibilités ou des failles de sécurité.

**Protocole D -** Protocole de gestion des échanges entre un terminal et un réseau numérique à intégration de services. Le message d'établissement dans le protocole D peut faire une cinquantaine d'octets.

**Protocole Internes -** Les protocoles internes sont dédiés à la gestion des routeurs à l'intérieur d'un domaine. Une de leurs principales caractéristiques est de trouver automatiquement les autres routeurs et de découvrir la topologie du réseau pour déterminer le chemin le plus adapté.

Les routeurs, pour construire leurs tables de routage, doivent connaître l'état du réseau. Il faut que chaque équipement diffuse les informations le concernant, mais la diffusion ne doit pas conduire à des boucles ou à des duplications de message.

Les protocoles de type IGP (Interior Gateway Protocol) assurent le dialogue entre deux routeurs situés à l'intérieur d'un système autonome.

Il existe deux grandes familles de protocole de routage interne : Les algorithmes basés sur le Distant vector où chaque routeur n'a qu'une vision partielle du réseau, et les algorithmes basés sur le protocole État de liaisons où chaque routeur construit une vision totale du réseau.

- L'algorithme de vecteur de distance est basé sur l'échange d'informations entre routeurs adjacents, c'est-à-dire s'il y a une liaison directe entre eux (s'ils ont un lien sur le même réseau local). Chaque routeur ne connaît initialement que le coût de ses propres liaisons. Les routeurs diffusent vers les noeuds adjacents leur table de routage rudimentaire constituée de ses différents voisins accessibles et du coût de la liaison. Quand un routeur reçoit une nouvelle table, il effectue l'algorithme de Bellman-Ford pour chaque entrée de la table reçue :
  - Si l'entrée n'est pas dans la table, il la rajoute,
  - Si le coût de la route proposée par la table plus le coût de la route pour venir est plus petit que celui de la route stockée, la table de routage est modifiée pour prendre en compte cette nouvelle route.
  - Sinon, il n'y a pas de changement.
  - Le protocole de *vecteur de distance* le plus utilisé est le RIP

Le vecteur de distance peut conduire à des boucles qui ralentissent sa convergence. La technique de l'horizon coupé (split horizon) permet d'en supprimer certaines en utilisant la connaissance de proximité que possède chaque station du réseau.

Un algorithme de type protocole « État de liaisons » permet d'obtenir la connaissance de la topologie réseau (le calcul des meilleures routes est fait localement). OSPF (Open Shortest Path First) et IS-IS (Intermediate System to Intermediate System) sont les protocoles État de liaisons les plus souvent utilisés.

**Protocole IP -** Le protocole IP (pour Internet Protocol) gère la transmission des informations sur Internet. Chaque fichier (ou donnée) transitant sur Internet est décomposé en "paquets". Ceux-ci empruntent les voies les plus rapides pour arriver à destination et sont alors ré assemblés pour reconstituer le fichier de départ. Voir IP.

**Proxy -** Equipement (mandataire) effectuant une tâche à la place d'un autre équipement. Dans le domaine des firewalls, le proxy est un processus effectuant un certain nombre de contrôles sur le trafic entrant. Ce mécanisme peut nuire aux performances du firewall.

Proxy (proxies au pluriel) est un terme général utilisé en informatique pour désigner un service qui se substitue ou concours à un autre de façon automatique. L'anglais se traduit par "mandataire", "délégué", ce qui donne l'idée.

Sur Internet, "proxy" recouvre quelque chose d'à peine plus précis: c'est un serveur (logiciel, machine) qui va ajouter automatiquement une fonction à un service, et de façon quasi ou totalement transparente pour son utilisateur.

Les premiers proxies dont l'usage s'est généralisé sont les proxy-cache. Le proxy-cache joue le même rôle que la mémoire cache de votre ordinateur: il retient les dernières données utilisées et lorsque celles-ci sont demandées à nouveau, les restitue beaucoup plus rapidement que si elles devaient être recherchées à nouveau en mémoire.

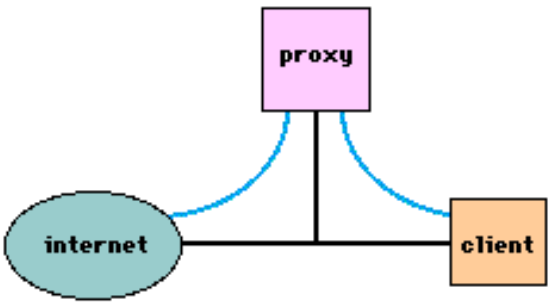
Sur le web, le proxy-cache mémorise les pages demandées par les utilisateurs sur ses disques locaux. Lorsqu'un autre utilisateur demande la même page, celle-ci est servie depuis les disques locaux, évitant ainsi son transfert sur Internet. L'efficacité du proxy-cache est bien sûr statistique, mais l'expérience montre que son utilisation élimine beaucoup de transmissions inutiles et accélère la consultation.

**Proxy-cache -** Vous êtes connecté à un sous-réseau de l'Internet: celui de votre entreprise, de votre université, ou votre Fournisseur d'Accès Internet (FAI) via un modem. Ce sous-réseau met à votre disposition un proxy dont il vous donne l'URL. Vous déclarez cet URL dans les préférences de votre navigateur.

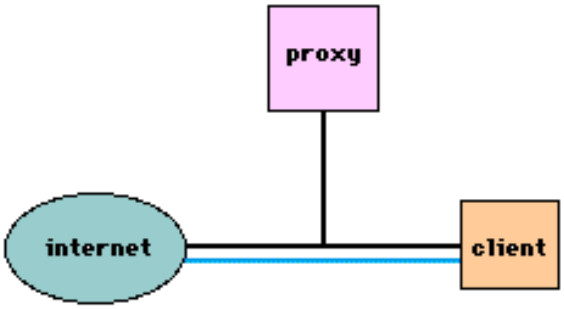
Lorsque vous demandez un document web, au lieu de le demander au site d'origine votre navigateur va le demander à votre proxy. Si celui-ci le détient (et si il est à jour), il vous renvoie sa copie locale. Sinon, il va la chercher sur le réseau.

Ainsi conçu, le proxy est un service supplémentaire offert par votre sous-réseau ou votre FAI. Pour vous, c'est une option. Vous pouvez l'utiliser ou pas (ce qui est heureux car il arrive qu'il tombe en panne). Pour cela, il vous suffit de le désactiver dans de votre navigateur. Le dialogue se trouve en général dans le menu "Préférences" option "Réseau".

Notez que les fameux "Kits d'installation" fournis par les FAI contiennent un navigateur déjà préconfiguré pour leur proxy s'ils en ont un. Voici comment (liens bleus) circuleront les données dans les deux cas (schémas ci-après). Vous pouvez court-circuiter le proxy car vous êtes relié directement à l'Internet (liens noirs) :




Proxy-cache activé

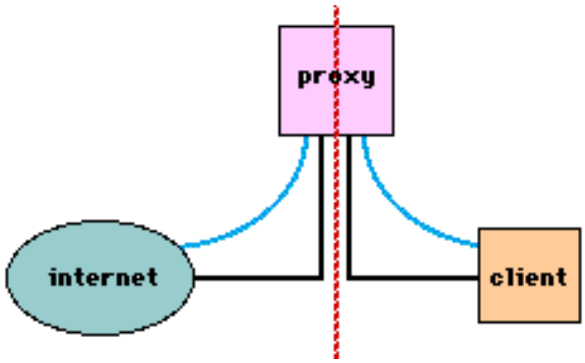



Proxy-cache désactivé

**Proxy-filtre -** Celui-ci est la combinaison d'un proxy-cache et de la technique de firewall (pare-feu). Un firewall s'interpose entre votre ordinateur et l'Internet en général pour des raisons de sécurité. Le firewall examine les données transmises et reçues et les traite selon des règles données

Le firewall est très utile pour limiter les tentatives d'intrusion dans un réseau ainsi qu'effectuer des opérations de routage, masquage, traduction sophistiquées. Cependant, en fonction des règles qu'on lui donne, il peut être utilisé pour à peu près tout ce qu'on veut. Par exemple, pour réaliser un proxy-cache en interceptant les données du web (port 80). On parle alors de proxy-filtre.

Le proxy-filtre présente une différence importante avec le proxy-cache: vu qu'il fonctionne automatiquement, par interception des donnés, il n'est pas nécessaire de le déclarer à votre navigateur. Du même coup, il devient impossible de le contourner.




Proxy-filtre

Le proxy cache crée une frontière entre votre ordinateur et l'Internet (ligne rouge). Il n'existe plus de continuité directe. Tous vos transferts passent par votre mandataire obligatoire: le proxy-filtre.

Que peut-on faire avec un proxy-filtre? TOUT! Aussi bien accélérer le chargement des pages et réduire l'encombrement du réseau, que de bloquer les sites pornographiques à des accès dits "familiaux", mais aussi superposer son propre flux d'information et analyser le vôtre. Cela ouvre grand la porte à deux besoins fondamentaux des marchands: ouvrir un canal publicitaire vers votre écran et analyser vos comportements pour mieux vous cibler.

**PSDN -** Packet Switching Data Network - Expression anglo-saxonne pour désigner un réseau à commutation de paquets.

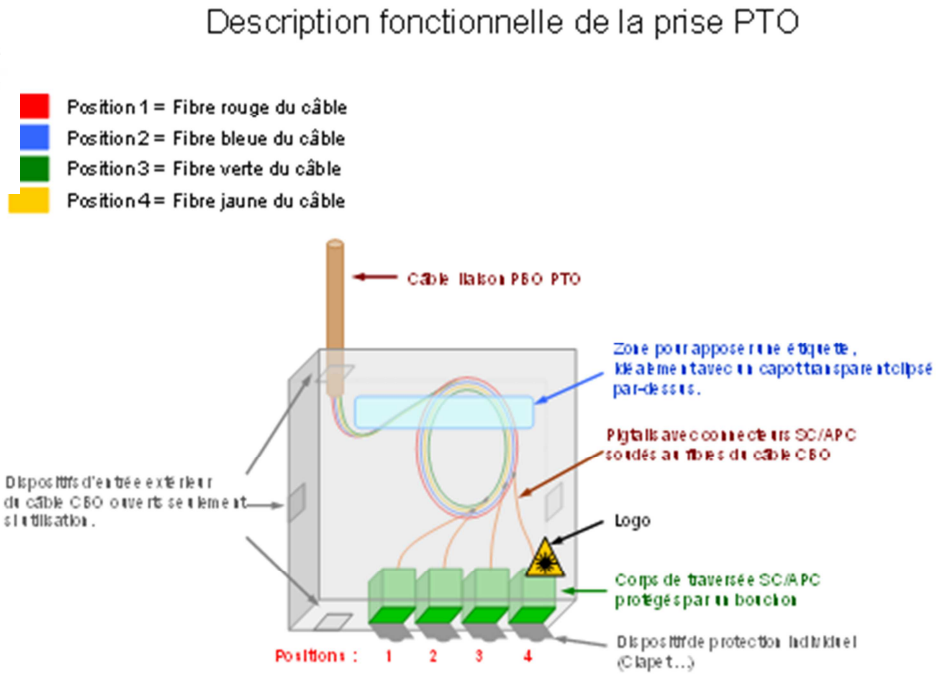
**Pseudo-Modem -** Equipement DCE qui amplifie un signal de données pour le transmettre sur des distances de câbles supérieures à la limite de 15 mètres du RS 232, et ce à plusieurs kilomètres.

**PSN -** Public Switched Network - Réseau public commuté.

**PSTN -** Public Switched Telephone Network - Réseau commuté public de téléphonie. Correspond à l'acronyme français RTC (Réseau téléphonique commuté).

**PTO -** Prise Terminale Optique - Prise située dans un logement ou local professionnel qui constitue le point de terminaison du réseau FTTH.

La prise terminale optique est le dernier élément d'infrastructure optique d'un réseau FTTH.




**Publiphonie -** Réseau de cabines publiques permettant la transmission de la voix, l'accès à des bases de données et à INTERNET et bientôt le transfert d'argent (le publiphone devient un terminal de paiement). Différents types de cartes à mémoire sont utilisés : cartes prépayées, cartes d'abonnés, cartes bancaires magnétiques ou à puces, PME (porte monnaie électronique).

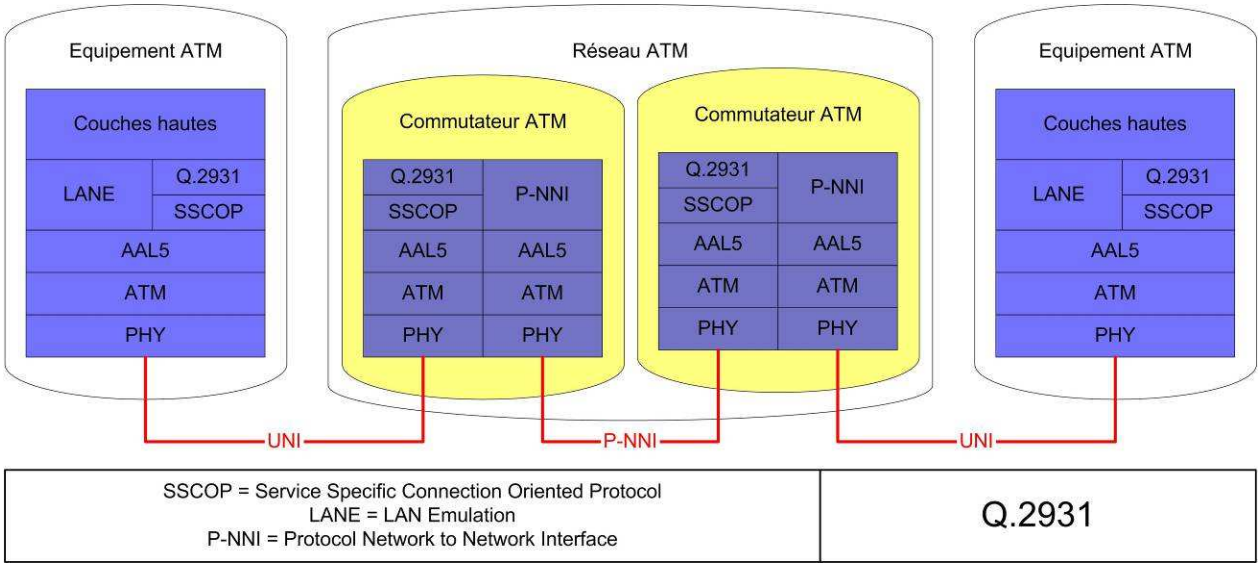
**Pureté des graves -** Audio - C'est la mesure des déformations générées par des harmoniques sur trois fréquences fondamentales du grave, 40, 50 et 60 Hz.

**PVC -** Permanent Virtual Circuit - Circuit virtuel permanent dans un réseau à commutation de paquets. Circuit alloué par avance pour un flux de données.

# Q

**Q.2931 -** Le protocole de signalisation Q.2931 supporte la création dynamique de voies virtuelles ATM. Si un système désire créer une voie virtuelle avec un autre système, il utilise Q.2931 pour l'établir. Une fois crée, la voie virtuelle reste ouverte jusqu'à ce qu'elle soit fermée par ses utilisateurs ou qu'il se produise une défaillance réseau [1e]. Ces voies virtuelles dynamiques (appelées aussi voies virtuelles à la demande), diffèrent des voies virtuelles permanentes qui sont automatiquement rétablies après une défaillance du réseau.

Cette norme permet de définir trois types de connexion. Le demandeur peut établir une voie unidirectionnelle vers une destination, une voie bidirectionnelle vers une destination (point-to-point), ou un arbre de diffusion multiple unidirectionnel ou bidirectionnelle (point-to-multipoint). Une évolution vers du multipoint à multipoints est en phase de développement.




Q.2931 est simplement un jeu de règles définissant comment les extrémités émettrices et réceptrices négocient les caractéristiques de la connexion avec le réseau ATM. Les règles de communication entre les commutateurs à l'intérieur du réseau ne font pas partie de cette norme.

**QOS -** Quality Of Services - Ensemble de règles qui vont définir la qualité de service d'un média ou d'un réseau.

La Qualité de Service (QoS) et la Différenciation de classes de services (CoS) sont deux méthodes qui fournissent une gestion du trafic sur un réseau.

La qualité de services (QoS) est un terme vague qui se réfère aux techniques permettant de classifier les différents types de trafics. La classe de service est généralement assimilée à la discrimination des services, autrement dit à la définition de classes différenciées de services. Mais cela signifie aussi garantir un service et pour cela réserver des ressources.

La QoS englobe tous les mécanismes permettant de différencier les types de trafic ceux-ci pouvant être classés et administrés différemment à travers le réseau.

Les classes de services différenciées représentent une alternative à la QoS qui a été développé en raison du coût de la classification du trafic en flux et de la maintenance et de l'utilisation de l'information par flux. Tandis que la QoS classifie les trames de paquets en flux individuels de trafic, chacun desquels possèdent des caractéristiques de qualités uniques (taux d'erreurs, délai de latence …), le principe de la CoS est plus simple. Elle n'essaie pas de différencier parmi les flux individuels. En contrepartie elle utilise une méthode plus simple pour classifier les paquets dans une des quelques catégories répertoriées.

Tous les paquets d'une catégorie identifiée sont traités de façon identique, avec les mêmes paramètres de qualité, définit par les responsables du réseau.

Clairement la CoS est une technologie plus simple que la QoS.

**QPI -** Quote Part Internationale définie dans le cadre du système des taxes de répartition.

**QSIG -** Protocole numérique unifiant la communication entre PABX différents.

**Qualité de filtrage -** Audio - C'est la mesure des résidus audibles de l'information numérique initiale, signe d'inefficacité des filtres destinés à tout "nettoyer "lors de la transformation en analogique.

**Quantification -** Quantizing - Transformation de la valeur instantanée d'un signal analogique; l'intervalle continu des valeurs possibles étant remplacé par une suite de valeurs discrètes, la valeur transformée est "la plus proche possible" de la valeur instantanée.

**Quarte -** Désigne un groupe de deux paires de fils, unité de câblage fréquemment utilisée en téléphonie.

**Quartz -** Composant électronique utilisé pour délivrer un signal d'horloge stable.

**Queue -** Liste d'entités en attente. Par extension, désigne aussi bien le contenant que le contenu.

**QXML -** Langage fondé sur XML et conçu pour l'échange d'informations produites dans le secteur de l'industrie de détail. QXML est le premier format d'échange basé sur XML et destiné à optimiser l'approvisionnement, à simplifier l'intégration d'informations et à étendre les gammes d'informations produits échangées entre partenaires commerciaux.

# R

**Raccordement client -** Opération consistant à installer un câble comprenant une ou plusieurs fibres optiques entre le PBO et la PTO.

**Raccordement « palier » -** Cas particulier du raccordement client, lorsque le Point de Branchement Optique est situé dans les étages d'un immeuble, ou encore dans le domaine public.

**RACE -** Research in Advanced Communication technologies in Europe - Programme européen de recherche "précompétitive" en matière de télécommunications avancées. Le centre du projet concerne les techniques de réseaux à très large bande, capables de transporter voix, données et images à très grande vitesse.

**Rack -** Boîtier vertical aux dimensions normalisées (le plus souvent de 19 pouces de large) destiné à accueillir différents serveurs, équipements de connectivité réseau ou de sécurité de hauteur variable (de 1U à 7U ou plus).


**Radar(s) -** Ils émettent des signaux pulsés. La puissance maximale peut être très élevée mais la puissance moyenne est faible à l'exception de certains radars militaires fixes, de très forte puissance, dont l'accès est de toute façon interdit.

Aussi appelés boites à image, il s'agit là de cinémomètres à onde réfléchie permettant de mesurer la vitesse de déplacement d'un véhicule. Dans ce cas de figure, la portée du cinémomètre peut atteindre voir dépasser le kilomètre. Ce n'est pas une donnée informatique, télécoms ou réseau, mais c'est une définition possible du terme et aussi, pour beaucoup d'entre nous, le début probable d'une "séquence émotion". ☺

**Radio Professionnelle -** Réseaux privés de radiocommunications mobiles dont le marché s'étend à de nombreux secteurs : force de sécurité, services d'urgence, compagnies de transport, distributeurs d'énergie, etc. parmi lesquels on distingue particulièrement :

- 3RP : réseaux radioélectriques à ressources partagées
- 3RPC : réseaux commerciaux mettant en œuvre la technologie 3RP
- RPN (radiocommunications mobiles professionnelles numériques) : réseaux fonctionnant en technologie numérique à la norme Tetra ou Tetrapol.
- 2RC : réseaux à usage partagé commun.
- 3R2P : réseaux exploités pour les besoins propres de l'utilisateur mettant en œuvre la technologie 3RP.
- RPX : réseaux locaux à usage partagé (nouvelle catégorie de réseaux).

**Radiocom 2000 -** Système de radiotéléphonie cellulaire analogique commercialisé par France Télécom il y a quelques années.

**Radiocommunications -** Ensemble de techniques de télécommunications utilisant la propagation des ondes hertziennes.

**Radiomessagerie -** Système de radiocommunications qui permet à ses utilisateurs de recevoir sur un boîtier, messager ou "pager", un indicatif d'appel (bip) ou des messages composés de chiffres (numériques) ou de chiffres et de lettres (alphanumériques). Les trois principales marques commerciales de radiomessagerie en France sont Tam-Tam, Tatoo et Kobby.

**Radiomessagerie Bilatérale ou Bidirectionnelle -** Two-way Paging - Transmission de messages numériques ou alphanumériques en provenance ou à destination d'un terminal mobile.

**Radiomessagerie Unilatérale -** RMU - Système de radiocommunications capable uniquement d'émettre de courts messages vers des récepteurs portables. Alphapage (France Télécom) et Opérator (TDF) sont les deux principaux systèmes commercialisés en France.

**Radiotéléphonie -** Ensemble de techniques permettant d'utiliser des téléphones portables par l'intermédiaire des ondes radio.

**Radiotéléphonie Cellulaire -** Le radiotéléphone établit des liaisons téléphoniques avec des abonnés en mouvement. La radiotéléphonie cellulaire associe les ondes radio et l'informatique. Le territoire est divisé en cellules, chacune d'elles étant dotée de fréquences bien définies. Le système appelé "hand over" permet à l'automobiliste usager en cours de communication de quitter sa cellule sans risque de coupure.

**Radius -** Remote Authentification Dial In Users Services - Protocole développé par Livingston Enterprises Inc., utilisé comme protocole d'authentification et de gestion de serveur d'accès. Le protocole est un

protocole d'authentification standard, défini par un certain nombre de RFC.(2058,2059, 2865, 2866, 2138,…)

Le serveur Radius, parfois baptisé triple A pour Authentication, Authorization, Accounting a une fonction unique : s'assurer de l'identité des utilisateurs entrant sur un réseau d'entreprise. Radius se contente de répondre à la demande d'authentification formulée par un client (un agent logiciel implanté sur le routeur, le coupe-feu ou le serveur d'accès).

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il s'agit du protocole de prédilection des fournisseurs d'accès à internet car il est relativement standard et propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.

Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS peut être chiffré et authentifié grâce à un secret partagé.

Le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci (voir aussi dans les annexes les traces complètes) :

- ⇒ Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance
- ⇒ Le NAS achemine la demande au serveur RADIUS
- ⇒ Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthodes d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
  - o ACCEPT : l'identification a réussi
  - o REJECT : l'identification a échoué
  - o CHALLENGE : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un "challenge"
  - o CHANGE PASSWORD : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.
- ⇒ Suite à cette phase dit d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

Paquet Radius (requête d'authentification, type access accept):

```
 sai-paris -> radius_siris1 UDP D=32881 S=1645 LEN=312
  code            2 (Access-Accept)
  identifier      134 (0x86)
  longueur        304 octets (0x0130)
  authenticator   6eed28f631331f7f0c2bd49d857920be
  --------------------------------
  211 Proxy-Action(211)                 = AUTHENTICATE
    4 NAS-IP-Address(4)                 = 192.168.161.79
    5 NAS-Port(5)                       = 5664
   61 NAS-Port-Type(61)                 = Async
    1 User-Name(1)                      = inf1/199601000049447@infonie.test
    3 CHAP-Password(3)                  = ...}..!F..K..5.[.
    6 Service-Type(6)                   = Framed
    7 Framed-Protocol(7)                = PPP
  222 User-Id(222)                      = inf1/199601000049447
   32 NAS-Identifier(32)                = 192.168.161.79
   60 CHAP-Challenge(60)                = ..~B...S........
  223 User-Realm(223)                   = infonie.test
   33 Proxy-State(33)                   = 0
   64 Tunnel-Type(64)                   = L2F
   65 Tunnel-Medium-Type(65)            = IP
   67 Tunnel-Server-Endpoint(67)        = @HGInfonieSiris
   69 Tunnel-Password(69)               = RPVAC_Infonie
   66 Tunnel-Client-Endpoint(66)        = RAS_Infonie@siris-ac.net
    6 Service-Type(6)                   = Framed
   11 Filter-Id(11)                     = 100.in
   25 Class(25)                         = 364c38e8.1.manager-paris
  145 LAS-Start-Time(145)               = 910964968
```

**RAID -** Redundant Area of Inexpensive Disks - Sous-système de stockage composé de simples disques et d'un contrôleur destiné à accroître les performances et/ou la sécurité des données. Le mirroring, la répartition des données et le contrôle de parité sont combinés dans les sous-systèmes Raid.

Il existe plusieurs niveaux de RAID qui sont exprimés par des valeurs numériques (RAID 0, RAID 1…) :

- Raid 0 : répartition des données entre plusieurs disques pour améliorer la bande passante.
- Raid 1 : duplication des données sur un deuxième disque miroir pour une sécurité accrue.
- Raid 5 : répartition des données sur trois disques au minimum avec gestion de la parité pour un bon compromis performance/ sécurité.
- Raid 6 : Idem Raid 5, les informations de parité étant écrites deux fois.

**Rain Fading -** (en BLR ou transmission Radio) - Atténuation d'un signal Radio due à la pluie. Elle peut atteindre 11 dB pour une pluie de 35 mm/h.

**Rappel Automatique sur Occupation -** Procédure automatique lancée par le demandeur avant de raccrocher et qui peut être déclenchée en cas d'occupation de la ligne du demandé, et selon laquelle le réseau surveille cette ligne. Dès qu'elle se libère, la procédure appelle le demandeur puis le demandé si le demandeur décroche.

Le complément de service, normalisé par l'UIT, existe dans le réseau téléphonique public commuté (RTPC) de certains pays, dans la plupart des réseaux numériques à intégration de services (RNIS) et dans les réseaux de communication avec les mobiles de type GSM.

**Rapport signal/bruit -** Audio - Recul du bruit de fond par rapport signal musical. Le décibel étant une unité logarithmique, une faible augmentation de valeur correspond à un fort accroissement du bruit.

**Rapport signal/bruit -** Ratio comparant un signal à la quantité de perturbations aléatoires qui l'altère. Exprimé en décibels, ce rapport mesure la qualité d'une transmission.

**RARE -** Réseaux Associés pour la Recherche Européenne. Association d'universités et de centres de recherche européens visant à promouvoir la création d'un système de télécommunications avancées dans le monde scientifique.

**RARP -** Reverse Address Resolution Protocol - Permet l'attribution d'une adresse IP à une station.

En réalité le protocole RARP est essentiellement utilisé pour les stations de travail n'ayant pas de disque dur et souhaitant connaître leur adresse physique.

Le protocole RARP permet à une station de connaître son adresse IP à partir d'une table de correspondance entre adresse MAC (adresse physique) et adresses IP hébergée par une passerelle (gateway) située sur le même réseau local (LAN).

Pour cela il faut que l'administrateur paramètre le gateway (routeur) avec la table de correspondance des adresses MAC/IP. En effet, à la différence de ARP ce protocole est statique. Il faut donc que la table de correspondance soit toujours à jour pour permettre la connexion de nouvelles cartes réseau.

RARP souffre de nombreuses limitations. Ce protocole nécessite beaucoup de temps d'administration pour maintenir des tables importantes dans les serveurs. Cela est d'autant plus vrai que le réseau est grand. Cela pose les problèmes de la ressource humaine, nécessaire au maintien des tables de correspondance et des capacités des matériels hébergeant la partie serveur du protocole RARP. En effet, RARP permet à plusieurs serveurs de répondre à des requêtes, bien qu'il ne prévoit pas de mécanismes garantissant que tous les serveurs soient capables de répondre, ni même qu'ils répondent de manière identique. Ainsi, dans ce type d'architecture on ne peut avoir confiance en un serveur RARP pour savoir si à une adresse MAC peut être liée à une adresse IP parce que d'autres serveurs ARP peuvent avoir une réponse différente. Une autre limitation de RARP est qu'un serveur ne peut servir qu'un LAN.

Pour pallier les deux premiers problèmes d'administration, le protocole RARP peut être remplacé par le protocole DRARP, qui en est une version dynamique. Une autre approche, consiste à utiliser un serveur DHCP, qui lui, permet une résolution dynamique des adresses. De plus, DHCP est compatible avec le protocole BOOTP. Comme ce dernier il est routable ce qui permet de servir plusieurs LAN. Il ne marche qu'avec IP.

**RAS -** Remote Access Server - Equipements utilisés par les opérateurs et les ISP dans le cadre des services d'accès à Internet par le réseau téléphonique commuté. Ils servent à transformer les communications téléphoniques en flux de données IP en assurant l'interface entre le réseau téléphonique commuté et le réseau de transport de données IP.

Composés de modems analogiques et numériques, ils assurent la terminaison de l'appel et la gestion du maintien de la communication pendant toute la durée de la session de l'utilisateur. Les RAS doivent aussi, lorsque le service le nécessite, assurer des fonctions de réassemblage de paquet localement (si les sessions sont multilink) et au besoin assurer en plus une fonction de routage.

**RBL -** Realtime Blackhole List - (anti-spam) - Littéralement "liste trou noir". Référentiel dressant la liste des sites, segments IP, domaines ou alias SMTP considérés de façon certaine comme spameurs. Tout site inscrit dans une RBL voit son trafic e-mail fortement affecté. Son défaut: risque de "blacklister" un domaine "ami".

**RDF -** Resource Description Framework - Métalangage spécifié par le W3C qui consiste à coder la sémantique de documents web de manière à obtenir une meilleure pertinence des résultats fournis par les moteurs de recherche. RDF est rédigé suivant la syntaxe de XML.

**READSL2 -** Reach extended ADSL2 - Technologie permettant d'apporter le haut débit jusqu'à 512 kbit/s à des abonnés qui n'avaient pas pu jusqu'à présent bénéficier de l'ADSL en raison de leur éloignement du central téléphonique. C'est une évolution de la norme ADSL qui permet de prolonger la portée des signaux par rapport à la norme ADSL "classique" pour des débits allant jusqu'à 512 kbit/s, et donc d'améliorer l'éligibilité au haut débit pour les lignes longues du réseau commuté.

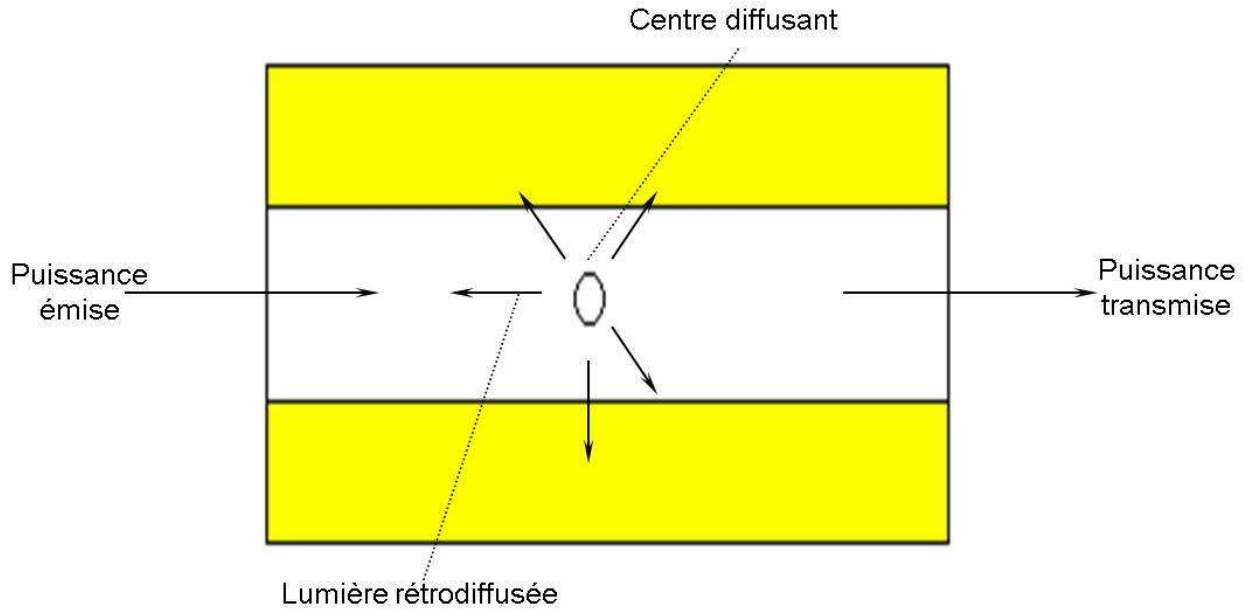
La longueur maximale d'une ligne éligible passerait ainsi de 5.5km à 8 km.

**Redondance -** Technique consistant à ajouter à un message des mots supplémentaires destinés généralement à la vérification de la bonne réception. La parité (voir ce mot) est un système de redondance.

**Référencement -** Opération visant à favoriser la visibilité d'un site web à travers les outils de recherche (moteurs de recherche et annuaires). Le référencement passe par l'indexation au moyen de mots-clés d'un site web. Le référencement de sites web s'effectue selon deux stratégies distinctes et complémentaires : le référencement naturel et les liens sponsorisés. La première stratégie passe par une phase d'indexation (= prise en compte) du site par les outils de recherche, puis une phase de positionnement de ces sites sur les résultats naturels des outils de recherche lors d'une recherche faite par les internautes. La seconde est payante et permet de voir apparaître son site dans une fenêtre en haut de page (sur Google par exemple) .

Le référencement est une des principales sources de création de trafic sur un site aujourd'hui. En effet, il permet aux internautes d'accéder à un site sans connaître son adresse. L'afflux principal provient des moteurs de recherche, mais nombre de visiteurs passent également par des annuaires.

**Réflectomètre -** Appareil de mesure permettant de déterminer les caractéristiques d'un lien en injectant un signal et en interprétant la partie du signal renvoyée vers l'émetteur, par les ruptures d'impédance dans un câble cuivre ou par une impureté ou une rupture dans une fibre optique.




**Réfraction -** Déviation angulaire de tout rayon lumineux, à la frontière de deux matériaux d'indices de réfraction différents. Le rayon se rapproche ou s'écarte de la perpendiculaire au plan formé par la surface de séparation de ces deux matériaux

**Régénérateur -** Equipement capable de reconstituer un signal affaibli. Utilisé surtout dans les câbles longue distance pour pallier à l'atténuation progressive du signal en fonction de la distance.

**Régie d'abonnés -** Partie d'une installation privée de téléphonie connectée au réseau public et gérant plusieurs émetteurs-récepteurs.

**Régulation -** Dans le secteur des télécommunications, la régulation peut se définir comme l'application, par l'autorité compétente, de l'ensemble des dispositions juridiques, économiques et techniques qui permettent aux activités de télécommunications de s'exercer librement, ainsi que le prévoit la loi. Ainsi, la régulation des télécommunications est essentiellement une régulation économique ; tel n'est pas le cas par exemple dans le secteur de l'audiovisuel où il existe une régulation des contenus, subordonnée à des objectifs culturels

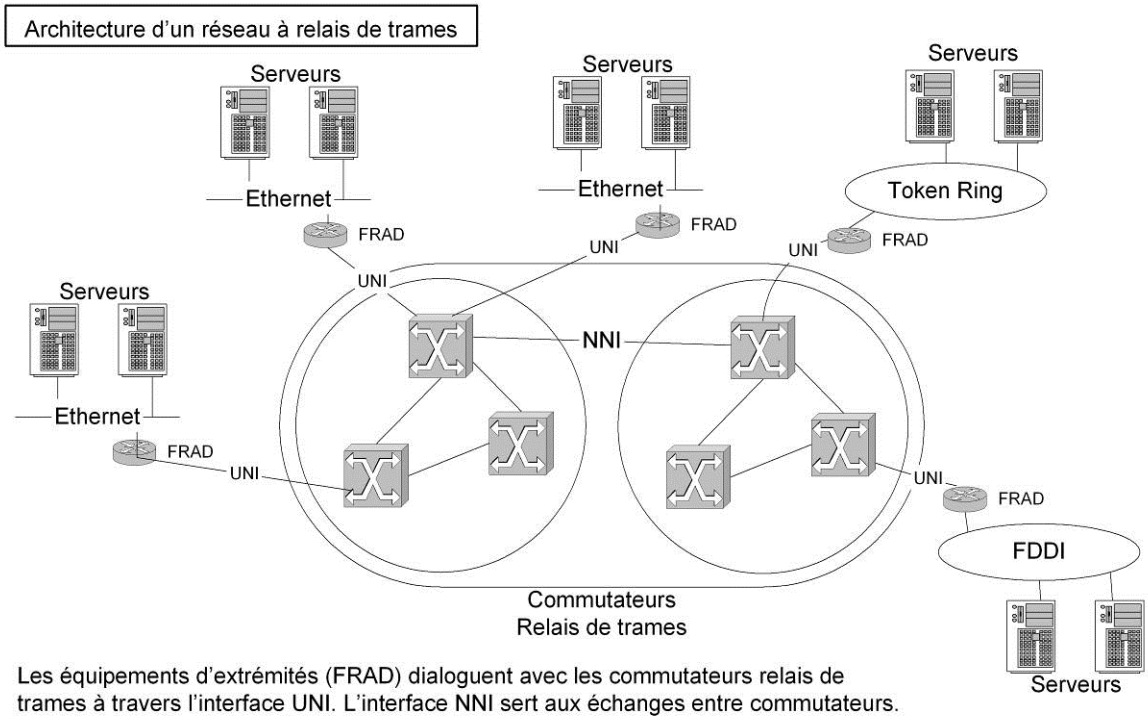
**Régulation asymétrique -** La régulation est dite asymétrique lorsqu'elle met en œuvre les obligations spécifiques qui s'appliquent à l'opérateur historique, en raison de sa position dominante sur le marché. Il s'agit par exemple d'obligations spécifiques en matière d'interconnexion, du contrôle a priori de ses tarifs de détail ou de ses obligations au regard du service universel.

**Régulation économique -** Elle consiste, pour l'autorité de régulation, à veiller à l'exercice d'une concurrence effective, loyale et durable. Elle s'appuie sur une connaissance précise des évolutions économiques du marché, sur des outils juridiques propres à établir une concurrence loyale (par exemple le règlement des différends, l'approbation des conditions techniques et financières d'interconnexion ou les sanctions) ainsi que sur une analyse approfondie des coûts des opérateurs.

**Réinitialisation TCP -** Réponse possible à une attaque de hacker d'une sonde Cisco Secure IDS ou d'un routeur Cisco IOS Firewall. Une commande est émise par ces équipements afin d'arrêter la connexion par laquelle l'attaque est effectuée, obligeant ainsi l'attaquant à établir une nouvelle connexion.

**Relais de trame -** (voir Frame-Relay) - Désigne un protocole de niveau 2 du modèle OSI. Comparable à X.25, il n'implique pas le contrôle de chaque paquet et se révèle donc plus rapide.

Le relais de trame est un service réseau en mode connecté, conforme à l'avis Q.922 de l'UIT-T, affecté au multiplexage de circuits virtuels du niveau 2 de l'OSI. La signalisation est assurée par un canal sémaphore. Elle permet d'établir un service de liaison virtuelle entre la source et le destinataire, liaison qui peut être un circuit permanent, commuté, ou établie pour de la bande passante à la demande.




Les équipements d'extrémités (FRAD) dialoguent avec les commutateurs relais de trames à travers l'interface UNI. L'interface NNI sert aux échanges entre commutateurs.

Le but d'une commutation au niveau de la liaison, qui se décline en commutation de trames et Relais de Trames, est d'améliorer en performance la commutation de paquets, en simplifiant le nombre de niveaux de l'architecture à prendre en compte. En reportant la commutation au niveau 2 de l'architecture, on simplifie considérablement le travail des noeuds.

En effet, dans les commutations de paquets, on attend de recevoir correctement une trame, avec des retransmissions potentielles, puis on travaille sur le paquet. Un acquittement est envoyé vers le noeud précédent et on garde une copie tant que le noeud suivant n'a pas fait parvenir un acquittement positif. Un autre avantage du Relais de Trames est l'introduction d'une signalisation séparée du transport de données. La mise en place de la connexion de niveau 2 s'effectuera par une connexion logique différente de celle de l'utilisateur. Les nœuds intermédiaires n'ont donc pas à se préoccuper de maintenir cette connexion.

Les contrôles d'erreurs et de flux sont reportés aux extrémités de la connexion. La simplification du travail effectué par les noeuds intermédiaires est très importante. La principale recommandation technique se trouve dans le document Q922 que l'on retrouve aussi dans la recommandation I.441. Cette recommandation limite à 2Mbits/s cette technique de relayage. Dans les faits, rien n'empêche d'aller beaucoup plus vite. Cette limitation peut s'expliquer par un manque de vue à long terme concernant cette technique. En effet, la technique de transfert à terme est l'ATM (Asynchronous Transfer Mode) et le Relais de Trames n'est vu que comme une étape transitoire capable de combler un trou de quelques années entre la commutation de paquets et la commutation de cellules.

Dans la commutation de trames, il s'agit de transporter des trames d'un bout à l'autre du réseau sans avoir à remonter au niveau paquet. Pour cela, il faut utiliser un protocole de liaison suffisamment puissant pour posséder un adressage multipoint, un adressage de niveau réseau et les fonctionnalités remplies par la couche réseau. De plus, les fonctions du niveau 2 doivent être prises en compte. Le taux d'erreurs en ligne a été très fortement diminué durant ces dernières années, devenant acceptable puisque négligeable. Cette dernière propriété sera utilisée dans le Relais de Trames qui n'est autre qu'une simplification supplémentaire

des services rendus aux noeuds intermédiaires.

La norme, qui a été retenue dans la commutation de trames, est la même que celle rencontrée sur les canaux D du RNIS : Le LAP-D. Cette recommandation respecte les fonctionnalités demandées par le modèle de référence ; on y trouve, en particulier, la détection et la correction des erreurs.

Dans la commutation de trames et dans le Relais de Trames, il est nécessaire de retrouver les grandes fonctionnalités du niveau 3 reportées dans le niveau 2 telles que l'adressage, le routage et le contrôle de flux. On utilise l'adressage du niveau trame pour effectuer le routage sans avoir à remonter au niveau 3 comme le préconise le modèle de référence. Cet adressage ne correspond plus à une norme internationale : c'est l'adressage que l'on pourrait qualifier de privé. En ce qui concerne le routage, il est lié à l'adressage et de nombreux algorithmes peuvent être utilisés.

Enfin, le contrôle de flux peut utiliser les trames RNR (Receiver Not Ready) qui permet d'arrêter le flux à la demande du récepteur.

**RELIT -** Règlement LIvraison Titres - Association professionnelle dans le secteur des banques, de la finance et de la Bourse chargée de mettre sur pied des procédures d'Echange de données informatisé (EDI) pour les "règlements livraisons" des transactions. Elle utilise la même architecture que le SIT (Système Interbancaire de Télé compensation).

**Remise -** Terme utilisé pour la messagerie électronique et désignant le dépôt final d'un message dans la boîte à lettres du destinataire.

**Rendement -** Audio - Exprimé en décibel, c'est le niveau sonore mesuré par un micro situé à 1 mètre qu'une enceinte est capable de restituer lorsqu'on lui envoie une puissance de 1 Watt. C'est un paramètre essentiel pour optimiser le couplage ampli-enceintes au niveau de la puissance: pas d'enceinte de rendement très faible sur un ampli de faible puissance ! La valeur de ce rendement résulte des choix techniques des concepteurs de l'enceinte, mais n'a pas de relation systématique avec sa qualité.

**RENPAC -** Réseau à commutation de paquets brésilien.

**Renvoi Temporaire -** Service supplémentaire fourni par les autocommutateurs électroniques. Il permet à un abonné, par simple manœuvre de son clavier, de commander que les appels aboutissant à son poste soient réacheminés vers un autre poste situé dans la même circonscription de taxe.

**Répartiteur -** Dispositif permettant de répartir les fils de cuivre composant les lignes d'abonnés entre les câbles reliés au commutateur d'abonnés et dont la fonction est de regrouper plusieurs lignes sur un même câble.

Dans un câblage, désigne un centre de distribution intermédiaire (armoire, coffret, local...) concentrant des câbles desservant les usagers.

Élément de panneau de brassage qui permet l'interconnexion et la répartition des sources et des lignes utilisateurs.

**Répéteur -** Equipement servant à régénérer ou à remettre en forme un signal affaibli. Il ne modifie pas le contenu du signal et n'intervient qu'au niveau 1 (Physique) du modèle OSI.

Un répéteur est un amplificateur de signaux qui a au minimum deux connexions réseau. Il travaille au niveau 1 du modèle OSI. Dès qu'il reçoit sur l'une de ses entrées les premiers bits d'une trame, il la retransmet instantanément sur toutes ses sorties, un répéteur n'opère donc aucune modification de données. Les répéteurs interconnectent des réseaux ayant la même couche physique, les supports (média) peuvent être différents. On utilise des répéteurs quand la longueur totale du câble dans un réseau est supérieure au maximum permis par ce type de câble. Ils permettent donc d'étendre localement les segments ou les anneaux.

**Reprise -** Désigne une opération ou une procédure visant, après une erreur, à reprendre le déroulement de la communication en un point déterminé (point de reprise).

**Répudiation -** Le fait, pour une entité impliquée dans une communication, de nier avoir participé à tout ou partie des échanges.

**Réseau -** Ensemble de ressources de transmission mises en commun pour les besoins d'une pluralité d'équipements. Désigne également la troisième couche du modèle OSI, assurant les fonctions de mise en relation à travers des nœuds intermédiaires.

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.

Selon le type d'objet, on parlera parfois de:

- Réseau de transport = ensemble d'infrastructures et de disposition permettant de transporter des personnes et des biens entre plusieurs zones géographiques.
- Réseau téléphonique = infrastructure permettant de faire circuler la voix entre plusieurs postes téléphoniques.
- Réseau de neurones = ensemble de cellules interconnectées entre-elles
- Réseau de malfaiteurs = ensemble d'escrocs qui sont en contact les uns avec les autres.
- Réseau informatique = ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques.

Il n'existe pas un seul type de réseau parce qu'il existe plusieurs types d'ordinateurs, communiquant selon des langages divers et variés avec des supports physiques de transmission les reliant hétérogènes, que ce soit au niveau du transfert de données (circulation de données sous forme d'impulsions électriques, sous forme de lumière ou bien sous forme d'ondes électromagnétiques) ou bien au niveau du type de support (lignes en cuivres, en câble coaxial, en fibre optique, ...). On pourrait imaginer établir des canaux de transmission point à point entre chaque couple d'émetteur - récepteur, mais cette solution conduirait à un immense gâchis de liaisons inutiles :

- Gâchis dans l'espace car chaque émetteur n'a pas forcément besoin de communiquer avec tous les autres émetteurs.
- Gâchis dans le temps car il n'a pas besoin non plus d'avoir à sa disposition permanente une liaison avec tel autre récepteur.

On aura donc intérêt à constituer une infrastructure de transmission partageable par l'ensemble des récepteurs et émetteurs potentiels. Partageable dans l'espace, en reliant plusieurs terminaux à un même canal, et partageable dans le temps, en affectant un même canal successivement à plusieurs terminaux. C'est cette mise en commun des canaux de transmission qui fonde la notion de réseau.

Dans l'industrie du mobile, réseau fait référence à l'infrastructure qui permet la transmission de signaux mobiles. Un réseau relie les divers éléments entre eux et autorise le partage des ressources.

**Réseau 1G -** Réseau de première génération - De type analogique, avant 1991. Radiocom 2000 de France Télécom, l'AMPS aux Etats-Unis par exemple.

**Réseau 2,5G -** Technologie numérique d'échange de données sans haut débit (par exemple PDC Packet au Japon, le CDMA One aux Etats-Unis, au Japon et en Asie).

**Réseau 2G -** Réseau de seconde génération, de type numérique, pour les communications vocales (GSM 900 MHz ou 1800 MHz et DCS 1800 MHz en Europe, GSM 1900 MHz en Amérique, PDC au Japon).

**Réseau 3G -** Réseau de troisième génération pour les échanges de données et de contenus multimédia à haut débit en mode paquet. Différentes mises en œuvre au monde : W-CDMA baptisé UMTS en Europe et au Japon, CDMA 2000 aux Etats-Unis, Asie du Sud-est et Japon.

**Réseau à large bande -** Broadband Network - Expression utilisée pour désigner un réseau de transmission numérique capable d'acheminer de grands débits d'informations (à partir de plusieurs Mbit/s).

**Réseau à valeur ajoutée -** RVA - Value Added Network, VAN - Réseau dans lequel un traitement ajoute de la valeur à l'information acheminée.

**Réseau d'accès -** Réseau sur lequel les utilisateurs connectent directement leurs équipements terminaux afin d'accéder aux services. (voir "cœur de réseau").

Ensemble des moyens servant à relier des terminaux de télécommunication à un commutateur de réseau d'infrastructure.

**Réseau d'Infrastructure -** Partie centrale d'un réseau de télécommunication qui comprend un certain nombre de commutateurs et les liaisons entre ces commutateurs.

**Réseau de données -** Data Network - Ensemble des unités fonctionnelles qui établissent des circuits de données entre des terminaux.

**Réseau étendu -** Wide Area Network, WAN - Réseau généralement constitué de plusieurs sous-réseaux hétérogènes et s'étendant sur une région ou un pays entier.

Ne s'utilise que pour les données. Pour le téléphone, on parle de réseau interurbain ou de réseau à grande distance (trunk network, toll network, long distance network).

**Réseau filaire -** Réseau utilisant comme support des câbles métalliques ou des fibres optiques.

**Réseau indépendant -** Désigne, selon la réglementation française des télécommunications, un réseau et ses installations réservés à l'usage d'une entreprise, ou d'un ou plusieurs groupes ou communautés fermés d'utilisateurs.

**Réseau Intelligent -** Concept facilitant notamment l'introduction de nouveaux services : vote à distance, sondage d'opinion, libre appel, taxation partagée, GSM, etc.

**Réseau local -** LAN - Système de communication mettant en relation permanente par des câbles plusieurs équipements informatiques (stations de travail, minis ou micro-ordinateurs, terminaux) desservant un ensemble d'utilisateurs. Il peut correspondre aux besoins des personnes travaillant dans une seule pièce, un service, un étage ou un bâtiment complet. Il se définit par son système de câblage, sa vitesse, sa méthode d'accès et son logiciel de gestion. Les deux principales familles de réseaux locaux sont Ethernet et l'Anneau à jeton.

Réseau de données à haute vitesse et à faible taux d'erreur couvrant une zone géographique relativement petite (jusqu'à quelques milliers de mètres). Les réseaux locaux interconnectent des stations de travail, des périphériques, des terminaux et d'autres équipements dans un seul immeuble ou autre zone géographique limitée. Les standards de réseaux locaux spécifient le câblage et la signalisation au niveau des couches physiques et liaison de données du modèle OSI. Ethernet, FDDI et Token Ring sont des technologies de réseau local largement utilisées.

**Réseau Local d'Entreprise -** RLE - Local Area Network, LAN - Réseau de télécommunication privé et qui ne dépasse pas quelques kilomètres.

**Réseau maillé -** Une architecture de réseau selon laquelle tous les nœuds sont accessibles entre eux et ce par des liaisons (ou chemins) multiples. Le maillage d'un réseau augmente son niveau de sécurité puisqu'il offre des alternatives en cas de rupture d'une ou plusieurs liaisons.

**Réseau Métropolitain -** Metropolitan Area Network, MAN - Réseau qui s'étend sur une zone géographique de la taille d'une ville.

**Réseau ouvert au public -** Tout réseau de télécommunications établi ou utilisé pour la fourniture au public de services de télécommunications.

**Réseau par Satellite -** Réseau utilisant les fréquences hertziennes relayées par satellite

**Réseau par satellite -** Réseau utilisant les fréquences hertziennes relayées par satellite.

**Réseau radio mobile -** Réseau utilisant les fréquences hertziennes pour relier les mobiles au réseau fixe ou mobile.

**Réseau radioélectrique à ressources partagées ou 3RP -** Trunked System - Réseau de radiocommunications avec des mobiles, dans lequel des moyens de transmission sont partagés entre les usagers de plusieurs entreprises ou organismes pour des communications internes. Ce partage se caractérise par le fait que l'attribution de ces moyens aux usagers ne se fait que pour la durée de chaque communication.

**Réseau radioélectrique réservé aux données ou 3RD -** Réseau radio numérique qui offre des services de radio transmission de données avec des mobiles. Les 3RD, comme le Mobipac, utilisent la radio transmission de données par paquets.

**Réseau téléphonique -** Le réseau le plus répandu reste le réseau téléphonique. Il est commuté, d'ou le nom qui lui est couramment donné de RTC (Réseau Téléphonique Commuté). Le RTC a donc été conçu comme un réseau de transport de la voix. Mais il peut servir à transporter des données, avec l'avantage d'être bon marché et disponible en tout point du territoire. Le RTC demeure du reste le principal réseau de transmission de données, si l'on compte en nombre d'accès. Le réseau téléphonique apparaît globalement comme une ressource analogique, nécessitant donc pour transporter des données le recours à un modem. Son débit reste limité même en utilisant les perfectionnements apportés par la compression.

**Réseau Téléphonique Commuté ou RTC -** Public Switched Telephone Network, PSTN - Réseau téléphonique commuté construit et géré par un exploitant publique.

**Réseaux à Valeur Ajouté -** Réseaux dédiés à des transmissions de données spécifiques (à une profession par exemple) et loués par l'opérateur aux entreprises et institutions intéressées.

**Réseaux ad hoc -** Type d'architecture applicable aux réseaux locaux sans fils type WLAN et concernant les utilisateurs souhaitant avoir un réseau local sans fil, sans infrastructure (surtout sans Point d'Accès). Ceci peut permettre le transfert de fichiers entre deux utilisateurs d'agenda ou pour une rencontre hors de l'entreprise.
Le standard 802.11 répond à ce besoin par la définition du mode d'exécution "ad hoc ". Dans ce cas, il n'y a pas de Point d'Accès, et une partie de ses fonctionnalités sont reprises par les stations elles-mêmes (comme les trames balise pour la synchronisation). D'autres fonctions ne sont pas utilisables dans ce cas (relayage des trames ou mode d'économie d'énergie).

**Réseaux câblés -** Ce terme désigne les réseaux de télédistribution audiovisuelle établis en application de la loi n°82-652 du 29 juillet 1982 sur la communication audiovisuelle et de l'article 34 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication.

**Réseaux Photoniques -** Dans les réseaux télécoms, la transmission est optique = on envoie des impulsions lumineuses chargées de l'information dans des fibres optiques. Mais la commutation reste électrique : à chaque noeud du réseau, la lumière est convertie en signaux électriques, ensuite commutés, puis de nouveau transformés en lumière. D'où l'idée de ne plus passer par cette phase optique/électrique/optique, et de commuter directement les faisceaux lumineux. C'est ce qu'on appelle des commutateurs photoniques. Deux types de commutations en cours d'élaboration :

- la commutation par micro-miroirs MEMS (Mirror Electromechanical Switch). Grâce à la commutation optique, les rayons lumineux sont directement aiguillés vers leur destination au lieu d'être transformés en courant électrique pour emprunter des commutateurs classiques. Le cœur de celui-ci est composé d'une batterie de micro miroirs (un par longueur d'onde). Ils sont si petits que cent d'entre eux tiendraient sur une tête d'épingle. Ils sont motorisés par un dispositif électromécanique et travaillent à la vitesse de la nanoseconde. Lorsqu'un rayon lumineux frappe un miroir, celui-ci le renvoie vers le port d'entrée s'il ne doit pas être commuté ou le dévie par le micro miroir vers un port de sortie s'il doit l'être. Le développement de fonctions tout optique, telles que la conversion et la régénération de longueur d-onde sont en cours.
- la commutation par matrice "bulles ". Chez Agilent, on construit une matrice de guides de lumière dans laquelle on injecte les faisceaux lumineux. La commutation s'effectue en fonction de la présence ou non d'une bulle (comme dans les imprimantes à jet d'encre) au point de croisement entre une entrée et une sortie de la matrice : s'il n'y a pas de bulle, la lumière passe tout droit, s'il y a une bulle, elle est réfléchie vers la sortie correspondant à ce point de croisement. Le système est capable de produire et d'effacer des centaines de bulles par seconde sachant que la matrice compte 32 entrées et 32 sorties.

**RETD -** Réseau public à commutation de paquets espagnol.

**RETIF -** Réseau téléinformatique ferroviaire. Réseau privé de transmissions de données de la SNCF.

**Retour d'appel -** (tonalité de) - Indication audible transmise à l'abonné appelant pour lui signaler que la connexion a été établie et que la sonnerie retentit chez son correspondant.

**RFC -** Request For Comment - Procédure utilisée par les initiateurs de standards. Première étape vers une future norme. Par extension, les RFC portant sur le protocole IP sont des normes de facto.

**RFID -** Radio Frequency Identification - Technologie d'identification automatique d'objets fondée sur les radiofréquences. Apparue en 1948 pour distinguer les avions amis des avions ennemis, elle a été ensuite utilisée pour reconnaître le bétail avant de se répandre dans l'industrie, la distribution et les services. Parmi ses récentes applications figure le télépéage autoroutier.

Pour fonctionner, la RFID nécessite un lecteur, un composant placé sur l'objet à identifier et une antenne. Le composant (appelé tag ou étiquette) se présente sous la forme d'un petit morceau de plastique, gros comme deux allumettes, dans lequel une puce en silicium de 1 mm2 est soudée à une bobine.

La puce est programmée avec des données (jusqu'à 512 bits, soit 64 fois plus que le code à barres) qui identifient l'objet sur lequel elle est placée. Pour cela, le lecteur active la puce en émettant un signal radio ou électro-magnétique via l'antenne. En réponse, les données stockées dans la puce sont alors émises puis captées par l'antenne du lecteur. Celui-ci les décode puis les transmet à l'ordinateur chargé des traitements. Le lecteur reçoit une réponse du tag dans un délai inférieur à 100 millisecondes.

II existe deux types de tags :

Ils peuvent être actifs dès lors que les distances de lecture sont supérieures à 10 mètres, comme dans le cas du télépéage. Ils sont alors équipés d'une pile qui alimente le transmetteur-récepteur radio intégré afin d'augmenter la puissance du signal. La durée de vie de la pile est de l'ordre de trois ans.

À l'inverse, avec les tags passifs, c'est le lecteur qui fournit l'énergie nécessaire. Ce type de tags est plus léger, moins coûteux et offre une durée de vie quasi illimitée.

Autre particularité, les tags peuvent être de type « read only», autorisant uniquement la lecture des données, ou de type « read and write », permettant la lecture mais aussi l'écriture pour en modifier le contenu. Contraire-ment aux codes à barres. laRFID n'impose pas de manipuler les objets devant le lecteur pour les

identifier. Et même si les ondes sont sensibles à la proximité de certains liquides ou métaux, les tags peuvent être lus à travers la neige, le brouillard, la peinture ou le plastique.

Quatre fréquences sont utilisables (basse, haute, très haute et ultrahaute, de 125 kHz à 2,4 GHz) selon la distance et l'application.

**RFTS -** Remote Fiber Test System - Système de contôle et de surveillance à distance des réseaux optique. Permet de contrôler les réseaux à fibres optiques comportant des fibres noires ou des fibres en service.

**RG/U -** Abréviation US de Radio Government Universal. RG est la désignation militaire des câbles coaxiaux de la norme MIL-C-17. U "Utilisation Générale".

**RIP -** Routing Information Protocol - Premier protocole de routage utilisé dans Internet. Le premier protocole de routage développé afin de permettre à un routeur d'échanger des informations de routage avec un routeur voisin.

RIP est le protocole de routage interne le plus répandu. Il a été développé à l'université de Berkeley. C'est un protocole de routage par vecteur de distance, la plus ancienne famille de protocoles de routage. Il choisit le plus court chemin en fonction du nombre de nœuds traversés. Une route ne doit pas contenir plus de 15 sauts, c'est à dire pas plus de 15 autres rouleurs à traverser. Dans un système autonome utilisant RIP, chaque rouleur construit sa propre table de routage, c'est à dire qu'il indique vers quel nœud se diriger pour aller vers une machine donnée. Les rouleurs s'échangent leurs tables de routage afin que tous les chemins entre deux machines soient connus par chaque rouleur. Toutes les 30 secondes, un message de mise à jour de toutes les routes connues, contenant leur coût en sauts, est envoyé aux rouleurs qui l'ajoutent à leur table de routage. Les mises à jour servent à s'assurer qu'une route est toujours disponible. Si une route n'est pas actualisée par un message après 180 secondes, elle est considérée comme défaillante et se voit supprimée de la table de routage. RIP est incapable de répondre aux besoins de routage des grands réseaux comprenant beaucoup d'interconnexions.

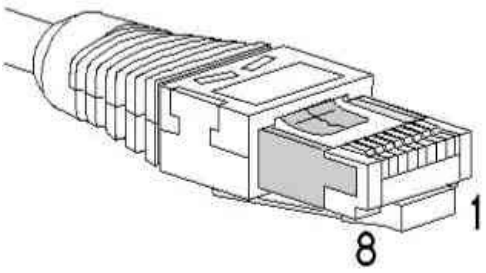
**RIP2 -** Routing Information Protocol 2 - Protocole de routage dynamique utilisé pour échanger des informations de routage. Il dérive d'un premier protocole développé par Xerox (RIP). Chaque machine qui utilise un protocole RIP2 a un processus qui envoie et reçoit des datagrammes transportés par de l'UDP port numéro 520.

**RIPX -** Protocole de routage dynamique de la famille Novelle Nexware. RIPX est utilisé pour collecter, maintenir et échanger des informations de routage correctes entre les passerelles dans Internet. Il ne faut pas confondre ce protocole avec celui de la famille TCP/IP ! !

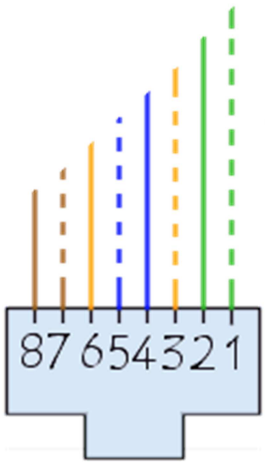
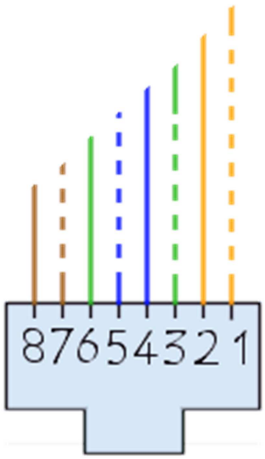
**Ripper -** C'est copier un DVD sur un disque dur en dissociant la vidéo, le son et éventuellement les protections☺.

**RITA -** Réseau Intégré de Transmissions Automatiques - Réseau de transmission de l'Armée de terre.

**RJ45 -** Petite fiche normalisée munie d'un clip de verrouillage et d'une capacité de 8 conducteurs utilisée dans la plupart des solutions de réseau local basées sur le cable UTP: ethernet 10bT et 100bT, token-ring, ...




Le connecteur 1 est à gauche sur une prise femelle (carte réseau ou bien prise murale) et à droite sur une prise mâle, connecteur vers soi, contacts vers le haut.
Les codes couleurs utilisés sont de deux types, ils sont normalisés :

| EIA/TIA 568A | EIA/TIA 568B |
|---|---|
|  |  |



Connecteur RJ45 sur une prise mâle vue de face, contacts vers le haut.

La norme de câblage communément utilisée pour réaliser des câbles droits est la norme EIA/TIA T568A. Il existe des câbles droits selon la norme EIA/TIA T568B sans incidence sur le fonctionnement dans la mesure où les fils sont reliés de la même façon.

**RJ48** - Petite fiche normalisée munie d'un clip de verrouillage et d'une capacité de 8 conducteurs, identique à la fiche RJ45 mais munie d'une petite excroissance plastique sur un de ses côtés: donc une fiche mâle RJ48 ne peut pas être enfichée dans une prise femelle RJ45 alors que l'inverse est possible. Ce détrompeur sur la fiche a pour but non pas de définir le sens d'utilisation (qui est de toute façon unique sur les fiches de la série RJ grâce au clip de verrouillage) mais plutôt d'éviter que l'on branche une prise RJ48 en générale utilisée pour des applications de téléphonie dans une prise RJ45 utilisée pour des applications de réseau et risquer d'endommager des cartes réseaux (la téléphonie utilise des courants et tensions plus élévés que les réseaux informatiques).

**RLAN -** Radio Local Area Network - Réseaux locaux radioélectriques (RLR)

**RLI -** Réseau Local Industriel.

**RLP -** Radio Link Protocol - Protocole de correction d'erreur utilisé lors de la connexion entre un terminal et le réseau GSM.

**RLR -** Réseaux Locaux Radioélectriques. Les réseaux locaux radioélectriques (RLR) appelés aussi "RLAN" (pour Radio Local Area Networks) sont constitués d'équipements de transmission de données à large bande permettant différents types d'applications sans fil (notamment des applications de bureautique et des applications de gestion professionnelles : entrepôts, hôpitaux, etc.). Une norme a été élaborée au niveau européen pour des équipements fonctionnant dans la bande de fréquence 2,4 GHz : l'ETS 300328. Cette norme d'application volontaire (chaque Etat peut décider ou non de la transposer, pour tout ou partie, dans son droit national) constitue la base d'une recommandation des administrations européennes des postes et télécommunications (CEPT), tendant à harmoniser le régime d'autorisation des équipements concernés afin de favoriser leur développement en Europe.

En France, la bande de fréquence concernée (plus précisément la bande de fréquence 2400 MHz - 2483,5 MHz), est encore utilisée partiellement par le Ministère de la défense, qui y a déployé récemment de nouveaux équipements, ce qui ne permet pas d'ouvrir la totalité de la bande de fréquence aux équipements RLR et impose certaines contraintes dues à la coordination avec les Forces Armées. Ceci nécessite notamment un agrément national basé sur une réglementation technique nationale mettant en œuvre l'ETS 300328 mais limitant la bande de fréquence utilisable : il s'agit de la spécification SP/DGPT/ATAS/23.

**RNA -** Raccordement Numérique Asymétrique - Technique de transmission numérique offrant deux canaux de données à haut débit sur une ligne téléphonique ordinaire en paire symétrique, le débit dans le sens du réseau vers l'utilisateur étant très supérieur au débit dans l'autre sens. Dans le sens du réseau vers l'utilisateur, le débit est suffisant pour permettre la distribution de programmes de télévision ou de documents multimédias, notamment en provenance de l'internet. Il est de l'ordre de 600 à 800 Kbit/s dans l'autre sens. En outre, le canal téléphonique est conservé.

L'expression "ligne numérique à paire asymétrique" ne doit pas être utilisée car il s'agit d'une transmission asymétrique sur paire symétrique. Voir ADSL. Abréviation employée : ADSL (Asymetric Digital Subscriber Line)

**RNIS -** Réseau Numérique à Intégration de Services - Réseau numérique dans lequel on utilise les mêmes commutateurs numériques et les mêmes conduits numériques pour établir des connexions pour différents services.

RNIS signifie Réseau numérique à intégration de services (ISDN ou Integrated Switched Digital Network en anglais). La différence qui existe entre le RNIS et le RTC, entre signaux numériques et analogiques, ressemble de très près à celle qui sépare le vieux microsillon au son analogique du disque compact au son numérique. La technologie numérique permet de n'enregistrer que les données pertinentes émanant de la source sonore et de transmettre le message numérique de façon beaucoup plus rapide et beaucoup plus précise que ne le fait la technologie analogique. Résultat, en ce qui concerne le RNIS, un son de haute qualité et une pléthore de services en complément des services supports proposés par le

réseau analogique: sous-adressage, identification de l'appelant, prise d'appel en instance, portabilité du terminal en cours de communication sont systématiquement fournis. Parmi les autres services sur option: sélection directe à l'arrivée, double appel va-et-vient, signalisation d'utilisateur à utilisateur avec possibilité d'envoyer un message de 32 caractères par le canal D.

Quand on parle de RNIS, on parle en effet de canal D, de canaux B, d'accès de base et d'accès primaire. Explications: à l'inverse de ce qui se passe sur le réseau analogique (NDLR: le réseau n'est numérique que jusqu'au commutateur de raccordement des abonnés; toutes les lignes de terminaison sont donc encore analogiques), où les signaux servant à l'établissement de la communication sont véhiculés sur les mêmes circuits utilisés pour transmettre les données sur le réseau RNIS, les données de signalisation sont acheminées sur un canal séparé dit canal D (D pour données ou data en anglais) à 16 Kbits/s dit encore canal sémaphore. Les données d'information à transmettre (voix, texte...) sont, quant à elles, acheminées sur deux canaux à 64 Kbits/s, dits canaux B (B pour bearer en anglais, c'est à dire support en français). L'intérêt de cette séparation sur des canaux différents des données de signalisation et des données d'information est de pouvoir communiquer sur deux lignes à la fois: continuer, par exemple, une conversation téléphonique tout en restant connecté à Internet. Ce débit total de 144 Kbits/s (1 canal D + 2 canaux B) constitue l'accès de base. L'accès de base intéresse notamment les PME et les toutes petites entreprises. L'accès primaire concerne les plus grandes entreprises. Il s'agit d'un accès totalisant 2 Mbits/s, constitué de 30 canaux B (30 x 64 Kbits/s) et d'un canal D qui cette fois véhicule les données de signalisation à 64 Kbits/s.

Concernant les raccordements RNIS, plusieurs configurations sont possibles selon la taille de l'entreprise. La plus simple consiste à placer sur un bus passif les prises en parallèle pour raccorder jusqu'à 8 terminaux. Mais il est également possible de disposer d'une régie privée à bus unique ou d'une régie à étoile de bus pour monter une installation de type réseau local. La régie à bus unique joue alors le rôle d'un petit autocommutateur qui permet de commuter les communications entre les terminaux ou simplement donne la possibilité aux terminaux de communiquer entre eux et de disposer du service sélection directe à l'arrivée (SDA). Enfin, la régie à étoile de bus convient pour des besoins plus importants puisqu'elle permet un raccordement en étoile autour d'une régie.

L'infrastructure nationale de télécommunications est en train de s'unifier pour devenir peu à peu totalement

numérique. Une offre de nouveaux services est donc disponible. A FT, cette offre porte le nom de Numéris, nom commercial du RNIS (*Réseau Numérique à Intégration de Services*) en anglais ISDN. Derrière cette offre, il faut considérer plusieurs composantes majeures : d'abord, l'accès à un service de commutation de circuits numériques, ensuite la possibilité de bénéficier sur le même accès de plusieurs services, une interface normalisée universelle pour tout type de service, et enfin un accès à une signalisation riche soit entre un usager et le réseau, soit entre deux usagers. La normalisation du RNIS est parfaitement définie pour les 3 couches basses du modèle OSI. La couche Physique (couche 1) décrit les interfaces dites S côté usager et T côté réseau, ainsi qu'une prise universelle à huit contacts (RJ45) prévue pour raccorder n'importe quel type de terminal. La couche Liaison de données (couche 2) utilise une procédure HDLC similaire à celle des réseaux à commutation de paquets X25. La couche Réseau (couche 3) est également identique à X25 avec en plus un protocole de signalisation spécial.

Sont ainsi définis, pour l'utilisateur, deux types d'accès:

L'accès de base prévoit un débit total de 144 Kbit/s découpé par multiplexage en deux canaux de 64 kbit/s, dits canaux B, et un canal de signalisation de 16kbit/s, dit canal D. L'interface est identifiée par la norme S0.

L'accès primaire, sous le nom d'interface S2, correspond à un débit global de 1 984 kbit/s, composé de trente canaux B de 64 kbit/s et d'un canal D à 64 kbit/s. Le nom de primaire provient du fait qu'il correspond à l'unité de concentration primaire dans la hiérarchie de multiplexage des réseaux publics.

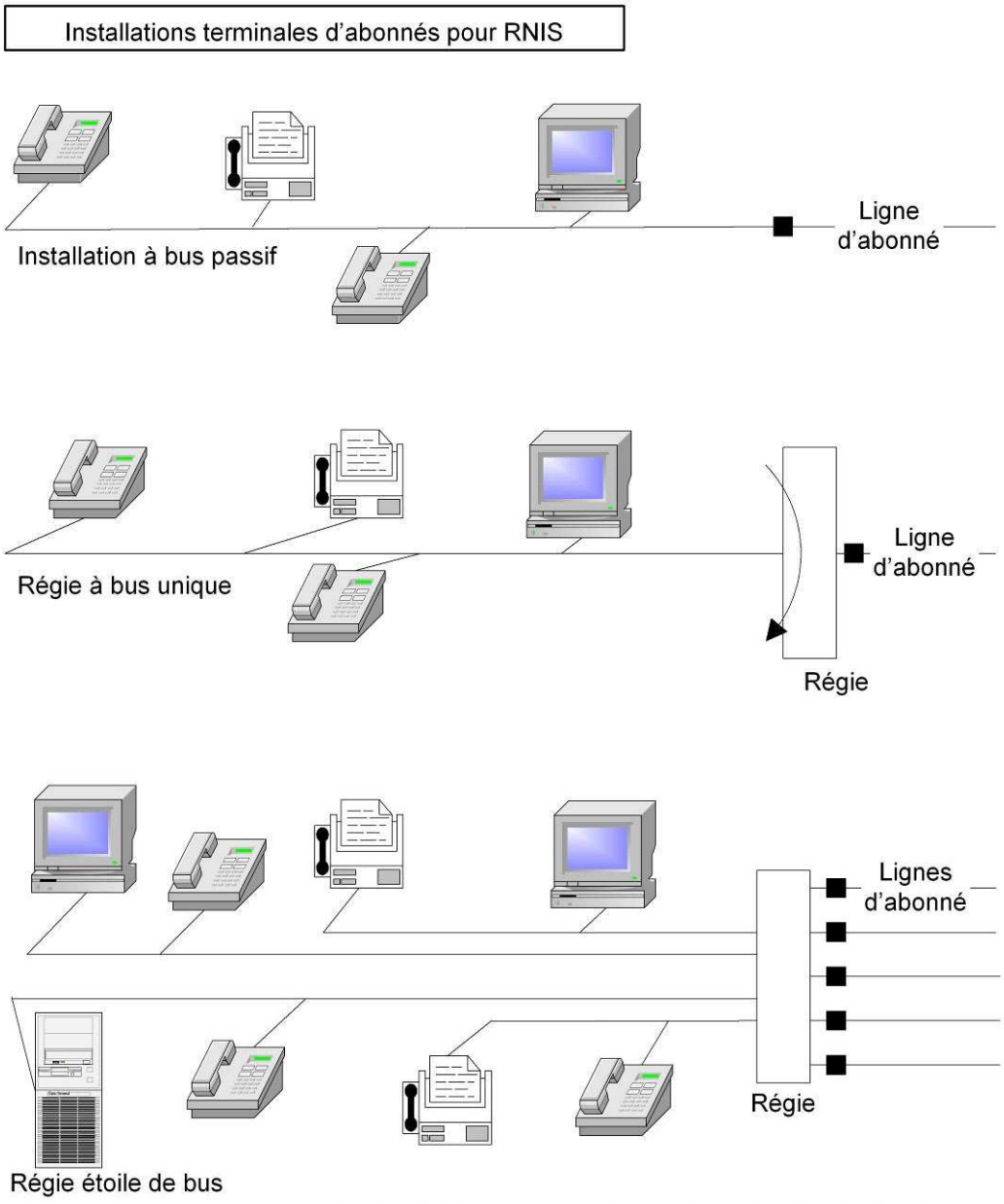
Les configurations de câblage sont de 4 types:

Bus court : 130m 10 prises max

Bus étendu : 130 à 500m (4 prises regroupées sur 30m)

Point à point: 800m

Distribution en Y : 2 branches de 90m (10 prises).




La régie à étoile de bus permet de raccorder en étoile jusqu'à 64 terminaux

**RNIS Large Bande -** L'utilisation des fibres optiques, permettant des débits à l'échelle du Gbit/sec, combinée aux nouvelles technologies de commutation et de transmission (ATM et SDH), conduit aux réseaux large bande. Le RNIS large bande est une architecture unique normalisée intégrant tous les services qui sont aujourd'hui offerts par des réseaux spécialisés (téléphone, TV, TRANSPAC, etc.). Ce réseau est capable d'absorber et de gérer, sur une même infrastructure, les trafics discontinus générés par chaque service, quelque élevés que puissent être les flux à un instant donné.

**RNRT -** Réseau National de Recherche en Télécommunication - Le RNRT fédère les pôles de compétences en télécommunications : Centre national d'étude des télécommunications (CNET), Institut national de recherche en informatique et en automatique (IRIA), Commissariat à l'énergie atomique (CEA), Centre national de la recherche scientifique (CNRS), Ecoles, Universités, Laboratoires industriels ou des opérateurs, etc… Ce réseau est opérationnel depuis le 1er Janvier 1998.

**Roaming** - Itinérance - Le roaming consiste à utiliser votre unité mobile en dehors de la zone de couverture locale assurée par votre opérateur de réseau. Des accords de roaming entre opérateurs permettent d'étendre la zone d'utilisation potentielle du téléphone. En général, les opérateurs facturent un tarif à la minute plus cher pour les appels passés en dehors de leur zone de couverture. Voir Itinérance.

**Rocade -** Câble multipaire utilisé pour relier les répartiteurs et les sous-répartiteurs dans les systèmes de pré-câblage.

**ROHS -** Reduction Of Hazardous Substances - Réduction des substances dangereuses - Directive européenne 2002/95/CE relative à la limitation de certains types de substances considérées comme dangereuses pour la santé ou nuisibles à l'environnement est entrée en vigueur le 13 février 2003, conjointement à la directive 2002/96/CE relative aux déchets d'équipements électriques et électroniques (DEEE). La directive a été suivie du décret 2005-829 puis d'arrêtés d'application fixant la date d'application au 1er juillet 2006.

La directive ROHS a pour objectif de limiter l'utilisation de substances dangereuses dans les équipements électriques et électroniques. La base légale des directives DEEE et ROHS se fonde sur les articles 95 et 175 du traité européen visant une protection de l'environnement.

L'objectif principal de cette directive est de réduire la diffusion de déchets de nature dangereuse pour l'homme et nuisible à l'environnement tout en proposant la possibilité de collecte, de réutilisation, de recyclage ou tout autre forme de traitement des déchets provenant de matériels électriques ou électroniques.

La directive ne confère pas de droit et n'impose pas d'obligations en tant que telles aux citoyens communautaires. Elles concernent uniquement les états membres, les droits et les obligations des citoyens ne découlant que des mesures prises par les autorités de chaque état membre les ayant mis en œuvre.

Les substances concernées sont (liste non exhaustive) : Le plomb, le mercure, le cadmium, le chrome hexavalent, les polybromobiphényles (PBB), les polybromodiphényléthers (PBDE)

Les équipements concernés (liste non exhaustive) : Gros appareils ménagers, petits appareils ménagers, matériel grand public, équipements informatiques et télécommunications, matériels d'éclairage, outils électriques et électroniques, jouets, équipements de loisirs et de sport, distributeurs automatiques…

Les distributeurs sont désormais tenus de verser une taxe à des organismes agréés par le ministère de l'Ecologie et du Développement durable. Ces organismes se chargent de la collecte et du recyclage des produits en fin de vie. (montant de la taxe = 15€ pour un produit valant 1000€). Le montant de cette taxe devra figurer sur les factures des distributeurs comme des revendeurs.

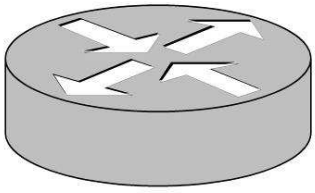
**ROI -** Return On Investment - En français = retour sur investissement - Nombre de mois au bout desquels l'économie réalisée par la mise en place d'un nouveau système en compense le coût.ra

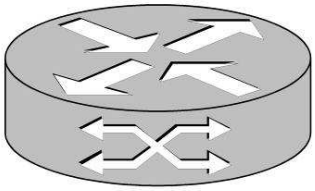
**ROSE -** Remote Operation Service Element - Sous-ensemble de protocole de la couche 7 dans le modèle OSI définissant un mode d'interconnexion entre applications sur le mode "questions-réponses".

**Routage -** Fonction d'acheminement d'une communication à travers un ou plusieurs intermédiaires. Cette fonction fait intervenir la notion de "chemin" et "d'adresse". Si elle s'effectue en tenant compte de la disponibilité des nœuds à un moment donné et de la charge du réseau, on parlera de routage "adaptatif". Dans le modèle OSI (Open System Interconnection) la fonction de routage est assurée dans la couche 3 (Réseau).

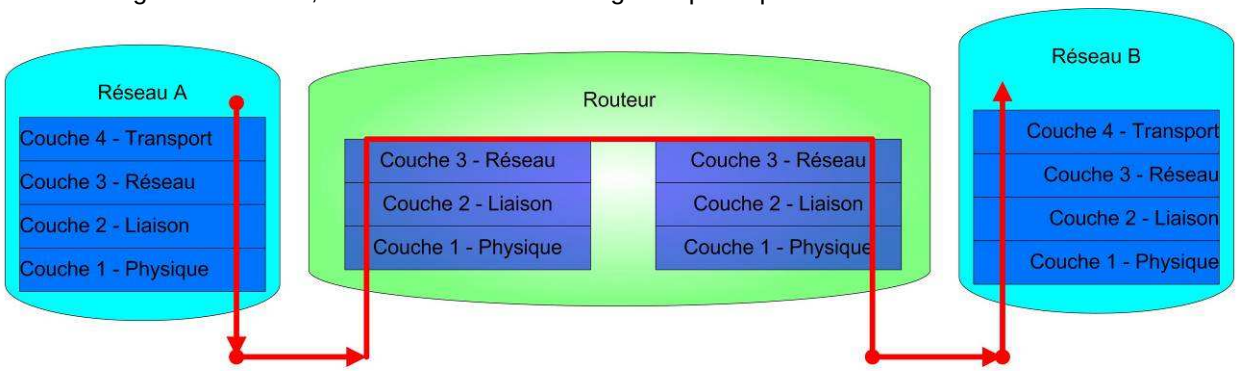
**Routeur -** Désigne une catégorie d'équipements assurant des fonctions de routage. Les routeurs, situés à des carrefours entre plusieurs nœuds de réseaux aiguillent les messages entrant en fonction de tables préprogrammées. Contrairement au pont, qui travaille au niveau de la couche 2 du modèle OSI, le routeur travaille au niveau de la couche 3 d'un réseau de télécommunication. Son rôle consiste à assurer, selon divers critères paramétrables, la meilleure transmission des informations d'un réseau à l'autre. La fonction de cet équipement est d'assurer une interface entre un ensemble de réseaux locaux hétérogènes et un réseau étendu constitué de liaisons fixes (offre Transfix de France Télécom) ou commutées (offre Numéris de France Télécom). Les fonctions type d'un routeur sont de grouper, réunir, filtrer, assembler par destination, les données véhiculées sur un réseau. Le routeur intervient au niveau 3 du modèle OSI et est donc dépendant du protocole réseau. Il peut relier deux réseaux locaux différents (Ethernet et Token Ring par exemple) en créant un réseau logique unique. Il faut toutefois noter que le routeur n'a pas de fonction de convertisseur de protocole, ceci étant la fonction d'une passerelle. Les routeurs installés sur des réseaux interconnectés doivent communiquer entre eux afin d'assurer le routage des protocoles de transport de données.


Routeur Cisco Type 4xxx


Représentation symbolique d'un routeur


Représentation symbolique d'un routeur avec ATM

Les routeurs réalisent une fonction d'adressage et doivent connaître la topologie des réseaux à interconnecter. Pour cette raison ils dépendent, contrairement aux ponts, du protocole utilisé. Les routeurs simples pourront, par exemple, connecter un réseau Ethernet à un Token-Ring, à condition que tous deux utilisent le même protocole. En réalité, cette limitation à été contournée par l'arrivée de routeurs multi protocoles. Le routeur est donc plus cher et moins rapide que le pont. Mais plus intelligent, il assure une meilleure intégrité du réseau, souvent avec des maillages sophistiqués.




Routeurs - Principes de fonctionnement.

Surtout utilisés pour des longues distances ou dans le cas d'interconnexion de nombreux réseaux locaux, les routeurs savent collaborer ensemble pour constituer une architecture de support maillée.

La technologie de routage s'appuie sur les protocoles de niveau 3 du modèle OSI. Ces protocoles sont par exemple TCP/IP, IPX ou Decnet.

Un routeur est constitué de 2 composantes essentielles : Une partie matérielle et une partie logicielle. La partie matérielle a pour objet de permettre au routeur de se raccorder à n'importe quel type de réseau (Ethernet, Token-Ring, FDDI, ligne série pour les réseaux longues distances, etc.). Le but de la partie logicielle est de router les paquets, c'est-à-dire de déterminer vers quelle interface envoyer le paquet.

La base du fonctionnement d'un routeur repose sur les deux concepts fondamentaux que sont l'adressage et le routage. Une adresse de niveau 3 se compose d'un numéro de réseau et d'un numéro de station au sein de ce réseau. Le routage consiste à acheminer un paquet parmi plusieurs routes possibles sans que les stations émettrices et réceptrices aient notion de la topologie des réseaux. L'intérêt principal du routeur est donc de segmenter le réseau de façon logique.

**Routeur VPN -** Routeur destiné à être installé dans les locaux du client. Ce type de routeur prend en charge la fonctionnalité VPN et offre des performances VPN optimales sur différents types de supports physiques et densités de ports.

**RPC -** Remote Procedure Call - Mode d'interconnexion par "appel de procédures" entre applications situées sur des machines différentes d'un réseau. Définit un cadre permettant de traduire les changements de contexte entre ces applications sans que l'application "appelante" ait à gérer ce changement. Les routines RPC permettent à des programmes d'appeler d'autres machines à travers le réseau.

**RPS -** Radiocommunications Professionnelles Simplifiées.

**RPV - (voir aussi VPN) -** Réseau Privé Virtuel - Un réseau privé virtuel consiste à partager l'utilisation d'un ou plusieurs réseaux ouverts au public pour les besoins internes d'un groupe fermé d'utilisateurs, défini, "comme un groupe qui repose sur une communauté d'intérêt suffisamment stable pour être identifiée et préexistante à la fourniture d'un service de télécommunications". Cette offre permet de répondre aux besoins de communications tant internes (à l'intérieur du groupe d'utilisateurs concerné), qu'externes (vers des utilisateurs du réseau public). Elle permet notamment aux entreprises qui ont des sites éloignés entre eux de bénéficier, sur le réseau de leur opérateur, d'un accès simulant un réseau privé avec un plan de numérotation interne à l'entreprise : une simulation qui offre le même service qu'un autocommutateur privé (PABX) et évite au client de réaliser les investissements correspondants.

**RPV SSL -** Réseau Privé Virtuel + SSL - Les RPV SSL utilisent la technologie SSL (Secure Socket Layer) des navigateurs web pour réaliser des connexions inter ou intra sites sécurisées.

Les RPV SSL fonctionnent au niveau 5 du modèle OSI, au dessus du protocole TCP/IP (qui est en couche 3 et 4). Au contraire d'un RPV IP Sec qui établit un tunnel au niveau IP pour permettre à l'utilisateur d'accéder à l'ensemble du réseau d'entreprise comme si il y était physiquement raccordé, un RPV SSL établit un tunnel le temps de la session applicative.

Il est à noter que les principaux freins au développement des RPV IPsec sont économiques (il faut installer un logiciel client en local sur le poste de l'utilisateur distant ou mobile), s'accommodent mal des mécanismes de traduction d'adresse de type NAT. A contrario, la technologie RPV SSL est plus économique parce qu'elle réutilise le protocole intégré dans le navigateur, mais elle n'est facilement déployable que lors d'accès à des applications accessibles via http. Des modules permettant d'ouvrir les accès sont disponibles, mais payants (comme IP Sec).

**RRI -** Réseau Radioélectrique Indépendant du service mobile terrestre). Réseaux Radioélectriques Indépendants relevant de la l'article L 33-2 de la loi de 1996 sur les télécommunications. Voir Radio Professionnelle & PMR.

**RS 232 -** L'une des plus répandues des interfaces normalisées entre un Equipement terminal informatique (ETCD) et un Equipement d'adaptation (ETTD). L'interface RS 232 définit des caractéristiques physiques : prise à 25 points, longueur et dimension du câble, vitesse maximale de 19 200 bps. (sauf que depuis un certain temps les 25 points sont devenus neufs points et que les débits ont légèrement augmenté).

Standard Recommandé de l'EIA pour les équipements terminaux de traitement de données et de terminaison de circuits de données.

**RS 422 -** Norme EIA - Utilisée dans les communications point à point par des circuits à deux états. Elle définit une interface électrique en différentiel de tension équilibrée.

**RS 485 -** Interface équilibrée similaire au RS 422 mais utilisant des circuits à trois états pour les applications multipoints.

**RSA -** Rivest, Shamir, Adelman - Algorithme de cryptage à clé publique permettant de crypter ou de décrypter des données et d'appliquer ou de vérifier une signature numérique.

RSA est fondé sur des fonctions mathématiques de type exponentielle et modulaire.

La sécurité de RSA repose sur la théorie des nombres, et plus particulièrement de la difficulté de les factoriser. En effet, la clé publique et privée générée par le cryptosystème RSA sont des fonctions d'une paire de grands nombres premiers. Ainsi, retrouver un message en claire à partir d'une des clés et du texte chiffré équivaux à factoriser le produit de deux nombres premiers. Ceci apparaît très simple pour des petits nombres premiers, mais beaucoup plus ardu pour des nombres de l'ordre de 100 à 200 chiffres.

Le RSA cryptosystème RSA fait partieintégrante de beaucoup de standards dans le monde. L'ISO 9796 et l'ITU-T X509 référence RSA comme un algorithme cryptographique compatible. RSA est inclut dans le standard SWIFT (Society for Worldwide Interbank Financial Telecommunications) dans le domaine interbancaire mondiale, dans l'industrie financière française (ETEBAC 5), dans l'ANSI X9.31 DSA standard et X9.44 pour l'industrie bancaire Américaine. Les Australiens l'on aussi inclut dans le standard de gestion des clés AS2805.6.5.3. L'algorithme RSA se retrouve dans les standards de l'Internet et dans des protocoles de sécurité tel que S/MIME , IPSec, et TLS (le standard de l'Internet succèdent au SSL), au même titre que le standards PKCS dans l'industrie du logiciel.

**RSB -** Rapport Signal Bruit ou ACR - Différence entre paradiaphonie et affaiblissement. Permet de juger de la qualité d'un signal. Le rapport Signal Bruit s'exprime en dB.

**RSVP -** Resource Reservation Protocol - Protocole destiné à améliorer la qualité de service dans les réseaux par l'établissement d'une liaison réservée entre deux points du réseau. RSVP établit et maintient un état logiciel entre les nœuds constituant le chemin réservé. Par opposition à la réservation d'un chemin statique (par exemple, l'établissement d'un circuit virtuel), cet état logiciel est caractérisé par des messages périodiques de rafraîchissement envoyés le long du chemin pour maintenir l'état. RSVP fournit aussi une qualité de service dynamique tenant compte des modifications de ressources pouvant survenir du fait du destinataire ou de l'émetteur, ou encore, par l'introduction de nouveaux membres dans un groupe multicast.

Ce protocole agit sur le réseau au coeur des routeurs, pour en canaliser et en discipliner le comportement et le rendre compatible avec les impératifs du temps réel. Il est conçu pour optimiser la livraison de données temps réel en mode multipoint, d'un émetteur vers plusieurs destinataires. Le fonctionnement uni point, d'un émetteur vers un seul destinataire, en est un mode dégradé. RSVP est l'un des moyens qui permettra à un réseau IP de devenir un réseau "d'intégration de services", fournissant à la fois un service "pour le mieux" (best effort) et une Qualité de service de type temps réel. Lorsqu'une application réclamera un niveau de Qualité de service particulier pour son flux de données, le protocole RSVP demandera aux routeurs du ou des chemins entre la source et le ou les destinataire(s), de réserver suffisamment de ressources pour maintenir ce niveau de qualité.

RSVP est un protocole de contrôle qui permet de demander une certaine qualité de service entre différents

nœuds d'un réseau pour un flux de données. Les applications temps réel utilisent RSVP pour effectuer des réservations de ressources au niveau des routeurs sur la ligne de transmission.

RSVP est un mécanisme de signalisation, le signal étant constitué par l'information de contrôle de qualité de service. Il établit et maintient un état logiciel entre les nœuds constituant le chemin réservé.

Par opposition à la réservation d'un chemin statique (par exemple l'établissement d'un circuit virtuel), cet état logiciel est caractérisé par des messages périodiques de rafraîchissement envoyés le long du chemin pour maintenir l'état.

RSVP fournit aussi une qualité de service dynamique, tenant compte des modifications de ressources pouvant survenir du fait du destinataire ou de l'émetteur ou encore par l'introduction de nouveaux membres dans un groupe multicast.

Dans RSVP, le destinataire est responsable de la réservation de ressources pour la qualité de service.

L'émetteur RSVP envoie ses exigences au destinataire. Après réception, le destinataire RSVP utilise le même chemin pour renvoyer un message spécifiant la qualité de service souhaitée et fixer la réservation des ressources correspondantes dans chaque nœud. L'émetteur RSVP envoie alors les données.

Protocole très gourmand en ressources pour les équipements, susceptible de diminuer les performances de chaque nœud du réseau, RSVP se voit souvent décrié par les équipementiers.

Les flux RSVP sont simplex. RSVP distingue le receveur de l'envoyeur. Même si bien souvent les hôtes sont à la fois envoyeur et receveur, la réservation RSVP n'est effectuée que pour des flux de données dans une seule direction.

RSVP a été créé pour une utilisation à la fois multicast et unicast. Parce que les réservations sont initiées par les destinataires et le maintien de l'état de réservation se fait de façon logicielle, RSVP peut facilement gérer le changement de membres et de routes. Un hôte peut faire une demande pour joindre un groupe par IGMP.

L'agrégation de réservations permet à RSVP de s'étendre à de grand groupe multicast sans causer un ratio données utiles sur en-tête trop important.

RSVP est orienté receveur, et peut gérer des receveurs hétérogènes. Les receveurs sont responsables du choix de leur niveau de qualité de service en initiant la réservation et en la maintenant aussi longtemps qu'ils le souhaitent. Ceci permet aux receveurs de demander une qualité de service adaptée à leurs capacités.

RSVP offre une grande compatibilité. RSVP a été créé en vu de fonctionner sur IPv4 et IPv6. Il s'adapte aux parties du réseau ne supportant pas RSVP, en se montrant transparent.

**RTC -** Réseau Téléphonique Commuté - C'est le réseau téléphonique ordinaire nommé PSTN en anglais.

**RTCP -** Réseau Téléphonique Commuté Public - Réseau de téléphonie terrestre dit fixe, filaire ou classique, reliant les usagers entre eux au moyen de câbles (coaxiaux, fibres optiques...) et de liaisons satellites.

**RTP / RTCP -** Real-time Transport Protocol / Real-Time Transport Control Protocol - Protocole "standard" Internet pour le transport de données temps réel, comprenant de l'audio et de la vidéo. RTP peut être utilisé aussi bien pour des médias "à la demande "que pour des services interactifs comme la téléphonie par Internet.

RTP est constitué d'une partie donnée et d'une partie de contrôle : le RTCP.

La partie donnée de RTP est un protocole léger qui offre un support pour les applications avec des propriétés temps réel, comme les médias continus (audio et vidéo), en permettant une reconstruction de la synchronisation, un ordonnancement dans l'arrivée des paquets, une détection de perte, une sécurité et une identification de contenu.

RTCP permet de créer des groupes de conférences temps réel de taille quelconque sur Internet. Il permet une identification de la source et l'utilisation de passerelles. RTCP offre un retour de qualité de service du receveur vers le groupe multicast, ainsi que la synchronisation des différents flux de données.

L'utilisation de RTP se fait essentiellement sur un environnement UDP/IP, il vient se greffer en temps que protocole de transport à la suite de UDP. RTP n'assure pas une réservation de ressources ou un contrôle de qualité de service, il s'appuie pour cela sur des protocoles de type RSVP.

RTP offre des services pour permettre l'envoie de données avec des caractéristiques temps réel, comme la vidéo et l'audio interactive. RTP dépend de RSVP en ce qui concerne la réservation de ressources et l'octroi de la qualité de service appropriée.

RTP n'est pas dépendant du réseau. RTP fonctionne principalement sur UDP, mais est aussi compatible avec ATM AAL5 et Ipv6.

RTP n'offre pas de gestion de flux ni de garantis. Il ne fournit que des indicateurs de temps et des numéros de séquences qui peuvent être utilisés par les protocoles de niveau supérieur pour les implémenter.

RTP et RTCP fournissent les fonctionnalités pour transporter des données temps réels de bout en bout. La synchronisation et l'assemblage des données sont laissés à l'application.

RTCP surveille la qualité de service et effectue un contrôle de la congestion, identifie la source (SDES, Source DEScription, pouvant contenir par exemple le nom, le numéro de téléphone, l'adresse e-mail et d'autres informations relatives à la source), et contrôle le dimensionnement de l'information de contrôle

(Celui-ci n'excédera pas 5% du trafic temps réel généré par RTP).

RTP *(Real Time Protocol*) est un protocole de transport de données de bout en bout adapté aux applications temps réel. Il offre à ces applications des moyens pour reconstituer la base de temps des flux de données audio, vidéo et temps réel en général et permet de détecter rapidement la perte de paquets et d'identifier le contenu des données et permettre leur transmission sécurisée.

En VOIP, le protocole RTP a pour tâche de transmettre le flux de données multimédia (audio, vidéo, texte, etc.), c'est-à-dire de crypter les données et de les diviser en paquets qui sont ensuite transmis.

**RTSP** - Real Time Streaming Protocol - Protocole de présentation multimédia client-serveur qui permet d'envoyer un flux de donnée multimédia sur un réseau IP, et offre par ailleurs des méthodes de contrôle de flux à distance, tel que la pause, l'avance rapide le retour rapide…

Ce flux multimédia, plutôt que d'être stocké et lu par la suite par l'application, est lu "au fil de l'eau - au fur et à mesure" que les données arrivent.

RTSP est un protocole de niveau applicatif créé pour être utilisé de concert avec des protocoles de plus bas niveau tel RTP et RSVP, pour fournir un service de flux temps réel sur Internet. Il peut être utilisé dans le cas du multicast et de l'unicast.

RTSP est un protocole de niveau applicatif, avec une syntaxe et des opérations similaires à HTTP, mais qui est utilisée pour l'audio et la vidéo. Il utilise des URL, du type : "rtsp://address:RTSPPort/directory/path/file ". Un serveur RTSP doit maintenir les états, en utilisant des méthodes spécifiques. Les messages RTSP sont envoyés indépendamment des données. Le client et le serveur RTSP peuvent initier des requêtes. RTSP est disponible sur différents systèmes d'exploitation, ce qui le rend interopérable.

**RTTE -** Radio equipment and Telecommuncations Terminal Equipment

**RUBIS -** Réseau de transmissions de données et de radiocommunications de la Gendarmerie nationale.

**RVA -** Réseau à Valeur Ajoutée - Désigne un réseau public ou privé dont la capacité est revendue à des tiers, accompagnée de divers services (la valeur ajoutée). Cette valeur ajoutée peut être variable, allant de la simple mise en communication (avec éventuellement adaptation, conversion de protocoles, facturation, garantie de sécurité) à des prestations complexes (applications informatiques, stockages intermédiaires, accès à des bases de données d'information, archivage, le compostage (time stamp - important pour l'E.D.I.), la gestion d'accusé de réception par un tiers ...). Dans le cadre de l'E.D.I., le RVA peut être vu comme un tiers de confiance.

# S

**S (interface S) -** Point de référence, dans la terminologie du CCITT, désignant une interface entre le terminal et un réseau de données. Dans le cas du Rnis on distinguera par exemple l'interface S0 (S zéro), définissant un Accès de base, et l'interface S2, délivrant un Accès primaire.

**S/MIME -** Secure / Multipurpose Internet Mail Extensions - Protocole qui ajoute les fonctions de signatures digitales et d'encryption à MIME, qui est la proposition officielle pour le format des mails sur Internet.

**SAA -** System Application Architecture - Equivalent en anglais du sigle AUA - Architecture unifiée d'applications. Désigne un ensemble de règles architecturales édictées par IBM pour parvenir progressivement à ce que des applications informatiques développées sur un système IBM puissent être portées sur n'importe quel autre système IBM. SAA vise aussi à harmoniser les présentations (écrans notamment) de toutes les applications quels que soient le matériel et le logiciel, et à permettre à ces applications de communiquer entre elles vers d'autres systèmes IBM.

**SACD -** Super Audio Compact Disc - Nouveau format de gravure numérique haute définition pour les disques compacts avec un nouveau codage de la musique (Direct Stream Digital). La fréquence d'échantillonnage (la division du son en données numériques) est beaucoup plus élevée que pour un Compact Disc : 2,82 Mégahertz (au lieu de 44,1 Kilohertz pour un CD). On obtient ainsi une bande passante de 100 kHz (ce qui permet d'éliminer la perte des très hautes fréquences qu'impliquent les lecteurs de CD) et une dynamique de 120 dB. Le son est d'une bien plus grande finesse, plus clair et plus naturel.

L'enregistrement se fait sur 6 canaux non compressés (au lieu de 2 pour un CD normal) et (à condition de posséder le matériel adéquat, un ensemble "Home Cinéma" avec 5 ou 6 enceintes par exemple), l'auditeur bénéficie d'une spatialisation et d'une meilleure "présence" du son qui restitue l'ambiance sonore de la salle où le disque a été enregistré. Un menu intégré dans le lecteur permet de le configurer suivant le nombre de haut-parleurs dont on dispose pour s'adapter à chaque configuration de chaîne hi-fi. Les SACD peuvent être gravés en double couche : une couche "normale", permettant la lecture sur un lecteur de CD traditionnel (avec un son "basse définition") et une couche "Haute Définition" permettant la lecture au format SACD sur un lecteur SACD. Tous les SACD ne sont pas hybride et il faut donc veiller, si l'on ne possède pas de lecteur SACD, à n'acheter que des SACD hybrides. Toutefois, la quasi totalité des SACD disponibles actuellement sur le marché sont hybrides.

**SAN -** Storage Area Network - Solutions de stockage en réseau. Face au stockage en attachement direct (baie de disque Raid connectée à un serveur par un lien SCSI ou Fibre Channel), les solutions de stockage en réseau connaissent une croissance rapide. Elles répondent en effet aux besoins de consolidation et de mutualisation du stockage.

SAN ou NAS ?

Deux technologies se complètent aujourd'hui sur ce segment, le NAS (Network Attached Storage) et le SAN (Storage Aréa Network). Souvent opposées, elles sont en fait complémentaires, car elles correspondent à des besoins différents.

Dans le cas du NAS, la ressource de stockage est directement connectée au réseau Ethernet de l'entreprise. Le serveur NAS intègre le support de multiples "file systems réseau", tels que CIFS (Common Internet File System), le protocole de partage de fichiers de Microsoft, NFS (Network File System), un protocole de partage de fichier Unix ou AFP (Apple Share File Protocol), le protocole de partage de fichiers d'Apple. Une fois connecté au réseau, il peut jouer le rôle de plusieurs serveurs de fichiers partagés.

Dans le cas du SAN, un réseau spécifique est mis en place. Ce réseau, souvent sur interface Fibre Charnel, assure la connexion des serveurs de l'entreprise avec ses ressources de stockage (baies de disques, librairies de sauvegarde...). Il comporte ses propres équipements (câbles, commutateurs...). Les baies de stockage SAN n'apparaissent pas comme des volumes partagés sur le réseau. Elles sont directement accessibles en mode bloc par le système de fichier des serveurs. En clair, chaque serveur voit l'espace disque d'une baie SAN auquel il a accès comme son propre disque dur. L'administrateur doit donc définir très précisément les LUN (unités logiques) et le zoning, pour qu'un serveur Unix n'accède pas aux mêmes ressources qu'un serveur Windows utilisant un file system différent.

Le principal avantage d'un serveur NAS est sa simplicité de mise en œuvre. En fait, il se configure comme un serveur de fichiers. L'administrateur définit des volumes logiques sur la baie et les autorisations de partage. Puis il décide quels systèmes de fichiers seront disponibles. Ceci fait, les volumes du NAS apparaissent sur le réseau comme tout volume réseau partagé. Un PC voit ainsi les volumes CIFS comme des volumes de serveur Windows dans son voisinage réseau.

La limitation à un mode fichier dote le NAS de plusieurs atouts. Un volume logique peut ainsi être configuré pour être accessible via plusieurs systèmes de fichiers réseau (par exemple SMB/CIFS, AFP et NFS). Il peut alors être partagé en natif par des PC sous Windows, des Mac et des stations Unix/Linux pour s'échanger des fichiers. Ce genre de fonctionnalités explique le succès du NAS en environnement PME/PMI. En revanche, l'absence d'accès en mode bloc fait souvent préférer le SAN pour des applications intensives, telles les bases de données.

Au-delà du partage de fichiers en réseau, les serveurs NAS peuvent jouer d'autres rôles au sein d'une infrastructure de stockage. Par exemple, ils font office de serveurs web, HTTP est alors considéré comme un protocole de partage de fichiers parmi tant d'autres. Les serveurs NAS sont aussi utilisés dans des architectures de cache web ou comme dispositif de sauvegarde. Sans se substituer aux sauvegardes sur bandes, ils fournissent un niveau intermédiaire de stockage dans le cadre d'applications de stockage hiérarchique (HSM). L'étage bande est alors purement dédié à l'archivage, le NAS jouant le rôle de sauvegarde de premier niveau.

L'avenir est la convergence des SAN et des NAS en milieu et haut de gamme. L'idée est de bénéficier, dans le même dispositif, d'une ressource disque mutualisée, accessible à la fois en mode SAN et en mode NAS. Cela ne signifie toutefois pas que l'on pourra accéder au même volume logique à la fois en mode bloc et en mode fichiers à travers deux interfaces différentes. L'équipement présentera un espace de stockage global, dont une partie (un ou plusieurs LUN) pourra être dédiée aux applications NAS, le reste étant mis à la disposition du SAN. Dans la pratique, le système de gestion (les entrées/sorties interne du NAS accèdera en mode bloc à un volume logique, mis à disposition des postes de l'entreprise à travers des systèmes de fichiers réseau. Quant aux autres volumes logiques, on pourra y accéder en mode bloc via leurs systèmes de fichiers natifs par les divers serveurs du réseau.

**SAP -** Service Access Point - Mécanisme logiciel de pointeurs autorisant un logiciel réseau à utiliser les services d'une couche inférieure. Le SAP est un numéro unique qui permet d'identifier le logiciel qui a envoyé un paquet ou une trame.

Point d'Accès à un service à l'intérieur d'une couche OSI en environnement ATM.

**SAP -** Service Advertsing Protocol. Protocole de la famille Novell Netware. Le service SAP diffuse l'information sur la liste des serveurs connu à travers tout le réseau. Ces serveurs peuvent comprendre des serveurs de fichiers, des serveurs d'impression, des serveurs d'accès Netware, et des serveurs distants.

**SAR -** Specific Absorption Rate (DAS en français).

**SATA -** Voir Serial ATA.

**Satellite** - Communication par Satellite - Le satellite est la partie centrale du réseau, utilisant des éléments actifs, il assure les fonctions de relais hertzien dans le ciel. Il est formé de l'assemblage de différents sous-systèmes de télécommunication et d'antennes et dispose aussi d'équipements assurant les fonctions d' Alimentation en énergie, de Commande d'orientation, de Maintien sur orbite, de Régulation thermique des équipements, et de Télémesure et télécommande.

Les équipements de télécommunication (répéteurs) assurent les mêmes fonctions qu'un relais hertzien : ils reçoivent les émissions provenant de la Terre et les réemettent vers la Terre après amplification et transposition de fréquence. Les antennes associées à ces répéteurs sont spécialement conçues pour assurer la couverture des régions de la Terre intéressées par le réseau satellite.

Le satellite de télécommunications repose sur les technologies et les techniques employées dans la plupart des autres satellites artificiels. La technologie des répéteurs est cependant particulière à ce type de satellite et dérive de celle des équipements de télécommunications de Terre. Certains composants, tels que les cellules solaires ou les tubes à ondes progressives, sont spécifiquement conçues pour les satellites. Les autres sont issus de chaînes de fabrication ordinaires mais ont été triés et ont subi des contrôles spéciaux en cours de fabrication et des essais finals. L'aptitude d'une chaîne de fabrication à produire des composants de qualité spatiale est vérifiée par une opération dite de"qualification spatiale ".

**Satellite géostationnaire -** Geostationary satellite - Satellite qui, placé sur une orbite de 36 000 km d'altitude, semble fixe pour un observateur immobile à la surface de la Terre.

**SAX -** Simple API for XML - Type d'analyseur (parser) XML. Contrairement à un analyseur DOM, qui lit un document XML en bloc, un analyseur SAX renvoie les éléments d'un document au fur et à mesure de leur lecture.

**Scanneur -** Application professionnelle permettant à l'utilisateur d'identifier et de corriger les failles dans la sécurité du réseau avant qu'un hacker ne le découvre.

**SCP -** Service Control Point - Point de contrôle de service dans la terminologie Rnis.

**SCP -** Système de Câblage Polyvalent développé par la société POUYET.

**Screephone -** Terminal comparable au Minitel qui permet de téléphoner mais aussi de surfer sur Internet, d'envoyer des e-mails tout en gardant la fonction Minitel Vidéotex.

**Scrutation -** Invitation à émettre ou à recevoir. voir Polling.

**SCS -** Société de Commercialisation de Services - Société vendant et gérant les abonnements de téléphonie mobile pour le compte d'un opérateur.

**S-CSCF -** Services Call Session Control Function - Serveur permettant d'identifier l'appelant et détectant le type de service associés. Voir IMS

**SCSI -** Small Computer System Interface - Interface parallèle haut débit (jusqu'à 320 Mo/s), limitée en distance du fait de la perte de signal propre aux communications parallèles. Le SCSI a constitué pendant des années l'interface de référence pour les sous-systèmes de stockage. Les chaînes SCSI sont limitées à 25 mètres et ne gèrent qu'un maximum de 16 périphériques par contrôleur. Cette interface est déclinée en plusieurs versions ou évolutions en fonction des débits.

**SDA -** Sélection Directe à l'Arrivée. Système équipant certains autocommutateurs d'entreprise et permettant d'aboutir directement sur le poste d'un abonné sans passer par le standard.

**SDH -** Synchronous Digital Hierarchy - Hiérarchie numérique synchrone - Le système SDH définit des niveaux successifs de concentration et des multiplexages des voies de transmission. SDH est un système qui pallie les principaux défauts du PDH et supporte des débits très élèves. SDH est caractérisé par :

- Affluents synchrones entre eux
- Débit de base de 155,520 Mbits/s en Europe.
- Support Fibre Optique.
- Normalise UIT-T et ANSI 2048 Kbits/s en France.
- Supporte les affluents de la Hiérarchie PDH
- Sécurité Intégrée (basculement sur une liaison de secours)
- Gestion de réseaux intégrée

La transmission des données s'effectue dans une trame de base au débit de 155,520 Mbits/s appelée module de transport STM-1. Les débits les plus élevés se transmettent dans des trames aux débits multiples de 4 de cette trame de base.

Le SDH a pour origine un système similaire, le SONET (Synchronous Optical Network). Dans SONET, STS-1 signifie Synchronous Transport Signal Level 1 et OC-1 signifie Optical Carrier Level 1.

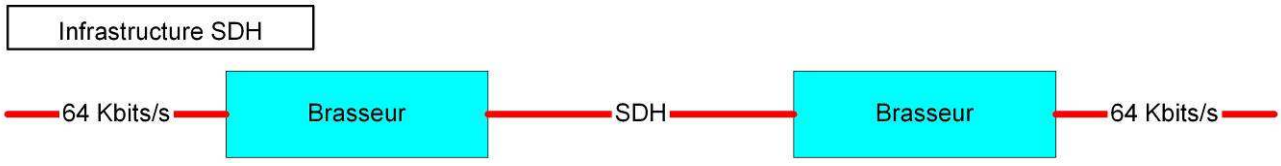
Comparaison/désignation SDH/SONET :

| Débit Brut exprimé en Mbits/sec. | Désignation SDH (IUT-T) | Désignation SONET (USA) |
|---|---|---|
| 51,84 | "STM-0" | STS/OC-1 |
| 155,520 | STM-1 | STS/OC-3 |
| 622,080 | STM-4 (4 x STM-1) | STS/OC-12 |
| 2488,320 | STM-16 (4 x STM-4) | STS/OC-48 |
| 9953,280 | STM-64 (4 x STM-16) | STS/OC-192 |

Le système SDH a fait son apparition à la fin des années 80 sur les réseaux de fibre optique, au moment où naissait aussi l'ATM. Le concept du SDH repose sur une structure de trame où les signaux qui doivent être transportés sont encapsulés dans un conteneur de la trame multiplexée. Un sur débit de conduit est associé à chacun de ces conteneurs et, les deux réunis, forment ce que l'on appelle un conteneur virtuel (VC). C'est ce dernier qui sera géré dans le réseau de transmission SDH, et ce, indépendamment du signal qu'il transporte. Si les réseaux SDH sont, comme leur nom l'indique, synchrones, les signaux peuvent arriver dans un nœud du réseau un peu chamboulés, le temps de propagation pouvant être différent dans le réseau. Si tel est le cas, le problème sera résolu par l'utilisation d'un pointeur qui indique la position relative du signal affluant et qui permet ainsi de repérer la phase des signaux.

Les réseaux SDH fonctionnent selon un mode de transmission parfaitement synchrone (l'émetteur et le récepteur sont calés sur la même horloge); ils sont plus faciles à gérer, la batterie de multiplexeurs caractéristique d'un réseau PDH étant remplacée par quelques brasseurs seulement. Les brasseurs SDH sont capables d'introduire et d'extraire des flux sans restriction de débit (de 155 Mbits/s à 2,5 Gbits/s). Ainsi, telle une gare de triage ferroviaire, le système SDH est capable d'aiguiller n'importe quel type de wagon de façon intelligente et quel que soit le débit des wagons de relais de trames ou des wagons ATM. Comme toute gare de triage aussi, le système SDH possède ses voies de services dédiées à l'exploitation du réseau.

Les brasseurs disposent en effet d'un sur débit d'exploitation réservé à la maintenance du réseau. Les réseaux ATM actuels s'appuient - ou s'appuieront - sur des réseaux SDH.




La trame de base SDH telle que définie par l'ex-CCITT (organe de normalisation de l'UIT) repose sur la technique de multiplexage synchrone. On parle de trame STM 1 (Synchronous Transfer Mode) lorsqu'il s'agit

de commuter des circuits à 155 Mbits/s (STM 4 pour des débits de 622 Mbits/s). La trame STM 1 est structurée en neuf rangées de 270 octets, soit une longueur de 2 430 octets pour une durée de 125 microsecondes et un débit de 155 Mbits/s. La trame a une capacité utile de 2 349 octets pour un débit de 150 Mbits/s et détient une capacité réservée à la gestion de 81 octets avec un sur débit de 5 Mbits/s. Le débit utile est celui correspondant aux conteneurs virtuels de base VC-4 (conteneur virtuel associé à un pointeur). À l'heure actuelle, le STM 1, le STM 4 (622 Mbits/s) et le STM 16 (2,4 Gbits/s) sont normalisés. L'introduction de débits supérieurs ne dépend que des évolutions technologiques.

Les recommandations de l'organisme de normalisation prévoient aussi une structure de multiplexage par laquelle un signal STM 1 peut transporter un nombre de signaux de charge utile à plus faible débit, permettant ainsi de transporter des signaux PDH sur un réseau synchrone. Enfin, le SDH permet aux utilisateurs de se voir allouer de la bande passante à la demande. Par exemple, dans le cas d'une vidéoconférence, l'utilisateur pourra obtenir la bande passante nécessaire en composant un simple numéro. Aujourd'hui, il faut bien souvent plusieurs jours avant de pouvoir obtenir cette bande passante. En résumé, le SDH élimine la complexité qui a tendance à freiner le développement de nouveaux services.

**SDLC -** Synchronous Data Link Control - Protocole développé par IBM dans le cadre de son architecture SNA. Protocole orienté bit (pas de notion de caractère), il travaille en mode synchrone bidirectionnel avec contrôle de redondance cyclique. Il est l'ancêtre des protocoles HDLC (High Level Data Link Control) dont il est très proche.

**S-DMB -** Salellite - Digital Multimedia Broadcasting - Protocle de diffusion par voie satellitaire, existe en deux versions :

- Coréen/Japonnais - Dérivé du SDMA, le protocole utilise la bande de fréquence Ku (12,214-12,239GHz pour le signal montant et la bande S (2,630-2,655 GHz) pour le signal descendant vers le mobile. L'architecture est hybride (MB sar) et réseau terrestre. Les débits sont de 7 Mbit / seconde lors de déplacement à 150 km/h. Il existe des services commerciaux au Japon et en Corée du Sud.
- Européen - Ce protocole de diffusion est assez proche de la version Japonnaise/Coréenne. Dérivé du W-CDMA (UMTS), ce protocole utilise la bande satellite IMT-2000 et l'UMTS. Des expérimentations sont en cours en Europe (décembre 2005).

**SDP -** Session Description Protocol - Le protocole SDP organise les codecs et les protocoles de transport utilisés entre les clients VOIP.

**SDSL -** Symmetric Digital Subscriber Line ou réseau de raccordement numérique à débit symétrique - Version à débit symétrique de l'ADSL qui s'adresse en priorité aux entreprises. Les débits varient de 192 Kbits/sec. à 2,3 Mbits/sec. La distance entre le central et le boîtier SDSL pourra atteindre 7 km alors que l'ADSL est limité à 4,5 km.

L'ADSL utilise une bande de fréquence comprise entre 20 kHz et 1,1 MHz sur la paire de cuivre, libérant la bande 0-4 kHz de la voix analogique. Le SDSL est appliqué dès 0 kHz et au-delà de 1,1 MHz (une seconde paire dont donc être raccordée pour la voix analogique). L'utilisation de hautes fréquences réduit la portée du SDSL (2 km pour 2 Mbit/seconde, si le câble a un diamètre de 0,4 mm) et augmente le risque d'interférence (donc de perte de paquets). Des travaux sont en cours pour augmenter la portée et le débit en passant d'une modulation PAM 16 à 8 ou 32, et réduire les interférences. L'annulation de "bruit" est déjà pratiquée en cas d'agrégation de liens.

En Europe, le terme générique SDSL est également utilisé pour désigner la technologie SHDSL (Symetric High-bit rate DSL), dont les débits s'élèvent à 2,3 Mbit/s.

**SDU -** Service Data Unit: unité de données échangées entre deux couches adjacentes ou homologues du modèle ISO pour "rendre le service" correspondant à ces couches.

**Secteur Spacial -** Désigne, dans un système de communication par satellite, l'ensemble constitué par les satellites et par les moyens qui assurent depuis le sol la poursuite, la télémesure, la télécommande et, d'une manière plus générale, le soutien logistique de ces satellites.

**Secteur terrien** - Désigne, dans un système de communication par satellite, l'ensemble constitué par les stations terrestres qui assurent l'émission et la réception des signaux de trafic de tout type en direction et en provenance des satellites et qui servent d'interface avec les réseaux de communications de la Terre.

Une station terrestre comprend l'ensemble des équipements terminaux d'une liaison par satellite. Elle joue un rôle équivalent à celui d'une station terminale de faisceau hertzien. Les stations terriennes comprennent en général les quatre parties principales suivantes :

- L'antenne d'émission et de réception dont le diamètre peut aller d'un mètre à plus de trente mètres. Les grandes antennes sont normalement munies d'un dispositif de poursuite automatique leur permettant de rester constamment pointées vers le satellite ; les antennes moyennes peuvent avoir des dispositifs de poursuite simple (système de poursuite par échelons, par exemple),
- Le récepteur, ayant un amplificateur d'entrée à sensibilité élevée et à faible bruit (de 40K, voire moins, à quelques centaines de K),
- L'émetteur dont la puissante peut varier de quelques watts à quelques kilowatts en fonction de la nature des signaux à transmettre et du trafic,
- Les équipements de modulation, de démodulation et de transposition de fréquence.

Un autre type de station terrestre est le téléphone mobile lui même ; il présente pratiquement les mêmes fonctionnalités qu'une passerelle.

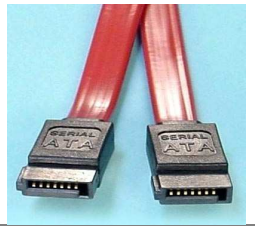
**Sélection du transporteur -** Possibilité offerte au consommateur de choisir entre plusieurs opérateurs de transport. La sélection du transporteur ne concerne que les appels longue distance et internationaux.

**Sémaphore -** Appellation d'un mode de signalisation (voir ce mot) normalisé sous le nom de CCITT n°7. Mis en place actuellement dans le réseau téléphonique national, il est accessible à l'utilisateur à travers le canal D (souvent appelé "canal sémaphore") du Rnis (Réseau numérique à intégration de services) français.

**Semi-duplex -** Mode de transmission bidirectionnel, mais non simultané, sur un canal de transmission. On dit aussi "half-duplex" ou "à l'alternat".

**SEPT -** Service d'Etudes communes des Postes et Télécommunications, basé à Caen.

**Serial ATA -** interface disque - Evolution de la norme ATA (appelée aussi IDE) avec transferts sériels, débit de 150 Mo/seconde à l'origine, puis 300 Mo/seconde et bientôt 600 Mo/seconde.



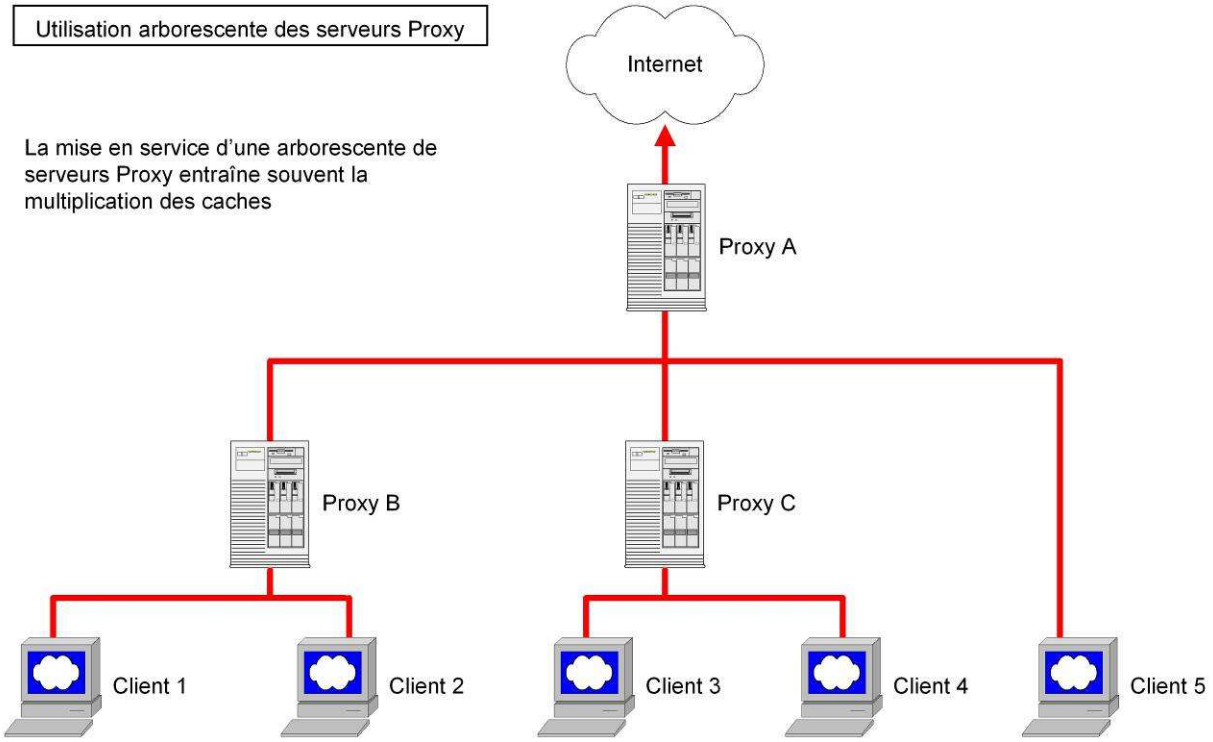

**Sérialisation -** Génération d'un signal faisant se succéder les bits les uns derrière les autres à partir d'un mot présenté en parallèle (tous les bits à la fois).

**Série -** Présentation en séquence des bits d'un message. S'oppose à parallèle.

**Serveur -** Désigne toute ressource informatique capable de délivrer une information où d'effectuer un traitement à la requête d'autres équipements. La notion de "serveur" est au Cœur de l'informatique, des télécommunications modernes et du mouvement de "décentralisation" des fonctions. Elle met en avant l'autonomie des équipements de requête par rapport à l'informatique centralisée où les initiatives ne pouvaient venir que de l'ordinateur central. Le mot "serveur" pourra ainsi désigner tout équipement capable d'assurer une fonction particulière à la demande d'un autre équipement. On parlera de "serveur d'informations", "serveur de messagerie", "serveur de calcul", "serveur de fichiers", "serveur de base de données"...

Système informatique destiné à fournir des services à des utilisateurs connectés et, par extension, organisme qui exploite un tel système.

**Serveur Proxy -** Souvent associé à un cache, il assure une réponse rapide aux ordinateurs d'un réseau local pour accéder à un système (à Internet en règle générale). Il permet de desservir rapidement les requêtes des utilisateurs tout en allégeant le trafic interne.




**Service -** Fonction assurée par une des couches du modèle OSI pour le niveau qui lui est immédiatement supérieur.

**Service de double transit -** Service figurant au catalogue d'interconnexion de France Télécom et permettant à un opérateur interconnecté au niveau d'un commutateur de transit (CT) d'atteindre les abonnés dépendant d'une autre zone de transit (ZT), n'importe où en France. Il permet ainsi d'atteindre toute la France.

**Service de Kiosque -** Service offert par un opérateur de télécommunication qui connecte un usager à un fournisseur de services à valeur ajoutée, consistant à assurer la facturation et le recouvrement de la totalité des sommes dues par l'usager et à reverser au fournisseur de services la part qui lui revient, sans lui révéler l'identité de l'usager.

**Service de messagerie vocale -** Service permettant d'orienter vers un répondeur enregistreur les communications à destination d'un abonné dont l'appareil n'est pas accessible. Le répondeur est intégré au réseau et non au terminal.

**Service de simple transit -** Service figurant au catalogue d'interconnexion de France Télécom et permettant à un opérateur interconnecté au niveau d'un commutateur de transit (CT) d'atteindre les abonnés dépendant de la zone de transit (ZT) à laquelle appartient ce CT, soit environ 2 millions de lignes.

**Service Intégré ou Unifié -** Service de télécommunication fourni par un exploitant de réseau ou un fournisseur de service, faisant appel aux moyens d'un ou plusieurs autres exploitants ou fournisseurs en utilisant des dispositions de guichet unique, et donnant aux utilisateurs l'impression d'accéder à un seul réseau de même aspect et sans discontinuité quelle que soit leur situation géographique.

**Service intra-CAA -** Service figurant au catalogue d'interconnexion de France Télécom qui correspond au raccordement d'un opérateur au niveau du commutateur d'abonné et permet d'atteindre 30 000 lignes.

**Service Support -** Bearer Service - Service de télécommunications offert à l'accès au réseau qui correspond aux couches basses du modèle OSI et assure donc le transport de l'information. Sa définition est indépendante des terminaux.

**Service téléphonique au public -** Service défini par la loi comme "l'exploitation commerciale pour le public du transfert direct de la voix en temps réel au départ et à destination de réseaux ouverts au public commutés, entre utilisateurs fixes ou mobiles".

**Service Universel -** Principale composante du service public des télécommunications défini par la loi qui a pour objet de fournir à tous un service téléphonique de qualité à un prix abordable. Il assure l'acheminement gratuit des appels d'urgence, la fourniture d'un service de renseignements et d'un annuaire imprimé et électronique, ainsi que la desserte du territoire en cabines téléphoniques sur le domaine public. Il prévoit des conditions tarifaires et techniques spécifiques, adaptées aux personnes qui ont des difficultés d'accès au service téléphonique en raison de leur handicap ou de leur niveau de revenu.

Ce service garantit, par la loi, à tous les français le même droit à l'accès au téléphone et à quelques services de base (publiphonie, annuaire, renseignements). FRANCE TELECOM a l'obligation de fournir ce service qui est cofinancé par les concurrents de l'opérateur historique.

**Services à coûts partagés -** Services dont le coût est divisé entre l'appelant et l'appelé.

**Services à revenus partagés -** Services dans lesquels l'utilisateur appelé bénéficie d'un reversement par le fournisseur du service de télécommunications.

**Servlet -** Un servlet est un programme Java classique, une applet qui met en œuvre une interface particulière : javax.servlet. A la différence d'une applet, le servlet s'exécute sur le serveur.

**Session -** Intervalle de temps pendant lequel tous les mécanismes d'une mise en communication sont activés et la communication rendue possible. Une session doit faire l'objet d'une ouverture et d'une fermeture. Celles-ci peuvent être physiques ou logiques. Dans le modèle OSI, le mot désigne la couche 5 qui assure les fonctions liées à la chronologie (contrôle de la séquence, interruptions, reprises...).

Flot de données caractérisé par sa destination et la couche transport du protocole de réseau qui le prend en charge. Chaque session est traitée par RSVP de manière indépendante.

**SET -** Secure Electronic Transaction - Protocole destiné à la sécurisation des transactions avec l'utilisation des cartes bancaires effectuées sur des réseaux informatiques comme Internet. Le but de ce projet fut de créer un protocole pour carte bancaire universel, évitant la création d'une multitude d'autres protocoles incompatibles entre eux.

Mastercard et Visa sont les deux principaux créateurs de ce protocole. De nombreuses sociétés informatiques ont collaboré à ce projet : IBM, Microsoft, GTE, La SAIC (Science Applications International Corporation), Verisign et Terisa Systems.

Ce protocole intervient entre le consommateur, détenteur de sa carte bancaire, et le commerçant. La banque du débiteur et la banque du créditeur utilisent toujours le même réseau bancaire.

Les intervenants dans une transaction SET sont :

- Le client, détenteur de la carte bancaire. La carte bancaire en question doit être conforme aux spécifications SET.
- Le serveur marchand.
- La banque du débiteur et la banque du créditeur.

Les transactions de SET fournissent :

- Une inscription des possesseurs de cartes et des marchands auprès des organismes de certification et la délivrance d'un certificat conforme aux spécifications SET.
- L'authentification, la confidentialité, l'intégrité et la non-répudiation des transactions (pour la non-répudiation, un certificat client est obligatoire, et c'est la passerelle entre le marchand et le réseau financier qui vérifie la validité des instructions de paiement).
- L'autorisation de paiement et l'enregistrement de celui ci pour initier la demande de compensation financière au profil du marchand.

Caractéristiques principales :

DES est utilisé pour obtenir la confidentialité. RSA est utilisé pour obtenir l'authentification et l'intégrité. Les acteurs d'une transaction SET sont munis de deux couples de clé : un pour signer les documents (clés de signature), l'autre pour échanger les clés durant la phase d'identification (clés de chiffrement ou clés d'échanges). La clé privée utilisée pour la signature provient du couple de clés de signature. La clé publique utilisée pour crypter la clé secrète provient du couple de clés de chiffrement.

SET utilise le concept dit de "signature duale ". Ce procédé permet d'utiliser une seule signature pour deux messages destinés à deux interlocuteurs différents. Cette méthode permet à un des destinataires de lire le message qui lui est destiné et de vérifier l'intégrité de l'autre message sans en connaître le sens. Cela permet à un consommateur d'envoyer dans un seul message une commande à un marchand et un ordre de paiement à une banque sans que les coordonnées bancaires soient lisibles pour le marchand et que la description des achats soit lisible pour la banque.

**Set Top Box -** Périphérique d'ensemble numérique. Le terme SetTopBox désigne le plus souvent un terminal numérique permettant d'accéder a un service multiplay (multiservices) et d'effectuer un décodage de flux vidéos.

**SFCA -** Services et Fonctionnalités Complémentaires et Avancés.

**SFP -** Small Form-Factor Pluggable. Transceiver Optique / Electrique. C'est une interface qui va convertir un signal optique en un signal électrique.

**SFR -** Société Française du Radiotéléphone - Société contrôlée par le groupe Vivendi dont le pôle Télécom se nomme CEGETEL, exploitant autorisé à concurrencer France Télécom sur les réseaux radioélectriques de téléphonie ouverts au public à une échelle nationale au même titre que Bouygues Télécom jusqu'en 1998.

**SGML -** (Standard Generalized Markup Language) - Standard international (ISD) décrivant la structure et le contenu de différents types de documents électroniques.

Langage de description du contenu des documents et de leur structure faisant appel à un système de marquage. Cette description normalisée, qui consiste à baliser les chapitres, paragraphes, table des matières, etc., permet d'exploiter les documents avec n'importe quel type de machine et tout type de traitement de texte.

**SHA -** Secure Hash Algorithm - Algorithme de hachage (chiffrement) utilisé pour l'authentification et la vérification de l'intégrité des communications.

**SHA-1 -** Secure Hash Algorithm - Algorithme de hachage (chiffrement). Sa version corrigée par la NSA (National Security Agency) produit des empreintes numériques de 160 bits pour des messages dont la taille doit être inférieure à 264 bits.

**Shannon -** Unité de mesure de l'information, égale à l'information concernant la réalisation de l'un de deux évènements équiprobables. La quantité d'information, exprimées en shannons, concernant la réalisation d'un évènement de probabilité déterminée est égale au logarithme binaire de l'inverse de cette probabilité. Le symbole du shannon est Sh.

**Shannon (Théorème de) -** Le théorème de Shannon stipule que pour pouvoir numériser correctement un signal, il faut échantillonner à une fréquence double (ou supérieure) à la fréquence du signal analogique que l'on échantillonne.

**Shareware -** Logiciel propriétaire, protégé par le droit d'auteur, qui peut être utilisé gratuitement durant une certaine période ou un certain nombre d'utilisations. Après cette période de gratuité, l'utilisateur doit rétribuer l'auteur s'il veut continuer à utiliser le logiciel. Durant la période d'utilisation gratuite, il est possible que certaines fonctions du logiciel ne soient pas disponibles.

**SHTTP -** Le protocole S-HTTP est une extension sécurisée du protocole HTTP. Ce protocole a été développé à l'origine chez Enterprise Integration Technologies. Ce protocole peut fonctionner avec différents algorithmes de cryptage (DES, triple DES IDEA, RC2,…) et différents modes d'identification (RSA, Kerberos). Le client et le serveur utilisent un protocole d'échange de paramètres de cryptage. Les messages sont cryptés un à un et il est possible de signer les messages. Les certificats respectent la syntaxe X509.

**Shunning -** Reconfiguration dynamique par un routeur Cisco de ses ACL afin de stopper toute attaque détectée et de bloquer toute nouvelle transmission de données de/vers l'adresse IP "attaquante", pour un laps de temps donné.

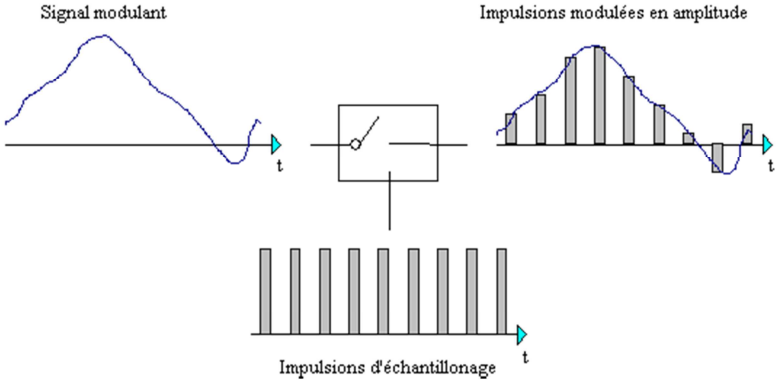
**SIG -** Système d'Information Géographique - Pateforme informatique permettant la création et l'exploitation des données cartographiques et technique d'un réseau.

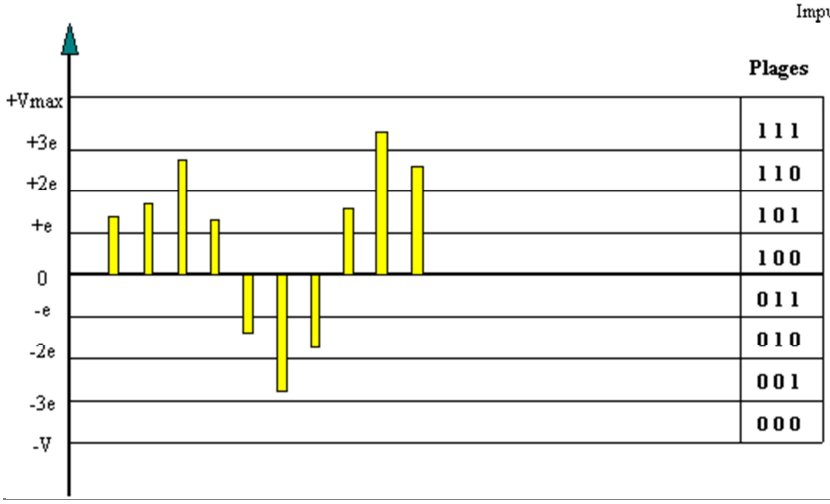
**Signal -** Représentation physique, généralement électrique, d'une information en cours de transmission.

Phénomène physique dont une ou plusieurs caractéristiques peuvent varier pour représenter des informations.

**Signal Numérisé -** Action qui consiste à convertir des signaux analogiques en signaux numériques.

Selon le principe de l'échantillonnage : le signal échantillonné n'a de valeur qu'à intervalle régulier. La précision de l'horloge est importante dans la transmission des données numérisées.




Selon le principe de quantification : le signal ne peut prendre qu'un nombre fini de valeur. Ces valeurs sont numérotées en base 2.

Signal numérique sortant : 101 101 110 101 010 001 010 101 111 110

**Signalisation -** Sur un réseau de télécommunications, la fonction de signalisation assure l'échange des informations internes au réseau nécessaires à l'acheminement des communications. A titre de comparaison, sur un réseau routier, les panneaux de signalisation permettent la circulation des véhicules ; sur un réseau de télécommunications, les informations de signalisation permettent la circulation des communications sur le réseau. Il peut s'agir, par exemple, des informations nécessaires à la reconnaissance de l'appelant pour établir la facturation des appels ou la présentation du numéro. Cette fonction peut être assurée directement par le réseau qui transporte les communications des abonnés. Elle est alors généralement intégrée aux commutateurs. Elle peut également être assurée par un réseau distinct, appelé réseau sémaphore.

C'est aussi un ensemble des informations de "service" nécessaires à l'établissement et au déroulement d'une communication sur un réseau public -numérotation, adressage, prise de ligne (décrochement), mise en attente, libération... Aujourd'hui, ces signaux de service peuvent emprunter d'autres voies que les voies de la communication elles-mêmes et donc fournir une gamme étendue de services (avertissement d'appel en attente, identification du numéro de l'appelant...). C'est le cas avec la nouvelle signalisation dite CCITT n° 7, encore appelée "sémaphore", mise en place dans le réseau français. Avec le Rnis (Réseau numérique à intégration de services), l'utilisateur pourra avoir Accès à cette signalisation sous le nom de "Canal D".

**Signature d'attaque -** Système d'identification d'activité malveillante sur le réseau. Les paquets de données entrants sont examinés en détail à la recherche de modèles logarithmiques identiques.

**Signature numérique -** Chaîne de bits ajoutée à un message électronique (hachage crypté) permettant l'authentification et l'intégrité des données.

**Signaux S-Video (Y/C) -** Les informations de luminosité (luminance ou "Y ") et de couleur (chrominance ou "C ") sont transférées séparément à l'aide de fils multiples, évitant ainsi de moduler et démoduler la vidéo et donc la perte de qualité d'image qui en résulte.

**Signaux synchrones -** Signaux plésiochrones - Des signaux synchrones ont des écarts de phase constante, les signaux plésiochrones ont des écarts de phase variables (mais légers).

La PDH (trame MIC, E1, E2, E3, E4, T1, T2, T3) est plésiochrone.

LA SDH (STM1, STM4, STM16) est synchrone.

Ce ne sont pas les seules différences.

**SIM -** Subscribe Identification Module - Carte d'identification de l'abonné. Le module d'identification de l'abonné (SIM) est une carte couramment utilisée dans un téléphone GSM. Elle renferme une puce qui stocke les informations et crypte les transmissions voix et données, rendant quasiment impossible l'écoute d'un appel en cours. La carte SIM renferme également des informations qui identifient l'appelant de l'opérateur réseau. Votre carte SIM renferme toutes les informations relatives à votre téléphone (numéro de téléphone, annuaire, compte, etc.), de façon à ce que vous puissiez accéder au réseau mobile et utiliser les fonctionnalités de votre appareil. Cette carte vous est fournie par votre opérateur mobile. Voir aussi Carte SIM.

**SIM Toolkit -** Outil de programmation stocké sur la puce de la carte SIM qui autorise les "menus déroulants "tout en améliorant l'ergonomie et le nombre de fonctionnalités du téléphone mobile.

**Simplex -** à l'alternat - Qualifie un mode d'exploitation selon lequel le transport des informations peut avoir lieu dans les deux sens, mais non simultanément, entre deux points.

**SIP -** Session Initiation Protocol - Protocole de communication basé sur IP qui établit les règles de communications entre deux applications de téléphonie souhaitant dialoguer. Emanation de l'IETF [RFC 3261] destinée à mettre en place des procédures d'appel et de contrôle lors d'une communication VOIP bi ou multipartite.

Situé au dessus de la couche TCP ou UDP, SIP est indépendant de la couche transport d'IP. Protocole composé de 8 routines (invite, register, bye, ack, cancel, options, subscribe, notify) et existant en 2 grandes classes d''objets :

- Les agents utilisateurs,
- Les serveurs.

SIP assure aussi des fonctions d'administration des appels pour ajouter, supprimer ou transférer des communications ou pour changer les paramètres d'une session en cours d'appel.

Le protocole SIP est un protocole de signalisation qui peut initialiser, modifier et fermer les sessions de plusieurs abonnés. Ce protocole texte basé sur HTTP est utilisé pour retransmettre les informations de la communication - comme la conversation - via des réseaux. Le format d'e-mail standard est utilisé pour annoncer les adresses des abonnées : "sip:utilisateur@domaine".

Les informations SIP sont donc transmises via le protocole TCP ou le protocole UDP. Il prend aussi en charge la transmission de l'identité de l'appelant ou le transfert d'appel sur des réseaux basés sur IP. Parce que SIP est orienté vers les applications distribuées sur Internet (mise en œuvre simple, extensibilité, modifiabilité, flexibilité), il est appelé à devenir le protocole standard de l'avenir pour la Voix sur IP d'après les experts et les agences de certification.

Il faut plus que le protocole SIP pour téléphoner via Internet. SIP ne fait qu'initialiser la communication. Les données réelles pour la communication sont gérées par d'autres protocoles = SDP et RTP.

Tout en étant utilisé dans le secteur de la Voix sur IP, SIP a aussi été consacré par le Projet de partenariat de troisième génération (le 3GP) comme étant le protocole pour le multimédia dans les communications mobiles 3G (UMTS).

**SIT -** Simple IPv6 Transition - voir IPv6 - Désigne les mécanismes de transition de IPv4 vers IPv6

**SIT -** Système Interbancaire de Télé compensation - Réseau mettant en communication des ordinateurs situés dans les banques pour assurer la compensation des moyens de paiement. Il utilise notamment le réseau Transpac pour les échanges. Il s'agit d'un des plus importants réseaux de ce type et l'un des premiers à avoir une démarche de normalisation systématique, si bien que certains des protocoles utilisés, comme PeSIT, sont repris dans d'autres applications. Aujourd'hui le SIT voit sa vocation s'élargir à d'autres applications (Bourse notamment).

**Skybridge -** Projet d'un ensemble de 64 satellites LEO (altitude 1457km) lancé par ALCATEL et constituant un système d'accès qui met à disposition des usagers du monde entier des services interactifs à large bande (accès rapide à INTERNET, visioconférence, télétravail, VOD, télémédecine, etc.).

**SLA -** Service Level Agreement - Engagement de Niveau de Service - Contrat qui définit les engagements de l'opérateur vis à vis de son client et les pénalités qu'il encourt en cas de manquement. Le fournisseur s'engage sur les performances de l'infrastructure et des systèmes, y compris systèmes logiciels associés (services IP, messagerie,…) qui sont vendu au client sous la forme d'un service. L'engagement de SLA se mesure selon des critères objectifs acceptés par les deux parties. Ces critères fixent le niveau de service attendus, comme le taux de disponibilité du service et sa fiabilité, la tolérance aux pannes, le temps de rétablissement du service en cas d'interruption, la sécurité, le délai de transmission…

**SLIP -** Serial Line Interface Protocol - Protocole d'encapsulation des paquets IP

**SMB -** Server Message Block - Protocole permettant à des stations d'un réseau local d'échanger des messages, notamment des messages de service pour gérer les opérations courantes des réseaux locaux (ouverture & fermeture de fichiers, verrouillage....). Il fonctionne au-dessus de NetBIOS (voir ce mot). Utilisé par Microsoft dans OS2/Lan Manager, il fait figure de standard possible.

**SMDS -** Switched Multimegabit Data Service - Service de transfert rapide de données (organisées en cellules de taille fixe, semblables à celles de l'ATM) sur longue distance, défini par les laboratoires américains BellCore. Il achemine du trafic issu de réseaux locaux. SMDS commence à être offert par certains exploitants de téléphonie outre-Atlantique sur des liaisons d'Accès à 1,45 (E1) et jusqu'à 45 Mbps. Conçu à l'origine pour fonctionner avec la technologie DQDB, SMDS s'est enrichi de plusieurs niveaux de raccordement : ATM, DXI (Data exchange information, trame HDLC).

**SMG -** Le comité SMG (Special Mobile Group) est chargé des télécommunications mobiles au sein de l'ETSI.

**SMS -** Short Message Service - Service permettant l'envoi et la réception de messages de textes courts sur un réseau sans fil GSM. Message écrit que l'on peut envoyer à partir d'un téléphone mobile ou d'un site web vers un autre téléphone mobile.

Fonctionnalité disponible sur certains téléphones mobiles ou fixes et qui vous permet d'envoyer et/ou de recevoir des messages alphanumériques courts. La messagerie en images vous permet d'envoyer et de recevoir des messages en images aussi bien que du texte. La fonctionnalité "chat" vous permet de "bavarder" avec votre famille et vos amis au moyen de messages SMS tout en gardant une trace de l'ensemble de la conversation. La messagerie multimédia MMS (Multimedia Messaging Service) est une nouvelle norme actuellement utilisée dans les terminaux mobiles avancés. Elle autorise la transmission en différé de divers types de contenus multimédias comme les images, le son, les clips vidéo, etc.

**SMTP -** Simple Mail Transfer Protocol - Protocole et service de courrier électronique. Langage standard et simple dans sa conception qui sert à véhiculer le courrier électronique sur l'Internet. SMTP, de même que HTML, et SNMP fait partie des standards de fait de l'Internet. Loin d'être nouveau, le protocole a été élaboré en 1982 par l'Arpanet (le réseau de la recherche américaine) à travers deux recommandations (RFC): la RFC 821, spécifiant les éléments de transmission et la RFC 822 pour la structure des messages, y compris celle de l'enveloppe. C'est le protocole qui permet aux serveurs de messagerie Internet de communiquer entre eux. Il achemine le courrier de serveur en serveur jusqu'au serveur destinataire.

Le modèle de communication est le suivant: après demande d'envoi d'un courrier de la part d'un client (expéditeur), le serveur de celui-ci établit une connexion avec un autre serveur (destinataire): en langage technique, on dit que la machine source établit une connexion TCP (Transmission control Protocol) avec le port 25 (un des ports applicatifs) de la machine distante. Car c'est le protocole TCP, standard de transmission de l'Internet, qui a la charge de transmettre les différentes applications: messagerie, pages Web...

Les différents objets qui constituent le modèle SMTP respectent des tailles minimales et maximales, ce qui permet de recevoir des messages et d'en émettre tout en étant sûr, à chaque implémentation de la norme sur une plate-forme matérielle donnée, que leur acheminement vers un destinataire rattaché à une autre plate-forme ne butera pas sur des problèmes de formats. Ainsi au niveau de l'utilisateur, SMTP a prévu un champ réservé au nom de l'utilisateur qui n'excède pas 64 caractères. Idem en ce qui concerne la longueur d'un nom de domaine ou d'un nombre, il ne devra pas dépasser 64 caractères. La longueur maximale d'un chemin (avant ou arrière, forward path et reverse path) est de 256 caractères, y compris les éléments de ponctuation et les éléments séparateurs. La longueur d'une ligne de commande n'excède pas pour sa part 512 caractères, y compris la commande proprement dite et le sigle de fin de commande <CRLF>. Idem en ce qui concerne la ligne de réponse qui reprend la même structure.

Avec SMTP, la ligne de texte, finissant par la butée <CRLP>, ne dépasse pas les 1000 caractères. Enfin. le nombre de récipients de réception qui peuvent être en mémoire tampon rie doit pas dépasser le chiffre de 100.

La plupart du temps, le chemin que le courrier emprunte sur le réseau n'est pas direct. Entre le serveur de l'émetteur et celui du destinataire, plusieurs serveurs doivent être traversés. Si cela est le cas, le chemin à parcourir est indiqué dès le départ dans le champ de messages réservé à cet effet. Ces indications sont simples: traverser le serveur 2, 3, 4. Au fur et à mesure que le courtier passe à travers les serveurs indiqués, le chemin à parcourir s'efface et le champ réservé aux indications sur le chemin parcouru se remplit, jusqu'à destination finale.

Le protocole SMTP fonctionne selon le principe de la fille d'attente (spooling). A savoir, qu'il permet de mettre en attente les messages à envoyer dans un "spooler". Le serveur va régulièrement vérifier dans celui-ci s'il y a des messages à envoyer. Si le destinataire n'est pas disponible. le serveur attend puis renouvelle l'opération plusieurs fois. Si, au final, le message ne peut être délivré, il est alors rejeté ou renvoyé vers l'expéditeur.

Cette série d'étapes selon laquelle le serveur garde le message à envoyer en attente tout en multipliant les tentatives de contact avec le destinataire vaut à SNMP sa réputation de "protocole de bout en bout". Cette dernière tient égaleraient au fait qu'il existe des passerelles SMTP pour dialoguer avec tous les systèmes propriétaires de messageries du marché (cc:Mail, MS/Mail, Notes, Mail Exchange, etc.).

Les trois composantes d'un email :

Un e-mail est composé d'une enveloppe, d'en-têtes et d'un corps de texte.

L'enveloppe est utilisée par le MTA, l'agent chargé du transfert, pour acheminer le message. Pour ce faire, le MTA se sert de deux champs d'information: la commande MAIL (exemple: from:<rsteven@internet.com) et la commande RCPT (destinataire) (exemple: To:>tagazou@overnet.com). C'est la recommandation RFC 821 qui fixe le contenu et l'interprétation des données de l'enveloppe.

Les en-têtes sont utilisés par les agents situés sur les postes utilisateurs. Exemples d'en-têtes: Received, Message-id (identifiant du message), From, Date, Reply-To... C'est la recommandation RFC 822 qui fixe les règles de lecture et d'interprétation de ces en-têtes dans SMTP.

Le corps du texte constitue le message proprement dit à transmettre. Ce message est converti en code ASCII (codage universel) avant sa transmission.

L'agent du poste utilisateur prend d'abord le corps du texte, lui ajoute les en-têtes et transmet la somme des deux à l'agent de transfert (MTA) situé sur le serveur de messagerie.

**SMURF -** (camouflage) Attaque malveillante consistant à envoyer un grand nombre de paquets Ping "spoofés" vers des adresses broadcast, afin d'amplifier le nombre de paquets par la réponse vers les adresses "spoofées". Cette technique offre des possibilités de saturation exponentielles, selon le nombre d'hôtes répondant à la requête.

**SNA -** Systems Network Architecture - Architecture générale de communications en couches définie par IBM pour ses systèmes informatiques. Ensemble de protocoles et de logiciels de communication développés par IBM.

**Snapshot -** Instantané - Reproduction de l'état de tout ou partie d'un système, disque dur, disquette, partie de mémoire, fichier à un instant déterminé. Pour un fichier, deux procédés sont applicables : la réplication ou l'enregistrement des adresses des blocs avant modification par un système de pointeurs.

**SNMP -** Simple Network Management Protocol - Protocole spécialisé pour l'administration de réseau. Développé comme prolongement du protocole d'interconnexion de réseaux locaux TCP/IP, SNMP est l'un des standards de fait en matière de gestion et d'administration de réseaux, notamment pour les réseaux de type Ethernet dans le monde des stations de travail. Il n'est cependant pas officiellement normalisé par l'ISO (International Standard Organisation) qui a mis au point les protocoles CMIS/CMIP. (voir administration de réseau).

Le protocole SNMP est le langage que les agents et les stations de gestion (managers) utilisent pour communiquer. C'est un protocole de type question/réponse asynchrone. Ce protocole est situé au niveau application du modèle OSI, c'est lui qui définit la structure formelle des communications. SNMP est encapsulé dans des trames UDP. La MIB (Management Information Base) regroupe l'ensemble des variables relatives aux matériels et aux logiciels supportés par le réseau, et définit les objets de gestion dans l'environnement TCP/IP. La SMI (Structure of Management Information), définit comment sont représentées , dans la MIB, les informations relatives aux objets de gestion et comment sont obtenues ces informations.

Les stations interrogent donc les agents pour observer leur fonctionnement et leur envoient des commandes pour leur faire exécuter certaines taches. Les agents renvoient les informations requises aux stations de gestion. Certains événements du réseau, tels que des erreurs de transmission, peuvent déclencher des alarmes envoyées aux stations de gestion. Cependant, l'envoi de messages de façon spontanée de l'agent vers le manager est limité. Les managers effectuent une interrogation périodique des agents de manière à vérifier leur état. La structure des paquets est définie en utilisant la syntaxe ASN1 (Abstract Syntax Notation).

SNMP a l'avantage d'être simple, cependant il a des capacités très limités au niveau sécurité, principalement pour l'authentification. Tous les systèmes SNMP doivent également supporter les protocoles DUPER et IP pour transporter les données entre les agents et les stations de gestion.

**Soap -** Simple Object Access Protocol - Recommandation du W3C, ce protocole de communication permet l'appel de méthodes sur un objet distribué sur le réseau Internet. Utilisant HTTP, il transmet les paramètres nécessaires à cet appel par un message XML. Il facilite ainsi l'interopérabilité d'applications hétérogènes pour la réalisation de services web.

**Social engineering -** Ingénierie Sociale - Obtenir des informations confidentielles (mots de passe, codes d'accès, plans, etc.) en exploitant les "failles" humaines, (bonne foi, négligence, habitudes...).

**Socks -** Les Socks représentent un environnement de protection permettant de filtrer les accès en entrée et en sortie d'un réseau.

**SONET -** Synchronous Optical NETwork - Equivalent américain de la SDH.

**Soumission Comparative -** Méthode de sélection des opérateurs utilisée lors de l'attribution des ressources rares (licences et fréquences pour la boucle locale radio ou l'UMTS, par exemple) en France. Elle se distingue de la mise aux enchères, car elle permet de sélectionner les candidats sur un ensemble de critères et non sur le seul critère financier.

**Source Routing -** Routage par la Source. Source Routing est un protocole utilisé dans un environnement Token Ring. Lorsque l'on est amené à relier différents réseaux locaux Token Ring par des ponts. Lorsqu'une station veut émettre elle doit trouver un chemin à travers les différents ponts. Comme il existe plusieurs chemin vers une station cela permet de "décongestionner "le réseau puisque tous les paquets n'emprunteront pas le même chemin. A chaque fois que la trame traverse un pont ou un LAN, on ajoute le numéro du pont ou du LAN : ainsi, une route consiste en une suite de numéro de pont, de LAN …

Méthode de routage utilisée dans les ponts d'interconnexion de réseaux. Utilisée notamment pour l'interconnexion d'anneaux à jeton, elle est basée sur le principe selon lequel les tables de routage sont contenues dans la station émettrice du message.

Le protocole "source routing "a été développé par l'IEEE 802.5, dans le but d'interconnecter des réseaux Token-Ring.

Quand une station A désire envoyer des informations à une station B, elle envoie une trame en diffusion de découverte du chemin. Lorsqu'une trame de ce type arrive sur le port d'un pont, celui-ci y ajoute sa propre adresse et re-transmet cette trame vers tous les réseaux auquel il est connecté, sauf celui par lequel la trame est arrivée. Une ou plusieurs trames arrivent donc à la station destination B, et celle-ci retourne à A toutes les trames reçues en utilisant les informations d'acheminement contenues dans chacune d'entre elles. Ainsi, la station A peut utiliser la ou les routes découvertes grâce à ce protocole. Son choix dépend de divers paramètres : nombre de ponts traversés, délai d'acheminement, longueur de trame permise.

Cette technique qui fait intervenir les ponts d'extrémités suppose un logiciel spécifique par pont. Par conséquent, la connexion entre réseaux locaux hétérogènes ne peut actuellement se faire que grâce à des solutions propriétaires. Le problème des bouclages et de la perte d'une liaison de communication est ici inexistant dans la mesure où des trames exploratrices sont immédiatement générées en cas de dysfonctionnement, de modification de la ligne de communication ou lors de la mise en service. L'unique inconvénient réside dans la multiplication des trames exploratrices dans le réseau qui peut limiter la bande passante utile.

**Sous-adressage -** Sub-addressing, SUB - Complément de service permettant à un abonné d'étendre sa capacité d'adressage au-delà de celle que permet le numéro de réseau. Dans Numéris, le sous-adressage s'exprime en faisant suivre le numéro à 10 chiffres du symbole * puis de un à quatre chiffres.

**Sous-répartiteur -** Dans un quartier l'ensemble des lignes abonnés cuivres ou optiques arrivent à un sous-répartiteur (armoire de rue). Du sous-répartiteur part un câble de grosse capacité qui relie l'ensemble des lignes au central.

**Spam -** Pourriel - E-mail non sollicité envoyé en masse, généralement après avoir récupéré l'adresse des destinataires de manière illicite. Les filtres anti pourriels agissent par détection de mots-clés dans les messages, par consultation des RBL, des bases de règles ou des bases de signatures de pourriels, à partir des listes noires et blanches définies par l'administrateur ou encore par analyse heuristique.

**Spanning Tree -** Littéralement "arbre recouvrant". Méthode de routage utilisée dans les ponts entre réseaux locaux, notamment de type Ethernet. Elle utilise un principe d'apprentissage par lequel chaque nœud, en observant l'adresse des trames qui lui sont envoyées, reconstitue peu à peu l'arborescence du sous-réseau qui le concerne.

Le protocole "spanning tree "a été développé par le comité IEEE 802.1, dans le but d'interconnecter tout type de réseau, et ce quelle que soit la topologie utilisée. Le but de ce protocole est de construire un arbre qui recouvre tout le réseau, pour que tout point du réseau soit accessible à partir de toutes les feuilles de l'arbre.

Sur un réseau local commuté, les segments sont souvent connectés entre eux de façon redondante afin d'obtenir une plus grande tolérance aux pannes, c'est ce qu'on appelle une architecture maillée. Le problème majeur de ces chemins redondants pour accéder à une même destination est la création de boucles. Or, au niveau 2, il n'est pas possible de détecter et d'éliminer une trame qui boucle (au niveau 3, c'est le TTL qui s'en charge). Ces boucles deviennent bloquantes pour le réseau en saturant la bande passante.

Le but du spanning tree est de détecter les boucles et de les supprimer en désactivant certaines interfaces de certains ponts afin d'obtenir une architecture arborescente du réseau local. Ainsi, à un instant donné, il n'existe qu'un seul chemin entre segments distants.

Les ports qui créent des boucles sont mis dans l'état "blocking ", c'est à dire dans un état passif, à l'exception des paquets BPDU (Bridge Protocol Data Unit), paquets échangés par les ponts et contenant les informations nécessaires au bon déroulement de l'algorithme du spanning tree.

Principe de fonctionnement :

- Election d'un pont racine sur tous les LAN, pour établir à partir de celui-ci un arbre recouvrant, sans boucles. A sa mise sous tension ou bien lorsqu'il est isolé, tout pont considère qu'il est lui-même le pont racine. Il émet donc périodiquement (toutes les 2s) des trames en diffusion sur les réseaux auxquels il est raccordé, indiquant qu'il est racine, et précisant son identificateur sur 8 octets. Cet identificateur est composé de 2 octets de priorité (fixé par l'administrateur) et des 6 octets de l'adresse MAC "la plus faible "du pont. Le pont élu est celui de plus haute priorité, c'est à dire ayant

l'identificateur le plus faible.

Chaque fois qu'un pont reçoit une BPDU d'un pont racine qui lui est supérieur, il cesse de s'annoncer en tant que pont racine et répercute les messages annonçant le nouveau pont racine.

- Calcul de la distance entre le pont racine et les autres ponts.
- Election d'un pont désigné sur chaque LAN (le plus proche de la racine en terme de coûts), et désactivation de certains ports des autres ponts.
- Choix d'un port racine sur chaque pont désigné.

Les ports racines sont ceux qui sont du côté du pont racine, les autres ports sont les ports désignés. Sur chaque réseau éloigné (auquel le pont racine n'est pas directement connecté), les ponts vont s'informer mutuellement de l'identificateur du pont qu'ils ont élu racine, et du coût du chemin proposé vers ce pont racine. Le choix se porte sur le pont qui propose le chemin le moins coûteux. Ce coût (Path cost) est normalement la somme de l'inverse des débits des réseaux traversés, soit encore proportionnel à la somme des délais d'émission.

Les autres ponts vont placer leur port dans un état passif (blocking) de manière à éliminer les boucles. Dans le cas d'un litige, lorsque des ponts proposent le même "Path Cost", la décision se fait par rapport à l'identificateur des ponts. Dans le cas où un pont aurait luimême plusieurs ports connectés au réseau, le port de plus faible identificateur est choisi.

Le spanning tree, spécification de l'IEEE 802.1d, est un protocole de niveau 2 du modèle OSI (couche liaison de données). Il est employé sur les réseaux d'entreprise pour permettre aux ponts et commutateurs de communiquer entre eux pour découvrir et circonvenir les boucles physiques d'un même réseau.

Ce protocole spécifie un algorithme que les commutateurs utilisent pour créer une topologie logique sans boucle basée sur un arbre de recouvrement unique dit"spanning tree ". Cet arbre est construit à partir d'un commutateur racine appelé root bridge. Chaque commutateur va alors calculer le plus court chemin vers le root bridge et modifier l'état de ces ports (état bloqué ou passant) pour éviter les éventuelles boucles et repérer les chemins redondants.

La construction de l'arbre s'effectue grâce à l'échange de messages appelé BPDU (Bridge Protocol Data Unit) à intervalles réguliers entre tous les commutateurs tournant STP sur une adresse multicast de niveau MAC.

A chaque changement de topologie du réseau, ajout d'un nouveau switch, défaillance d'un lien, l'arbre STP est recalculé, il y a donc reconfiguration des ports des commutateurs évitant ainsi les pertes de connectivité et la création d'éventuelle boucle.

Pour chaque vlan est associé une instance de STP, on parle alors de PVST (Per Vlan Spanning Tree).

On peut avoir une seule instance STP pour l'ensemble des Vlans, qui est moins gourmand en charge CPU sur les commutateurs ainsi qu'en bande passante sur les liaisons inter-swicthes, alors que le PVST permet une plus grande latitude dans la gestion du spanning tree.

- Le bridge id

Chaque commutateur possède un identifiant unique appelé"bridge id ". Cet identificateur est l'association de deux éléments :

⇒ Le bridge priority : c'est en entier codé sur 2 octets variant de 0 à 65535. Sur les catalysts CISCO, la valeur de bridge priority est définie par défaut à 32768.

⇒ L'adresse MAC codée sur 6 octets. Le commutateur gère un pool d'adresse MAC et s'y attribue une adresse MAC par vlan.

La valeur de bridge id est très importante dans le STP car il permet à l'algorithme de STP de déterminer le root bridge, la racine de l'arbre STP. Le root bridge est l'élément central du spanning tree et contrôle l'arbre qui permet d'éviter des boucles. Il donc important de normaliser ce paramètre.

Comme il y a une instance STP par vlan, un switch peut avoir un rôle de root bridge pour un vlan donné et pour un autre vlan ne pas avoir ce rôle. Un switch va donc posséder plusieurs valeurs de bridge id.

- Le port cost

Ce paramètre est un entier codé sur 2 octets variant de 1 à 65535 qui permet d'associer à chaque port un coût de transmission des trames. Ce coût est basé sur le média utilisé ou la bande passante, plus une liaison sera rapide, plus son coût sera petit. Le port ayant le coût le plus petit sera préféré.

Il est calculé par défaut à l'aide de la formule suivante :

1000 / débit du média utilisé en Mbit/s

Cependant, cette règle n'est plus valable pour les liens supérieurs à 10 Mbps.

L'IEEE préconise l'utilisation des valeurs suivantes.

Ces valeurs sont celles à respecter lors de l'implémentation de STP.

| Cost | Type de lien |
|---|---|
| 100 | 10 Mbps |

| | |
|---|---|
| 30 | 100 Mbps FDDI |
| 19 | 100 Mbps |
| 14 | 155 Mbps |
| 4 | 1 Gbps |
| 2 | 10 Gbps |
| 1 | Au delà de 10 Gbps |

Ce paramètre sert également au calcul du chemin le plus court vers le root bridge ou le root path cost.
Du fait d'avoir une instance STP par vlan, le port du switch peut très bien avoir un coût différent par vlan.

- Le port priority

En plus d'attribuer au port un coût, on peut lui spécifier une priorité. A coût égal, cette priorité permettra de spécifier le port qui sera chargé de transmettre les trames. Ce rôle sera tenu par le port ayant la priorité la plus petite. Si tous les ports ont la même valeur de port priority, c'est le port qui possède le plus petit identifiant, port Id qui sera choisi.
Les valeurs port priority sont comprises entre 0 et 63. La valeur par défaut est 32.
Pour favoriser l'utilisation d'un port à un autre (lorsque le coût est identique) la valeur doit être inférieure à 32.
La préconisation est donc de diviser par 2 le port priority, permettant ainsi d'intercaler d'autres ports entre ces 2 priorités.
Du fait d'avoir une instance STP par vlan, le port du switch peut très bien avoir une priorité différente par vlan.

- L'algorithme Spanning Tree

Tous les switchs tournant STP s'échangent des messages BPDUs à intervalle régulier.
Ces messages BPDUs contiennent les informations suivantes :

⇒ Root BID : le Bridge ID du swich considéré comme Root Bridge
⇒ Root Path Cost : Le coût du chemin pour atteindre le root bridge à partir du port d'émission
⇒ Sender BID : Le bridge Id du switch envoyant le BPDU
⇒ Port Id : l'identifiant du port qui émet le BPDU

L'algorithme STP se décompose en trois phases :

⇒ L'élection du root bridge
⇒ L'élection des root ports
⇒ L'élection des Designated Ports

- L'élection de root bridge

Au démarrage, chaque switch se considère comme le root bridge.
Ils émettent donc un BPDU contenant dans le champ Root BID leur valeur de Bridge Id. Quand un switch reçoit un BPDU, il compare sa valeur Bridge ID avec la valeur Root Bid reçue. Si la valeur reçue est plus petite, il garde en mémoire cette valeur et transmet des BPDUs en conséquence.
Au final, le switch, possédant la plus petite valeur de bridge id, sera désigné Root Bridge.
Si plusieurs switchs possèdent la même valeur de bridge id, le critère de choix retenu est l'adresse MAC. Le switch possédant la plus petite adresse MAC sera alors désigné root bridge.
Il est possible de prendre en compte d'autres paramètres pour désigner le root bridge.
Pour un réseau donné, Il n'existe qu'un seul root bridge.
Tous les ports du root bridge sont dits"designated ports " qui sont généralement dans l'état"forward ". Dans cet état, le port peut transmettre et recevoir du trafic. Le root path cost associé à chaque port du root bridge vaut zéro.

- L'élection des root port

Une fois le root bridge désigné, tous les non root bridges vont calculer pour chacun de leurs ports le coût du chemin pour atteindre le root bridge.
Il n'y a qu'un root port par switch. Le port possédant le plus petit chemin pour atteindre le root bridge ou"root path cost ", sera désigné"root port ".
Si plusieurs ports possèdent le même"root path cost ", le critère de sélection est :

⇒ Le cost port : le port ayant le coût le plus petit sera choisi. En cas d'égalité, la décision s'effectuera en fonction du port priority.
⇒ Le port priority : le port ayant la plus petite priorité sera choisi. En cas d'égalité, le choix s'effectuera en fonction port id.
⇒ Le port Id : le port ayant le plus petit port Id sera choisi.

Les ports des switchs directement connectés au root bridge seront les roots ports.

Le root port est dans l'état"forward ".

- L'élection des designated ports

Une fois le root port désigné, chaque switch va transmettre dans ses BPDUs le root path cost de son root port.

Sur le segment, le port qui sera désigné comme designated port sera celui qui émet un BPDU contenant le meilleur root path cost, donc le plus petit. Pour un segment, il n'y a qu'un seul designated port.

Si plusieurs ports émettent sur le segment un root path cost identique, le critère de sélection est :

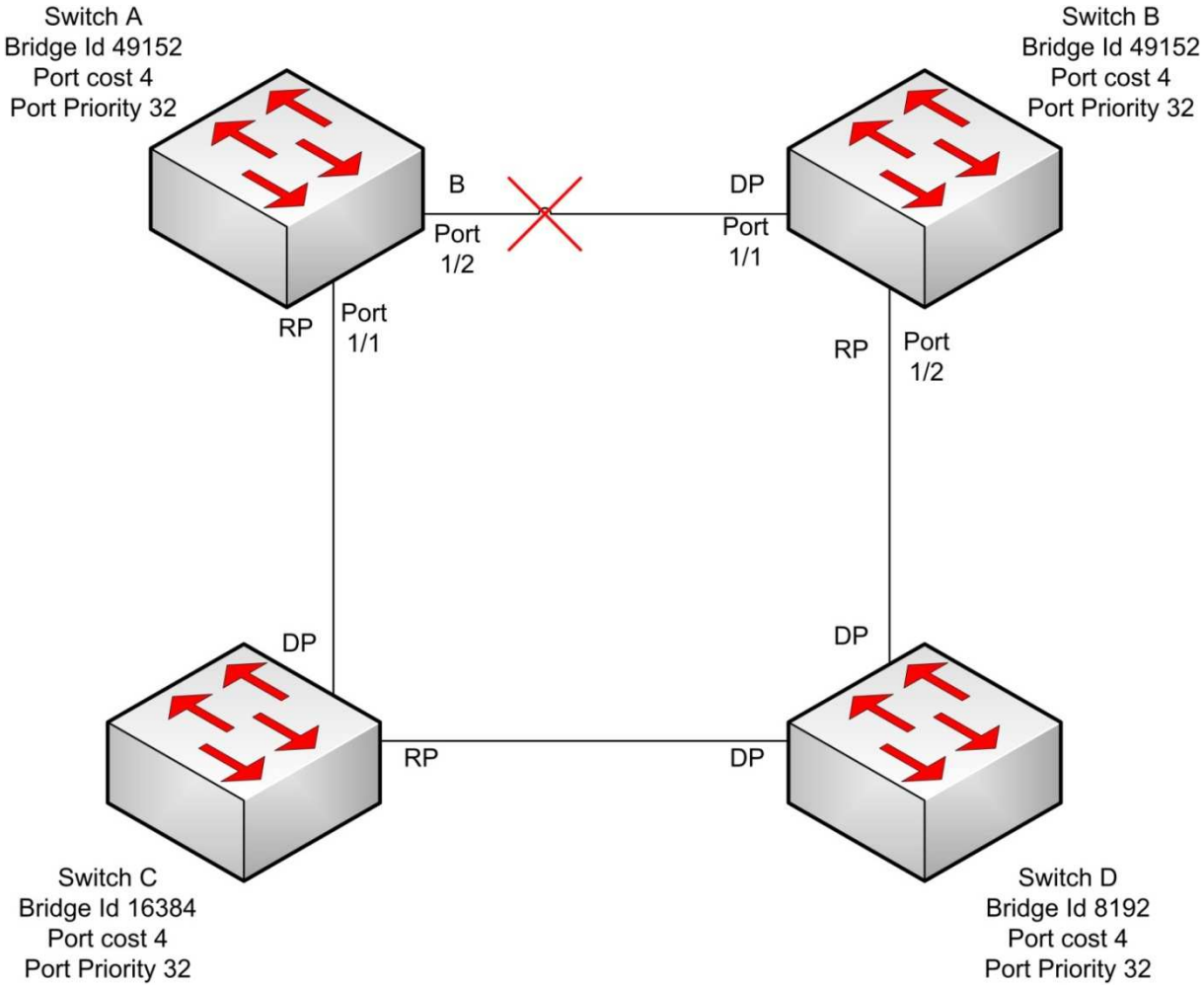
⇒ Le sender bridge id **:** le port du switch possédant la plus petite valeur de bridge id sera choisi. En cas d'égalité, le choix s'effectuera sur la valeur de port cost,

⇒ Le port cost : le port possédant la plus petite valeur de port cost sera choisi. En cas d'égalité, la décision se fera en fonction du port priority.

⇒ Le port priority : le port ayant la priorité la plus petite sera choisi. S'il y a toujours égalité, il y aura comparaison du port id.

⇒ Le port Id : le port ayant le plus petit port Id sera choisi.

Les ports dits"designated ports " sont dans l'état"forwarding ", le trafic peut être reçu et émis par ce port. Les autres ports seront des non designated port et seront mis dans l'état"blocking " aucun trafic ne passera par ces ports, ils écouteront seulement le BPDU.




Le root bridge est le switch D car il possède la valeur de bridge id la plus petite. Donc tous ses ports sont dits designated port.

Le port du switch C qui est directement connecté au root bridge. Il est donc le root port du switch C. Même chose pour le switch B.

Le port 1/1 et le port ½ du switch A ont le même root path cost qui vaut 8. Ils ont le même port cost et le même port priority la décision s'effectue donc au niveau du port id. le port 1/1 est donc le root port du switch A.

Détermination du Designated port sur la liaison switch A-C : Le meilleur root path cost du switch A est 8, le meilleur root path cost du switch C est 4 donc le port du switch C sera le DP.

Détermination du Designated port sur la liaison switch A-B : Le meilleur root path cost du switch A est 8, le meilleur root path cost du switch B est 4 donc le port 1/1 du switch B sera le DP et le port 1/2 du switch A

sera bloqué.

- Etat des ports

En mode normal, un port peut être dans l'état"blocking " ou l'état"forwarding ". Lors d'un changement de topologie réseau, un port dans l'état"blocking " peut passer à l'état"forwarding ". Seulement, ce changement d'état ne se fait pas immédiatement. Le changement d'état s'effectue de la manière suivante :

⇒ Etat blocking : le port reste environ 20 secondes dans l'état"blocking ". Dans cet état, le port ne laisse passer aucun trafic mais continue d'écouter les BPDUs. Ensuite, il passe dans l'état"listening ".

⇒ Etat listening : Le port dans cet état, il écoute l'ensemble des trames mais ne transmet toujours pas de trames. Il reste dans cet état 15 secondes (valeur par défaut du timer fwdelay), puis passe dans l'état"learning ".

⇒ Etat learning : Dans cet état, le port scrute les trames pour remplir sa table de MAC adresses mais il ne transmet aucune trame. Cette phase dure environ 15 secondes (valeur par défaut du timer fwdelay). A la fin de cette phase d'apprentissage, le port passe dans l'état"forwarding ".

⇒ Etat forwarding : le port continue à remplir sa table MAC adresse et transmet les trames.

Par défaut, le passage de l'état"blocking " à l'état"forwarding " prend 50 secondes. Ce temps peut être diminué pour améliorer la convergence STP en jouant sur la valeur des timers STP ou bien en activant sur les ports différents mode comme le mode portfast.

Mettre un port dans le mode"portfast " permet à celui-ci de passer de l'état"blocking " à l'état l'état"forwarding " sans passer par les états intermédiaires"listening " et"learning ". Cette fonction doit être activée de préférence sur les ports connectés directement à des hosts. Cependant si le host est un hub, un concentrateur ou un swich, une boucle temporaire peut être créée. Ce mode est à utiliser à bon escient.

Ce mode n'est pas supporté par les liens trunks.

**S-PCS -** Services de communication personnelle par satellites. Ensemble de satellites en orbite basse destinés à constituer des réseaux de radiotéléphonie. Les deux principaux projets sont Globalstar et Iridium.

**Spectre électromagnétique -** C'est l'ensemble des fréquences des champs électromagnétiques qui va des champs statiques aux rayons gamma. Les ondes électromagnétiques se caractérisent par leur longueur d'onde, leur fréquence ou leur énergie, ces trois paramètres étant liés entre eux. La fréquence est d'autant plus élevée que la longueur d'onde est courte. Les émissions de radiodiffusion en AM, par exemple, ont des fréquences de l'ordre de 1 MHz et une longueur d'onde d'environ 300 mètres. Les réseaux DCS 1800 fonctionnent à une fréquence de 1800 MHz, correspondant à une longueur d'onde de 17 centimètres.

**SPIROU -** Signalisation Pour l'Interconnexion des Réseaux Ouverts - Interface de signalisation définie par le comité de l'interconnexion sous l'impulsion de l'Autorité et chargée d'adapter au réseau français le standard européen ISUP adopté par l'ETSI. Cette interface comprend l'ensemble des spécifications incluant la signalisation de commande de l'appel téléphonique de base, des services et fonctionnalités avancées, des spécifications d'inter fonctionnement avec les signalisations d'accès usagers et les protocoles de "réseaux intelligents".

**Spoofing -** Usurpation - Tentative d'accès à un système réseau par usurpation (utilisateur, système ou programme autorisés). Désigne une méthode de piratage souvent utilisée qui consiste à modifier l'adresse IP de l'attaquant pour devenir anonyme ou contourner un coupe-feu.

**Spread Spectrum -** Le principe de la modulation à étalement de spectre consiste à étaler l'information sur une bande de fréquences beaucoup plus large que la bande nécessaire, dans le but de combattre les signaux interférents et les distorsions liées à la propagation : le signal se confond avec le bruit. Le signal est codé au départ, un code est assigné à chacun des usagers afin de permettre le décodage à l'arrivée. L'étalement est assuré par un signal pseudo aléatoire appelé code d'étalement. A la réception le signal est perçu comme du bruit si le récepteur n'a pas le code. Le signal étant émis à un niveau plus faible que celui du bruit, le débit reste faible. La modulation avec étalement de spectre est ainsi optimisée pour lutter contre le bruit, dont elle limite mieux les effets.

**SPX -** Sequenced Packet Protocol - Protocole de transport de l'environnement réseau de Novell. Ce protocole fonctionne en mode connecté, à l'instar de TCP dans le monde IP.

SPx est la version Novell du Sequenced Packet Protocol de Xerox (SPP). C'est un protocol situé au niveau de la couche liaison et il permet une distribution des paquet à des applications tierces.

**Spyware -** Logiciel espion chargé de transmettre des informations à un serveur, à l'insu de l'utilisateur. Les données transmises sont variées, allant de l'historique de la navigation sur Internet aux données personnelles en passant par des informations professionnelles.

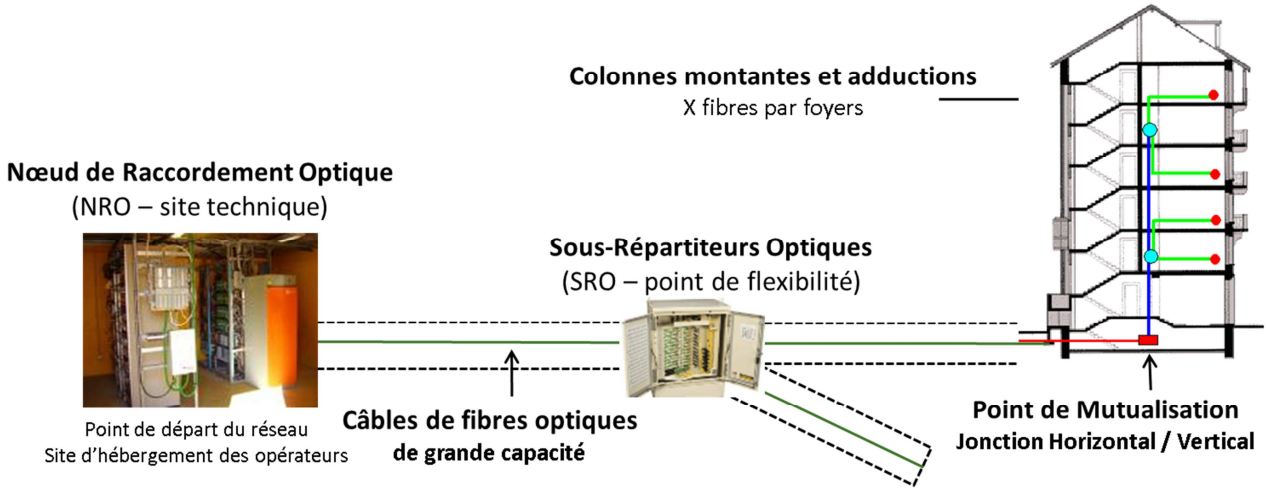
**SQL -** Structured Query Lanquage - Langage de requêtes pour bases de données relationnelles développé par IBM. Grâce à une syntaxe puissante et simple à la fois, SQL est devenu un standard adopté par tous les acteurs du marché des bases de données.

**SRAN -** Satellite Radio Access Network - Réseau d'accès radio satellitaire, composé de la station terrestre (terminal de réception ou antenne de réception) et du satellite.

**SRNS -** Service de Radionavigation par Satellite

**SRO -** Sous Répartiteur Optique - On peut définir le SRO en FTTH comme un répartiteur de liaison. C'est un point de construction dans lequel il est possible de réaliser des liaisons connectorisées en mode P2P ou GPON.

Un SRO se caractérise par son type, sa zone d'emprise, le nombre de logement raccordables et dans certains cas son niveau dans l'arborescence de distribution (SRO1, SRO2,…)




**SS7 -** Système de signalisation qui a été normalisé pour le réseau téléphonique et le RNIS bande étroite.

**SS7oIP -** Appelé autrement SIGTRAN. Technologie permettant de véhiculer les signaux SS7 sur un réseau IP. SS7oIPest transparent pour les protocoles de signalisation "applicatifs "grâce à la notion de "couches d'adaptation "(M2UA, M3UA, SUA, …) créée pour l'occasion.

**SSH -** Secure Shell - Ensemble de programmes et de protocoles qui, à distance, permettent d'établir des sessions sécurisées entre deux hôtes.

**SSID -** Abréviation de ESSID - Il représente le nom du réseau sans fils, et constitue le premier niveau de sécurité dans la mesure où il faut le connaître pour s'y connecter (tous les points d'accès n'effectuent pas un broadcast de leur ESSID).

**SSII -** Société de Service et d'Ingénierie Informatique - Société dont la vocation est d'aider ( ?) les sociétés à gérer leur système d'information.

**SSL -** Secure Socket Layer - Protocole de sécurisation des échanges. Protocole généraliste de sécurisation des échanges informatiques. Actuellement le protocole le plus utilisé dans les applications de commerce électronique sur Internet.

Développé par Netscape, SSL est intégré aux navigateurs depuis 1994, et permet d'assurer la sécurité des échanges de manière transparente entre une machine cliente et une machine serveur sur un réseau informatique comme Internet.

SSL en est actuellement à sa version 3, qui élimine les faiblesses de la version d'origine, la version 2 (la version 1 fut testée en interne par les employés de Netscape). SSL version 3 a servi de base au groupe de travail TLS de l'IETF et WTLS, TLS étant un protocole visant à sécuriser la couche transport, et WTLS étant le protocole TLS appliqué aux téléphones mobiles (Wireless TLS).

SSL étant placé entre la couche transport du modèle OSI (4), et la couche session du modèle OSI (5), il peut être utilisé pour sécuriser tous les échanges supérieurs au niveau 4 OSI comme HTTP, Telnet, FTP, SNMP, etc . Comme SSL se place au dessus de la pile TCP/IP, il ne peut pas sécuriser les échanges faits par le protocole UDP.

SSL offre le service d'authentification, par l'échange de certificats X509 (v3) lors de l'établissement de la session. Cette étape était optionnelle dans la version 2, mais elle est obligatoire pour le serveur dans la version 3. L'échange des clés durant la phase d'authentification et généralement fait avec l'algorithme RSA.

SSL offre le service de confidentialité, par le cryptage des données échangées avec un algorithme symétrique avec une longueur de clé de 40 ou 128 bits. Les algorithmes qui sont utilisés ici sont DES, DES40, triple DES, RC2, RC4 ou IDEA.

SSL fournit le service d'intégrité des données, par l'utilisation d'une fonction de hachage sur les messages transmis. Les fonctions de hachage utilisées sont SHA ou MD5. Avec ces éléments, il est possible d'obtenir des signatures électroniques et donc de permettre le service de non répudiation.

Le protocole SSL se décompose en quatre sous protocoles :

- Handshake, qui prend en charge l'authentification des parties, du choix des algorithmes de cryptage et de hachage et de l'échange d'un secret, nommé le PreMasterSecret.
- Record, qui protège les données à transmettre et les messages reçus des autres sous protocoles par rapport aux paramètres de sécurité choisis durant la phase Handshake.
- ChangeCipherSpec, qui signale à la couche record les modifications sur les paramètres de sécurité.
- Alert, qui signale les erreurs pendant la phase de vérification des messages transmis et des incompatibilités des paramètres choisis entre les deux parties durant la phase handshake.

Les sous protocoles Handshake, ChangeCipherSpec et Alert permettent la gestion des paramètres et des erreurs. C'est le sous protocole Record qui est le cœur de SSL.

Un client et un serveur établissent une session. Cette session peut contenir plusieurs connexions, ce qui permet d'effectuer différents échanges avec différents paramètres de cryptage. Une session SSL se caractérise par deux parties :

- Une phase préliminaire, pendant laquelle ont lieu l'authentification des parties et la négociation des paramètres cryptographiques utilisés au cours de la session (échanges des clés, choix des algorithmes).
- Une phase d'échanges de données de manière sécurisée, à partir des clés et des algorithmes choisis durant la phase préliminaire.

**SSL/TLS -** Secure Socket Layer/Transport Layer Security - SSL est un protocole assurant la sécurité des connexions Internet. TLS, version 3 de SSL, améliore l'authentification. Ils permettent de négocier un échange de clé entre un serveur et un client pour mettre en place un tunnel chiffré.

**SSO -** Single Sign-On - Il s'agit en général d'une gamme d'outils qui mémorise l'ensemble des codes et procédures d'accès pour l'utilisateur. L'utilisateur n'a plus qu'à s'authentifier une seule fois, par exemple lors de l'ouverture de sa session de travail. Les mots de passe peuvent être stockés de façon centralisée (dans un annuaire par exemple) ou localement (dans une carte à puce par exemple).

Le but est de centraliser l'authentification afin de permettre à l'utilisateur d'accéder à toutes les ressources (machines, systèmes, réseaux) auxquels il est autorisé d'accéder, en s'étant identifié une seule fois sur le réseau. L'objectif ainsi de propager l'information d'authentification aux différents services du réseau, voire aux autres réseaux et d'éviter ainsi à l'utilisateur de multiples identifications par mot de passe.

Toute la difficulté de l'exercice réside dans le niveau de confiance entre les entités d'une part et la mise en place d'une procédure de propagation commune à toutes les entités à fédérer.

**Standard -** Norme en anglais. Mais ce mot peut désigner aussi bien les normes officielles (de jure) que les normes de fait (de facto).

**Standardisation -** La standardisation n'a pas de définition officielle. Néanmoins, elle peut s'entendre comme toute tentative par un ou plusieurs acteurs privés d'imposer des spécifications techniques sur le marché. Ainsi, on retrouve les diverses sociétés groupées en forums, clubs ou associations ; particulièrement présents dans le secteur informatique. On peut citer l'organisme de standardisation de l'Internet, ou l'Internet Engineering Task Force (IETF), l'Enterprise Computer Telephony Forum (ECTF) qui font partie de cette catégorie.

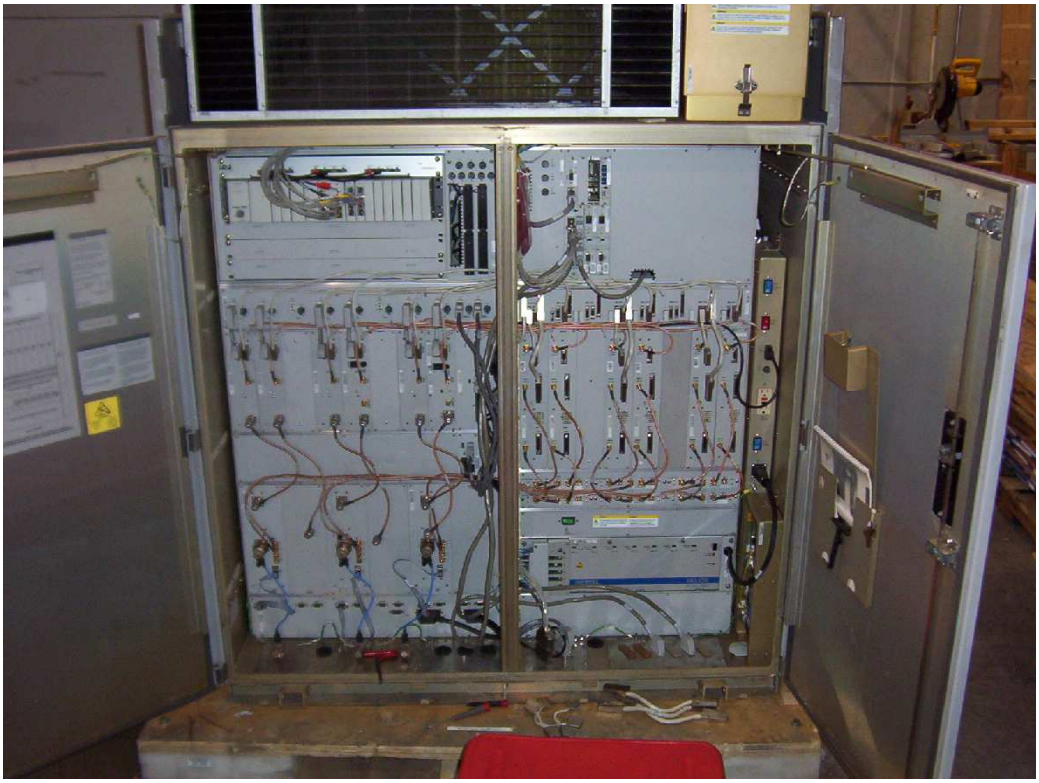
**Starlan -** Standard de réseau local défini par AT&T à l'intérieur de la norme 802.3 (Ethernet). Il fonctionne à 1Mbps sur un câblage en étoile fait de paires torsadées de type téléphonique.

**Start-Stop -** Mode de transmission asynchrone dans lequel chaque mot est délimité par un bit de début (start-bit) et un ou deux bits de fin (stop-bits).

**Stateful inspection -** Employé dans les coupe-feu, le state full inspection ou filtrage dynamique de paquets pousse l'inspection des paquets de données jusqu'aux couches 3 et 4 du modèle OSI. Le coupe-feu conserve une table des sessions actives, et s'assure que les données proviennent d'une session autorisée.

**Station de base -** BTS - Base Transceiver Station - Emetteur récepteur assurant principalement la transmission du signal radio de et vers le mobile, à partir des antennes (de 1 à 3) qui lui sont directement reliées.

Elle relaie les communications à l'intérieur d'une ou plusieurs "cellules ". Leurs antennes mesurent environ 2 mètres de long (pour le réseau GSM à 900 MHz), sont montées sur des pylônes de 15 à 50 m de hauteur ou sur le toit des bâtiments. Elles émettent un faisceau radiofréquence étroit, comparable au faisceau d'un projecteur, quasi-parallèle au sol. Etant donnée la faible ouverture du faisceau dans le plan vertical, l'intensité du champ radiofréquence au sol directement au-dessous de l'antenne, est faible et diminue rapidement avec la distance.



*Nortel S8000 BTS*

**STM 1 -** Module de transport synchrone - Standard pour la transmission sur fibre optique à 155 Mbits/s.

**STM 4 -** Module de transport synchrone - Standard pour la transmission sur fibre optique à 622 Mbits/s.

**Store and Forward -** Mode de fonctionnement standard d'un commutateur. La trame qu'il reçoit est entièrement stockée avant que débute le travail de commutation .

**STP -** Shielded Twisted Pair - Blindage Général Tressé. Caractéristique d'un câble.

**STP -** Signal Transfer Point - Point de transfert de signal dans la terminologie Rnis.

**Streaming -** Technique de transfert de données en un flux (stream) régulier et continu, permet la diffusion de fichiers multimédias par Internet, à la demande et en temps réel.

Technique de transmission audio/vidéo où les informations sont téléchargées et lues en simultané, grâce à un tampon qui se charge de compenser les variations de débit de réception.

**Stripinq -** Dans un système à disques entrelacés (Striping Raid ou Raid 0), les données sont réparties séquentiellement sur au moins deux disques, sans redondance. Le Raid 0 améliore les performances, mais pas la sécurité : si un disque tombe en panne, toutes les données sont perdues.

**Support de Transmission -** Chaque support de transmission est caractérisé par un débit utilisable avec un affaiblissement et un niveau de bruit acceptables.

Parmi les supports de transmission il faut distinguer :

Les supports guidés :

Supports cuivre :

Paires torsadées : débit de 1 Mbits/s à 1Gbits/s

Câbles coaxiaux : débit de qq 10Mbits/s à 100Mbits/s

Supports optiques :

Fibres optiques : débit de 50 Mbits/s à 10 Gbits/s

Les supports non guidés :

Émissions radios dirigées :

Faisceaux hertzien : débit de 10 Mbits/s à 1 Gbits/s

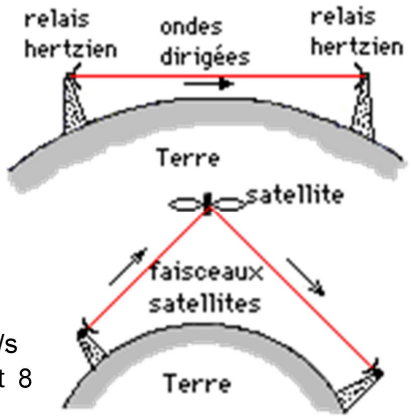
Satellite : débit de 2 Mbits/s à 50 Mbits/s

Émission radios non dirigées :

Téléphonie cellulaire : débits jusqu'à 4 Mbits/s

Radio diffusion: plusieurs dizaines de canaux à 128 Kbits/s

Télé diffusion : débit de 19 chaînes entre 4 Mbits/s et 8 Mbits/s




**SVCD -** Propose un codage MPEG2 à 2600000 Bits/s en VBR, ce qui procure 35 minutes de vidéo sur un CD.

**SVI -** Service Vocal Interactif - Apparu au début des années 70 aux États-Unis et au début des années 80 en France. Il fut le premier équipement à intégrer à la fois des technologies venant du monde de la téléphonie et du monde de l'informatique. Ce fut ainsi à l'époque une petite révolution, mais surtout l'ouverture d'un nouveau marché très attrayant et lucratif pour les équipementiers. D'autre part, le SVI a introduit la notion d'interactivité grâce au fait qu'il pouvait être commandé à distance grâce à une fonction de sur-numérotation. La sur-numérotation permet en effet de commander le SVI à l'aide d'un simple téléphone, par l'intermédiaire des codes DTMF. Le SVI possède à la fois une fonction vocale, une fonction téléphonique et une fonction informatique sur une même plate-forme, et peut être interfacé directement sur le RTC ou bien derrière un PABX.

**S-Video -** Avec les sorties SVHS : Format de vidéo de 500 points par lignes.

**Synchrone -** Mode de transmission dans lequel l'émetteur et le récepteur fonctionnent au même rythme, calés sur une même horloge. En mode synchrone, la transmission est réalisé par un accord préalable de l'émetteur et du récepteur sur un rythme d'horloge constant - Mode de transmission de données dont lequel le rythme d'émission est calé sur celui d'une horloge. Mode de transmission dans lequel l'émetteur et le récepteur fonctionnent au même rythme, calés sur une même horloge.

**Synchronisation -** Mise en phase de deux équipements qui se calent sur le même rythme d'horloge. Peut être réalisée de deux manières: soit un rythme d'horloge unique est distribué à tous les équipements, soit un équipement envoie à l'autre une suite de bits particulière sur laquelle le second cale sa propre horloge.

**Système central -** Ordinateur de grande taille (mainframe) jouant un rôle de concentration et de direction dans un système informatique hiérarchisé.

# T

**T -** Point de référence, dans la terminologie officielle du CCITT, définissant une interface entre l'extrémité d'un réseau numérique public et le réseau abonné. Ainsi dans le Rnis, on pourra trouver une interface T0 pour l'Accès de base et une interface T2 pour l'Accès primaire.

**T1, T2, T3... -** Désignent aux Etats-Unis une norme de ligne spécialisée numérique. Ainsi, T1 désignera une ligne à 1 544 Kbps (24 circuits de base à 64 Kbps), T2 à 6,312 Mbps (96 X 64 Kbps), T3 à 44 Mbps (670 X 64 Kbps) selon la hiérarchie américaine. Attention, ne pas confondre avec la définition T, les hiérarchies américaine et européenne étant différentes.

Le terme anglais T-Carrier désigne des lignes de télécommunications capables d'acheminer de la voix ou des données. Le chiffre qui suit correspond à une hiérarchie des capacités de bande passante. En Amérique du Nord et au Japon, le chiffre correspond à une combinaison de plusieurs flux (un multiplexage) de 24 canaux de 64 Kbits/seconde.

**TACACS+ -** Terminal Access Controller Access Control System Plus - Protocole AAA principalement utilisé pour la gestion des connexions commutées.

**TACS -** Total Access Coverage Service (standard radiocom cellulaire anglais)

**Tag Switching** - Technologie de commutation de paquets développée par CISCO Systems, dont l'architecture est dotée de deux composantes principales : acheminement (forwarding) et contrôle.

L'acheminement est effectué en utilisant des techniques de label-swapping, tandis que pour le contrôle, on utilise les protocoles de routage niveau réseau existants ainsi que des mécanismes pour la liaison et la distribution des étiquettes (tags).

Même si le tag switching ne repose pas sur ATM, il peut être directement appliqué aux switchs ATM.

Le Tag Switching allie la souplesse et la richesse de fonctionnalités fournies par le routage niveau 3 (Network Layer routing) avec la simplicité du label swapping. Cette simplicité permet d'améliorer les performances d'acheminement tout en maintenant un rapport qualité/prix compétitif.

Les ingrédients du tag switching.

Un réseau tag switching est constitué de 2 sortes d'équipements :

- Les Tag Edge Routers sont des équipements de routage niveau réseau qui sont situés en bordure d'un réseau tag switching. Ils examinent les paquets arrivant dans le réseau et leur appliquent le tag, ou label, approprié, avant qu'ils ne soient acheminés vers leur noeud suivant (next hop) Pour les paquets qui quittent le réseau tag switch, les tag edge routers effectuent l'opération inverse en retirant les tags des paquets. Ces routeurs effectuent aussi des services à valeur ajoutée niveau réseau tels que la sécurité ou la classification de la QOS. Les tag edge routers utilisent les protocoles de routage standard pour créer les tables de routage qui identifient les routes au travers du réseau. En se basant sur les tables de routage, les tag edge routers utilisent le protocole de distribution des tags (TDP : tag distribution protocol) pour appliquer et distribuer les tags aux autres tag edge routers ou aux tag switchs.
- Les tag switchs sont au coeur du réseau tag switching. Ils acheminent les paquets marqués de tags. Les switchs ATM peuvent être utilisés en tant que tag switchs. Les tag switchs reçoivent, grâce au TDP, les informations provenant des tag edge routers et construisent leur propre base de donnée d'acheminement. Les tag switchs commutent alors les paquets en se basant seulement sur les tags, sans regarder l'entête niveau 3.

Tag Distribution Protocol (TDP)

Le Tag Distribution Protocol (TDP) est utilise par les équipements de tag switching afin de distribuer, requérir et mettre à jour les informations d'association de tag pour les protocoles IP dans le réseau. TDP ne remplace pas un protocole de routage. Il utilise plutôt les informations fournies par les protocoles de routage afin de créer les associations de tags.

Les bases d'information.

Le tag switching utilise 3 types de bases d'information pour enregistrer et retrouver les informations d'acheminement :

- La Forwarding Information Base (FIB) : Forme condensée de table de routage contenant les adresses de destination, les adresses de next hop, et les interfaces sortantes. Les routeurs basent les décisions d'acheminement sur l'adresse de destination d'un paquet, plus l'information contenue dans la FIB.
- La Tag Information Base (TIB) : Sert à associer un tag entrant à un ou plusieurs des éléments suivants : Tag sortant, Adresse de destination, Outgoing link-level information…Une TIB peu exister entièrement pour un commutateur, une interface ou une combinaison des 2.
- La Tag Forwarding Information Base (TFIB): elle utilise les informations de la FIB et de la TIB pour construire l'information d'acheminement constituée de l'interface entrante, l'adresse de destination, le tag entrant, le next hop le plus efficace, et l'interface de sortie.

Les composantes du Tag Switching.

Le Tag Switching comprend 2 composantes: l'acheminement et le contrôle. Afin d'assurer l'acheminement des paquets, la composante d'acheminement utilise les informations des étiquettes (tags) contenues dans les paquets et les informations d'acheminement de tag maintenues par un tag switch. La composante de contrôle est chargée de maintenir correctes les informations d'acheminement de tag au sein d'un groupe de tag switchs interconnectés.

- La composante d'acheminement.

Le paradigme fondamental d'acheminement utilisé dans le tag switching est basé sur la notion de label swaping. Quand un paquet contenant un tag est reçu par un tag switch, le commutateur utilise le tag comme un index dans sa base d'information : la Tag Infomation Base (TIB). Chaque entrée dans la TIB est constituée d'un tag d'entrée, et de une ou plusieurs sous-entrées de la forme : (tag sortant, interface de sortie, niveau d'information de la liaison sortante). Si le commutateur trouve une entrée avec le tag entrant égal au tag contenu par le paquet, alors pour chaque tag sortant, interface de sortie, niveau d'information du lien sortant de l'entrée, le commutateur remplace le tag du paquet par le tag de sortie. Il remplace aussi le niveau d'information de la liaison (adresse MAC) dans le paquet par le niveau d'information de la liaison sortante. Il achemine enfin le paquet à travers l'interface de sortie. La décision d'acheminement est basée sur l'algorithme de correspondance exacte qui utilise comme index un tag de longueur fixe, assez court. Ceci permet une procédure d'acheminement plus simple comparée à celle mise en oeuvre dans la couche réseau. La procédure d'acheminement est suffisamment simple pour autoriser directement une implémentation matérielle. Le même algorithme d'acheminement s'applique à la fois pour l'unicast et le multicast - une entrée unicast possèderait une unique sous-entrée (tag de sortie, interface de sortie, niveau d'information de liaison sortante), alors qu'une entrée multicast possède une ou plusieurs sous-entrées de même type. (Pour les liaisons multi-accès, le niveau d'information du lien sortant inclurait dans ce cas une adresse MAC multicast). Ceci illustre comment avec le tag switching, le même paradigme d'acheminement peut être utilisé pour supporter différentes fonctions de routage.

- La composante de contrôle.

La notion d'association entre un tag et le routage niveau réseau est essentielle. Le tag switching supporte un large choix de granularités d'acheminement afin de fournir de bonnes caractéristiques de dimensionnement et accommoder en même temps diverses fonctionnalités de routage. Un tag pourrait être associé à un groupe de routes, ou encore un tag pourrait être associé au flux d'une application individuelle. Il pourrait aussi être associé à un arbre multicast.

La composante de contrôle se charge de créer des associations de tags et de distribuer ensuite les informations d'association de tags parmi les tag switchs. La composante de contrôle est structurée comme une collection de modules, chacun étant conçu pour assurer une fonction de routage particulière. De nouveaux modules peuvent être rajoutés pour supporter de nouvelles fonctions de routage.

Le routage basé sur la destination.

Le tag switching peut supporter le routage basé sur la destination. Le routeur décide de l'acheminement en se basant sur l'adresse de destination contenue dans le paquet et de la base d'information d'acheminement (FIB) maintenue par le routeur. Un routeur construit sa FIB en utilisant les informations qu'il reçoit des protocoles de routage (OSPF, BGP).

Il existe 3 méthodes différentes pour l'allocation du tag et la gestion de la TIB (Tag Information Base) : l'allocation du tag en aval, l'allocation du tag en aval sur demande, l'allocation du tag en amont.

Dans tous les cas, un switch alloue les tags et les associe à des préfixes d'adresse dans sa FIB. Dans le cas de l'allocation en aval, le tag qui est véhiculé par un paquet est généré et associé à un préfixe par le switch à l'extrémité aval du lien (en tenant compte de la direction du flux de données). Dans le cas de l'allocation en amont, les tags sont alloués et associés au niveau de l'extrémité amont du lien. L'allocation sur demande signifie que les tags vont être alloués et distribués par le switch en aval seulement lorsque le switch en amont en fait la requête.

Dans le cas de l'allocation en aval, un switch est responsable de la création des associations de tags qui s'applique aux paquets de données entrants, et reçoit par ses voisins les associations de tags pour les paquets sortants. Dans le cas de l'allocation en amont, un switch est responsable de la création des associations de tags pour les tags sortants (c'est à dire pour les tags qui s'appliquent aux paquets de données qui partent du commutateur) et reçoit par ses voisins les associations de tags pour les paquets entrants. Le schema de l'allocation des tags en aval fonctionne de la manière suivante: pour chaque route de sa FIB, le switch alloue un tag, crée une entrée dans sa TIB (Tag Information Base) avec le tag entrant fixé sur le tag alloué, et avertit ensuite de l'association entre le tag et la route vers les commutateurs adjacents. Cet avertissement peut se faire en mettant l'association sur le dos du protocole de routage existant, ou bien en utilisant un protocole de distribution des tags (TDP : Tag Distribution Protocol) séparé. Quand un tag switch reçoit une information d'association de tag pour une route et que cette information provient du noeud suivant (pour cette route), le commutateur place le tag (porté comme faisant partie de l'association d'association) dans le tag de sortie de l'entrée dans la TIB associée avec la route. Ceci crée l'association entre le tag sortant et la route.

Avec le schéma de l'allocation des tags en aval sur demande, on opère comme suit. Pour chaque route dans sa FIB, le switch identifie le prochain noeud (next hop) pour cette route. Il envoie ensuite une requête (via TDP) au prochain noeud dans la route pour l'association de tag. Quand le noeud suivant reçoit la requête, il alloue un tag, crée une entrée dans sa TIB en fixant le tag entrant sur le tag alloué, et retourne ensuite l'association entre le tag (entrant) et la route au commutateur qui est à l'origine de la requête. Quand le commutateur reçoit les informations d'association, il crée une entrée dans sa TIB dans laquelle le tag sortant prend la valeur reçue du noeud suivant.

On utilise le schéma de l'allocation des tags en amont de la manière suivante. Si un tag switch possède une ou plusieurs interfaces point à point, pour chaque route de sa FIB dont le noeud suivant peut être atteinte via une de ces interfaces, le commutateur alloue un tag et avertit le noeud suivant de l'association entre le tag (sortant) et la route. Quand le commutateur du noeud suivant reçoit les informations d'association, il place le tag dans la TIB en l'associant à la route. Une fois que l'entrée de la TIB est remplie avec les tags entrants et les tags sortants, le tag switch peut acheminer les paquets pour les routes associées aux tags en utilisant l'algorithme d'acheminement du tag switching. Quand un tag switch crée une association entre un tag sortant et une route, le commutateur, en plus de remplir sa TIB, met aussi à jour sa FIB avec les informations d'association. Cela permet au commutateur d'ajouter des tags aux paquets qui en sont dépourvus.

Hiérarchie de la connaissance de routage.

L'architecture de routage IP modélise un réseau comme une collection d'ensembles de routages. Au sein d'un domaine, le routage s'effectue via un routage interne (ex : OSPF), tandis que le routage au travers des différents domaines s'effectue en utilisant un routage externe (ex : BGP). Tous les routeurs au sein de domaines qui portent du trafic de transit (ex : les domaines formés par les ISP) doivent maintenir les informations fournies par le routage interne mais aussi celles fournies par le routage externe. Cela est à l'origine de certains problèmes. Tout d'abord, la quantité d'information n'est pas insignifiante ce qui rajoute de la demande en ressources nécessaires aux routeurs. De plus l'augmentation du volume des informations de routage augmente bien souvent le temps de convergence de routage, ce qui dégrade les performances générales du système.

Le tag switching autorise le découplage du routage interne et externe. De cette façon, seuls les tag switchs situés en périphérie d'un domaine sont requis pour maintenir les informations de routage fournies par le routage externe, tandis que tous les autres switchs maintiennent uniquement les informations de routage fournies par le routage interne au domaine (qui sont généralement moins volumineuses que les informations de routage externe). En conséquences, la charge de routage des commutateurs qui ne sont pas en périphérie est réduite et le temps de convergence est écourté.

Afin de supporter cette fonctionnalité, le tag switching autorise un paquet à porter un ensemble de tags et non un seul. Cet ensemble est organisé comme une pile. Le tag switch peut échanger le tag du sommet de la pile, ou dépiler un tag, ou échanger le tag et empiler un ou plusieurs tags de la pile.

Quand un paquet est acheminé entre 2 commutateurs (en périphérie) de domaines différents, la pile du paquet contient seulement un tag. Quand un paquet est acheminé à l'intérieur d'un domaine, la pile du paquet contient 2 tags, le 2ème étant empilé par le tag switch à l'entrée du domaine. Le tag de sommet de la pile permet d'acheminer le paquet jusqu'au tag switch approprié à la sortie du domaine. Le tag suivant dans la pile permet l'acheminement correct du paquet à la sortie du domaine. La pile est dépilée soit par le commutateur de sortie du domaine, soit par l'avant dernier.

Multicast.

La notion de "spanning tree" est essentielle pour le routage multicast. Des procédures de routage multicast (ex : PIM) sont responsables de la constRAction de tels arbres (les feuilles représentent les récepteurs), alors que l'acheminement multicast est responsable de l'acheminement des paquets multicast en suivant les arbres.

Pour supporter une fonction d'acheminement multicast avec le tag switching, chaque tag switch associe un tag à un arbre multicast. Quand un tag switch crée une entrée d'acheminement multicast ainsi que la liste des interfaces sortantes pour cette entrée, le commutateur crée également des tags locaux (un par interface sortante). Le commutateur crée une entrée dans sa TIB et la remplie avec cette information pour chaque interface sortante en plaçant un tag généré localement dans le champ de tag sortant. Ceci crée une association entre un arbre multicast et le tag. Le commutateur avertit alors, au-delà de chaque interface sortante, de l'association entre le tag (associé à cette interface) et l'arbre. Quand un tag switch est averti de l'association entre un arbre multicast et un tag provenant d'un autre tag switch, si cet autre switch est son voisin en amont (en suivant l'arbre multicast), il place le tag associé dans la composante de tag entrant de l'entrée de la TIB qui est associée à l'arbre.

Routage flexible (routes explicites).

La propriété fondamentale du routage basé sur la destination est que la seule information utilisée pour acheminer le paquet est l'adresse de destination. Tandis que cette propriété permet un routage hautement précis, elle limite aussi la possibilité d'influencer le chemin suivi par les paquets. Ceci limite la capacité de distribuer le trafic parmi des liaisons multiples en allégeant la charge des liaisons les plus utilisés et en

redistribuant cette charge sur les liaisons moins sollicitées.

Pour acheminer vers des chemins différents de celui déterminé par le routage basé sur la destination, la composante de contrôle du tag switching autorise l'installation d'associations dans les tag switchs qui ne correspondent pas aux chemins du routage basé sur la destination.

Tag Switching avec ATM.

La technologie du tag switching peut s'appliquer aux commutateurs ATM en implémentant la composante de contrôle du tag switching.

L'information de tag nécessaire pour le tag switching peut être portée par le champ VCI. Si on a besoin de 2 niveaux de tagging, le champ VPI peut être lui aussi utilisé bien que la taille du champ VPI limite la taille du réseau.

Pour supporter la fonction de routage basé sur la destination avec le tag switching sur un commutateur ATM, il faut que le switch maintienne plusieurs tags associés à une route (ou à un groupe de routes possédant le même next hop). Il est indispensable d'éviter l'enchevêtrement des paquets qui proviennent des différents tags switchs en amont mais qui sont envoyés simultanément au même next hop. On peut utiliser l'allocation de tag sur demande en aval ou bien utiliser le schéma de l'allocation en amont pour l'allocation des tags et les procédures de maintenance de la TIB avec les commutateurs ATM.

Par conséquent, un commutateur ATM peut supporter le tag switching, mais il a au minimum besoin d'implémenter des protocoles de routage niveau réseau ainsi que la composante de contrôle du tag switching sur le commutateur. Il a aussi besoin de supporter l'acheminement niveau réseau.

L'implémentation du tag switching sur un commutateur ATM simplifie l'intégration des routeurs et des commutateurs ATM. Un commutateur ATM capable de faire du tag switching apparaît comme un routeur pour le routeur adjacent. Les schémas d'adressage, de routage et de signalisation ATM ne sont plus nécessaires.

Qualité de service.

On utilise 2 mécanisme pour fournir une gamme de qualité de service aux paquets qui traversent un routeur ou un tag switch. On a tout d'abord besoin de ranger les paquets dans différentes classes. On doit ensuite s'assurer que la manipulation des paquets est telle que les caractéristiques appropriées de QOS sont fournies à chaque classe.

**TAPI -** Telephony Application Programming Interface - Interface de programmation d'applications CTI développée par Microsoft et Intel. Cette interface de programmation a pour fonction de rendre disponible l'ensemble des services offerts par le PABX à l'application de commande téléphonique. Il est établi un lien bidirectionnel avec le PABX ainsi le serveur informatique peut commander le PABX. Il est à noter que TAPI ne prend pas en compte CSTA.

Parmi toutes les API de téléphonie, TAPI est la plus populaire pour deux raisons : TAPI est intégré au système d'exploitation Windows de Microsoft depuis 1995 et une application est simple à déployer avec un modem et ceci se fait sans frais supplémentaires.

La première version de TAPI 1 était microcentrique (centrée sur le PC). Celui-ci se connectait directement au PABX (architecture dite First Party). Ce fut un échec car Microsoft pensait imposer l'achat d'une carte permettant le dialogue entre les outils informatique et téléphoniques, ceci par PC. Mais l'investissement est trop important pour une entreprise qui dispose d'un réseau conséquent. Le système de cartes individuelles n'était donc pas au point.

TAPI 2 est plutôt une toute nouvelle version avec une architecture revue imitant celle de son concurrent Novell (avec TSAPI). TAPI 2 est désormais client-serveur et son intégration à Windows NT Server ainsi que la migration des entreprises vers NT voit sa part de marché augmenter nettement. Cette approche serveur-centrique (architecture dite Third Party) permet de ne faire communiquer qu'un serveur avec le PABX au lieu de plusieurs micro-ordinateurs avec TAPI 1. De plus, TAPI 2 a intégré des fonctions qui n'étaient pas offertes dans le cadre de TAPI 1, comme la gestion des files d'attente, les statistiques ou encore la gestion des statuts des postes des télé opérateurs.

TAPI 3.0 est sorti avec Windows 2000 en début d'année 2000 et améliore TAPI 2.0 en étendant son champ d'action : TAPI 3 fournit un langage de haut niveau, orienté objet alors que TAPI 2 est une API écrite en C ; TAPI 3 fournit de nouvelles fonctionnalités mais surtout une nouvelle connectivité avec les bases de données, les périphériques comme les caméras numériques. De plus, TAPI 3 encapsule TAPI 2.

**Taux d'erreurs -** Error Rate - Rapport du nombre de bits erronés au nombre total de bits transmis.

**Taux d'erreurs Résiduelles -** Residual error-rate - Rapport du nombre des bits incorrectement reçus mais non détectés comme tels, au nombre total de bits transmis.

**Taxe de base -** Unité utilisée par France Télécom pour facturer l'utilisation du réseau téléphonique commuté. Elle correspond à l'incrémentation d'un compteur de taxation qui "tourne" plus ou moins vite selon les services, les horaires, la distance et parfois le volume transporté. Longtemps utilisée comme base de calcul de tous les tarifs de France Télécom, le prix d'un service s'exprimant en nombre taxe de base, elle n'y joue plus aujourd'hui le même rôle central dans son système tarifaire en dehors du Réseau téléphonique commuté.

**Taxes de répartition -** Système qui établit les principes de tarification auxquels satisfont les conventions d'interconnexion entre opérateurs au plan international afin de permettre de répartir les recettes des communications internationales entre l'opérateur du pays d'origine et celui du pays de destination, qui acheminent conjointement ces communications. Pour les communications correspondant à une destination internationale donnée, l'opérateur du pays d'origine fixe un prix de vente aux usagers (tarif de détail) appelé taxe de perception. Parallèlement, l'opérateur du pays d'origine et celui du pays de destination négocient un montant par minute appelé taxe de répartition. C'est sur la base de cette taxe que la répartition des recettes s'effectue, en fonction d'une clé de répartition, qui fixe la quote-part versée par l'opérateur du pays d'origine à celui du pays d'arrivée. Cette quote-part est le plus souvent égale à la moitié de la taxe de répartition.

**TBR -** Normes harmonisées établies par l'ETSI servant de base aux réglementations techniques communes utilisées pour définir les exigences essentielles auxquelles doivent répondre les équipements terminaux.

**TCO -** Total Cost of Ownership - Coût total de possession - Le coût total d'un équipement ou d'un service ne se résume pas à son prix d'acquisition, le TCO doit tenir compte de l'exploitation de l'équipement, les périodes de pannes, la maintenance, le remplacement et/ou le recyclage de l'équipement.

En détaillant encore un peu plus, il va falloir comptabiliser le CAPEX et l'OPEX prévisibles pour "reventiler" le TCO très précisément sur la période d'utilisation prévue de l'équipement, en tenant compte des garanties.

**TCP -** Transmission Control Protocol - Protocole de transport de l'architecture TCP/IP, notamment utilisé dans le monde Internet. Protocole de niveau 4 fonctionnant en mode connecté. Il opère avec le protocole IP et permet de résoudre des problèmes de perte de niveau inférieur.

TCP permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP). Lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP, en fixant le champ protocole à 6 (Pour savoir que le protocole en amont est TCP...). TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission.

Les caractéristiques principales du protocole TCP sont les suivantes:

- TCP permet de remettre en ordre les datagrammes en provenance du protocole IP
- TCP permet de vérifier le flot de données afin d'éviter une saturation du réseau
- TCP permet de formater les données en segments de longueur variable afin de les "remettre" au protocole IP
- TCP permet de multiplexer les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources (applications par exemple) distinctes sur une même ligne
- TCP permet enfin l'initialisation et la fin d'une communication de manière "courtoise"

Grâce au protocole TCP, les applications peuvent communiquer de façon sûre (grâce au système d'accusés de réception du protocole TCP), indépendamment des couches inférieures. Cela signifie que les routeurs (qui travaillent dans la couche Internet) ont pour seul rôle l'acheminement des données sous forme de datagrammes, sans se préoccuper du contrôle des données, car celui-ci est réalisé par la couche transport (plus particulièrement par le protocole TCP).

Lors d'une communication à travers le protocole TCP, les deux machines doivent établir une connexion. La machine émettrice (celle qui demande la connexion) est appelée client, tandis que la machine réceptrice est appelée serveur. On dit qu'on est alors dans un environnement Client-Serveur. Les machines dans un tel environnement communiquent en mode connecté, c'est-à-dire que la communication se fait dans les deux sens.

Pour permettre le bon déroulement de la communication et de tous les contrôles qui l'accompagnent, les données sont encapsulées, on ajoute aux paquets de données un en-tête qui va permettre de synchroniser les transmissions et d'assurer leur réception.

Une autre particularité de TCP est de pouvoir réguler le débit des données grâce à sa capacité à émettre des messages de taille variable, ces messages sont appelés segments.

TCP permet d'effectuer une tâche importante: le multiplexage/démultiplexage. Ces opérations sont réalisées grâce au concept de ports (ou sockets). Un numéro est associé à un type d'application, qui, combiné à une adresse IP, permet de déterminer de façon unique une application qui tourne sur une machine donnée.

L'entête d'un segment TCP est constitué comme suit:

- Port Source (16 bits): Port relatif à l'application en cours sur la machine source
- Port Destination (16 bits): Port relatif à l'application en cours sur la machine de destination
- Numéro d'ordre (32 bits): Lorsque le drapeau SYN est à 0, le numéro d'ordre est celui du premier mot du segment en cours. Lorsque SYN est à 1, le numéro d'ordre est égal au numéro d'ordre initial utilisé pour synchroniser les numéros de séquence (ISN)
- Numéro d'accusé de réception (32 bits): Le numéro d'accusé de réception également appelé numéro d'acquittement correspond au numéro (d'ordre) du prochain segment attendu, et non le numéro du dernier segment reçu.
- Décalage des données (4 bits): il permet de repérer le début des données dans le paquet. Le

décalage est ici essentiel car le champ d'options est de taille variable
- Réservé (6 bits): Champ inutilisé actuellement mais prévu pour l'avenir
- Drapeaux (flags) (6x1 bit): Les drapeaux représentent des informations supplémentaires:
- URG: si ce drapeau est à 1 le paquet doit être traité de façon urgente.
- ACK: si ce drapeau est à 1 le paquet est un accusé de réception.
- PSH (PUSH): si ce drapeau est à 1, le paquet fonctionne suivant la méthode PUSH.
- RST: si ce drapeau est à 1, la connexion est réinitialisée.
- SYN: Le Flag TCP SYN indique une demande d'établissement de connexion.
- FIN: si ce drapeau est à 1 la connexion s'interrompt.
- Fenêtre (16 bits): Champ permettant de connaître le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception
- Somme de contrôle (Checksum ou CRC): La somme de contrôle est réalisée en faisant la somme des champs de données de l'en-tête, afin de pouvoir vérifier l'intégrité de l'en-tête
- Pointeur d'urgence (16 bits): Indique le numéro d'ordre à partir duquel l'information devient urgente
- Options (Taille variable): Des options diverses
- Remplissage: On remplit l'espace restant après les options avec des zéros pour avoir une longueur multiple de 32 bits
- Les données.

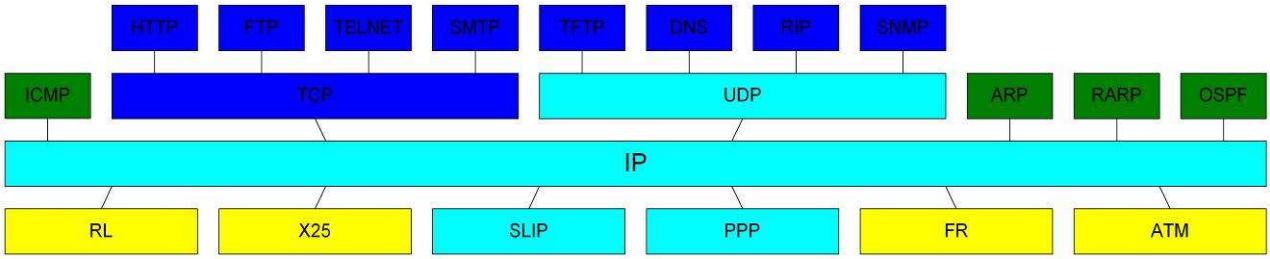
Le protocole TCP permet d'assurer le transfert des données de façon fiable, bien qu'il utilise le protocole IP, qui n'intègre aucun contrôle de livraison de datagramme. En réalité, le protocole TCP possède un système d'accusé de réception permettant au client et au serveur de s'assurer de la bonne réception mutuelle des données. Lors de l'émission d'un segment, un numéro d'ordre (appelé aussi numéro de séquence) est associé. A réception d'un segment de donnée, la machine réceptrice va retourner un segment de donnée dont le drapeau ACK est à 1 (afin de signaler qu'il s'agit d'un accusé de réception) accompagné d'un numéro d'accusé de réception égal au numéro d'ordre précédent. De plus, grâce à une minuterie déclenchée dès réception d'un segment au niveau de la machine émettrice, le segment est réexpédié dès que le temps imparti est écoulé, car dans ce cas la machine émettrice considère que le segment est perdu... Toutefois, si le segment n'est pas perdu et qu'il arrive tout de même à destination, la machine réceptrice saura grâce au numéro d'ordre qu'il s'agit d'un doublon et ne conservera que le dernier segment arrivé à destination.

**TCP/IP -** Transmission Control Protocol / Internet Protocol - Protocole de communication développé par Vinton Cerf et Bob Kahn à la demande du Département américain de la Défense pour faire communiquer des machines hétérogènes sur un réseau de données en transmission par paquet.

Ce protocole doit surtout son succès au fait qu'il a été l'un des premiers protocoles à permettre d'interconnecter entre eux plusieurs réseaux locaux hétérogènes.

A partir du 1er janvier 1983, le réseau de l'Arpa - Arpanet - le réseau de la recherche publique, Milnet - réseau crée pour l'usage des militaires, CSNet - réseau crée pour la communauté scientifique et Bitnet - réseau crée pour les échanges entre universités sont tenus d'utiliser les protocoles TCP/IP.

Non retenu dans le cadre de la normalisation officielle de l'ISO pour l'interconnexion de réseaux hétérogènes, il reste cependant le plus utilisé dans le monde des stations de travail sous Ethernet et Unix.




L'architecture TCP/IP comprend un ensemble de protocoles dont les principaux sont représentés ci-dessus. A l'origine, TCP/IP a été conçu pour s'appuyer sur Ethernet et les réseaux distants de type X25. Par la suite, l'interfaçage avec l'ensemble des réseaux locaux a été réalisé, et l'implémentation sur les protocoles haut débits effectués. Des protocoles de lignes ou de liaisons spécialisées en mode point à point (SLIP et PPP) ont été développés.

L'ensemble des protocoles regroupés sous le sigle TCP/IP (Transmission Control Protocol et Internet Protocol) règne aujourd'hui en maître sur le monde des réseaux, qu'ils soient locaux ou étendus. Preuve de leur consécration: ce sont "les" protocoles par excellence du réseau des réseaux: l'Internet.

Ce succès, TCP/IP le doit à sa simplicité et à son pragmatisme. Simple car, contrairement au très complexe modèle de communication des systèmes OSI (7 couches), TCP/IP ne comprend que deux couches: la couche réseau "IP" (correspondant au niveau 3 de l'OSI) et la couche transport "TCP" (similaire à la couche 4 de l'OSI).

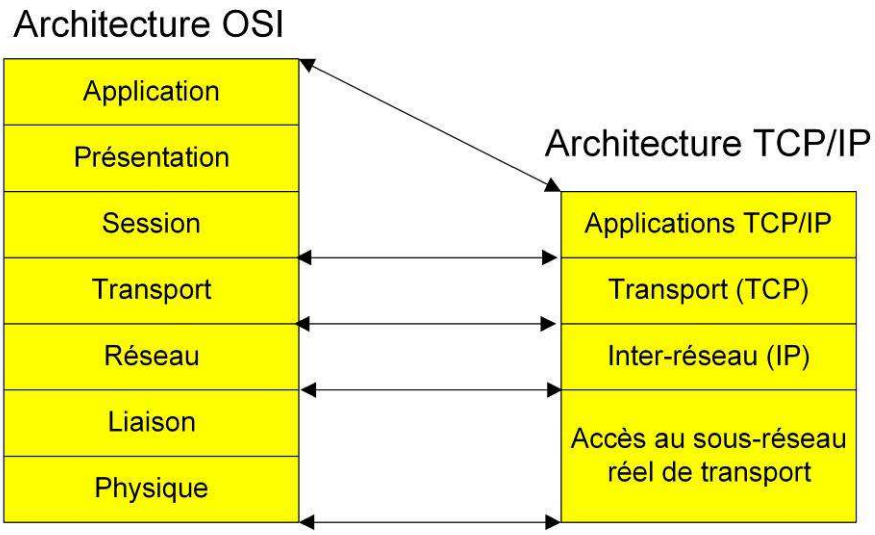
TCP intervient au dessus de la couche IP pour assurer (via des règles bien codifiées) l'établissement de bout en bout de la communication. Ces règles incluent des services de contrôle des flux, de fourniture de bulletins d'acquittement et des fonctions de sécurité.

IP, en dessous de la couche TCP, est le protocole qui permet d'interconnecter deux sous réseaux ayant des caractéristiques physiques différentes. En clair, la transmission selon le protocole TCP/IP se produit comme suit: c'est TCP qui se charge de découper les données en paquets (entre 30 et 500 octets) en incluant dans chaque paquet un entête.

C'est ensuite IP qui achemine les paquets de routeur en routeur à travers le réseau. À l'arrivée, c'est à nouveau TCP qui intervient pour remettre les paquets dans le bon ordre et reconstituer les données initiales sur le système destinataire.

A cette simplicité et ce côté pragmatique du protocole, s'ajoutent divers facteurs qui ont consolidé le succès de TCP/IP: la disponibilité de ses spécifications dans le domaine public (sous forme d'appels à commentaires ou RFC, Request for comments), son intégration en natif sur les systèmes Unix et, bien sûr, les échecs de la normalisation OSI jugée trop complexe à mettre en Oeuvre par les utilisateurs et les constructeurs réunis.

Résultat: TCP/IP a été l'un des premiers protocoles à pouvoir interconnecter des réseaux locaux hétérogènes, à l'heure où l'informatique distribuée et le mode client serveur se développaient autour de systèmes d'information multi constructeurs. Si l'on rajoute à cette liste le fait que TCP/IP est parfaitement adapté aux technologies haut débit des réseaux locaux et aux contraintes des réseaux longue distance, on comprend pourquoi cet ensemble de protocoles est devenu le protocole de référence des années quatre-vingt-dix et sans doute celui des années à venir.




Le modèle TCP/IP comprend 2 couches principales. Il n'y a pas de couche application au sens OSI du terme

Les rôles des différentes couches sont les suivants :

- Couche Accès réseau : elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé (Ethernet, Token Ring, FDDI…)

La couche accès réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en oeuvre afin de transmettre des données via un réseau.

Ainsi, la couche accès réseau contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local (Anneau à jeton - token ring, ethernet, FDDI), de connexion à une ligne téléphonique ou n'importe quel type de liaison à un réseau. Elle prend en charge les notions suivantes :

  - Acheminement des données sur la liaison
  - Coordination de la transmission de données (synchronisation)
  - Format des données
  - Conversion des signaux (analogique/numérique)
  - Contrôle des erreurs à l'arrivée

- Couche Inter-réseau : elle est chargée de fournir le paquet de données (datagramme)

C'est cette couche qui définit les datagrammes, et qui gère les notions d'adressage IP. Elle permet l'acheminement des datagrammes (paquets de données) vers des machines distantes ainsi que de la gestion de leur fragmentation et de leur assemblage à réception.

La couche Internet (inter-réseau) contient 5 protocoles :

- Le protocole IP
- Le protocole ARP
- Le protocole ICMP
- Le protocole RARP
- Le protocole IGMP

Les trois premiers protocoles sont les protocoles les plus importants de cette couche...

- Couche Transport : elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.

La couche transport permet à des applications tournant sur des machines distantes de communiquer. Le problème consiste à identifier ces applications. En effet, suivant la machine et son système d'exploitation, l'application pourra être un programme, une tâche, un processus... De plus, la dénomination de l'application peut varier d'un système à un autre, c'est la raison pour laquelle un système de numéro a été mis en place afin de pouvoir associer un type d'application à un type de données, ces identifiants sont appelés ports.

La couche transport contient deux protocoles permettant à deux applications d'échanger des données indépendamment du type de réseau emprunté (c'est-à-dire indépendamment des couches inférieures...), il s'agit des protocoles suivants :

- TCP, un protocole orienté connexion qui assure le contrôle des erreurs
- UDP, un protocole non orienté connexion dont le contrôle d'erreur est archaïque

- Couche Application : elle englobe les applications standard du réseau (Telnet, SMTP, FTP, ...)

La couche application est la couche située au sommet des couches de protocoles TCP/IP. Celle-ci contient les applications réseaux permettant de communiquer grâce aux couches inférieures. Les logiciels de cette couche communiquent donc grâce à un des deux protocoles de la couche inférieure (la couche transport) c'est-à-dire TCP ou UDP.

Les applications de cette couche sont de différents types, mais la plupart sont des services réseau, c'est-à-dire des applications fournies à l'utilisateur pour assurer l'interface avec le système d'exploitation. On peut les classer selon les services qu'ils rendent :

- Les services de gestion (transfert) de fichier et d'impression
- Les services de connexion au réseau
- Les services de connexion à distance
- Les utilitaires Internet divers

A chaque niveau ou couche, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches :

- Le paquet de données est appelé message au niveau de la couche Application
- Le message est ensuite encapsulé sous forme de segment dans la couche Transport
- Le segment une fois encapsulé dans la couche Internet prend le nom de datagramme
- Enfin, on parle de trame au niveau de la couche Accès réseau.

**TCU -** Transmission Control Unit - Sous-ensemble d'un frontal de communication assurant la gestion physique des lignes. En français UCT, Unité de contrôle des Transmissions.

**TD/CDMA -** Time Division / CDMA - Mode d'accès radio exploitant des bandes de fréquences de 5 MHz. Combine les modes d'accès radio TDMA et TDD. Exploite une seule porteuse (fréquence) partagée dans le temps pour l'émission et la réception. Un des modes d'accès radio de l'UMTS. En théorie débits supérieurs au WCDMA.

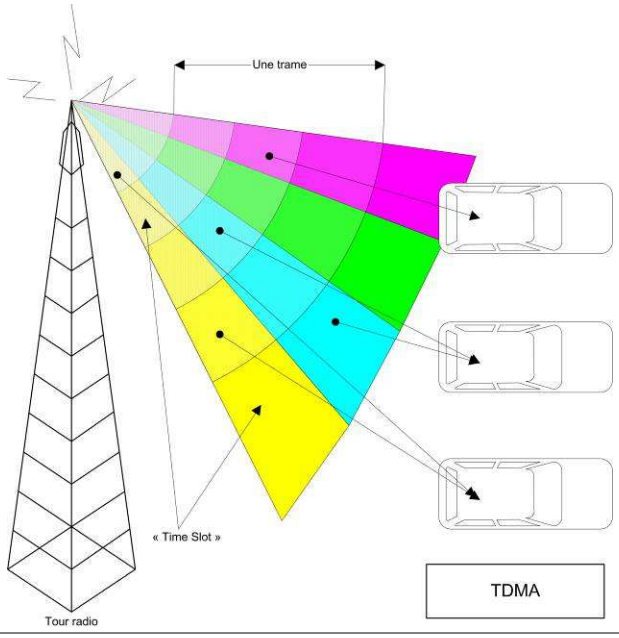
**T-DAB -** Terrestrial-Digital Audio Broadcasting

**TDCAM -** Réseau de transmissions de données du Crédit Agricole.

**TDF -** Télédiffusion De France - Société responsable des diffusions de programmes radio et télévision en France.

**TDM -** Time Division Multiplexing - Multiplexage temporel.

**TDMA -** Time Division Multiple Access - Technique de partage en temps divisant les porteuses en intervalles. (mode d'accès multiple par répartition temporelle) - Voir UMTS et AMRT




**T-DMB -** Terrestrial - Digital Multimédia Broadcasting - Protocole de diffusion de télévision par voie terrestre issu de la technologie Eureka 147 (le DAB - Digital Audio Broadcasting). Ce protocole existe en version terrestre (T-DMB et satellite (S-DMB). Le T-DMB déployé en Corée est inadapté à la réception mobile. Les flux sont encodés en MPEG4.

**TD-SCDMA -** Time Synchronous Code Division Multiple Access - Un des standard de la 3G (avec WCDMA - statndard retenu par l'Europe & CDMA 2000 EV-DO retenu par les nord américains). Ce standard a été retenu par la Chine pour les réseaux mobiles de 3eme génération.

**Téléalarme -** Service permettant, par l'addition d'un équipement particulier à un poste téléphonique, de lancer, par une manœuvre très simple, un appel de détresse vers un centre de secours.

**Téléassistance -** Service d'assistance ou éventuellement de dépannage, accessible à distance par un moyen de télécommunication.

**Téléchargement -** Opération consistant à transporter sur des lignes de télécommunications un logiciel "exécutable" sur l'ordinateur du destinataire. L'expression s'emploie dans de nombreux contextes -il peut s'agir de lancer des programmes sur une station de travail qui n'en dispose pas au démarrage (cette technique est notamment utilisée pour des raisons de sécurité sur des stations de réseaux locaux sans disque; il peut s'agir de mettre à jour l'environnement d'une station avec la nouvelle version d'un logiciel; il peut s'agir enfin tout simplement d'acquérir un logiciel. Aux Etats-Unis notamment, et en France sur le réseau vidéotex Télétel, des logiciels sont achetés par ce moyen.

**Télécom 1&2 -** Nom des satellites de télécommunications français lancés à partir de 1984. Ils assurent des missions multiples : fourniture de circuits de téléphonie vers certains territoires d'outre-mer; liaisons téléphoniques et numériques pour l'armée; liaisons numériques à hauts débits (2 Mbps) pour le service Transdyn. Cette dernière mission ne touche cependant qu'un petit nombre d'utilisateurs et le système de satellites Télécom 1 est surtout rentabilisé par le transport de programmes télévision ou d'émissions de radio. Une nouvelle génération a été mise en place sous le nom de Télécom 2. Désormais tous lancés, les derniers satellites du programme Télécom sont progressivement entrés en service courant 1997.

**Télécommunication -** Toute transmission, émission ou réception de signes, de signaux, d'images, de sons ou de renseignements de toute nature par fil, optique, radioélectricité ou autres systèmes électromagnétiques.

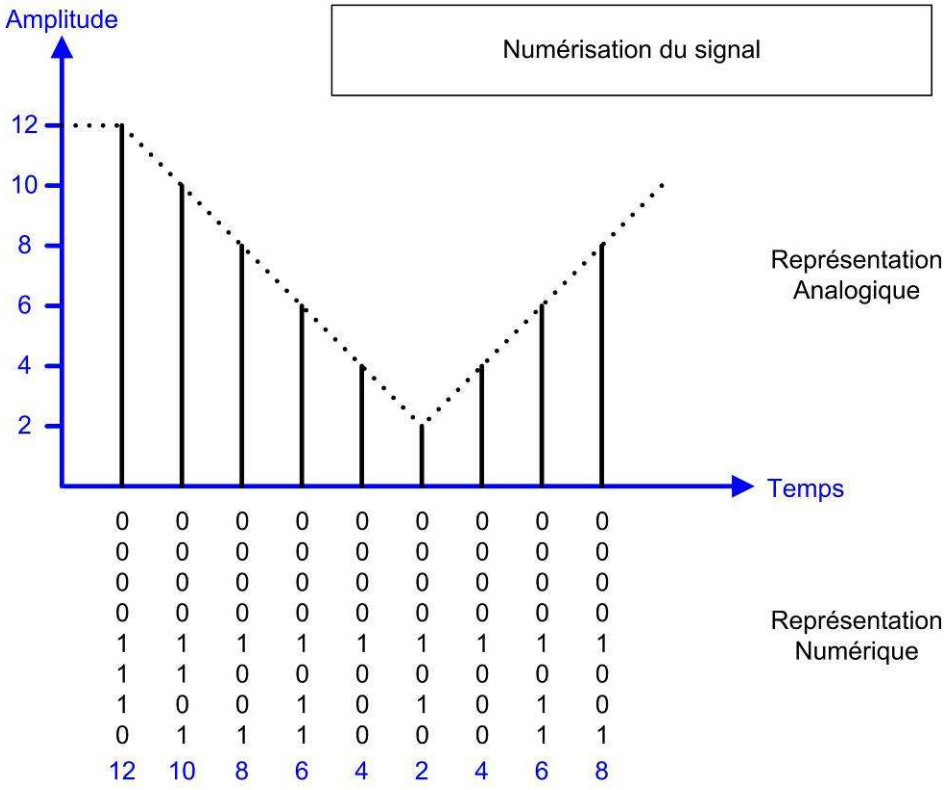
**Télécommunications -** Ensemble des techniques de transmission à distance, quel qu'en soit le support (définition officielle de l'UIT, Union internationale des télécommunications). C'est la transmission d'informations multimédia d'un point à un autre en utilisant au moins un support de transmission le plus rapidement possible le plus sûrement possible et au moindre coût.

**Télécommunications analogiques -** On a d'abord cherché à transporter le signal tel qu'il est émis, c'est à dire dans le cas de la téléphonie en analogique. Le téléphone, la radio, la télévision continuent à utiliser majoritairement, dans le monde, des supports de transmission analogiques, qu'il s'agisse de fils de cuivre ou de l'atmosphère pour les transmissions dites hertziennes. Les seules transformations que l'on fait subir au signal sont des transformations analogiques: amplification du signal pour le régénérer car il a tendance à s'affaiblir avec l'augmentation des distances et surtout conversion analogique, comme celle qui transforme dans un microphone les vibrations d'une membrane, au contact des vibrations sonores de l'air, en oscillations d'un signal électrique (*ou l'inverse dans une enceinte acoustique*). Dans le monde des télécommunications analogiques, on cherche donc surtout à transporter sans altération le signal émis par l'émetteur. Ceci n'est pas simple car les supports de transmission ne laissent pas passer toutes les fréquences provoquant ainsi un appauvrissement du signal (ex: différence entre une voix au téléphone et la même voix en direct). De plus l'électronique analogique est sensible à des bruits parasites et génère elle-même ses bruits de fond.

**Télécommunications numériques -** Pour supprimer les inconvénients des télécommunications analogiques, on a imaginé d'avoir recours à la transmission numérique. Cela signifie qu'au lieu de transporter une variation (*ou modulation*) des ondes qui reproduit la forme très complexe du signal émis, on transporte une "représentation" de ce signal sous une forme beaucoup plus simple.

La représentation du signal d'origine sera obtenue par une conversion analogique-numérique: ce dispositif électronique, aujourd'hui contenu dans un composant, prélève à intervalles réguliers des échantillons du signal, mesure leur amplitude en la comparant à des étalons et attribue une valeur numérique à chaque échantillon. C'est ce train d'informations, constitué des valeurs des différents échantillons représentant les valeurs successives du signal d'origine, qui sera transporté. Pour peu que l'on ait prélever suffisamment d'échantillons avec suffisamment de précision, il sera possible à l'autre extrémité, par une opération inverse dans un convertisseur numérique-analogique, de reconstituer le signal d'origine. Les avantages d'une telle solution sont considérables : puisque la transmission est faite de quelques valeurs discontinues, elle se présente beaucoup plus simplement que le signal qu'elle représente. De ce fait une transmission numérique est beaucoup moins sensible au bruit et aux légères variations dus aux imperfections de la transmission.

En conséquence, la transmission numérique pourra se contenter de lignes de moins bonne qualité, ou plutôt à qualité égale on pourra transmettre plus de signaux sur la même ligne.




**Télécompensation -** Opération de mise à jour des virements et prélèvements bancaires entre établissements financiers, effectuée à travers un réseau. En France, le réseau SIT (Système de télécompensation interbancaire) assure cette fonction.

**Téléconférence -** Réunion ou conférence à distance grâce à un système de radio ou de télévision. Conférence dans laquelle les interlocuteurs sont répartis dans deux (ou plus de deux) lieux reliés entre eux par des moyens de télécommunications.

**Télécopie -** Service de télécommunication permettant la reproduction à distance d'un document graphique sous la forme d'un document graphique géométriquement semblable à l'original.
Le télécopieur transforme un document (texte écrit ou dessin) en signaux numériques transmis sur le réseau téléphonique jusqu'au terminal appelé qui recompose le message initial.

**Télédisc -** Projet de lancement de 288 satellites LEO (à 700km d'altitude) initié par MICROSOFT et devant offrir, dès 2002, des services interactifs à haut débit.

**Téléécriture -** Système, le plus souvent associé à l'audioconférence, permettant la transmission d'informations graphiques, au fur et à mesure de leur tracé manuscrit, et la reproduction de ce tracé sur un écran ou un autre support.

**Téléfax -** Service public de télécopie de France Télécom.

**Téléinformatique -** Association de techniques de télécommunication et de l'informatique en vue de traitement d'informations à distance.

**Télémarketing -** Marketing téléphonique. Utilisation du téléphone comme moyen de marketing (études, détection de clientèle, mise à jour de fichiers...) ou plus simplement de vente. On devrait dans ce dernier cas parler de télévente, mais les deux expressions tendent à se confondre.

**Télématique -** Expression inventée dans les années 70 par Simon Nora et Alain Minc pour désigner le mariage des techniques de télécommunications et de l'informatique. Dans l'esprit de ses auteurs, ce néologisme englobait la téléinformatique, mais la dépassait largement en s'ouvrant vers le grand public. Aujourd'hui, on tend à retenir surtout cette acception grand public du terme, en la réduisant parfois aux techniques de vidéotex.

Dans le domaine des télécommunications : Ensemble des services, autres que les services télégraphique et téléphonique usuels, qui peuvent être obtenus par les usagers d'un réseau de télécommunication. Note : Les services qui mettent généralement en œuvre des techniques de téléinformatique permettent d'envoyer ou de recevoir des informations publiques ou privées, ou d'effectuer certaines opérations telles que consultation de fichier, réservation, opérations commerciales ou bancaires.

Dans le domaine de l'informatique : Ensemble des services de nature ou d'origine informatique pouvant être fournis à travers un réseau de télécommunication.

**Télémessage -** Message numérique émis sur un réseau de radiocommunication avec les mobiles. Un télémessage peut être un minimessage, limité à un nombre déterminé de caractères alphanumériques, ou un message multimédia.

**Télépac -** Nom des réseaux à commutation de paquets de la Suisse et du Portugal.

**Téléphone mobile -** Expression utilisée indifféremment avec téléphone cellulaire ou portable. A l'origine, le téléphone mobile faisait référence à un téléphone de voiture qui utilisait la batterie du véhicule et possédait une antenne extérieure. Les téléphones mobiles se distinguaient alors des téléphones portatifs, portables et sans fil.

**Téléphone portable -** Téléphone monobloc tenant dans la main qui est alimenté par batterie intégrée et peut être utilisé sans batterie ni antenne extérieures. Voir également téléphone mobile, téléphone portatif.

**Téléphone portatif -** Téléphone mobile pouvant être retiré d'une automobile et utilisé de façon autonome avec un bloc-piles, parce qu'il n'est pas alimenté par la batterie du véhicule. Appelé également téléphone "transportable" en référence au bloc d'alimentation qui doit accompagner l'appareil et pour le différencier des petits téléphones cellulaires légers qui tiennent dans le creux de la main et qui sont les plus fréquents aujourd'hui. Voir également Téléphone mobile.

**Téléphonie sur IP -** Service de communication vocale utilisant le protocole de télécommunications créé pour l'Internet appelé "IP" pour Internet Protocol.

**Téléphonie vocale -** La directive ONP "téléphonie vocale" du 26 février 1998 définit la téléphonie vocale comme "un service mis à la disposition du public pour l'exploitation commerciale du transport direct de la voix en temps réel à travers le ou les réseau(x) public(s) commuté(s), et permettant à tout utilisateur d'utiliser l'équipement connecté à un point de terminaison en position fixe du réseau pour communiquer avec un autre utilisateur d'équipement connecté à un autre point de terminaison." Le terme "téléphonie vocale" est ainsi utilisé par les directives communautaires pour désigner le service téléphonique classique.

**Télépoint -** Service mobile terrestre téléphonique dans lequel des stations de base, publiques ou privées, servent d'intermédiaire à des téléphones portatifs pour communiquer entre eux ou avec le réseau téléphonique commuté. Pointel désigne le service télépoint de France Télécom.

**Téléport -** A l'origine, ce mot désignait des antennes de réception collectives en radiocommunication. Aujourd'hui, le sens du mot s'est élargi pour désigner une installation collective regroupant en un seul point une large gamme de moyens d'émission et de réception, notamment par satellite, d'images de voix ou de données. Il est surtout employé dans un contexte d'aménagement du territoire, avec l'espoir que des ressources de télécommunications concentrées pourraient optimiser les dépenses et surtout attirer des sociétés à la périphérie de ces installations.

**Téléservice -** Service de télécommunication offert à l'interface usager-terminal et correspondant aux couches 1 à 7 du modèle OSI. Le type de terminal et ses protocoles sont spécifiés. La télécopie groupe 4, la téléphonie à 3 kHz ou à 7Khz sont des exemples de téléservices.

**Télétel -** Service de consultation de banques de données offert par France Télécom et associé au terminal Minitel. Nom commercial du réseau de vidéotex français.

**Teletex -** Evolution du telex normalisée par le CCITT, l'améliorant avec la prise en compte des caractères accentués, une vitesse supérieure, des transmissions bidirectionnelles, des possibilités de stockage et de traitement de texte, ainsi que la possibilité d'échanger des images.

**Telnet -** Système de terminal virtuel qui permet l'accès distant aux applications.

**Temporel -** Qualifie un système de multiplexage ou de commutation dans lequel des portions de messages de plusieurs voies sont transmises successivement sur un même canal.

**Temps de communication -** Le temps enregistré par les opérateurs pour établir leur facturation. L'utilisation tient compte des appels passés et reçus (notamment pour les mobiles utilisés à l'extérieur de la zone de couverture de l'opérateur) et des autres transmissions mobiles du type fax, e-mail ou fichiers de données.

**Temps de latence -** Il s'agit du délai qui existe entre le moment ou une trame arrive dans un commutateur et le moment où elle en sort depuis le port de destination.

**Temps de montée -** Audio - Plus il est bref, plus il exprime la faculté de transmettre des informations musicales complexes dans leur totalité, surtout dans les fréquences élevées.

**Temps de réponse -** Délai de réaction d'un système à un événement.

**Temps différé -** batch ou "par lots" - Fonctionnement d'un système où les tâches à accomplir ne sont pas traitées au fur et à mesure de leur arrivée, mais d'abord regroupées dans une file d'attente avant d'être exécutées en une seule séquence continue. S'oppose à "temps réel".

**Temps partagé - Time sharing -** Fonctionnement d'un système dans lequel une portion seulement du temps total est affectée à chaque utilisateur selon un ordre bien déterminé (tournant ou en fonction d'un plan de priorité).

**Temps partagé -** Time Sharing - Fonctionnement d'un système dans lequel une portion seulement du temps total est affectée à chaque utilisateur selon un ordre bien déterminé (tournant ou en fonction d'un plan de priorité).

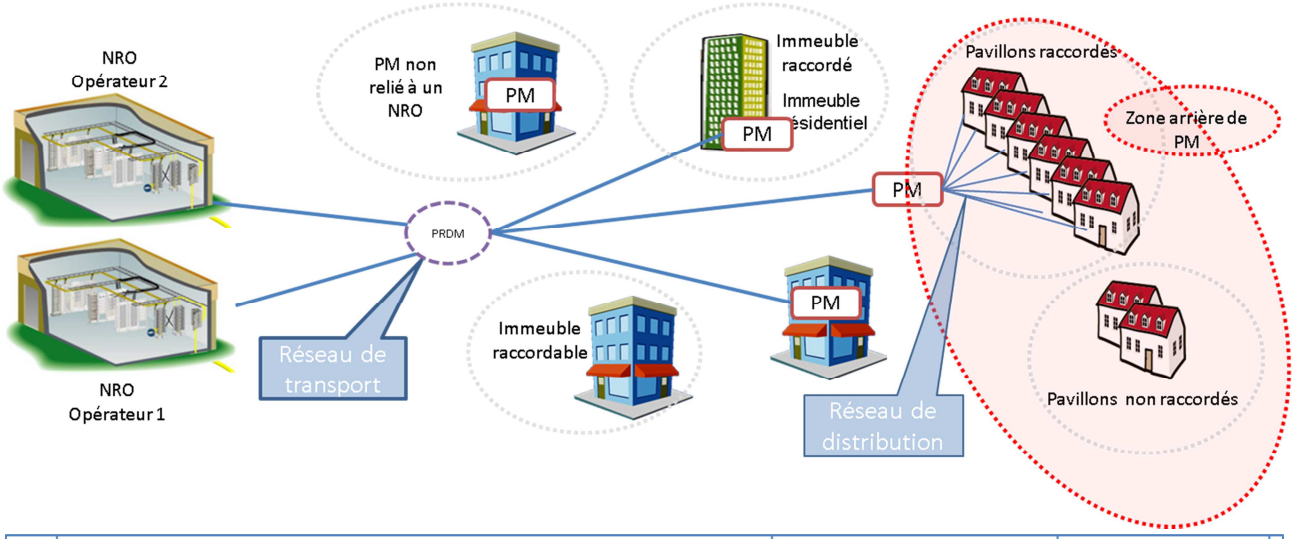
**Temps réel -** Fonctionnement d'un système dans lequel les différentes tâches sont traitées immédiatement au fur et à mesure de leur apparition. L'expression est employée dans la gestion pour désigner les systèmes "transactionnels en ligne" ou dans le monde industriel, par exemple, dans le contrôle de procédés.

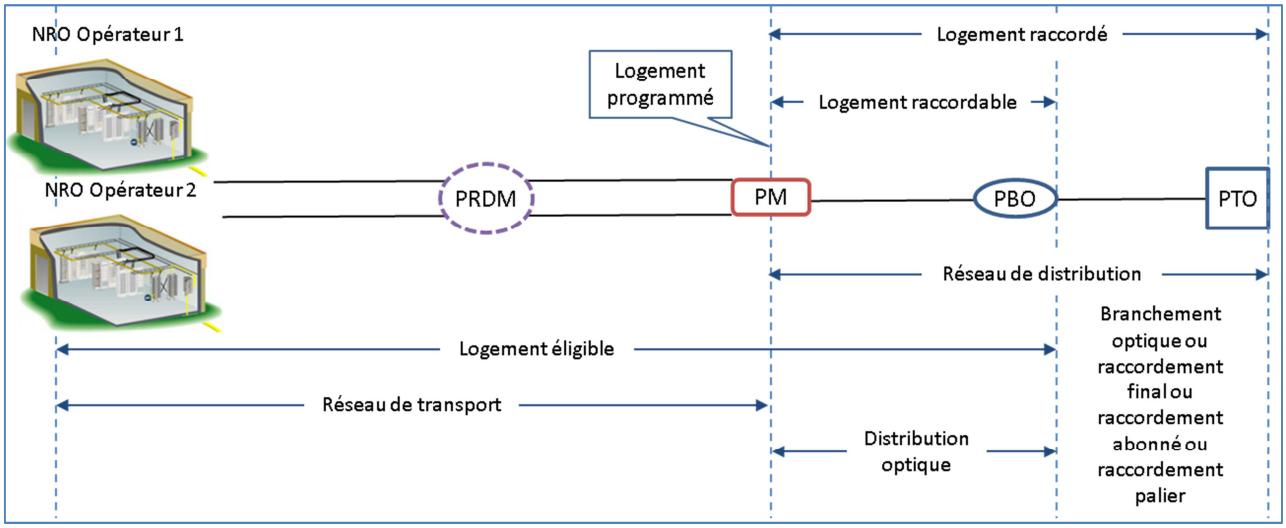
**TenNet ou 10Net -** Réseau local mis au point par Fox Research utilisant la méthode d'Accès CSMA/CD sur paire torsadée.

**Terminal -** Equipement périphérique d'un système informatique fournissant un support directement assimilable par l'utilisateur (écran, imprimante...). Appareil permettant l'accès à distance à un système informatique.

**Terminal Propriétaire -** Terminal défini selon la spécification particulière déterminée par l'industriel qui l'a développé.

**Terminologie FTTH -** Les schémas et dessins suivants représentent la terminologie FTTH tels que définit par l'ARCEP dans le cadre du déploiement des réseaux très hauts débnits en France.




**TETRA -** Terrestrial Trunked Radio Access - Réseau 3RD européen. Norme de radiocommunication mobile professionnelle (voir PMR) définie par l'ETSI.

TETRA un standard numérique conçu pour le marché privé des communications radios mobiles. Alors que le GSM est aujourd'hui le standard sur le marché des télécommunication personnel, TETRA offre une large palette de services répondant aux besoins spécifiques des professionnels, cette norme gère au mieux le spectre radio en allouant les ressources à la demande et offre de nouveaux services.

Pour les groupes d'utilisateurs professionnels (forces de police, service d.urgence, transports etc..) TETRA offre un moyen sécurisé et efficace de communication mobile et ceci de manière portable.

TETRA fut développé, depuis le début, comme un standard numérique de radiocommunication professionnel (Private Mobile Radio PMR) en collaboration avec l'ETSI. Le besoin de mettre en place un standard était de plus en plus urgent. Les premiers systèmes de radiocommunication professionnels étaient propriétaires.

Les avantages d'un tel standard sont multiples, agrandir le marché en permettant des économies d'échelle, permettre aux utilisateurs d'utiliser différents fournisseurs… Cela permet aussi d'augmenter la concurrence entre les fabricants.

- Les systèmes analogiques :

Les premiers systèmes de radiocommunication professionnel sont analogiques et propriétaires. Cependant un système a réussi à s'imposer et est supporté par plusieurs constructeurs. Il s'agit de LTR (Logic Trunked Radio) développé par E F Johnson. Un autre standard analogique est le MPT1327 (Ministry of Post and Telecommunications) qui a été développé en angletterre dans la fin des années 1980 et est aujourd'hui aussi utilisé dans le monde. Ce système est un peu plus complexe et coûteux qu'un simple système analogique, il est assez efficace en terme d'utilisation de bande passante et offre quelques possibilité de transmission de données. Il permet aussi comme tous les PMR des services de voix tel que des groupes d'appels ou encore un système de priorité.

- Les systèmes numériques :

Les premiers systèmes conformes à la norme TETRA ont été implantés en 1997. Durant les années 1980 de nombreux autres systèmes numériques se sont développés.

- EDACS (Enhanced Digital Access Communication System) est un système propriétaire développé par Ericsson. Les premiers systèmes de ce type ont été opérationnels vers la fin des années 80. Surtout utilisés aux Etats Unis par les militaires et les services de secours, ce système est l'un des premiers à pouvoir transmettre des données.
- Geotek-FHMA utilise une technique de saut de fréquence basé sur FDMA. Il existe une douzaine de réseaux de ce type dans le monde.
- APCO25 (Association of Puiblic-safety Communications Officials), Il s'agit d'un autre standard basé sur la technologie FDMA, le premier système de ce type se nomme "ASTRA "et à été lancé en 1996.
- IDEN est un système propriétaire de Motorola, il offre un fort niveau de modulation (16-QAM) et permet une très bonne efficacité du spectre radio, il offre 6 canaux de communications, il existe beaucoup de système de ce type dans le monde mais aucun en Europe.
- TETRAPOL est un système basé sur la technologie FDMA, développé par Matra, ce système offre une solution moins cher que les systèmes basé sur le "trunking "comme TETRA. Le principal avantage de TETRAPOL était d'être disponible, en effet il n'existait aucun système opérationnel basé sur TETRA. Ainsi, TETRAPOL fut déployé dans plus de 15 pays et est utilisé dans les secours. En Europe TETRAPOL se heurte à la norme TETRA qui est reconnu comme le standard approuvé par l'ETSI.

Le système TETRA représenté dans le modèle OSI se place essentiellement dans les couches 1 à 3. La particularité du système TETRA réside dans la définition des interfaces plutôt que dans l'implémentation des systèmes., cela à pour but de garantir une interopérabilité entre les différents réseaux TETRA même ci ceux ci sont constitués de constructeurs différents.

- Les principaux paramètres de TETRA :

Espacement de porteuse = 25 kHz

Modulation = π/4-DQPSK

Débit de la porteuse = 36 kb/s

Débit du codeur Voix = ACELP (4.56 kb/s net, 7.2 kb/s gross)

Méthode d'accès = TDMA avec 4 time slots/porteuse

Débit utilisateur = 7.2 kb/s par time slot

Debit maximum = 28.8 kb/s

Débit (avec protection d"erreurs) = <19.2 kb/s

**TETRAPOL -** Norme propriétaire de radiocommunication adoptée par les polices européennes. Voir TETRA.

**TFTP -** Trivial File Transfer Protocol - Dérivé de FTP très simplifié, sert, pour sa part, à transférer les fichiers de configuration d'une machine sans disque en s'appuyant sur le protocole UDP (User Datagram Protocol), équivalent à TCP mais qui, lui, fonctionne en mode non connecté, c'est-à dire sans les mécanismes de contrôle de flux, de reprise sur erreurs... Malgré ce manque de fiabilité, il est souvent utilisé aujourd'hui en lieu et place de FTP pour sa simplicité et sa relative efficacité.

**Théorie de la relativité restreinte -** Formulée par Albert Einstein en 1905, cette théorie décrit les relations entre entre notions d'espace et de temps, et par là même, le cadre dans lequel s'inscrivent toutes les autres relations. La théorie décrit l'existence d'une vitesse indépassable atteinte en particulier par la lumière. La formule E=MC2 relie la vitesse limite avec lénergie et la masse. *En 1905…*

**TIA -** Telecommunication Industry Association.

**TIB -** Teknekron Information Bus - Bus logiciel destiné à transmettre des messages et cela, indépendamment de l'architecture sur laquelle s'exécutent les programmes ou du réseau sur lequel circulent les données. Ces messages sont identifiés par des titres.

Le Bus logiciel a été développé par la société TIBCO qui s'est orienté, dès sa création, dans la technologie Middleware en développant le TIB : un bus applicatif ayant pour objectif de simplifier et d'uniformiser les mécanismes de liaisons. Destiné aux salles de marché, le TIB répond à une forte demande de temps réel de la part des places financières.

Depuis la version 5 de TIB/RendezVous, le bus supporte le multicast. Si l'utilisation du multicast apporte un gain de performance significatif, il reste toutefois peut développé sur le TIB. La technologie TIB repose sur le modèle Publish/Subscribe : les données sont envoyées sous forme de messages eux-même classés par sujet sur le TIB. Ces messages peuvent êtres consultés en s'abonnant à un sujet spécifique. Les producteurs d'information ne savent pas qui consulte leurs messages et les consommateurs, en s'abonnant à un sujet, reçoivent des informations sans savoir de quel publicateur elles proviennent.

En comparaison avec la méthode classique Request/Reply (également supporté par le TIB) qui consiste à émettre une requête sur le bus pour obtenir l'information voulue. Le modèle Publish/Subscribe présente l'avantage de consommer moins de bande passante et moins de ressources systèmes.

**Tiers de confiance -** Organisme tiers qui délivre les certificats et les clés publiques et certifie qu'ils appartiennent bien à la bonne personne. La sécurité de l'utilisation du cryptage asymétrique repose sur l'identification de la clé publique du destinataire, et donc sur la présence de tiers de confiance.

**Time Out -** Délai maximal admis au bout duquel un équipement n'ayant pu accomplir sa tâche fera l'objet d'un signal déterminé (message d'erreur, mise hors circuit...).

**Titane -** Le titane se distingue par des caractéristiques comme la légèreté, la robustesse, la résistance à la corrosion et aux chocs, un transfert de chaleur élevé, la biocompatibilité et une esthétique raffinée. Le potentiel offert par le titane en matière de haute technologie et de design innovant a été révélé par son utilisation dans la construction d'avions, de satellites, d'ordinateurs, de téléphones et de bijoux.

**TKIP -** Temporal Key Integrity Protocol - Protocole qui consiste à fournir de nouvelles clés pour chaque paquet de 10 Ko de données transmis. Proposé par la Wi-Fi Alliance pour remédier aux failles de WEP, il évite la répétition des vecteurs d'initialisation et permet le remplacement automatique des clefs de chiffrement.

**TMA - Tierce Maintenance Applicative -** Service consistant pour une SSII à prendre en charge la responsabilité complète de la gestion d'une ou plusieurs applications du système d'information de son client.

**TMN -** Telecommunications Management Network - Réseau de gestion des télécommunications, normalisé par l'UIT-T, recouvrant cinq domaines fonctionnels : configurations, anomalies (alarmes, pannes, tests), performances (qualité, trafic), sécurité et facturation.

**TN3270 -** Commande qui permet d'émuler des terminaux IBM 3270 dans un mode client-serveur.
La commande est définie dans les standards suivants :

- La RFC 1576 qui décrit le fonctionnement général de TN3270
- La RFC 1041 qui décrit les régimes d'option à implémenter dans TN3270
- La RFC 1647 qui présente les améliorations de TN3270 dans un nouveau standard : TN3270E

**TNR -** Terminaison Numérique de Réseau - Coffret mettant en contact la ligne interne de l'abonné et le réseau public dans le Réseau numérique à intégration de services (Rnis) Numéris de France Télécom.

**TNT -** Télévision Numérique Terrestre - Norme de diffusion de télévision via les ondes hertziennes qui utilise un codage numérique pour le transport. Ce codage permet de multiplexer les données, ce qui, conjugué à de la compression, offre une multiplication des chaines tout en utilisant la même bande passante que la télévision analogique. La TNT est moins sensible aux interférences, les décodeurs pouvant offrir une extrapolation des signaux au besoin. Par contre, la TNT ne modifie aucunement la qualité de l'image ; il ne s'agit pas de Haute Définition.


**TOIP -** Téléphonie Over IP - Téléphonie sur IP - Solution de communication qui s'appuie sur un réseau en mode paquets pour acheminer des communications téléphoniques. Par opposition aux systèmes traditionnels centralisés en mode circuit, la téléphonie sur IP reposent sur des services téléphoniques fournis par un ensemble de serveurs qui communiquent entre eux par des standards. Outre une meilleure intégration au Système d'Information d'une entreprise (SI), ce système autorise la mise en œuvre de nouvelles applications dont :

- L'intégration LDAP qui devient commun avec le SI et simplifie au passage les opérations d'exploitation,
- La messagerie unifiée qui est une évolution de la messagerie vocale. Elle permet de consulter les messages depuis n'importe quel média, quelle qu'en soit la localisation géographique,
- L'amélioration de l'efficacité personnelle par le développement d'applications utilisant pleinement les interactions possibles via le protocole TAPI.

Souvent propriétaire, la signalisation utilisée en TOIP n'a pas favorisé l'interopérabilité entre les différents fournisseurs. Le protocole de signalisation permettant l'interopérabilité est SIP.

Les offres triple play des différents FAI incluent une solution de TOIP, sans que les abonnés n'en mesurent les conséquences directes et indirectes, et/ou techniques. Le facteur économique des offres et la facilité d'utilisation passant en premier.

**TOIP Déploiement -** La technologie TOIP demande des compétences particulières et une gestion de projet bien plus affutée que la téléphonie traditionnelle.

Un projet de déploiement de TOIP ne peut se mener aussi "simplement" que le déploiement d'un PABX classique. Une tel projet requiert la mise en œuvre simultanée de compétences multiples et variées qui vont des spécialistes de la téléphonies et spécialistes des réseaux IP en passant par un programme de formation de tous et une gestion du changement solide et méthodologique, le tout sous couvert d'une rigueur absolue apportée par la gestion de projet. Souvent, le projet est abordé et conduit comme un vaste projet

informatique.

La démarche idéale se structure en 6 phases :

1. Définition - Définir ses besoins - Etudes d'opportunités couvrant l'existant, les enjeux financiers, l'accompagnement, le type d'exploitation.
2. Conception - Conception des besoins - Etude de faisabilité couvrant les performances, la sécurité, l'interopérabilité…
3. Intégrer - Soigner son intégration - Intégration des spécifications couvrant les aspects maquette, développement, planification…
4. Déployer - Réussir son déploiement en tenant compte de la recette, des formations, de l'accompagnement au changement.
5. Exploiter - Opérer - Gérer les incidents et les problèmes, les changements, les nouvelles versions, les documentations d'exploitation…
6. Optimiser - Piloter - Mettre en place les outils de pilotage, de reporting, les tableaux de bord et les SLA associés.

1 - Définition :

L'objectif de cette étape est de définir un cahier des charges. Il est essentiel de bien définir les besoins et de réfléchir à la cible visée en terme de fonctionnalités. Une implication des utilisateurs est recommandée dès le début du projet pour obtenir une cible précise et inventoriant les besoins des utlisateurs précisément.

L'analyse de l'existant en téléphonie se doit d'être aussi exhaustive que possible, elle sera complétée d'un audit de câblage (performances et disponibilités d'espaces libres, capacité d'extension), d'une revue des contrats de services des différents opérateurs pour les liens externes en voie et data, d'un revue (bilan) des équipements actifs du réseau (capacité de traitement, gestion de la QOS, alimention des équipements en PoE…)

Les impacts humains et financiers doivent d'hors et déjà être évoqués parce qu'ils sont structurants dans la mise en œuvre des plans de formation adaptés à la convergence des compétences, et aussi parce que ces impacts sont à prendre en compte dans le choix entre hébergement ou externalisation.

On peut tenter le calcul du ROI pendant cette phase, mais il sera à ajuster plus précisément après les appels d'offres.

2 - Conception :

Cette étape est celle de la conception de la solution de TOIP. Elle comprend au moins l'étude de faisabilité, l'analyse des performances (dont audit du réseau local), la prise en compte des aspects de sécurité et le rencensement des besoins d'interropérabilité. C'est aussi lors de cette phase que devront être étudiés et retenus les protocoles d'interconnexion de la solution envisagée, et que seront définis les critères de sécurité. La capacité d'interropérabilité permet d'assurer un bon fonctionnement de la solution de TOIP sur l'infrastructure en place.

3 - Intégrer (en environnement de tests) :

Cette étape marque le début du "marquage à la culotte" (suivi étroit) par le chef de projet du projet de déploiement de la solution. C'est une phase d'évaluation. C'est aussi le début de la phase opérationnelle, avec la réalisation des maquettes, le développement des interfaces (annuaires, applications métiers,…). C'est dans cette phase que vont être testées en situation réelle les différentes solutions. N'hésitez pas pendant cette phase à bien évaluer le savoir-faire de l'intégrateur et/ou des différents intervenants.

4 - Déployer :

Cette étape est plus ou moins complexe selon la taille et l'environnement du projet, le nombre de site à installer influe directement sur la complexité de l'étape. C'est lors de cette phase que l'on aborde les aspects" formation des utilisateurs", "formation des administrateurs", la conduite du changement…

La migration de l'ancien système vers la TOIP doit cependant faire l'objet d'une attention toute particulière, de part sa plannification tout d'abord, mais aussi sur l'accompagnement des utilisateurs en mettant en œuvre un dispositif humain proche des utilisateurs.

5 - Exploiter :

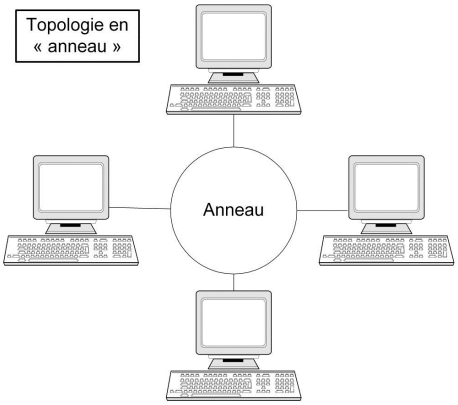
C'est l'étape à la fois la plus simple et la plus complexe. La plus simple pour qui l'aborde comme un projet d'exploitation informatique, la plus complexe pour qui pense que la téléphonie sur IP s'exploite comme un PABX traditionnel. La Téléphonie sur IP doit être comparée à des serveurs informatiques, et doit donc en conséquence être gérée comme tel. Les procédures doivent être définies pour la gestion des incidents, des problèmes, des sauvegardes, le suivi des changements, des correctifs, les tests de non régression…

6 - Optimiser :

Qu'elle soit ou non internalisée, une solution de TOIP doit être suivie au travers de compteurs judicieux. Le reporting d'utilisation permet d'assurer le retour sur investissement et de modéliser les optimations de traffic sur le réseau interne et sur les achats de communications téléphoniques.

Quand le projet est externalisé, c'est un des moyens de mesure le SLA du projet.

**Token Ring -** La norme ISO 8802.5 (IEEE 802.5) définit un réseau local ayant une topologie de type anneau. Chaque station est reliée à une station amont et une station aval par des supports unidirectionnels, exploités en bande de base, avec un protocole à jeton (trame vide). Ce processus est déterministe est permet un accès réseau équitable et prévisible. Il peut fonctionner à 4, 16, 32 ou 100 Mb/s. Les signaux sont régénérés par toute station active du réseau. Le réseau local à jeton utilise comme support de transmission des câbles à paires torsadées blindées (STP) ou non blindées (UTP), ainsi que la Fibre Optique pour accroître les distances.




Chaque station du réseau est connectée à l'anneau par une unité de raccordement (ou concentrateur) tels que l'IBM 8228 ou l'IBM 8230. Le nombre maximum de stations est limité à 260 postes pour un anneau. Les anneaux peuvent être interconnectés par des ponts sans limiter le nombre de stations.

Réseau développé par IBM :

- En 1981 : premier prototype
- En 1985 : ratification norme IEEE 802.5 à 4 Mbps
- En 1989 : ratification fonctionnement à 16 Mbps
- Les évolutions vers le haut débit
- En 1990 : apparition des réseaux Dedicated Token Ring (DTR) - Transmission full-duplex entre une station et un commutateur Token-Ring
- En 1998 : apparition des réseaux High Speed Token-Ring - Version à 100 Mbps des réseaux DTR

Couche Physique :

Support de communication entre stations et MAU ou entre MAU

- UTP : au plus 100 m si Cat. 3 et 225m si Cat. 5
- STP : au plus 400 m si Cat. 5
- Fibre : au plus 2000 m entre MAU

Connecteurs IBM (DIX / DB9 côté station et hermaphrodite côté MAU) puis RJ-45 (des deux côtés)

Mode de transmission : Code Manchester différentiel

- Bit à 0 : transition au début et au milieu du temps bit
- Bit à 1 : transition seulement au milieu du temps bit

Deux symboles de contrôle

- J : pas de transition pendant un temps bit
- K : une transition au début du temps bit

Principes de base :

- Une seule station à la fois peut émettre sur le support
- Pour émettre, une station doit posséder le jeton (Token)
- Pour éviter toute collision, il y a un seul jeton transmis de station en station
- Pour garantir un droit équitable à émettre, la possession du jeton est limitée dans le temps (peut permettre d'émettre une ou plusieurs trames).

Principes de la gestion de l'anneau :

Gestion centralisée avec deux types de station :

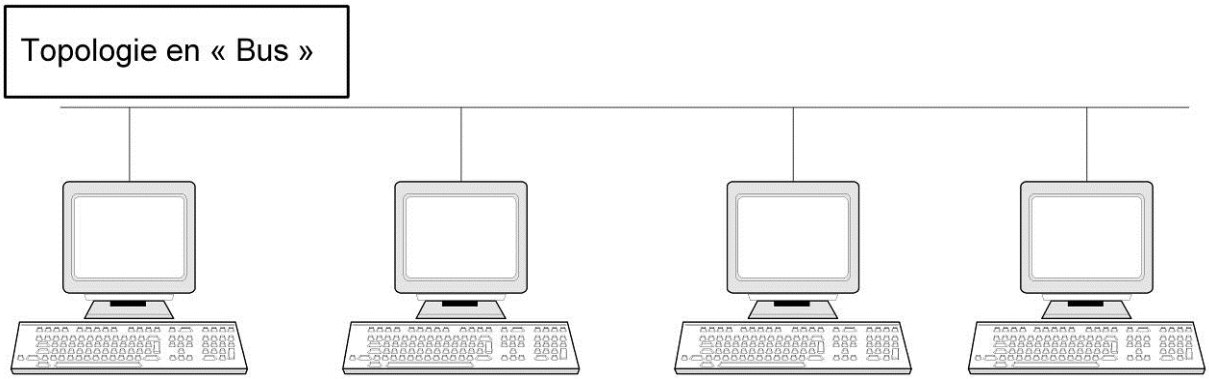
- Un moniteur actif qui contrôle l'intégrité de l'anneau (circulation de 1 jeton et un seul)
- Des moniteurs en veille (standby monitor) qui surveillent la présence du moniteur actif et sont capables de détecter une défaillance du moniteur actif et de prendre la relève

L'initialisation de l'anneau nécessite l'élection de la station qui sera le moniteur actif. La station élue sera la station active dont l'adresse MAC est la plus grande. Une trame "Claim-Token" circule de station en station en mémorisant l'adresse source la plus grande comme étant l'adresse du nouveau moniteur actif.

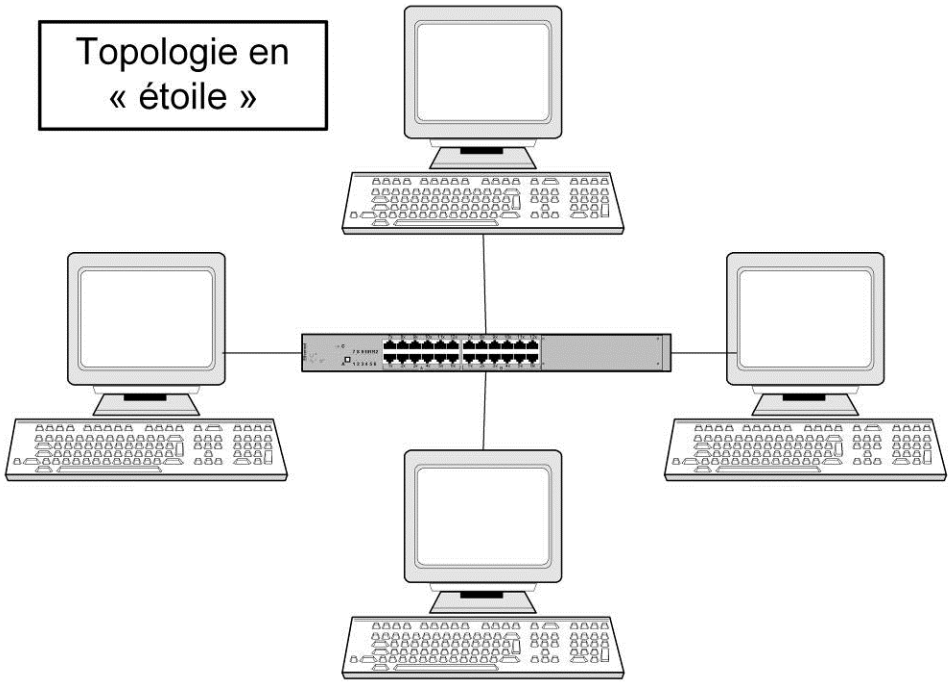
**TOP -** Technical Office Protocol - Ensemble de protocoles développés à l'origine par Boeing pour la bureautique des ingénieurs (CAO) et des responsables travaillant dans le domaine de la production industrielle. Destiné dans un premier temps à compléter les couches basses du réseau local industriel Map, Top s'en est peu à peu émancipé pour devenir le premier ensemble de protocoles normalisés complet conforme au modèle OSI d'interconnexion des systèmes ouverts en 7 couches. Il utilise en particulier le réseau local Ethernet, un système de messagerie X400 et un protocole de terminal dit "virtuel" donc indépendant du type de terminal réellement utilisé.

**Topologie de réseau -** Mode d'organisation d'un réseau dans l'espace. En réalité, ce mot est plus souvent à prendre dans son sens "logique" (organisation des connexions les unes par rapport aux autres) et non pas "géographique" (plan de câblage - Design du réseau)

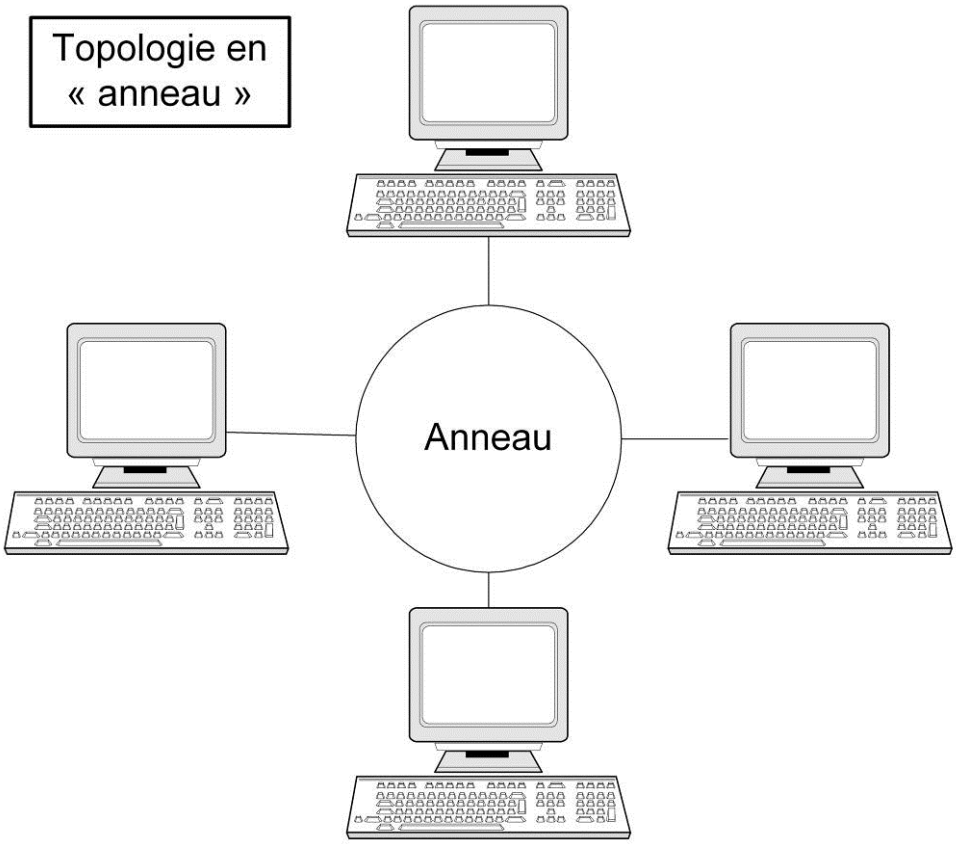
La topologie d'un réseau décrit comment sont reliés les différents nœuds d'un réseau. À l'origine, le réseau Ethernet n'utilisait qu'un câble coaxial sur lequel étaient reliées les différentes machines. Cette topologie de base constitue un bus. Dans ce cas de figure, lorsqu'une machine diffuse un message, toutes les autres le reçoivent. Il n'y a pas de hiérarchisation. Les problèmes d'accès qui s'ensuivent sont résolus par des algorithmes spécifiques. Indépendamment des problèmes de câblage, l'affaiblissement du signal constitue l'inconvénient majeur de la topologie en bus. Pour pallier cette difficulté, il faut régénérer périodiquement le signal, ce que réalisent les répéteurs posés sur le câble.



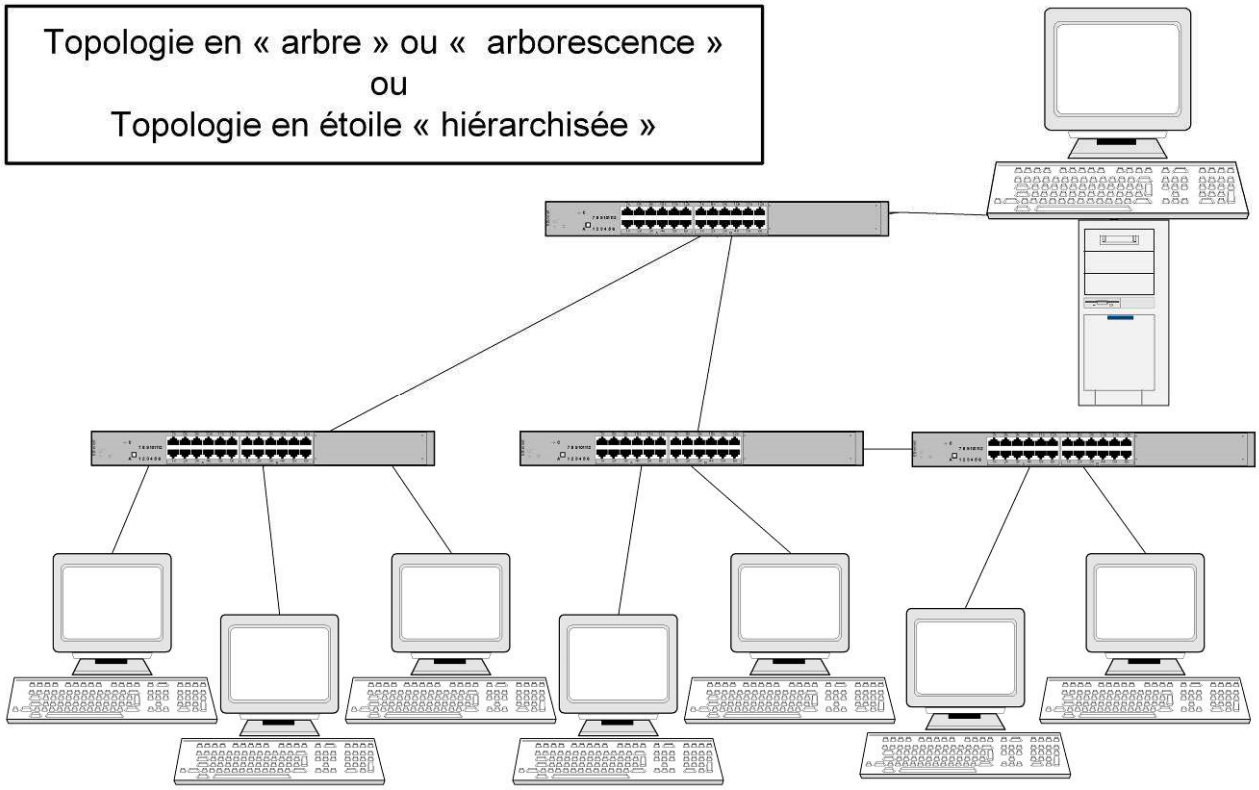

Dans une topologie en étoile, des liaisons point à point convergent vers un nœud central ou concentrateur. Tous les messages transitent par ce nœud qui, dans les réseaux locaux, est généralement désigné par le terme de "hub" ou concentrateur. S'inspirant des deux topologies - bus et étoile - celle dite en "arbre" est une variante de la configuration "bus" de base. L'arbre correspond à une hiérarchisation d'étoiles formant généralement des sous-bus. Le hub émule un bus et participe à la régénération du signal. L'exemple le plus connu de ce panachage entre étoile et bus est le réseau Ethernet sur paire torsadée.




Troisième possibilité: l'anneau à jeton, connu aussi sous l'appellation "token ring". Dans ce type de configuration, chaque nœud est connecté au suivant, le dernier bouclant sur le premier. Les messages transitent par toutes les machines. Chaque machine participant à la régénération du signal, l'anneau autorise des débits et des distances inter nœuds importantes. Cette topologie est aussi celle des réseaux FDDI (Fiber-Distributed Data Interface).



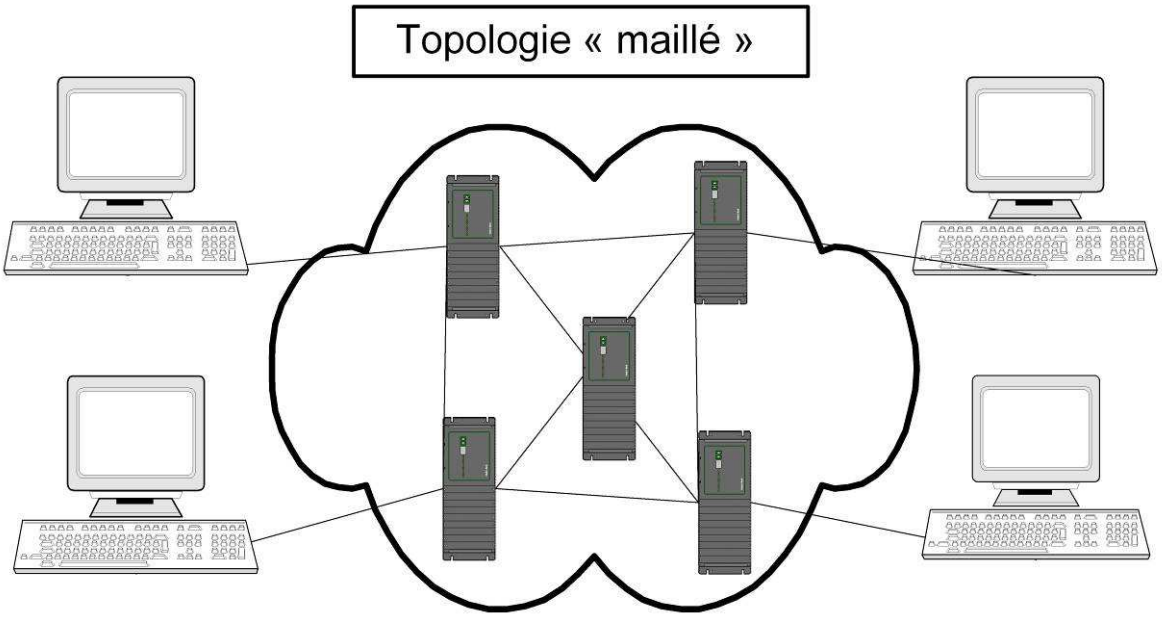

Ces différentes topologies sont utilisées dans les réseaux locaux (LAN, Local Area Network) mais en principe, elles ne sont jamais utilisées telles quelles. En réalité, le câblage en étoile, autour d'un local technique dit "local de brassage", s'est généralisé. La topologie originelle étant alors reconstituée par brassage. Ce qui a conduit à distinguer la topologie physique, celle du câblage, de la topologie logique qui concerne les méthodes d'accès des diverses stations au réseau. C'est ainsi que le réseau Ethernet sur paires torsadées (10BaseT) est une étoile physique au niveau du câblage, un arbre hiérarchisé au niveau du brassage et un bus logique en ce qui concerne la méthode d'accès.




A des fins de fiabilité dans les grands réseaux (WAN, Wide Area Network), les différents nœuds peuvent être atteints par différents chemins. Ces réseaux sont dits maillés. Définir la topologie d'un tel réseau constitue une tâche délicate dans laquelle de nombreux paramètres sont à prendre en compte comme le

nombre et la localisation des points d'accès, le débit offert, le niveau de redondance nécessaire (sécurité), le coût...

La réalisation d'un réseau privé dans une entreprise donnée est assez simple. En effet, l'emplacement des points d'accès au réseau est connu. Seuls les points de concentration et les liaisons entre les différents sites sont à déterminer. Ces réseaux sont généralement arborescents. Le maillage n'intervient qu'en second lieu et essentiellement sur des critères de sécurité.




Il existe de nombreux algorithmes pour optimiser la topologie des réseaux. Les algorithmes de Prim et de Krustal sont les plus simples et les plus connus.

**TOPVAL -** Système français de diffusion d'informations boursières via des liaisons hertziennes (classiques ou par satellite).

**TOR -** The Onion Router - Réseau décentralisé permettant, grâce à une technique de routage en oignon, d'anonymiser les connexions sur Internet.

Les systèmes d'anonymat sont basés sur un système de mix dont le routage en oignon est une variante. Le principe est de mélanger vos communications à celles des autres utilisateurs du réseau afin de les noyer dans la masse et ainsi, de ne pas pouvoir les faire correspondre avec votre identité. Plus il y a d'utilisateurs, meilleure est la sécurité du réseau. C'est une des raisons qui poussent les développeurs à travailler sur la facilité d'utilisation de Tor. En effet, un système simple à utiliser n'est pas, dans le cadre d'un réseau d'anonymat, une fonctionnalité accessoire, mais plutôt une composante essentielle du système. Si Tor est compliqué à utiliser, le nombre d'utilisateurices restera faible, et l'anonymat ne sera pas garanti.

Le principe fondamental du routage en oignon, est que le client Tor va sélectionner de manière aléatoire plusieurs noeuds parmi la liste des serveurs disponibles, et qu'il va créer un circuit de tunnels cryptés entre eux. Ainsi si Alice veut se connecter au site web de framasoft, son client va créer un tunnel crypté jusqu'au premier noeud. Puis, de là, un autre tunnel crypté jusqu'au deuxième noeud, puis éventuellement à travers d'autres noeuds, jusqu'à atteindre le dernier noeud, puis finalement le serveur du site web de framasoft. Le message initial (la requête HTTP destinée au serveur framasoft) sera donc crypté avec la clé publique du dernier noeud (le noeud de sortie). Ce message crypté sera ensuite re-crypté avec la clé de l'avant dernier noeud, et ainsi de suite jusqu'au premier noeud auquel on va envoyer le tout. C'est cette technique de cryptage par "couches" qui a donné le nom de routage en oignon. Le premier noeud saura qu'Alice est à l'origine de la requête, mais n'aura en sa possession, après décryptage, que l'adresse d'un autre noeud Tor, et un message indéchiffrable. Les noeuds intermédiaires ne pourront connaître ni l'origine, ni la destination finale. Seul le dernier noeud sera capable de déchiffrer la requête au serveur de Framasoft, mais il n'aura aucun moyen de savoir qu'elle a été envoyée par Alice. Le serveur framasoft recevra la requête depuis ce dernier noeud, il lui renverra la réponse (par exemple la page d'accueil du site), mais ne pourra pas connaître l'adresse IP (adresse Internet) d'Alice. Cette réponse sera traitée par le noeud de sortie - devenu noeud d'entrée pour le chemin de retour - afin de lui faire prendre le même circuit dans le sens inverse, vers l'ordinateur d'Alice.

Le gros avantage de cette méthode, par rapport aux systèmes comme the Cloak ou autres techniques basées sur un proxy unique, est que même si l'un des serveurs est corrompu, malveillant, ou tout simplement surveillé, l'anonymat est préservé. En fait, il suffit qu'un seul de ces serveurs soit fiable pour que l'anonymat soit garanti. Il est donc important que de nombreux serveurs, gérés par des personnes diverses, et situés dans des lieux géographiques différents, soient déployés.

Tor utilise SOCKS, et permet donc d'anonymiser toutes les applications qui supportent ce protocole (un

grand nombre de clients de messagerie internet par exemple). En couplant Tor à un outil comme privoxy (un proxy web avec lequel il s'intègre très bien), on peut protéger facilement toutes les communications HTTP (navigation, lecture de fils RSS, wget , apt-get). Mais on peut "Tor-iffier" d'autres programmes en utilisant par exemple tsocks ou dsocks qui sont capables d'intercepter les connexions faites par les applications pour les rediriger vers un serveur socks. Socat, transocks ou d'autres outils fonctionnent aussi selon des principes similaires. Le wiki noreply propose des procédures pour un grand nombre d'applications. On peut choisir d'utiliser Tor en tant que client uniquement, mais on peut également décider de participer à la réussite de ce réseau en configurant Tor en tant que serveur pour donner un peu de sa bande passante. On peut définir une "politique de sortie" qui permet de décider quels adresses et ports de destination sont accessibles depuis notre noeud, ce qui permet de limiter les abus qui semblent provenir de notre adresse IP. On peut aussi contrôler la quantité de bande passante que l'on souhaite allouer.

Tor offre donc une protection non négligeable contre toute une gamme d'attaques. On ne peut pas, en écoutant votre trafic sortant, savoir avec qui vous communiquez ; on ne peut pas, en écoutant le trafic entrant d'un serveur, savoir que vous en êtes l'initiateur. Un noeud du réseau Tor, ou un·e observateurice ne peuvent jamais connaître à la fois les deux extrémités d'un trafic. Néanmoins, Tor ne protège pas contre un·e attaquant·e global·e qui serait capable d'observer votre trafic ainsi que le trafic de tous les noeuds de sortie. Il lui serait facile, grâce à un type d'attaque nommée attaque temporelle, de retrouver la trace de vos communications. De plus, un·e attaquant·e qui se doute que vous vous connectez à framasoft, pourra (toujours par le biais d'une attaque temporelle) confirmer ses soupçons en écoutant à la fois votre trafic sortant et le trafic entrant de framasoft. Certains systèmes (Mixminion ou Mixmaster par exemple) permettent de se protéger contre ce genre d'attaques, mais sont beaucoup plus lents que Tor. Entre la protection contre ce type d'attaque, et une rapidité suffisante pour la messagerie instantanée et le surf web, un choix doit être fait. À l'heure actuelle, la recherche fondamentale n'offre pas de solution à ce dilemme. Il faut aussi être conscient·e que le projet Tor, démarré en 2004, est toujours en phase de développement intense, et que la conception ou l'implémentation des techniques qu'il emploie peuvent comporter des bugs et des imperfections. D'après les développeurs, il ne faut par se fier au réseau Tor actuel si vous cherchez réellement une grande confidentialité.

Effets fâcheux et effets vertueux :

Comme pour tout système visant à protéger la vie privée ou la confidentialité des échanges, des questions légitimes liées à l'abus de cette confidentialité sont posées. En effet, et cela est valable aussi bien dans le monde "réel" que dans le monde numérique, certaines personnes utilisent l'anonymat pour des activités répréhensibles. Parmi les utilisations indésirables qui ont déjà été faites via le réseau Tor, on peut noter : envoi de spam sur Usenet, demandes de rançon anonymes à des entreprises, utilisation de l'irc pour troller ou insulter les autres utilisateurices, vandalisme sur wikipedia ou dans les commentaires de Slashdot. Enfin, bien que le réseau Tor ne soit pas conçu pour le transfert de gros fichiers, certain·e·s s'en servent tout de même pour télécharger de la musique ou des films de manière illégale. Les services victimes de ces abus réagissent différemment vis à vis du réseau Tor : wikipedia bloque les noeuds Tor de manière régulière, mais essaye de réfléchir à des solutions permettant aux utilisateurices de bonne foi de participer tout de même. Certains serveurs irc bloquent Tor, d'autres, annoncent, lors de la connexion d'un·e utilisateurice à un canal qu'ille se connecte via Tor. Cela a pour effet de les exposer à une vigilance plus accrue de la part des responsables, et a suffi à réduire sur le réseau Freenode, le nombre de propos malintentionnés de la part d'utilisateurices de Tor. On peut remarquer que tous ces abus existaient avant l'apparition de Tor et que, comme le soulignent ses concepteurs, il existe déjà des moyens de parvenir à l'anonymat bien meilleurs que Tor, comme par exemple, le vol de téléphones portables, l'intrusion dans les ordinateurs de particuliers, ou d'autres techniques de vol d'identité. Pour celleux qui ne souhaitent pas nuire à d'autres personnes en leur volant leur matériel ou leur identité, Tor fournit un moyen d'obtenir la protection de l'anonymat. Tor est donc un réseau offrant un niveau de confidentialité élevé sur Internet. Le projet encore jeune, est tout à fait prometteur. Il permet en plus, via une fonctionnalité de services cachés, de mettre un service (site web, messagerie instantanée, etc) à disposition des autres utilisateurices du réseau, sans devoir en révéler l'emplacement géographique. Ceux et celles qui, pour diverses raisons, ont besoin d'anonymat, peuvent donc accéder à du contenu, et en proposer, sans compromettre leur identité. En terme de performances, Tor ralentit les communications de manière perceptible, notamment le surf web, mais la vitesse reste tout de même acceptable, même pour une utilisation intensive.

**TP2 -** Transport Protocol - Protocole de transport du modèle OSI.

**TPE -** Terminal de Paiement Electronique.

**TPV -** Terminal Point de Vente.

**TRAC -** Technical Regulations Applications Committee - Comité dépendant historiquement de la CEPT et chargé de rédiger les règles techniques communes (CTR) pour les équipements terminaux.

**Tradanet -** Réseau à valeur ajoutée de la société britannique INS pour les échanges de données informatisés (EDI) dans le commerce.

**Trafic -** Densité d'événements (messages, trames, bits...) sur un canal de transmission.

**Trame -** Ensemble de bits qui est diffusé sur un support. Suite définie d'informations constituant une entité logique de base pour la transmission dans un réseau. Une trame comporte les informations à transmettre proprement dites et des informations de contrôle qui précèdent et suivent celles-ci (enveloppe). La notion de trame est généralement associée au mode de transmission synchrone où les processus de synchronisation ne sont pas effectués à chaque mot, mais une fois pour toutes au niveau de chaque trame. C'est également l'unité d'information au niveau 2 du modèle OSI.

**Transaction -** Unité de dialogue entre deux équipements aboutissant à la modification d'un élément (table, état, donnée d'une base de données...) d'un des deux équipements. Exemple -demande d'enregistrement d'un prélèvement bancaire ayant pour conséquence de modifier le solde.

**Transactionnel -** Parfois utilisé à tort comme synonyme de "conversationnel" ou "interactif", ce qualificatif désigne au sens strict le mode de fonctionnement d'un système informatique dans lequel un dialogue se conclut par une transaction, c'est-à-dire la modification immédiate d'un élément du système (voir Transaction.).

**Transceiver -** Transmetteur - Appareil diffusant une source de signaux vers plusieurs destinataires, et cela de manière passive (sans modifier ces signaux). Principalement utilisé dans les réseaux locaux Ethernet, sous la forme d'un composant situé à l'intersection du câble desservant une station et du câble coaxial matérialisant le bus central Ethernet.

Résultat de la compression des termes "transmitter" et "receiver", un transceiver désigne un équipement à double fonction, un émetteur récepteur qui, comme son nom l'indique reçoit un signal venant d'une station distante et l'émet, après amplification, dans une autre direction (de temps en temps sous une autre forme électrique et/ou optique).

Les Tranceivers sont des équipements de transformation de signal physique d'une nature en un autre signal d'une autre nature. Par exemple, de BNC-10Base2 à FOIRL (Fibre Optical Inter Repeater Link) ou de AUI (Access Unit Interface) à 10BaseT.

Ces équipements, qui ne possèdent pas d'adresse physique, ne régénèrent pas le signal et ne peuvent donc pas augmenter la distance maximum de transmission, contrairement aux répéteurs.

**Transcodage -** Transformation d'informations d'un code dans un autre.

**Transcom -** Service de transmission de données à 64 kbit/s. L'ETTD de l'utilisateur communique avec le réseau RTC 64 par l'intermédiaire d'un coffret de raccordement ou régie d'abonné (ETCD). L'interface ETTD/ETCD est de type V35 ou X21.

**Transfert Intercellulaire -** Intercell Handover, Intercell Hand-off - Dans un système cellulaire de radiocommunication avec les mobiles, possibilité de passage d'une cellule à une autre sans interruption de la communication.

**Transfix -** Le nom de transfix désigne l'appellation commerciale des liaisons numériques permanentes proposées par France Télécom. Toutes bidirectionnelles, elles se distinguent essentiellement par leur débit. Les lignes à bas débit permettent des liaisons à 2 400, 4 800, 9 600 ou 19 200 Kbit/s, les moyens débits offrent 48, 56 ou 64 Kbit/s et les hauts débits de 128 à 1 920 kbit/s. On peut mentionner aussi les lignes MIC permettant d'obtenir des débits à 1 984 Kbit/sales lignes MIC, ainsi nommées par habitude, du nom de la modulation numérique utilisée sur le réseau (Modulation par Impulsions Codées).

**Transmission -** Sur un réseau de télécommunications, la fonction de transmission assure le transport des informations sur le réseau d'un point à un autre de ce réseau. Les supports de cette transmission peuvent être des câbles en cuivre ou en fibre optique, mais également des faisceaux hertziens. (voir "commutation").

Selon les définitions officielles, la transmission suppose une source de données et un récepteur de données communiquant au travers d'un canal de données. Source et récepteur sont des Equipements Terminaux de Traitement de Données (ETTD) ou en anglais Data Terminal Equipment (DTE). La connexion du terminal au canal de transmission nécessite généralement une adaptation de la vitesse, de la forme du signal.... Cette adaptation est réalisée par un Equipement Terminal de Circuit de Données (ETCD) ou en anglais Data Communication Equipment (DCE). Les points de contact entre ces différents éléments, entre ETTD et ETCD, et entre ETCD et canal de données, font l'objet d'une normalisation internationale dans le cadre de l'UIT (ex CCITT) ou de l'ISO. Ces organismes définissent des avis, normes ou recommandations que l'on désigne généralement par des lettres suivies d'un numéro : V24, V28, X21, ISO 8802.3... Ces normes peuvent concerner les caractéristiques électriques, physiques ou logiques (organisation des séquences de dialogues).

**Transmission de données -** Transfert de données d'un point à un autre par télécommunication. Les transmissions de données forment encore un monde à part et disposent de leurs propres codages et protocoles. Conséquence : il a fallu bâtir séparément des grands réseaux spécialisés dans le transport des données. L'équipement de base qui connecte l'utilisateur à ces réseaux est le modem. Les progrès technologiques dont il a bénéficié récemment en matière de sécurité et de débit de transmission en font un terminal de plus en plus performant pour... le réseau téléphonique analogique.

Télécommunication dans laquelle les informations transmises sont représentées par des données provenant de ou destinées à un système informatique.

**Transpac -** Société française filiale de France Télécom (via Cogecom) chargée de la commercialisation et de la gestion du réseau public à commutation de paquets du même nom. Avec plus de 80 000 raccordements d'abonnés à la mi-91, ce réseau était le plus important du monde utilisant cette technique (normalisée sous le nom de X25). Outre la vocation de base de gestion de ce réseau Transpac, la société Transpac propose maintenant des services à valeur ajoutée, notamment le service de messagerie X400. Elle réalise également des réseaux à commutation de paquets privés en France et à l'étranger, dont le Royaume-Uni.

**Transparence -** Désigne un mode de transmission indépendant de la configuration interne des bits en mots et du code utilisé. Dans ce mode, tous les mots sont acceptés, aucun ne pouvant être pris pour un mot de commande.

**Transparence -** Transparency - Une transmission est transparente si elle ne modifie pas les informations transmises. La transparence peut être sémantique (les valeurs binaires sont toutes conservées), ou temporelle (les intervalles de temps entre les bits sont conservés).

**Transpondeur -** Ce mot vient des techniques radioélectriques où il a une signification voisine à Transceiver. Il désigne l'équipement d'amplification associé à un seul canal de transmission qui est placé dans les satellites de télécommunications

Le transpondeur (ou répéteur) est l'appellation donnée au réémetteur embarqué à bord du satellite. Sa fonction est d'amplifier puis transposer en fréquence les signaux reçus de la station de montée vers une partie précise du globe. Le transpondeur est associé à une ou plusieurs antennes d'émission, qui déterminent, par leurs formes et leurs orientations, la puissance et la zone de couverture du faisceau émis.

Amplification : la puissance à l'entrée du récepteur du satellite est de l'ordre de 100 pW à 1 nW. La puissance du signal à la sortie de l'amplificateur d'émission du transpondeur est de l'ordre de 10 W à 100 W. Le gain en puissance est donc de l'ordre de 100 à 130 dB.

Un satellite comprend quelques 12 à 20 transpondeurs, chacun ayant une bande passante de 36 à 50 MHz. Un transpondeur disposant d'une potentialité de débit de 50 Mbits/s peut-être utilisé aussi bien pour transmettre un unique flux numérique à 50 Mbits/s que 80 canaux téléphoniques à 64 Kbits/s. Deux transpondeurs peuvent utiliser des modes différents de polarisation électromagnétique des ondes radio, ce qui leur permet d'utiliser sur un même satellite une même bande de fréquences sans risque d'interférences.

**Transport -** Fonction de communication assurant l'acheminement complet des informations entre deux points terminaux d'un réseau. Dans la terminologie du modèle OSI d'interconnexion des systèmes ouverts, le transport désigne la couche 4, assurant la liaison de bout en bout entre émetteur et destinataire, sans avoir à se préoccuper du chemin à parcourir (fonction prise en compte par la couche 3 Réseau), ni du contenu du message (pris en compte par les couches supérieures).

**Transrel -** Nom d'un service d'interconnexion de réseaux locaux commercialisé par France Télécom (pour réseaux Ethernet ou Token-Ring).

**Transveil -** service de télé-action proposé par France Télécom. Utilisant le réseau téléphonique commuté en Accès et Transpac pour le transport, il permet de transmettre automatiquement en tous points du territoire de courts messages avec une périodicité garantie. Les principales applications concernent le déclenchement d'alarme, la télémétrie, le télé relevé de compteurs, la télé autorisation...

**Trap (snmp) -** Message d'alerte qu'émet un agent SNMP pour prévenir le Manager d'un événement particulier (dysfonctionnement de l'équipement, par exemple).

**Trashing -** Pratique qui consiste à fouiller dans les poubelles pour y découvrir des secrets industriels.

**Tresse -** Entrelaçage de fils fins sur le périmètre d'un conducteur ou d'un câble qui assure une protection contre les basses fréquences parasites.

**Triple DES -** Algorithme DES combiné à une, deux ou trois clés pour le cryptage/décryptage de paquets de données.

**Triple Play -** Offre combinée voix-internet-TV sur accès haut débit - Offre commerciale issue de différents fournisseurs d'accès à Internet, le Triple Play consiste à proposer aux abonnés un accès Internet (souvent à haut débit), la téléphonie (sur IP en local et national - Voir TOIP) et un bouquet TV.

Ensemble de fonctionnalités regroupant l'accès à l'Internet, la téléphonie et la télévision. Appelation francophone : Multiservices. Le Triple-Play est très à la mode chez les FAI mais laissera vite sa place au quadruple-play.

**Trunk -** Voir 3RP

**TSAPI -** Telephony Services Applications Programming Interface - Développée par Novell - La norme TSAPI s'inscrit dans la norme CSTA (co développé par Novell et AT&T). Basée sur une architecture serveur-centrique (ou Third Party) fut un succès et TSAPI était l'API la plus utilisée en 1998 pour la bureautique. Cette norme cherche à relier deux équipements partagés : PABX et serveur CTI, non pas téléphone et PC qui sont des équipements personnels.

**TTL -** Time-To-Live.

**Tunnel -** Connexion sécurisée et cryptée entre deux points passant par un réseau public ou tiers.

**TVHD -** TéléVision Haute Définition. La définition prévue est de :

- 720x576 lignes pour la TV actuelle en Europe,
- 1280x720 lignes pour la HDTV 720p50 (TVHD qualité intermédiaire),
- 1940x1080 lignes pour la HDTV 1080i25 (version haute résolution entrelacée).

Le son est encodé au format Dolby Digital 5.1 (comme la plupart des DVD de 2004).

**Twinax -** Câble coaxial composé d'une paire torsadée, entourée d'un diélectrique, d'une tresse et d'une gaine. Ce type de câble à largement été utilisé sur les premières installations de terminaux pour AS400.

# U

**U -** Unité de mesure relative à la hauteur d'un équipement rackable. 1U = 1,75 pouce = 4,44 cm.

**UAT -** Union Africaine des Télécommunications

**UDDI -** Universel Description Discovery and Integration - Ce standard permet de créer des services d'annuaires en ligne référençant les services web disponibles sur Internet. Il facilite les échanges entre entreprises partenaires référencées. UDDI est fondé sur les standards du W3C et de l'IETF, tels XML, HTTP et DNS.

**UDP -** User Datagram Protocol - Protocole proche du niveau applicatif qui délivre un minimum d'information de service, pas de numéro de séquence, ni de contrôle de flux, ni de correction d'erreur.

Ce protocole est conçu pour les applications ne nécessitant pas la remise en ordre des datagrammes, il intervient au même niveau que TCP. Un entête UDP qui est placé devant les données, exactement comme l'entête TCP. Toutefois l'entête UDP est plus court que celui de TCP, il ne comporte pas de numéro d'ordre (il y a tout de même les ports source et destination ainsi que le total de contrôle de l'entête).

Le protocole UDP (User Datagram Protocol) est un protocole non orienté connexion de la couche transport du modèle TCP/IP.

L'en-tête du segment UDP est donc très simple:

- Port Source: il s'agit du numéro de port correspondant à l'application émettrice du segment UDP. Ce champ représente une adresse de réponse pour le destinataire. Ainsi, ce champ est optionnel, cela signifie que si l'on ne précise pas le port source, les 16 bits de ce champ seront mis à zéro, auquel cas le destinataire ne pourra pas répondre (cela n'est pas forcément nécessaire, notamment pour des messages unidirectionnels.
- Port Destination: Ce champ contient le port correspondant à l'application de la machine destinataire à laquelle on s'adresse.
- Longueur: Ce champ précise la longueur totale du segment, en-tête comprise, or l'en-tête a une longueur de 4 x 16 bits (soient 8 x 8 bits) donc le champ longueur est nécessairement supérieur ou égal à 8 octets.
- Somme de contrôle: Il s'agit d'une somme de contrôle réalisée de telle façon à pouvoir contrôler l'intégrité du segment.

Le protocole User Datagram Protocol (UDP) est défini dans le but de fournir une communication par paquet unique entre deux processus dans un environnement réseau étendu. Ce protocole suppose l'utilisation du protocole IP comme support de base à la communication.

Ce protocole définit une procédure permettant à une application d'envoyer un message court à une autre application, selon un mécanisme minimaliste. Ce protocole est transactionnel, et ne garantit ni la délivrance du message, ni son éventuelle duplication. Les applications nécessitant une transmission fiabilisée et ordonnée d'un flux de données implémenteront de préférence le protocole TCP (Transmission Control Protocol) .

Le Port Destinataire a une signification dans le cadre d'adresses Internet particulières.

La Longueur compte le nombre d'octets dans le datagramme entier y compris le présent en-tête. (Et par conséquent la longueur minimale mentionnée dans ce champ vaut huit, si le datagramme ne transporte aucune donnée).

Le Checksum se calcule en prenant le complément à un de la somme sur 16 bits des compléments à un calculé sur un pseudo en-tête constitué de l'information typique d'une en-tête IP, l'en-tête UDP elle-même, et les données, le tout additionné d'un octet nul éventuel afin que le nombre total d'octets soit pair.

La pré en-tête ajoutée avant l'en-tête UDP contient l'adresse IP source, l'adresse IP destinataire, le code de protocole, et la longueur du segment UDP. Cette informationpermet d'augmenter l'immunité du réseau aux erreurs de routage de datagrammes. La procédure de calcul du Checksum est la même que pour TCP.

Si le calcul du checksum vaut zéro, il sera transmis tous ses bits à un (le complément à un). UN Checksum transmis avec une valeur zéro a effectivement une signification particulière. Dans ce cas, le segment indique qu'aucun Checksum n'a été calculé (pour des besoins de mise au point ou pour des protocoles de niveaux supérieurs qui rendent cette vérification inutile).

Interface Utilisateur

L'interface utilisateur doit permettre l'ouverture de nouveaux ports de réception, la réception des données et leur transmission ainsi que celle de l'adresse source à l'application sur le port de réception mis en place, et doit mettre en place une commande permettant l'émission d'un datagramme, par laquelle seront spécifiés les données, l'adresse et ports source et destination à utiliser.

Interface IP

Le module UDP doit extraire les adresses source et destination de l'en-tête IP, et vérifier le numéro de protocole. Une interface UDP/IP plausible pourrait retourner le datagrammeentier y compris l'en-tête Internet en réponse du datagramme reçu. Une interface devra pour cela permettre à UDP de passer un datagramme

Internet complet avec une en-tête IP à la couche IP elle même pour émission. IP n'aura plus qu'à vérifier la cohérence des champs d'en-tête IP préparés par UDP et calculer le Checksum.

Applications du Protocole

Ce protocole sera utilisé principalement pour les communications avec les serveurs de noms de domaines , et dans les transactions utilisant le protocole Trivial File Transfer.

Numéro de protocole

Ce protocole porte le numéro 17 (21 en octal) lorsqu'il est transporté par le Protocole Internet. D'autres numéros de protocoles pour d'autres couches support sont données dans la référence .

**UER -** Union Européenne de Radiotélévision

**UIT -** Union Internationale des Télécommunications - Organisme international siégeant à Genève et chargé, dans le cadre de l'Onu, des questions de télécommunications. Il contrôle en particulier le CCITT, Comité Consultatif International Télégraphique et Téléphonique, chargé du développement et de l'adoption des normes internationales en matière de télécommunications.

Organisme appartenant à l'ONU et chargé de coordonner et de promouvoir le développement des télécommunications dans le monde. Ses principaux objectifs sont de stimuler les avancées technologiques et de garantir la compatibilité des réseaux nationaux pour permettre les communications internationales. Pour en savoir plus : http://www.itu.int

**UIT-T -** ex Comité Consultatif International Télégraphique et Téléphonique. Organisme international de normalisation en télécommunications dépendant de l'Union Internationale des Télécommunications (UIT) siégeant à Genève. Il délivre des "avis" qui fixent les principales normes techniques dans le domaine des télécommunications, en particulier les avis en V (exemple V23, V24) pour l'utilisation des lignes analogiques ou en X (exemple X25) pour réseaux de données. La liste et le contenu officiel de ces avis sont mis à jour tous les 4 ans.

**UL -** Underwriters Laboratories - Organisme américain de test et certification.

**Ultra Large Bande -** Technique de transmission consistant à émettre et recevoir des impulsions extrêmement courtes de radiofréquences, avec pour résultat des signaux dont le rapport de a largeur de bande à la fréquence centrale est très grand.

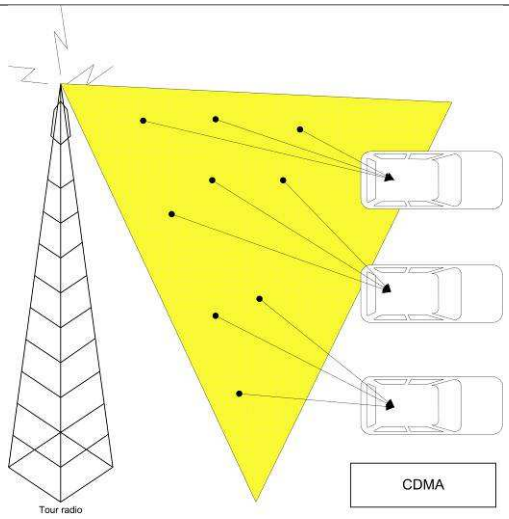
**UMA -** Unlicensed Mobile Access - Technologie permettant d'assurer un roaming transparent entre les réseaux mobiles des opérateurs et les réseaux sans fil, afin de permettre aux utilisateurs de mobiles de passer d'un réseau à l'autre sans coupure et à des coûts intéressants (mais pour qui ?).

Le 3GPP (The Third Generation Partnership Project) a intégré le concept de l'UMA à la release 6 de l'UMTS, en parlant de "generic access". Le 3GPP a renommé UMA en GAAI (Generic Access to A/Gb Interface)

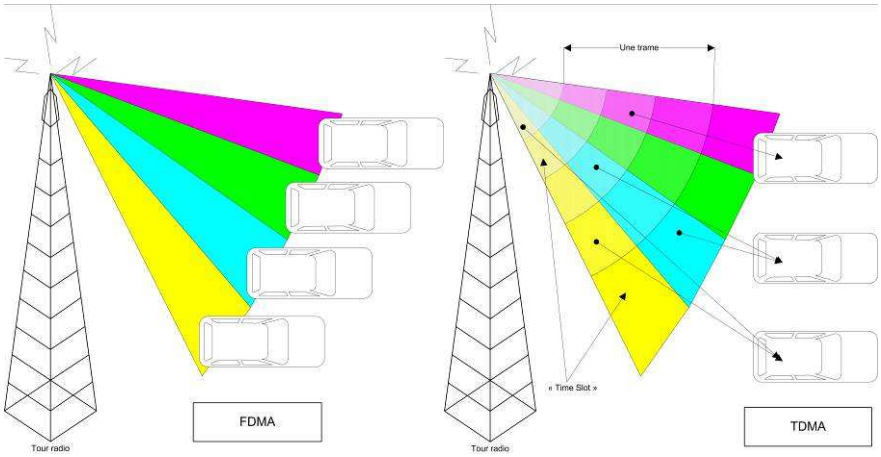
**UMTS -** Universal Mobile Telecommunication System - Système de télécommunications mobiles universelles. Norme pour le réseau radio mobile dit de 3ème Génération, support de services multimédias à haut débit et en mobilité.

Dénomination de la norme retenue en Europe pour les systèmes de radiocommunications mobiles de troisième génération, qui permettront d'offrir une large gamme de services, intégrant la voix, les données et les images. Dans le cadre de l'UIT, il existe plusieurs normes concurrentes pour ces systèmes, dans le cadre de l'appellation générique "IMT 2000".

Il est bien connu que l'UMTS (Universal Mobile Telecommunication System) est une technologie radio basée sur le CDMA (Code Division Multiple Access), une méthode d'accès extrêmement complexe qui a été utilisée sur les réseaux de 2e génération en Amérique et en Asie.




Dès lors, le profane peut s'interroger sur l'intérêt de s'appuyer sur cette technologie inconnue, notamment en Europe, plutôt que sur la technologie du GSM, le TDMA... Mais seule l'évolution 3G du CDMA [autrement dit le Wideband CDMA] est capable de répondre aux exigences en bande passante de la nouvelle génération de téléphonie mobile.




Les capacités du CDMA sont en effet plus performantes en regard des autres générations de réseaux de radiocommunication (voir graphique). La première génération, celle par exemple du service Radiocom 2000 des années 1980, allouait une fréquence pour un utilisateur : c'est le FDMA (F pour Frequency Division Multiple Access). Le TDMA (T pour Time Division Multiple Access), technologie utilisée par Le GSM actuel, ajoute le temps comme variable, permettant à plusieurs utilisateurs de partager la même fréquence de façon séquentielle, ce qui offre déjà une bien meilleure utilisation du spectre radio. Le CDMA franchit une étape supplémentaire, en permettant à tous les utilisateurs d'émettre en même temps, à la même fréquence. Pour reconnaître chacun d'entre eux, un code leur est attribué à chaque établissement de communication, codage qui est reconnu par les stations de base UMTS. Les ressources radio sont alors optimisées en minimisant le niveau d'interférence. Bien évidemment, ce gain de capacité de transmission a un revers : la complexité. L'UMTS est en effet un savant compromis entre capacité et couverture, entre capacité et performances radio, et ce pour chaque cellule.

L'occasion de démontrer que l'expérience en technologie Radio sera indispensable pour optimiser l'UMTS. Deux fonctions vitales qui, bien que décrites dans la norme, nécessiteront une mise au point très fine par l'équipementier (et devront être finement encadrées par les opérateurs):

- Le contrôle de puissance est un algorithme destiné à s'assurer que chaque mobile reçoit avec la même puissance le signal. Ce dialogue constant entre la base émettrice et tous les terminaux s'effectue à une rapidité étonnante : 1 500 fois par seconde !
- L'algorithme appelé soft handover sert à relier un terminal UMTS jusqu'à 6 stations de base en même temps. Cette technique très complexe offre l'avantage d'éviter les coupures et minimise la puissance nécessaire au terminal car il est "écouté" par plusieurs stations de base.

Ces deux algorithmes ont été mis au point sur la base des réseaux CDMA déployés par des équipementiers et assurent à l'opérateur la maîtrise de son réseau.

Mais avant d'exploiter tous ces raffinements de la technologie CDMA, les opérateurs seront confrontés au déploiement optimisé de leur réseau UMTS. Là encore, il existe une gamme de logiciels capables de planifier, d'optimiser et, au-delà, d'adapter le réseau en fonction des retours d'utilisation en grandeur réelle. Ces outils assureront une fiabilité et une efficacité plus grande des réseaux. Ils permettront également de

réduire considérablement le temps de déploiement.

L'UMTS est une norme définissant la troisième génération des systèmes de télécommunication en Europe. Elle a pour but de prendre la relève des systèmes de la deuxième génération tel le GSM.

Les limites du GSM : Ces dernières années, les télécommunications ont vu un essor à l'échelle mondiale des services de communications avec les mobiles. Ainsi, on comptait 10 millions de mobiles en 1991 et 210 millions en 1997. On espère aujourd'hui atteindre + de 900 millions en 2000. Cette croissance est actuellement assurée par le GSM mais pour des raisons d'allocation de spectre de fréquences, cet essor ne pourra être totalement assuré que par des systèmes de troisième génération tels l'UMTS. Par ailleurs, un deuxième changement radical dans les télécommunications doit être intégré au marché des mobiles : il s'agit de l'explosion du trafic et des réseaux Internet. A cela s'ajoute le rapide développement des services multimédias. On pourrait assister à une convergence de ces deux marchés vers un marché de services mobiles multimédias. Enfin, la dynamique d'innovation et la diminution des coûts devraient permettre de maintenir la croissance de la vente des mobiles. Toutefois, ce développement implique des besoins en ressources spectrales car il risque d'atteindre les limites du GSM. Ce développement fait donc appel à une nouvelle génération de systèmes à plus fort débit tel l'UMTS qui permettront de surcroît une meilleure répartition des spectres.

Cette même répartition des spectres est le problème principal de la mise en place de l'UMTS qui actuellement n'a encore aucune plage de fréquences allouée. Les bandes de fréquences qui seraient concernées dans le Règlement des Radiocommunications (qui a valeur de traité international) sont à l'échelle mondiale : 1885-2025 Mhz et 2110-2200 Mhz. Pour les services mobiles par satellites ce sont les bandes à : 1980-2010 Mhz et 2170-2200 Mhz. Or en France par exemple, certaines sont attribuées au ministère de la Défense et à France Télécom. D'autres bandes sont affectées à des services de l'espace. L'ERC (European Radiocommunications Committee) demande aux états de mettre à disposition de l'UMTS 2x40 Mhz dans les bandes de fréquences concernées. En France, le ministère de la défense est favorable à cette libération de spectre et France Télécom c'est engagé à restituer la bande qu'elle utilise pour 2005. Toutefois, ces changements ont un coût. Ainsi, le ministère de la défense a présenté en 1998 un plan de dégagement des bandes à auteur de 630 Millions de francs. Après de nombreuses négociations, les bandes concernées ont été attribuées à l'UMTS.

L'UIT qui, alors que le GSM n'avait pas encore fait ses preuves, préparait un autre système : l'IMT2000, voit aujourd'hui ce projet réalisable techniquement. En parallèle en Europe le standard UMTS est en voie d'aboutissement après de nombreux colloques. C'est pourquoi, il a été établi que, à l'instar de l'IMT2000, l'UMTS pourrait jouir d'une plage de fréquences voisines des 2 GHz. La découpe en canaux se fait, alors, par tranche de 4 à 5 MHz. Une telle largeur de bande permet d'avoir un spectre en fréquence d'autant plus large que le bruit pourra être atténué et isolé. L'UMTS Forum, préconise donc l'attribution à chaque opérateur UMTS de 35 MHz (soit 2*15+5) pour satisfaire les besoins jusqu'en 2005. Sur 30 MHz les communications seront assurées pour un seul sens de transmission, alors que sur 5 MHz nous aurons deux sens de transmission pour une même fréquence. Au delà, une reprise des bandes GSM pourrait être envisagée (GSM : autour des 900 MHz et 1800 MHz). Dans un premier temps, il faudra assurer la compatibilité des troisièmes générations avec les terminaux et cellules de deuxième génération. C'est pourquoi les bandes de fréquences doivent être des multiples de 20 KHz (bande de fréquence des GSM) et les débits devront se dériver d'une horloge commune de celle du GSM (13 ou 26 MHz).

La couverture se fera dans un premier temps par "taches de léopard", c'est à dire que seul les villes et les centres d'affaires seront équipés en UMTS. Ce phénomène est dû à plusieurs raisons. En effet, le territoire est globalement couvert par les systèmes de deuxième génération, ceci par l'intermédiaire de trois types de "cellules", les macro-cellules, (couverture sur 15Km de rayon), les microcellules (500m) et les pico-cellules (100m). Du fait d'un débit et d'une fréquence d'utilisation plus élevés pour l'UMTS, les cellules utilisées seront plus petites. L'UMTS se développera donc dans un premier temps dans des îlots de couverture : en milieux urbains, centres d'affaires… et se déploiera de façon progressive. L'UMTS s'appuiera donc sur le GSM pour la couverture globale, le but étant qu'en tout point géographique l'UMTS soit accessible directement soit à haut débit soit de façon dégradé lorsque le GSM prendra le relais. Cette méthode de couverture nécessitera donc l'élaboration de terminaux multimodes GSM/UMTS pour permettre la continuité du service.

Pour obtenir un débit plus important et une meilleure utilisation des spectres de fréquence, l'ETSI à décidé d'utiliser un protocole de communication baptisé UTRA. L'UTRA est basé sur la technique CDMA qui permet à une même fréquence d'accueillir plusieurs utilisateurs grâce à la modulation à étalement de spectre. Au départ le signal utile a un débit d. Artificiellement nous augmentons ce débit en insérant un code ou séquence d'étalement entre plusieurs symboles (bit après codage pour la protection des données). Le débit obtenu est alors D. Comme la séquence de codage est pseudo aléatoire, le signal émis est donc fortement parasité, c'est un signal aléatoire à spectre beaucoup plus large que le signal initial.

Le récepteur capte le signal qu'il envoie dans le module radio fréquence, qui ramène celle-ci centrée sur 0. Puis le module de dé étalement génère la même séquence de codage. Or toutes ces séquences sont orthogonales entre elles. Donc seul le signal désiré est démodulé par convolution. Le spectre apparaît alors sous forme gaussienne. Soit Q le facteur de qualité du signal, on a la relation suivante Q=(D/d)/M avec M le

nombre d'utilisateurs sur une même fréquence. Donc pour un facteur de qualité donné, nous pouvons déterminer le nombre de code à établir sur un même canal.

Les mobiles devant sans cesse être en communication avec une cellule, lors du transfert intercellulaire (soft handover), le terminal est en relation avec deux à trois bornes simultanément afin de déterminer lequel sera le plus apte à faire transiter les données.

Méthode d'étalement de spectre à séquence directe. Sur une bande de 5 MHz, le débit de ship (bits de la séquence de codage) est très élevé, 4.096Mships/sec. On bénéficie donc d'une très grande diversité de fréquence dans la plupart des environnements. Le facteur d 'étalement peut varier de 4 à 256. Pour un seul code, le débit maximal est de 384 Kbits/sec. Pour atteindre 2 Mbits/sec, on pourra utiliser 5 codes sur un même canal.

C'est un système hybride, composé d'une composante AMRT (Accès multiple à répartition dans le temps), et une composante d'étalement de spectre à l'intérieur des intervalles de temps ("time slot") avec séparation par codes (CDMA). Chaque liaison est donc caractérisée par une porteuse, une séquence de codage et un intervalle de temps. Grâce au CDMA, 9 paquets peuvent être envoyé dans le même intervalle de temps. Le système est donc adaptable au débit des données qui transitent. Ces deux méthodes peuvent offrir des débits allant jusqu'à 2 MBits/sec, ce qui ouvre de nombreuses perspectives futures d'emplois de terminaux mobiles.

Le client du début du XXIe siècle emportera avec lui un ou plusieurs terminaux mobiles lui permettant toute sorte de communications: le téléphone mobile, dont l'usage sera complètement généralisé, le visiophone de poche, le communicateur personnel pour gérer agenda, messagerie, fax rapide, et recevoir de multiples informations. Avec son PC portatif mobile, il pourra se connecter à l'Intranet de son entreprise, et bénéficier de capacités de visioconférence, et tout le confort nécessaire pour travailler en situation de mobilité et de télétravail.

De nombreuses applications spécifiques utiliseront les capacités des systèmes mobiles à acheminer son, données et images fixes et animées: télémédecine, reportage, localisation, télésurveillance, information et guidage routier.

Les moyens de télécommunication du XXIe siècle se feront à partir de véritables bureaux mobiles, par exemple dans les voitures ou sur les chantiers.

En clair, l'UMTS offrira un service de mobilité universelle dépassant les limitations dues à la multiplicité des systèmes et des réseaux. Ainsi le terminal mobile permettra de communiquer dans tous les environnements d'utilisation: domicile, bureau, rue, automobile, train, …

Le concept de "Virtual Home Environnement "(VHE)

Le concept de VHE permettra à l'utilisateur de retrouver ses services avec la même ergonomie quels que soient sa localisation et le réseau visité, lui donnant ainsi la sensation de garder au cours de ses déplacements le même environnement de communication que dans sa zone de service nominale.

Les systèmes satellites offrent une grande couverture et sont donc d'un précieux apport dans l'obtention d'un service universel tel celui que vise la prochaine génération de téléphonie mobile. Le système à satellite viendra en complément de l'infrastructure cellulaire dans les zones où celle-ci sera soit peu rentable soit difficilement déployable.

L'UMTS est résolument la norme du IIIème millénaire, orientée vers des applications de plus en plus coûteuses en ressources, l'universalité et la simplicité de communiquer. Partenariat entre de grands groupes, c'est aussi un pari sur l'avenir. Avant son installation, de nombreux points doivent encore être éclaircis, d'où une grande effervescence dans le monde des télécom.

**UMTS TDD -** Universal Mobile Telecommunication System Time Division Duplex - Norme plus connue sous l'appellation TDD-CDMA, l'UMTS TDD fait partie de la batterie de spécifications définissant l'UMTS aux côtés de l'UMTS FDD (Frequency Division Duplex, appelée aussi WCDMA).

Contrairement à cette dernière, qui utilise un duplexage fréquentiel (transmission bidirectionnelle sur deux fréquences), l'UMTS TDD met en œuvre un duplexage temporel (transmission bidirectionnelle sur la même fréquence en alternance.

La technologie UMTS TDD vient pour l'heure se positionner, à l'instar du WiMAX, en concurrente de celles d'accès Internet haut-débit radio (Wi-Fi) et fixe (DSL), avec une couverture d'un rayon de 29 km autour de l'antenne avec des débits d'accès théoriques compris entre 128 kbit/s et 2 Mbit/s (contre 384 kbit/s pour le WCDMA).

**UNI -** User to Network Interface - Interface Réseau utilisateur - Protocole de communication permettant aux routeurs de communiquer avec les commutateurs Frame Relay du réseau.

UNI est une interface qui permet aux utilisateurs d'accéder à un réseau Frame Relay public ou privé et d'établir un chemin de Communication à l'intérieur du même réseau. Le Relais de Trames UNI est un protocole qui permet à l'utilisateur d'accéder à un réseau public ou privé.

En ATM : Protocole de signalisation à l'interface Usager-Réseau (UNI) - Les réseaux ATM fonctionnent en mode connecté, c'est à dire qu'il faut établir une connexion entre l'émetteur et le récepteur et assigner un VCI/VPI spécifique à la connexion à chaque saut avant de pouvoir transmettre des données. Le protocole qui effectue ces tâches est appelé protocole de signalisation ou d'établissement d'une connexion.

Le forum ATM et l'ITU-T ont travaillé tous deux sur un protocole de signalisation appelé Q.93B, actuellement Q.2931 pour l'ITU-T et UNI 3.0 pour l'ATM forum. Q93B est une version modifiée du protocole de signalisation RNIS Q.931.

**Unicast -** Mode de transmission le plus simple qui consiste à envoyer les paquets de données en spécifiant l'adresse IP de l'ordinateur cible. Les éléments actifs et passifs du réseau dirigent l'information dans la bonne direction pour que les trames arrivent au bon endroit. Seule la machine ayant l'adresse contenue dans la trame traite l'information.

**Unidirectionnel (réseau)** - Se dit d'un réseau sur lequel le dialogue ne se fait que dans un seul sens.

**Uplink -** Terme anglais désignant le lien montant entre un satellite et une station au sol.

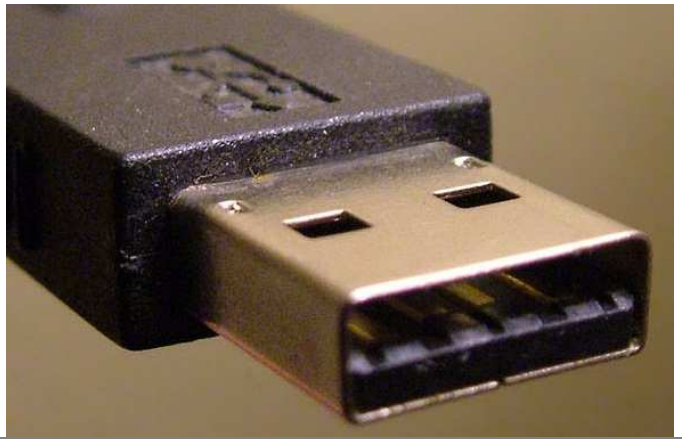
**URA -** Unité de Raccordement d'Abonné - Sur le réseau de France Télécom, partie d'un commutateur téléphonique sur laquelle sont raccordées les lignes d'abonnés et qui procède à la numérisation des informations.

**URI -** Uniform Resource Identifier - Identificateur Uniforme de Ressources - Permet de définir et de localiser sans ambiguïté sous une forme standard les ressources disponibles sur Internet. Les deux types d'URI sont les URL et les URN.

**URL -** Universal Resource Locator - Stratégie d'adressage standardisée pour accéder à des documents hypertexte et à d'autres services au moyen d'un navigateur.

Composé de l'identifiant d'un service précédé d'un protocole particulier utilisé pour accéder à la ressource, l'URL permet par exemple de localiser une page d'information sur un serveur web. Il sera remplacé à terme par l'URN (uniform resource name) et/ou l'URI (uniform resource identifier) identifiant d'une ressource indépendamment de sa localisation physique

**USB -** Universal Serial Bus - Concurrent de Firewire, c'est aussi une interface permettant la connexion Plug & Play (à chaud). La première génération n'offrait que 12 Mégabits par secondes (Mbps) que la deuxième offre désormais 480 Mégabits par secondes (Mbps).



**Usenet -** Réseau mondial constitué des utilisateurs de système Unix dans le domaine universitaire et de la recherche. Résultant d'une harmonisation internationale de divers réseaux de recherches, il est probablement le plus gros réseau mondial avec 30 000 machines et plusieurs millions d'utilisateurs potentiels. Il ne possède pas de centre de contrôle.

**UTE -** Union Technique de l'Électricité.

**Utipac -** Association des utilisateurs de Transpac.

**UTISAT -** Bien que le sigle d'origine soit Association des utilisateurs de services avancés de télécommunications, les buts de cette association se sont élargis pour couvrir l'ensemble des services numériques d'entreprise, et sa dénomination officielle est désormais Association des usagers pour l'utilisation des liaisons numériques et des transmissions télévisuelles. Elle regroupe essentiellement de très grandes entreprises françaises.

**UTP -** Unshielded Twisted Pair - Dans le câblage, cet acronyme désigne un câblage non blindé, non écranté.

**UTRA FDD -** Universal Terrestrial Radio Access Frequency Division Duplex - Terme utilisé pour désigner l'interface radio WCDMA et l'UMTS au sein du 3 GPP. Nécessite des bandes de fréquences appariées.

**UTRA TDD -** Universal Terrestrial Radio Access Time Division Duplex - Terme utilisé pour désigner l'interface radio WCDMA et l'UMTS et TD/SCDMA (UTRA TDD Bande étroite) au sein du 3 GPP

**UUCP -** Unix to Unix Copy Program - Programme pour faciliter la transmission de fichiers entre des systèmes Unix qui utilisent des liaisons série pour envoyer les données par le réseau téléphonique commuté.

**UWB -** Ultra Wide Band - Réseaux locaux d'une couverture de 100 m et d'un débit de 500 Mbit/s à 1 Gbit/s, interconnectés via des commutateurs LAN à 1 Gbit/s pour constituer un immense réseau sans fil doué d'intelligence. Le standard 802.15 reposant sur cette technologie est en cours de développement à l'IETF. Les débits offerts par cette technologie progressent d'année en année grâce à un spectre radio quatre-vingts fois plus large (de 3,1 à 10,6 GHz - Signal de type "impulsion").

A noter : La technologie radio n'est pas encore définie précisément, certains préconisent la technologie MB-OFDM et d'autres exploitent la technologie DS-CDMA.

# V

**V -** Lettre servant de préfixe dans la désignation des avis du CCITT concernant les réseaux publics analogiques. Exemple : V32 est un avis portant sur l'interface d'une liaison deux fils à 9 600 bps sur un réseau public.

**V.11 -** Jonction définie par le CCITT - Traite des caractéristiques électriques des circuits de jonction symétriques. La présente recommandation traite des caractéristiques électriques du générateur, du récepteur et des conducteurs d'interconnexion d'un circuit de jonction (symétrique) utilisant des signaux différentiels avec un décalage de tension continue optionnel.

Le générateur symétrique et les composantes de la charge sont conçus de façon à causer un brouillage mutuel minimal avec les circuits de jonction (symétriques ou non).

Un circuit de jonction symétrique est constitué, par définition, d'un générateur symétrique connecté par une paire symétrique d'interconnexion à un récepteur symétrique. Pour un générateur symétrique, la somme algébrique des deux différences de potentiel des sorties par rapport à la terre devra rester constante pour tous les signaux transmis, les impédances de sortie par rapport à la terre devront être égales.

Domaine d'application :

Les caractéristiques électriques spécifiées dans l'interface V.11 sont applicables aux circuits de jonction fonctionnant à des débits binaires pouvant atteindre 10 Mbit/s, qui sont prévus pour être utilisés en premier lieu dans les équipements de terminaison du circuit de données (ETCD) et équipements terminaux de traitement de données (ETTD) faisant usage d'une technologie en circuit intégrés.

Bien que les circuits de jonction symétriques soient conçus en premier lieu pour fonctionner aux débits binaires supérieurs, on peut être contraint de les employer même aux débits inférieurs dans les cas suivants:

- Quand le câble d'interconnexion est trop long pour qu'un circuit dissymétrique fonctionne correctement,
- Quand des sources extérieures de bruit rendent impossible le fonctionnement d'un circuit dissymétrique,
- Quand il est nécessaire de réduire les brouillages avec d'autres signaux.

L'équipement en service de chaque côté de l'interface peut comprendre des générateurs et des récepteurs, combinés d'une façon quelconque .En conséquence, la représentation symbolique du circuit de jonction définit à la fois un point de jonction de générateur et un point de jonction de charge.

Pour les applications de transmission de données, on admet couramment que le câblage de l'interface est fourni par l'ETTD. La ligne de démarcation se situe entre l'ensemble constitué par l'ETTD plus le câble et l'ETCD . Cette ligne est aussi appelée "point de jonction": elle est réalisée matériellement par un connecteur. Ces applications exigent également des circuits de jonction pour les deux sens.

Conseils sur les contraintes d'utilisation imposées par les paramètres du câble telles que sa longueur, sa symétrie et les impédances de fermeture.

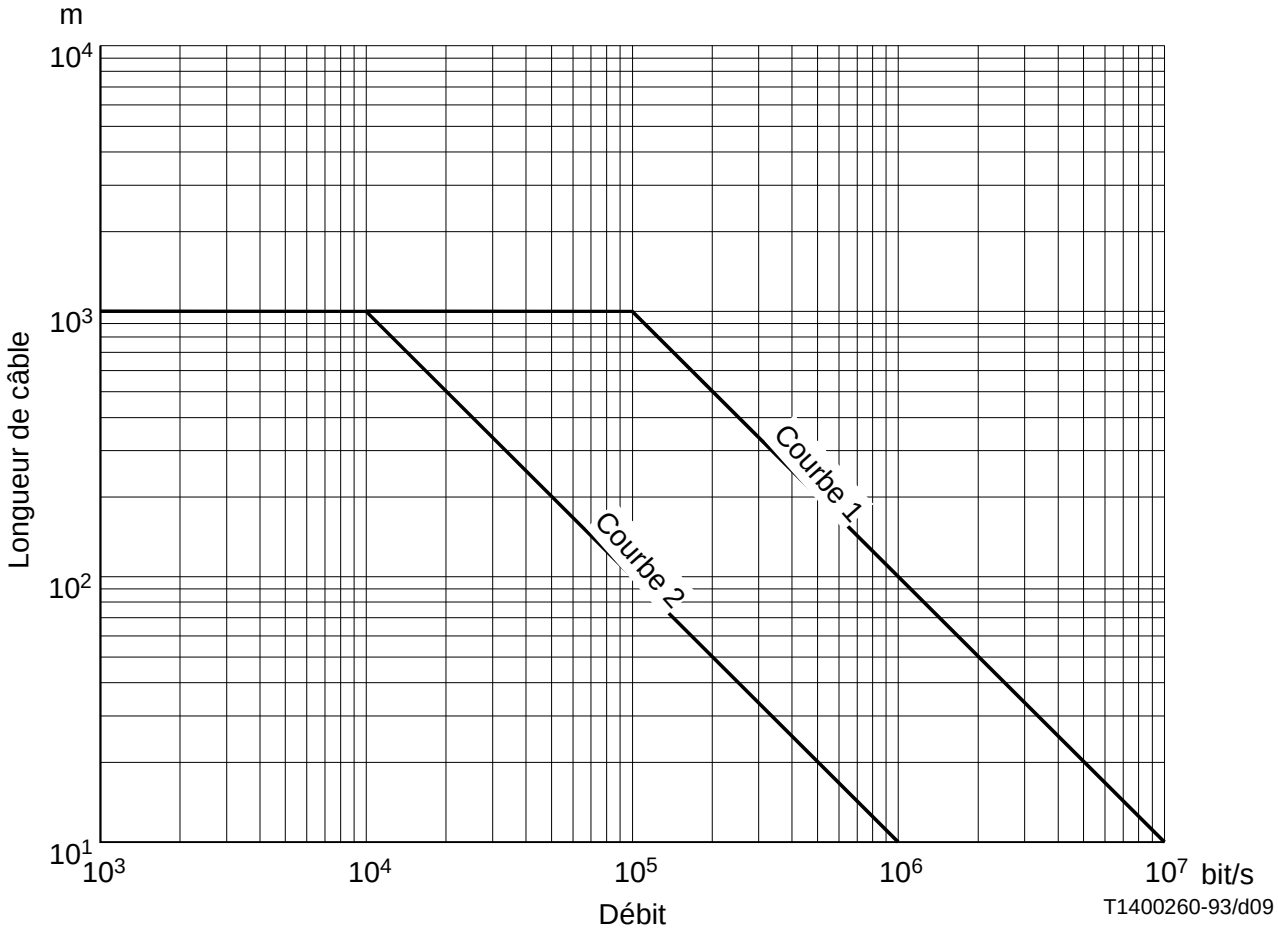
Câble :

Sur toute la longueur du câble, les deux conducteurs devraient présenter essentiellement les mêmes valeurs de:

- Capacité par rapport à la terre;
- Résistance et inductance;
- Coefficients de couplage avec les circuits ou câbles adjacents.
- Longueur des câbles

La longueur maximale admissible pour le câble connectant le générateur et la charge dans une application point à point est fonction du débit. De plus, elle dépend de la distorsion du signal que l'on peut tolérer et des conditions extérieures telles que la différence de potentiel entre les terres et le bruit induit le long du câble. Une augmentation de la distance entre le générateur et la charge risque d'accroître le danger de faire face à une différence de potentiel entre les terres.

Pour illustrer ces conditions, le schéma suivant peut être utilisée comme aide à la détermination de la longueur de câble en fonction du débit.




Courbe 1 Circuit de jonction utilisant un dispositif de terminaison
Courbe 2 Circuit de jonction n'utilisant pas un dispositif de terminaison

Ces courbes ont été établies à partir de données empiriques obtenues en utilisant un câble téléphonique à paires torsadées (de diamètre 0,51 mm) avec ou sans dispositif de terminaison constitué par une résistance de 100 Ohms. Les limites de longueur de câble indiquées sur ces courbes sont basées sur les hypothèses suivantes concernant la qualité du signal à l'entrée de la charge:

- Temps de montée et de descente du signal inférieurs ou égaux à la moitié de la durée d'un élément de signal;
- Un affaiblissement maximal de la tension, entre générateur et charge, inférieur à 6 dB.

Pour les débits les plus élevés, la pente des courbes montre les limitations apportées à la longueur de câble par les conditions imposées sur les temps de montée et de descente du signal. La longueur de câble a été arbitrairement limitée à 1000 mètres par l'affaiblissement maximal de 6 dB.

Il est supposé, dans ces courbes, que les contraintes extérieures spécifiées dans la présente sont remplies. Aux débits les plus élevés, ces conditions sont plus difficiles à remplir à cause des imperfections du câble et du bruit de mode commun. En restant dans les limites de débits et de distances de la Figure ci-avant, on est assuré généralement que la distorsion du signal sera acceptable à l'entrée du récepteur. Cependant, de nombreuses applications peuvent tolérer une distorsion beaucoup plus élevée et, dans ces cas, on peut employer des longueurs de câble plus grandes que celles indiquées.

L'expérience a montré que, dans nombre de cas pratiques, la longueur du câble aux faibles débits peut atteindre plusieurs kilomètres.

Dans le cas d'une transmission synchrone, quand les signaux de données et de rythme sont transmis dans des directions opposées, il peut être nécessaire d'ajuster leurs phases respectives pour satisfaire aux exigences de la qualité des signaux aux points de jonction.

Dispositif de terminaison du câble

L'utilisation d'une résistance de terminaison de câble (Zt) est optionnelle et dépend de l'application spécifique. Aux débits les plus élevés (au-dessus de 200 kbit/s) ou à tout débit où le temps de propagation sur le câble est de l'ordre de grandeur de la moitié de la durée d'un élément de signal, un dispositif de terminaison devrait être utilisé afin de conserver le temps de montée du signal et de réduire les réflexions. L'impédance de terminaison devrait être adaptée aussi bien que possible à l'impédance caractéristique du câble dans tout le spectre de fréquences du signal.

En général, une résistance comprise entre 100 et 150 Ohms donnera un fonctionnement satisfaisant, les plus hautes valeurs permettant de diminuer la puissance dissipée.

Aux débits inférieurs, la distorsion et le temps de montée ne sont pas critiques et il peut être intéressant de ne pas placer de dispositif de terminaison afin de diminuer la puissance dissipée dans le générateur.

**V.24 -** Jonction définie par le CCITT - Spécifications des circuits de jonction entre l'ETTD et l'ETCD. La norme V.24 définit par le CCITT est assez semblable à la norme RS-232C définie par l'EIA (Electronic Industries Association, organisation de constructeurs américains). L'avis V.24 du CCITT définit les spécifications fonctionnelles de la jonction (et l'avis V.28* les caractéristiques électriques des signaux de la jonction).

L'avis V.24 s'applique aux circuits de jonction entre l'ETTD et l'ETCD, pour le transfert des signaux de données bivalents, de signaux de commande et de signaux base de temps.

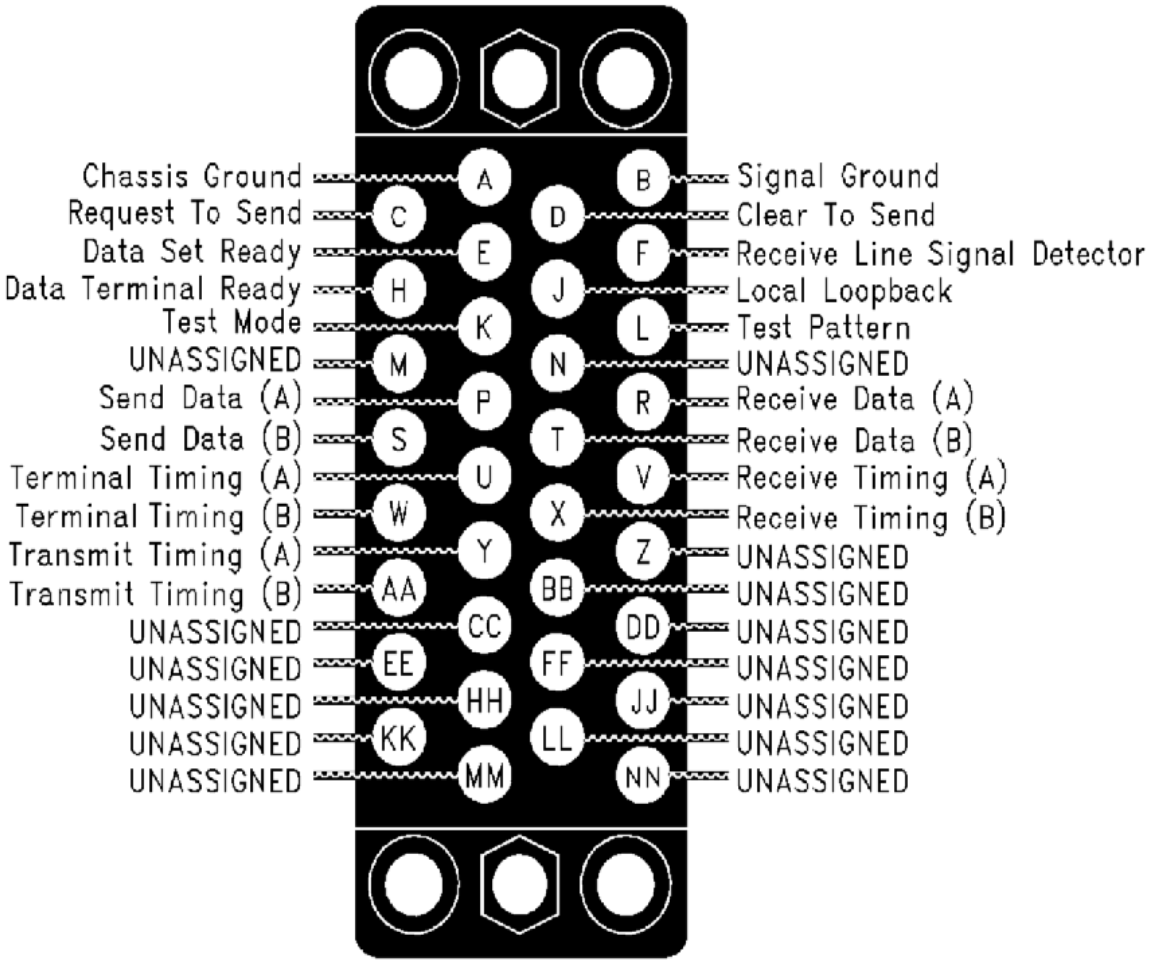
L'ensemble des circuits de jonction s'applique par exemple :

- Aux transmissions de données synchrones et asynchrones,
- Aux transmissions de données dans le service sur réseau avec commutation à deux ou à quatre fils,
- Aux services de transmission de données sur lignes louées à deux ou à quatre fils, dans l'exploitation entre deux points ou entre points multiples,
- Lorsque les câbles de connexion utilisés entre l'ETTD et l'ETCD sont courts.

ETCD peut comprendre des convertisseurs de signaux, des générateurs de signaux de base de temps, des régénérateurs d'impulsions ainsi que des circuits de commande et des équipements chargés d'autres fonctions (protections contre les erreurs, appel et réponse automatique).

* V.28 De façon générale, les caractéristiques électriques spécifiées dans cette norme s'appliquent aux circuits de jonction pour des débits binaires inférieurs à 20 kbit/s. Le Circuit de jonction est indépendant du fait que le générateur est installé dans l'ETTD et la charge dans l'ETCD ou vice versa.

**V.35 -** Jonction définie par le CCITT - Transmissions des données à haut débit. La jonction V.35 est utilisée pour la transmission des données à haut débit (48 Kb/s) au moyen de circuits en groupe primaire de 60 à 108 Khz. Il s'agit dans cette Recommandation d'un système particulier utilisant une onde pilote à 104,08 Khz.




**Interface physique V35**

Les principales caractéristiques recommandées pour l'exploitation simultanée dans les deux sens de la transmission sont les suivantes :

Entrée /sortie - Données binaires séries sous forme rectangulaire

Débit binaire de transmission - Le mode de transmission préféré est le mode synchrone avec un débit binaire de 48000 ± 1 bit/s. Les exceptions suivantes sont admises :

- Transmission synchrone avec débit binaire de 40800 ± 1 bit /s ;
- Transmission asynchrone de fac-similé bivalent, de nature essentiellement aléatoire, avec des éléments d'une durée comprise entre 21 microsecondes et 200 millisecondes.

Embrouillage et désembrouillage

Il convient d'embrouiller les données synchrones pour éviter des restrictions du format d'entrée des données. Ces restrictions pourraient être imposées par la nécessité de disposer de transitions suffisantes pour assurer la stabilité de l'horloge du récepteur évitant de répéter de courtes séquences de signaux de données qui entraîneraient un niveau élevé des composantes sur fréquences discrètes dans le signal de ligne. Il convient que les données synchrones soient embrouillées et désembrouillées au moyen des dispositifs logiques.

L'utilisation d'une porteuse pilote est nécessaire pour assurer une démodulation homochrone. Pour simplifier le problème de la reconstitution de la porteuse pilote aux fins de démodulation, il convient de modifier le signal de données binaires séries. Le signal émis doit avoir une fréquence porteuse du signal de données de 100 ± 2 Khz, un niveau nominal du signal de base de données codées à 48 kbit/s, avec porteuse supprimée et transposition de fréquence dans la bande de 60 à 104 Khz, équivalent à -5 dBm,…

**Valence -** Nombre d'états significatifs d'un signal.

**VAN -** Value Added Network - Equivalent anglo-saxon de RVA, Réseau à Valeur Ajoutée.

**VBR -** Variable bit rate - Debit variable - Informations qui peuvent être représentées digitalement par un ensemble de bits (par opposition à un flux). La plupart des applications de données génèrent du trafic VBR qui peut tolérer des flux de sortie avec des délais variables.

**VC -** Virtual Container - Conteneur virtuel qui regroupe les signaux encapsulés et un pointeur.

**VCC -** Virtual Channel Connexion - L'acheminement des cellules dans un réseau ATM se fait par établissement préalable d'une connexion de voie virtuelle de bout en bout entre les intervenants de la communication (source et destinataire).

Le protocole d'établissement d'une connexion fait partie d'un plan de signalisation. Les connexions sont établies de bout en bout et peuvent être établies en mode point à point ou point à multipoint, unidirectionnelles ou bidirectionnelles (dans ce dernier cas, symétrique ou asymétrique en terme de bande passante ).

L'identification d'une connexion virtuelle se fait donc par deux champs de l'entête de la cellule:

- VCI : identifie les connexions allouées dynamiquement,
- VPI : identifie les connexions statiques (semi-permanentes). Le champ VPI est codé sur 8 ou 12 bits et permet ainsi 256 ou 4096 conduit virtuels.

**VCD -** est calé une fois pour toutes à 1182400 Bits/s en MPEG1, et pas de VBR (Variable Bit Rate). Il offre 80 minutes de Video sur un CD-R 700.

**VCI -** Virtual Channel Identifier - Identificateur (ainsi que le lien emprunté) enregistré au moment de l'établissement dans VCL dans chaque noeud traversé par la connexion, dans une table de translation. Cet identificateur de voie virtuelle identifie les connexions allouées dynamiquement. Avec 16 bits, le champs VCI autorise jusqu'à 64000 connexions de voie virtuelle pour chaque conduit;

Les valeurs des VCI en entrée et en sortie du commutateur sont enregistrées avec les informations de routage dans une table de translation. Lors de la commutation d'une cellule, le commutateur effectue la translation des valeurs de VCI en même temps qu'il route la cellule sur le lien adéquat en sortie.

Comme plusieurs dizaines de milliers de connexions virtuelles peuvent traverser un commutateur, la table de translation peut occuper un espace mémoire considérable et le temp de recherche à l'intérieur de la table devenir important. Pour pallier cet inconvénient, les connexions virtuelles de l'utilisateur sont multiplexées dans des connexions de conduit virtuel ( VPC - Virtual path Connection )

**VCL -** Virtual Chanel Link - Connexion virtuelle ATM - Concaténation de tronçons de voie virtuelle juxtaposés. Un tronçon de voie consiste à choisir le chemin que doit emprunter la connexion virtuelle dans le réseau en fonction de ses besoins en bande passante et des ressources disponibles. Une fois la connexion établie, les cellules transmises sont transférées en séquences sur le chemin tracé.

La connexion virtuelle est identifiée sur chaque tronçon de voie virtuelle par un identificateur de voie virtuelle appelé VCI

**VDI -** Voix Données Images.

**VDSL -** Very high bit rate Digital Subscriber Line - Système numérique à très haut débit (symétrique ou asymétrique) pour ligne métallique d'abonné. Plusieurs systèmes de modulation et de débits utiles sont proposés à la normalisation internationale.

**VDSL2 -** Very high bit rate Digital Subscriber Line 2. Cette évolution de la technologie VDSL offre des débits très élevés (jusqu'à 100 Mbit/seconde) sur de courtes distances. Cette technologie est complémentaire des fibres optiques utilisées dans les réseau FFTH.

**VDU -** Visual Display Unit - Unité d'affichage - Désigne un écran d'ordinateur.

**VGA -** Vente en Gros de l'Abonnement téléphonique - Type d'inscription en dégroupage total permettant de s'affranchir d'une ouverture de ligne FT. Cette inscription est à utiliser lorsque le logement n'a jamais eu de ligne de téléphone, ou que cette même ligne est résiliée depuis plus de 3 mois.

**VHE -** Virtual Home Environment - Emulation d'Environnement Domestique - Dans la technique UMTS, quel que soit le réseau d'accès auquel l'utilisateur se connecte, VHE lui permettra de retrouver son environnement personnel (fil d'actualités, messagerie, langue, etc.).

**VHS -** Format de vidéo de 240 points par lignes .Voir SVHS

**Vidéo (ou Streaming) -** Transmission unidirectionnelle de contenus vidéo et audio par Internet. La vidéo peut s'effectuer point-à-point ou d'un point d'origine à plusieurs récepteurs. Plusieurs stations de radio diffusent leurs émissions sur Internet, et les émissions vidéo ne cessent de gagner en popularité. Le streaming est également possible sur réseaux mobiles à large bande passante.

**Video8 -** Système vidéo utilisant une bande de 8 min. Les enregistreurs Vidéo-8 génèrent un signal composite.

**Vidéocommunication -** Ensemble des techniques de communication utilisant l'image sous sa forme électronique.

**Vidéoconférence -** Technique de réunion à distance utilisant un réseau de télévision pour mettre en relation les participants.

**Vidéodisque -** Disque permettant de stocker des informations (images, vidéo,...) sous forme analogique.

**Vidéopad -** Dispositif d'assemblage-désassemblage de paquets permettant au trafic provenant de terminaux vidéotex d'être transporter sur un réseau à commutation de paquets X25.

**Vidéotex -** Technique de communication utilisant le réseau téléphonique pour transmettre des images ou des pages d'écran (en France le service Télétel).

Système permettant à la demande de l'utilisateur la visualisation sur un écran de télévision de pages d'informations codées sous forme numérique et stockées dans une base distante.

Vidéographie dans laquelle le réseau des télécommunications assure la transmission des demandes de l'usager et des messages obtenus en réponse.

**Vidéotransmission -** Service de diffusion de programmes télévisuels spécifiques projetés sur grand écran dans des salles de spectacle ou de conférence.

**VIP -** Visual Information Projection - Nom de la procédure utilisée par Bull sur certains grands et moyens systèmes. Il s'agit d'une procédure orientée caractère fonctionnant en mode synchrone, bidirectionnelle, et selon un schéma maître-esclave. Elle utilise le code ASCII et un système de détection d'erreurs basé sur la parité longitudinale.

**Virtuel -** Logique - Qui ne correspond pas à une configuration physique déterminée. Ainsi, un circuit virtuel sera un circuit dont on ne connaît pas le cheminement physique exact, celui-ci étant déterminé par la lecture d'informations d'adresses accompagnant le message lui-même.

**Virus -** Programme informatique destiné à endommager un matériel et/ou dégrader les informations qui s'y trouvent, et capable de s'auto-dupliquer.

Les virus se déclinent par type :

- Les virus de boot : propagés généralement par les disquettes, ce type de virus infecte le secteur d'amorçage d'un support physique tel que dur, disquette, etc. En se positionnant sur cet emplacement, le virus de boot s'active donc au démarrage de l'ordinateur, avant même le chargement du système Il s'octroie ainsi un contrôle important sur l'ordinateur et peut occasionner des dégâts qui vont de la destruction de fichiers au reformatage complet des disques durs. La plupart des ces virus ne fonctionnent fort heureusement plus sur les systèmes d'exploitation actuels et tendent progressivement à disparaître.
- Les vers (ou Worms) sont des programmes dont la principale particularité est leur capacité à se reproduire. Ils n'ont pas besoin de support physique pour se propager car ils se déplacent en utilisant les mécanismes du réseau, dont notamment la messagerie qui constitue son support de prédilection. Ils utilisent des pièces jointes qui contiennent des instructions pour récupérer l'ensemble des adresses du carnet d'adresse du client de messagerie et qu'ils utilisent ensuite pour "s'auto-propager". Ils peuvent également s'installer lors du téléchargement d'une image ou via le code incorporé dans le courrier électronique On peut aisément se protéger de ces virus en refusant systématiquement les pièces jointes et en paramétrant son client de messagerie pour consulter et écrire ses courriers au format texte uniquement.
- Les chevaux de Troie (ou Trojans) ne sont pas en soi des virus mais ils sont propagés par des virus ou des logiciels (freewares en téléchargement, etc…). Il s'agit de programmes qui, une fois installés sur un poste de travail ou un serveur, ouvrent des ports de la machine, permettant ainsi à l'émetteur du cheval de Troie de prendre le contrôle de la machine à distance. Dangereux, ces programmes peuvent servir dans le cadre d'espionnage mais également à des fins de spam par exemple; le serveur de messagerie d'une société devenant alors le relais des spammeurs.
- Les Dialers utilisent le système infecté pour composer à l'insu de son propriétaire des numéros de téléphone.
- Les faux virus (ou hoax) sont en fait des rumeurs de propagation de virus imminente véhiculées généralement par des courriers électroniques dans le but d'inquiéter ou nuire à son destinataire. Inoffensifs, ces virus n'en déclenchent pas moins un surplus de trafic à gérer par le serveur de messagerie.

**Virus polymorphe -** Virus dont l'apparence change à chaque infection. Le corps du virus est chiffré avec une clé différente, et la routine de déchiffrement, restée en clair, est modifiée aléatoirement en insérant des instructions parasites ou choisies parmi des routines connues.

**Visioconférence -** Système de télécommunication entre plusieurs groupes de personnes, fondé sur la transmission d'images animées et de sons par l'intermédiaire de liaisons numériques à faible débit (inférieure à 2 Mbits/s). Le rythme et la définition des images vidéo dépendent du débit de la liaison numérique et sont inférieurs à la qualité habituelle des images de télévision.

Visioconférence - Le zoo des normes Née dans le monde des télécommunications, la visioconférence a investi celui de l'Internet. Elle définit les bases de l'architecture en trois couches qui sera utilisée plus tard

dans le media streaming:

- Un codec (compresseur/décompresseur) audio et un codec vidéo.
- Un packetiser (formatage des données) audio et un packetiser vidéo.
- Un protocole de transport et de signalisation.

Les normes ITU - L'ITU (International Telecommunication Union) est l'organisme normalisateur qui a établi les standards pour la visioconférence. Les deux séries qui nous concernent, G et H, pour des raisons qui nous échappent, ne sont consultables que par les abonnés.

Les normes "chapeau": H.320, H.321, H.323

- H.320 - Narrow-band visual telephone systems and terminal equipment (norme adaptée aux télécommunications (lignes téléphoniques)).
- H.321 - Adaptation of H.320 visual telephone terminals to B-ISDN environments (adaptation de la norme H.320 au réseau de téléphonie numérique ISDN (RNIS en France)).
- H.323 - Packet-based multimedia communications systems (norme adaptée aux réseaux locaux type Ethernet).

Les normes "video": H.261, H.263

- H.261 - Video codec for audiovisual services at p x 64 kbit/s (vise le RNIS (s'assemble donc avec H.321)).
- H.263 - Video coding for low bit rate communication (adapte H.261 aux bas débits (POTS)).

Les normes "audio": G.711, G.721, G.722, G.726 à G.729

- G.711 - Pulse code modulation (PCM) of voice frequencies
- G.721 - 32 kbit/s adaptive differential pulse code modulation (ADPCM)
- G.722 - 7 kHz audio-coding within 64 kbit/s
- G.722.1 - Coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss
- G.722.2 - Wideband coding of speech at around 16 kbit/s using adaptive multi-rate wideband (AMR-WB)
- G.726 - 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)
- G.727 - 5-, 4-, 3- and 2-bit/sample embedded adaptive differential pulse code modulation (ADPCM)
- G.728 - Coding of speech at 16 kbit/s using low-delay code excited linear prediction
- G.729 - Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)

Les normes "transport": H.221 à H.245

- H.221 - Frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices
- H.222 - Frame structure for 384-1920 kbit/s channels in audiovisual teleservices
- H.223 - Multiplexing protocol for low bit rate multimedia communication
- H.224 - A real time control protocol for simplex applications using the H.221 LSD/HSD/HLP channels
- H.225 - Call signalling protocols and media stream packetization for packet-based multimedia communication systems
- H.226 - Channel aggregation protocol for multilink operation on circuit-switched networks
- H.230 - Frame-synchronous control and indication signals for audiovisual systems
- H.231 - Multipoint control units for audiovisual systems using digital channels up to 1920 kbit/s
- H.242 - System for establishing communication between audiovisual terminals using digital channels up to 2 Mbit/s
- H.243 - Procedures for establishing communication between three or more audiovisual terminals using digital channels up to 1920 kbit/s
- H.244 - Synchronized aggregation of multiple 64 or 56 kbit/s channels
- H.245 - Control protocol for multimedia communication

Les deux normes importantes sont H.225 et H.245.

H.225 décrit le format des media audio/video, le packetiseur (découpage) et leur synchronisation.

H.245 décrit l'ouverture et la fermeture des canaux pour les medias et la negociation des formats.

Lors du passage Internet, elles seront transposées en normes IETF.

Les formats standards: CIF

Il s'agit tout simplement d'abbréviations pour les dimensions d'image couramment utilisées. Ces valeurs optimisent certains des algorithmes de compression/décompression.

- CIF: Common Interchange Format (352 x 288)
- QCIF: Quarter CIF (176 x 144)
- SQCIF: Sub quarter CIF (128 x 96)
- 4CIF: 4 x CIF (704 x 576)
- 16CIF: 16 x CIF (1408 x 1152)

Le mécano ITU

Les normes "chapeau" ("umbrella") sont des assemblages de normes de niveau inférieur. Ainsi :

- H.320-1 = H.261 (QCIF 7.5fps) + G.711
- H.320-3 = H.261 (CIF 30fps) + G.711 ou 722 ou 728
- H.323 = H.261 ou 263 + G.711 ou 722, 723, 728, 729

Le tableau suivant (tiré de http://www.ktln.com/Technical/pdfs/h323-2.pdf) résume ce mécano. Les normes T concernent le partage d'informations non audio-visuelles (applications du type whiteboard).

| | ISDN | Ethernet | POTS | ATM | Iso-Ethernet |
|---|---|---|---|---|---|
| | (H.320) | (H.323) | (H.324) | (H.321) | (H.322) |
| Video | H.261 | H.261 | H.261 | H.261 | H.261 |
| | | H.263 | H.263 | | |
| Audio | G.711 | G.711 | G.723 | G.711 | G.711 |
| | G.722 | G.722 | | G.728 | G.722 |
| | G.728 | G.728 | | | G.723 |
| | | G.729 | | | G.728 |
| | | G.728 | | | |
| Data | T.120 | T.120 | T.120 | T.120 | T.120 |
| | | | T.434 | | |
| | | | T.84 | | |
| Multiplex | H.221 | H.225 | H.223 | H.221 | H.221 |
| Signaling | H.230 | H.230 | H.245 | H.230 | H.230 |
| | H.242 | H.242 | | H.242 | H.242 |
| Multipoint | H.243 | N/A | N/A | H.243 | H.243 |

Les normes IETF

L'IETF (Internet Engineering Task Force) agit de son côté sur Internet. Il n'entre donc pas dans sa mission de se préoccuper du codage/décodage des informations audio-visuelles (codecs). Par contre, il prend le relais de l'ITU lorsqu'il s'agit de transporter ces données sur un réseau IP.

Deux lots de RFC distinctes prennent le relais de la série H.221-H.245 de l'ITU. Le premier est le "vieux" (1996) protocole RTP destiné au transport de données temps-réel. Le second est l'ensemble session SIP (1999), équivalent de ce qu'on appelle "signalisation" en téléphonie.

Les normes "protocole" et "payload": RTP

- rfc1889 - RTP: A Transport Protocol for Real-Time Applications.
- rfc2032 - RTP Payload Format for H.261 Video Streams.
- rfc2190 - RTP Payload Format for H.263 Video Streams.
- rfc2429 - RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video
- rfc3047 - RTP Payload Format for ITU-T Recommendation G.722.1.

Les normes "session": SIP

- rfc2543 - SIP: Session Initiation Protocol.
- rfc2848 - The PINT Service Protocol: Extensions to SIP and SDP for IP.
- rfc2976 - The SIP INFO Method.
- rfc3050 - Common Gateway Interface for SIP.
- rfc3087 - Control of Service Context using SIP Request-URI.
- rfc3104 - RSIP Support for End-to-end IPsec.
- rfc3105 - Finding an RSIP Server with SLP.
- rfc3219 - Telephony Routing over IP (TRIP).

Ce double héritage, riche à l'indigestion, est celui qui compose la visioconférence sur Internet aujourd'hui. Le passage du monde des télécommunications à celui des réseaux IP a exigé la transposition des nomes conçues pour les circuits commutés (ITU) vers d'autres conçues pour les réseaux à commutation de paquet (IETF). Cette transposition entre des concepts souvent non superposables a produit un résultat lourd et par endroits ambigu.

En particulier, la transposition à TCP/IP de H.225 (et son protocole Q.931) et H.245 pour ouvrir la session et négocier les canaux de transmission et capacités des terminaux, est source d'incompatibilités et interfère sérieusement avec les architectures orientées vers la sécurité (pare-feu, translation d'adresse).

Il est assez probable que nous vivions une situation intérimaire avant que la visioconférence et autres applications collaboratives ne soient totalement harmonisées avec l'architecture TCP/IP.

**Visiophone -** Equipement terminal permettant de transmettre en même temps la voix et l'image vidéo d'un correspondant.

Appareil permettant aux deux interlocuteurs d'une communication téléphonique d'obtenir sur un écran l'image animée de leur correspondant.

**VLAN -** Virtual Local Area Network - Réseau local virtuel - Il existe deux manières de définir un VLAN :

- On définit un VLAN comme un domaine de broadcast. Cette définition très basique, bien que correcte, ne permet pas de réaliser pleinement la notion de VLAN.
- On définit également un VLAN comme un ensemble de "end-stations ". Cette définition signifie que les VLANs permettent à des postes de travail situés dans des segments physiques différents de communiquer comme s'ils se trouvaient sur un même segment logique.

Par définition, un poste situé sur un VLAN ne recevra que le trafic des stations qui sont sur le même VLAN que lui indépendamment du support physique. Les VLANs reposent sur la commutation, qu'elle soit de niveau 2 ou supérieure. Il n'y a jamais de routage lorsque l'on parle de VLANs.

Il existe différents types de VLAN. A l'origine, les VLANs étaient basés sur les couches 1, 2 et 3 du modèle OSI. Mais on peut aujourd'hui créer des VLANs en établissant des règles sur les couches supérieures à la couche réseau, ce qui permet d'avoir une plus grande flexibilité dans l'organisation de ces VLANs. Il n'y a cependant encore aucune norme standard pour ces derniers, ce qui freine leur déploiement.

Les VLANs de Niveau 1 ou VLAN par port :

Les VLANs de niveau 1, aussi appelé VLAN par port, sont définis par un groupe de port d'un ou plusieurs équipements réseaux. Il s'agit donc de définir des domaines d'appartenance aux différents VLANs par rapport au numéro de ports sur un ou plusieurs commutateurs.

Dans ce cas, pour établir une communication entre 2 stations de VLANs différents, il faut mettre deux interfaces réseaux sur une des deux stations et l'assigner aux deux VLANs. Cette méthode est inadaptée aux réseaux possédant plus de 2 VLANs et aux grands réseaux car il faut alors beaucoup trop de matériel.

Le principal avantage des VLANs par port est leur facilité de mise en place. Les outils d'administrations actuels permettent de définir les VLANs par simple "drag &op "des ports du commutateur dans tel ou tel VLAN. De plus les performances obtenues dans les petits réseaux sont très élevées et le coût des équipements capable de réaliser ce type de VLAN est faible.

Le défaut majeur des VLANs par port est qu'un port ne peut appartenir qu'à un seul VLAN. De plus, tous les éléments présents sur le port sont associés au même VLAN. Un autre défaut des VLANs de niveau 1 est qu'ils requièrent une administration peu flexible car si un utilisateur change de port ou de switch il faut reconfigurer le VLAN en conséquence.

Les VLANs de Niveau 2 ou par adresse MAC :

Les VLANs de niveau 2, aussi appelé VLAN par adresse MAC, sont définis par un groupe d'adresses MAC. Il s'agit donc de définir des domaines d'appartenance aux différents VLANs par rapport à l'adresse MAC de l'équipement actif (ordinateur, imprimante…) et comme les adresses MAC sont définies de façon unique au monde (en théorie…) il est possible de désigner un élément sans confusion.

Le principal avantage de ce type de VLAN est la grande souplesse d'affectation des stations de travail. De plus tous les commutateurs utilisant la création de VLANs de niveau 2 peuvent retenir l'appartenance d'une station à un réseau virtuel quel que soit le lieu physique de la station. Il n'y a donc pas besoin de reconfigurer les appartenances aux VLANs lorsque les stations sont déplacées. Ceci facilite la gestion du VLAN puisqu'il n'est plus nécessaire d'assurer un suivi des éléments une fois que chacun a été affecté à un VLAN. De plus, la configuration graphique grâce aux logiciels des constructeurs peut se faire par des "drag & drop "et facilite ainsi la configuration des VLANs.

Un autre avantage est le gain de bande passante utile pour les stations du groupe : on peut obtenir plusieurs connexions client/serveur dans un VLAN sans diminuer la bande passante des autres VLANs situés sur le même commutateur.

L'un des inconvénients des VLANs par adresse MAC est que leur configuration si elle se fait manuellement peut devenir très fastidieuse dans le cas de grands réseaux. Lorsque le nombre d'éléments devient important cette opération demande une bonne organisation et on ne peut connaître les adresse MAC des nouvelles stations à l'avance, il faut donc mettre à jour constamment les VLANs.

Un autre inconvénient aux VLANs par adresse MAC est que leurs performances baissent considérablement lorsque l'on attribue différents VLANs sur le même port de l'équipement. En effet lorsque des stations de différents VLANs se trouvent sur un même port, le trafic correspondant à chaque VLAN passera sur ce port.

Il existe un dernier inconvénient qui est causé par l'existence d'ordinateurs portables en entreprise et se connectant sur des stations d'accueil. En effet dans ce type de configuration c'est la station d'accueil qui possède une adresse MAC le portable qui s'y connecte appartient alors au VLAN auquel appartient la station d'accueil. Or dans certaines entreprises, ces stations d'accueil sont régulièrement utilisées par différentes personnes de passage ne faisant pas partie du même groupe de travail. Il faut alors constamment changer le VLAN d'appartenance de la station d'accueil.

Les VLANs de Niveau 3

Les VLANS de niveau 3 sont définis depuis les en-têtes des paquets réseaux. Ce type de VLAN utilise seulement les informations contenues dans l'en-tête des paquet et n'effectue aucun travail de routage. Le but est en effet de pouvoir identifier les individus d'un VLAN pour savoir où envoyer les informations, et en fait délimiter les différents domaines de broadcast. Il ne s'agit ici en aucun cas de faire du routage, puisque les VLANs dans l'environnement commuté sont en accord avec l'algorithme du "Spanning Tree Protocol ". Les trames passant dans les différents switches sont donc commutées. Il existe deux types de VLANs de niveau 3 :

- Les VLANs par sous-réseaux. L'appartenance aux VLANs par sous-réseau se fait par l'examination des champs adresse des paquets IP. Ce type de VLAN est applicable uniquement avec des protocoles routables puisqu'il est nécessaire d'avoir une adresse de niveau 3.
- Les VLANs par protocole. L'appartenance aux VLANs par protocoles se fait à partir du protocole de niveau 3 utilisé par les stations de travail. L'information utile se trouve dans l'entête de la trame (au niveau 2). La seule lecture de cette information permet donc de déterminer dans quel domaine de broadcast doit être diffusée la trame. C'est le champ type de la trame Ethernet qui est utilisée pour créer les différents VLANs.

Le premier avantage qu'apporte ces VLANs est naturellement la souplesse des configurations abordables. En effet, on peut par exemple isoler des applications qui utilisent des protocoles différents, on peut isoler des stations appartenant à des sous réseaux particuliers et ainsi créer des règles de communications inter-VLANs en fonctions des sous-réseaux. Un avantage qui augmente les possibilités et l'intérêt de ces VLANs est la possibilité de créer plusieurs VLANs sur une même stations Un deuxième avantage est que ces VLANs tout comme les VLANs par adresse MAC laissent les utilisateurs se déplacer physiquement dans le réseau sans qu'il y ait besoins de reconfigurer les VLANs. .

Un autre avantage apporté par l'utilisation des VLANs au niveau 3 est que cela permet d'éliminer le besoin du Frame Tagging utilisé pour la communication inter-switch (toute l'information se situe sur le paquet de niveau 3), réduisant ainsi l'overhead.

Le principal désavantage des VLANs de niveau 3 est la baisse des performances. En effet, le fait d'inspecter l'adresse de niveau 3 dans les paquets nécessite plus de temps que d'inspecter l'adresse MAC dans les trames. Le second inconvénient vient du fait qu'il n'existe pas de normalisation bien définie pour tout les VLANs de niveau supérieur au niveau 2 du modèle OSI et que donc il reste souvent des incompatibilités lorsque l'on veut créer des VLANs avec du matériel de constructeurs différents. Il y a également un manque de sécurité évident car les utilisateurs peuvent changer de VLANs en changeant leur adresse IP ; il est donc indispensable de vérrouiller cette possibilité aux utilisateurs qui n'ont pas les privilèges d'administrateur.

Le tagging ou "étiquetage "

Le fait d'ajouter un label (un tag en anglais) à une trame pour l'identifier selon un critère non prévu par le protocole de la trame en question s'appelle le "marquage". Il existe deux types de marquage : le marquage implicite et le marquage explicite :

- Implicite : Dans ce cas le marquage n'ajoute pas d'informations dans la trame mais s'appuie sur l'un des champs pour différencier les trames (ex. : la MAC adresse ou le type de protocole utilisé).
- Explicite : Dans ce cas, il y a ajout d'un champ dans l'entête de la trame ou du paquet.

Dans le cas des VLANs, les deux types de marquages sont utilisés et cela est lié à l'absence de norme définitive pour les VLANs.

Pouquoi des VLANs ?

- Augmentation des performances :

La segmentation créée par les VLANs réduit la taille des domaines de broadcast et de ce fait le nombre de collisions sur ces domaines. De plus, les VLANs se basent sur la commutation (et non le routage) pour segmenter les domaines de diffusion ce qui permet un traitement bien plus rapide.

- Réduction des coûts :

L'utilisation de VLANs permet de simplifier l'administration du réseau. A chaque fois qu'un utilisateur change de LAN, il faut modifier l'adresse du poste et certains paramètres des routeurs. Tandis que si un utilisateur change de lieu physique mais pas de VLAN, il peut ne pas y avoir de modifications à faire (sous réserve de disposer de bons outils de gestion des VLANs).

De plus, l'utilisation des VLANs entraîne souvent la réduction du nombre de routeurs nécessaires, or les routeurs sont plus onéreux que les switches.

- Formation de groupes virtuels :

Il est courant de retrouver, dans les entreprises, des groupes de développement, de travail sur un projet spécifique, composés de membres qui viennent de différents départements (production, vente, R & D, etc.).

Ces groupes sont souvent formés pour un temps défini et à courte durée. Dans ce cas de figure, un VLAN pourrait être implémenté (sans avoir à déplacer les individus) pour les besoins ponctuels de ce groupe et ce pour plusieurs groupes différents dans l'entreprise. Ce qui permet de créer des groupes de travail de manière transparente vis-à-vis de l'architecture physique du réseau.

- Gain de sécurité :

Périodiquement, des données sensibles sont envoyées en broadcast sur le réseau par les machines (et plus particulièrement les serveurs). Les VLANs permettent d'isoler les serveurs dans un même domaine de broadcast et de les isoler par service.

Les VLANs apportent donc une grande flexibilité dans la gestion des réseaux ; les utilisateurs pourront être regroupés selon leur centre d'intérêt. Les VLANs sont réalisés sur une architecture commutée et le concept de VLAN est applicable dans un même bâtiment, entre plusieurs bâtiments ou sur un réseau WAN.

**VLR -** Visitor Location Register - Réseau mobile - Enregistreur de localisation des visiteurs. Il mémorise les données concernant l'abonné présent dans la zone qu'il couvre. Il contient une information que le HLR n'a pas : l'identité temporaire de l'utilisateur (TMSI). Lors d'un déplacement l'abonné change de VLR alors qu'il ne changera jamais de HLR.

Base de donné contenant les informations des usagers présents dans la zone de couverture de la MSC à laquelle il est relié.

**VOD -** Video on Demand **-** Se dit des flux de vidéo en pseudo-direct (comme Real Video et Windows Media Player). Il n'est alors plus nécessaire d'attendre que la totalité de la vidéo se charge sur le disque dur pour pouvoir la consulter, grâce à une mémoire tampon astucieuse. Des connexions haut débit sont encore nécessaires pour pouvoir les visualiser avec des dimensions et une fluidité correctes.

Service Internet permettant de visionner un film directement sur sa télévision sans être obligé de le télécharger. Service de télévision interactive permettant à un téléspectateur de visionner un film ou un documentaire à l'heure de son choix.

Ce service peut être proposé sur toutes les infrastructures de transport avec ou sans fil (ADSL ou Réseau sans fil haut débit).

**VoDSL -** Voice Over DSL - Voix sur DSL - Technologie exploitant plusieurs standards, chaque opérateur adaptant à sa convenance les standards qui répondent à son cahier des charges. Certaines recommandations ont été publiées par le DSL Forum, notamment en ce qui concerne la qualité de la voix. Par opposition à la téléphonie sur Internet, VoDSL emprunte en majorité les réseaux privés des opérateurs qui sont de type "qualité de service".

La voix analogique provenant d'un combiné classique est numérisée par un IAD (Integrated Access Device - Modem Routeur ADSL évolué) qui est chargé du traitement de la voix (élimination de l'écho…) puis l'IAD numérise la voix pour qu'elle soit transmise sur la ligne cuivre jusqu'au DSLAM de l'opérateur, puis du DSLAM vers le réseau de l'opérateur, où les données seront transmises vers la destination (DSLAM pour le cas d'un destinataire en VoDSL ou passerelle de conversion vers un réseau téléphonique classique).

**Voie -** Canal de transmission.

**Voie logique -** VL - Logical Channel - En commutation par paquets, moyen de transmission bidirectionnelle simultanée sur une liaison de données. Plusieurs VL peuvent exister sur une même liaison de données par entrelacement des paquets.

**VoIP -** Voix sur IP - Aussi connue sous le nom de téléphonie Internet, est une technologie qui vous permet de téléphoner via un réseau d'ordinateurs basé sur un protocole Internet.Protocole permettant de tenir une conversation téléphonique via Internet. Vous pouvez ainsi vous connecter à votre point de présence local et appeler un correspondant à l'autre bout du monde pour le prix d'une communication locale.

La différence essentielle par rapport à la téléphonie classique est que l'information vocale n'est pas transmise sur un réseau téléphonique via une connexion dédiée mais est divisée en paquets IP à réassembler par le récepteur téléphonique. L'avantage principal par rapport à la téléphonie classique est que la Voix sur IP utilise l'infrastructure réseau existante et donc ne requiert qu'un seul réseau.

Divers protocoles contrôlant la voix et le transfert de données ont été définis de façon à garantir que tous les types de sociétés et toutes les régions du pays puissent mettre en œuvre cette technologie. Les protocoles les plus importants sont le SIP et le H323, le protocole SIP étant la meilleure option pour l'avenir.

L'intérêt porté par les entreprises à l'intégration de la voix sur les réseaux initialement prévus pour les données est tout d'abord un intérêt financier de réduction des coûts. En effet, jusqu'à maintenant, de nombreuses entreprises possèdent deux réseaux complètement distincts : un réseau de données et un réseau téléphonique. La redondance du câblage et les politiques de réduction des coûts de

télécommunication ont entraîné la volonté d'intégrer la voix aux réseaux de données. L'augmentation de la capacité des réseaux de données ainsi que l'apparition sur le marché de produits permettant d'intégrer la voix sur les réseaux de données ont également contribué à l'émergence de ce nouveau besoin.

D'autre part, une telle intégration de plusieurs types de flux dans un même réseau permet de faciliter l'exploitation global des réseaux de télécommunication. De plus, le couplage de la téléphonie avec des applications informatiques permet l'utilisation de nouvelles applications de service telles que les centres d'appels ou de nouvelles applications Web.

L'évolution du paysage réseau / télécom entraîne un déplacement de la problématique : la réduction des coûts de télécommunication et plus particulièrement de la voix fait qu'une des raisons principales de l'évolution des réseaux d'entreprise vers une intégration voix/données est la possibilité d'ajouter des services à la téléphonie d'entreprise.

Néanmoins, bien que les progrès technologiques soient apparemment là, il ne faut pas perdre de vue qu'un passage d'un "double" réseau voix-données à un réseau intégrant ces deux types de flux ne peut se faire qu'à la condition où la qualité de service du nouveau produit soit au moins équivalente à celle de l'ancien produit. En effet, la téléphonie est considérée comme une application critique et l'utilisateur n'acceptera pas une dégradation de la qualité du service de téléphonie : La qualité de service au niveau du transport de la voix est caractérisée notamment par la qualité auditive de la restitution de la voix mais aussi et surtout par la capacité du réseau à respecter la caractéristique d'isochronisme de la voix.

De plus, la téléphonie étant un service dit critique pour les entreprises, la contrainte de disponibilité de ce service doit à tout prix être respectée.

Il faut également souligner le fait que l'intégration de la voix aux réseaux de données ne doive pas dégrader le service initialement rendu par le réseau c'est-à-dire le transport des données. Ceci engendre le respect de conditions de débit utilisé par le service de téléphonie.

Les contraintes techniques liées au transport de la voix par paquets :

- Le délai de transit - Le délai de transit ne doit pas dépasser 200 ms pour transporter la voix dans un réseau télécoms. Les réseaux à relais de trames des opérateurs garantissent un délai de transit inférieur à 100 ms. La variation du délai de transit appelée "gigue" ne doit donc pas dépasser 100 ms. Si l'on peut garantir un transfert en respectant les contraintes temporelles du transfert isochrone (ou en limitant la gigue à des proportions acceptables(>à 100 ms) il est alors possible de rassembler les différents échantillons de voix en paquets de taille constante et d'utiliser la commutation de paquets pour transmettre la voix.
- La compression de la voix et la mise en paquets - Les techniques de compression de la voix apportent une réduction importante de la bande passante en contre partie d'un temps de traitement non négligeable. Il convient alors de perdre le moins de temps possible à numériser et à compresser la voix. L'évolution des algorithmes de compression associée à la puissance des nouveaux processeurs a largement contribué au développement de la voix sur IP.
- La contrainte de temps versus contrôle d'erreurs - Incompatible avec les mécanismes de retransmission en cas d'erreur, la voix sur IP n'a pas les mêmes contraintes que le transport de données. Les meilleurs algorithmes de compression de la voix utilisent un codage de base qui représentent très peu de données à transmettre, donc statistiquement moins exposées aux erreurs. En cas d'erreur de transmission, le timbre de la voix est temporairement affecté mais la communication reste intelligible.
- Le phénomène d'écho - Le poste de l'usager est raccordé par deux fils (boucle locale) alors que la liaison distante est généralement réalisée en quatre fils (une paire émission et une paire réception). Le passage de deux à quatre fils est réalisé par un transformateur différentiel. Si l'adaptation d'impédance est mal réalisée, une partie de l'énergie est réfléchie. Ce phénomène s'appelle l'écho. L'écho local est peu gênant. Par contre, à partir d'un certain délai de transmission, fonction de la distance séparant les deux PABX, l'écho distant peut devenir gênant. Supérieur à 45 ms, il constitue un véritable trouble de la conversation. Ce phénomène ne pouvant être évité lorsque l'on transporte la voix sur un réseau, il convient de l'éliminer à l'aide de suppresseurs d'écho.

Principe du transport de la voix sur des réseaux de données :

La voix doit subir un certain nombre de traitements avant d'être envoyée sur un réseau IP. Elle doit être numérisée, compressée et mise en paquets IP. C'est l'émetteur qui est chargé d'effectuer tous ces traitements. Une fois "paquétisée", la voix est envoyée sur le réseau de transport IP, qui se charge de l'acheminer jusqu au destinataire. Les paquets IP circulant indépendamment les uns des autres peuvent arriver dans le désordre. Le récepteur devra donc les replacer dans le bon ordre. De plus, sachant qu'ils arriveront probablement à des intervalles différents de ceux dans lesquels ils ont été émis, il faudra les re synchroniser afin que la voix rendue soit fluide et constante. Le récepteur est donc chargé de bufferiser les paquets IP reçus afin de rattraper la gigue. C'est seulement après cette étape de reconstitution du flux que les paquets suivront le traitement de restitution : remise en forme, décompression, conversion en analogique, amplification et diffusion dans l'écouteur ou sur les haut-parleurs.

Les différentes configurations :

Pour transporter la voix sur un réseau IP, il existe plusieurs configurations :

- Liaison PC-PC - Ce type de liaison repose sur l'utilisation de logiciels de téléphonie. Il en existe une multitude sur le marché qui sont malheureusement incompatibles entre eux (les standards H323, T.120 et le protocole SIP devrait très rapidement améliorer cela). Cela signifie que pour l'instant il est préférable de disposer de deux ordinateurs possédant le même logiciel pour communiquer. Un effort d'interopérabilité a été entrepris avec les standards H.323, T.120 conçus à l'origine par l'UIT-T pour la visioconférence sur réseau local ainsi que le standard SIP qui prend de plus en plus d'importance sur es pltes formes.
- Liaison PC-téléphone - Il est également possible à partir d'un PC multimédia d'appeler un correspondant sur son poste téléphonique classique. Cette solution nécessite toutefois la mise en oeuvre d'une passerelle VoIP (Voiceover IP) située au plus près du correspondant final. Cette passerelle permet de faire le lien entre le réseau IP et le réseau de téléphonie classique. Ainsi, lorsque les paquets IP arrivent sur la passerelle, celle-ci se charge de re synchroniser le signal, de le remettre en forme, de le décompresser, de le convertir en un signal analogique et de l'envoyer sur le poste téléphonique du destinataire. Dans un contexte professionnel, la passerelle VoIP peut être directement raccordée au PABX de l'entreprise.
- Liaison téléphone-téléphone - Il est tout à fait possible à partir de son poste téléphonique classique de joindre son correspondant également sur son poste téléphonique en passant par un réseau de données IP, si les deux postes sont rattachés à une passerelle VoIP.
  - Les fonctions de base d'une passerelle VoIP sont : la conversion d'une partie du numéro demandé en adresse IP de la passerelle VoIP la plus proche du destinataire, la connexion qui permet à la passerelle source d'établir une connexion avec la passerelle destination, d'échanger la signalisation nécessaire à cette connexion, la numérisation, la démodulation pour les signaux de fax, la compression, la mise en paquets IP, la décompression, et la remodulation pour les signaux de fax.

Les problèmes techniques classiques :

- Le taux de perte des paquets - Lorsque des réseaux IP sont congestionnés, les équipements qui les composent libèrent de la bande passante (phénomène connu sous l'acronyme de "drop"). Une connexion via un réseau IP peut donc connaître un taux de perte important. Selon la route utilisée, l'éloignement des correspondants, le taux de perte des paquets peut passer de 5% à 50%. Au-delà de 20%, le signal est inaudible ; il a perdu trop d'informations. A débit constant, il n'y a pas de solution pour remédier aux pertes de paquets. Il faut élargir la bande passante pour éviter les congestions et remplacer les réseaux intermédiaires lents par des réseaux de plus fortes capacités. La garantie d'un service fiable et temps réel passe donc par la réservation de ressources dans le réseau par l'intermédiaire d'un protocole adapté, mais il n'y a pas de mmiracles si le réseau est extrèmement chargé.
- Un mode non connecté et non fiable - La contrainte de délai empêche toute tentative d'utilisation de protocole de transport fiable comme TCP. Tous les mécanismes de TCP (accusé de réception, contrôle de flux) sont inutilisables dans le cas d'une communication téléphonique. Les boucles d'allers et retours entre l'émetteur et le récepteur multiplieraient le délai de transmission et le mécanisme de la "fenêtre de congestion" aggrave la gigue.

Plusieurs outils et solutions permettent de retarder l'apparition des problémes classiques rencontrés en VoIP : La mise en œuvre du protocole RTP (protocole de transport temps réel), le passage en Ipv6 avec sa gestion des indices de priorité en natif, mise en œuvre de réservation de ressources via RSVP, et enfin les différentes solution matérielles dédiées à la compression.

**VORBIS -** Société à l'origine du développement d'un ensemble de codecs audio et vidéo libres, pour contrer les tentatives d'extorsion de fonds de certains organismes. Voir le format OGG (audio) pour le moment...

**VoWi-Fi -** Voice Over Wi-Fi - (voir aussi 802.11r) - Technologie hybride résultant du "mariage" des technologies Wi-Fi et VoIP (Voice Over IP). La norme VoWi-Fi exploite les mêmes mécanismes protocolaires que la technologie VoIP (H.323 et SIP) mais ne profite pas des affectations de classes de services Diffserv ou de réservation de flux RSVP. L'IEEE doit transcoder cette technologie dans une variante sous la référence 802.11e.

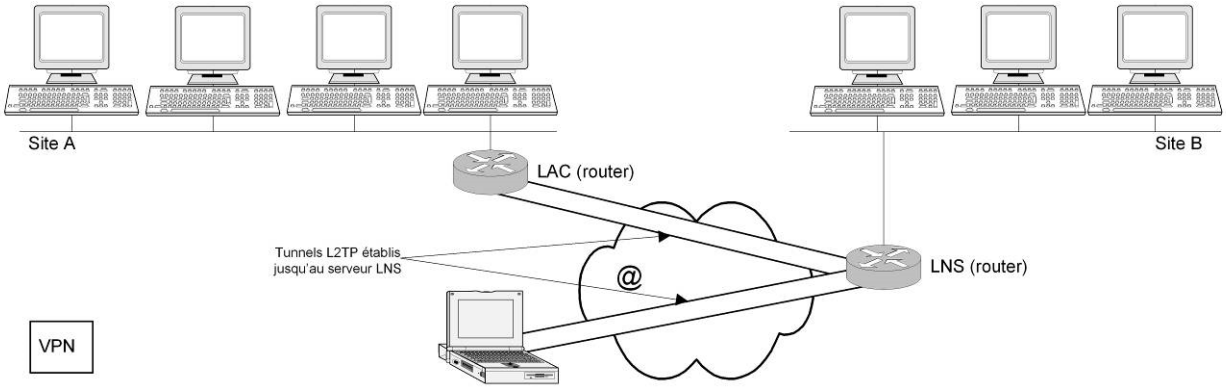
| Tableau de comparaison entre DECT et VoWi-Fi | | |
|---|---|---|
| Service ou fonction | Dect | VoWi-Fi |
| Immunité radio | Bande de fréquence peu sensible aux interférences et dédiée (1,9 GHz). | Bande de fréquence sensible aux interférences et non réservée (2,4 GHz). |
| Garantie de débit et délai | Le canal étant réservé (mode circuit), le débit et le délai sont garantis | Le fonctionnement s'effectue en mode paquet - Pas de mécanisme de QoS. |
| Couverture Radio | La portée des bornes va de 30 mètres en intérieur à 300 mètres en extérieur. | La portée des points d'accès va de 15 mètres en intérieur à 100 mètres en extérieur. |

| | | |
|---|---|---|
| Mobilité | Le roaming est le hand-over sont spécifiés dans le standard Dect | La gestion du roaming et du hand-over sont des protocoles propriétaires |
| Sécurité | L'authentification et le chiffrement sont compris dans le standard. | En attente du protocole de sécurité (2004 ?) 802.11i |
| Coût | Le coût des terminaux est peu élevé mais nécessite un réseau en parallèle | Le réseau peu être mutualisé mais les terminaux restent chers. |
| Terminaux | Terminaux téléphoniques classiques | PDA, téléphones, tablettes PC, … |
| Utilisation | Les terminaux servent uniquement pour la téléphonie | De nombreuses applications sont possibles alliant voix et données, mais aussi vidéo. |

**VPC -** Virtual path Connection - Connexion de conduit virtuel - Contient les faisceaux de voie virtuelle qui sont commutés ensembles comme une seule unité. Comme pour la voie virtuelle, la connexion de conduit virtuel est composée d'une concaténation de tronçons de conduits virtuels (VPL - Virtual Path Link ) juxtaposés. La connexion de conduit virtuel est établie par l'opérateur du réseau de manière permanente. La notion de conduit virtuel est transparente à l'utilisateur.

**VPLS -** Solution de réseau privé permettant de mettre en œuvre du MPLS dans les réseaux d'accès. Le VPLS devrait séduire les grands consommateurs de trafic utilisant des liaisons de type Ethernet métropolitain.

**VPN -** Virtual Private Network - Réseau Privé Virtuel. Terme très souvent utilisé pour désigner un système de communication utilisant une infrastructure public étendue (RTC, INTERNET, Frame Relay, ATM, …) mais dédiée via des circuits permanents. Un VPN peut être encrypté via IPSEC ou tout autre protocole d'encryption de données.




Afin d'interconnecter des réseaux au travers d'un réseau TCP/IP (par exemple Internet), l'encapsulation de leurs protocoles respectifs dans IP est réalisée grâce à L2TP, un autre protocole spécialement conçu pour répondre à ce besoin. Il constitue de fait une extension du protocole PPP: L2TP encapsule en effet du trafic PPP. Il en retient donc le mode de fonctionnement, notamment en ce qui concerne l'authentification. L2TP a été élaboré à partir des protocoles propriétaires PPTP de Microsoft, et L2F (Layer2 Forwarding) de Cisco. L'IETF s'est attaché à prendre le meilleur de ces deux protocoles afin de les inclure dans L2TP. Ce dernier est capable de transporter n'importe quel protocole réseau (IP, IPX, Appletalk...). Il ouvre en fait un tunnel entre deux réseaux ou entre un poste de travail et un réseau au travers du réseau ouvert Internet (voir schéma). Ce protocole est inaccessible depuis l'Internet afin de garantir l'intégrité du réseau de l'entreprise. Les routeurs sont ainsi capables de différencier le trafic d'un RPV du trafic Internet grâce à ce tunnel qui utilise une connexion virtuelle. Il est complètement indépendant du type de média sur lequel il est transporté, du moment qu'il s'agit d'un réseau IP. Afin de fonctionner, ce protocole a besoin de deux choses: un concentrateur d'accès L2TP, ou LAC (L2TP Access Concentrator), et un serveur de réseau L2TP, ou LNS (L2TP Network Server). C'est le concentrateur d'accès LAC qui a la mission de transmettre les paquets entre le système distant et le serveur LNS, ce dernier se situant à la terminaison logique de la connexion. Le protocole L2TP assure donc le dialogue entre ces deux équipements. Le LAC peut très bien être un PC, un routeur ou tout autre équipement capable d'initialiser une connexion L2TP (voir schéma).

Autre point important à prendre en compte lors du déploiement d'un RPV : la sécurité. Savoir que les données vont transiter en clair sur un réseau public n'est pas fait pour rassurer les entreprises. Certaines souhaiteront que les données soient cryptées afin d'échapper aux regards d'éventuels pirates ou de concurrents mal intentionnés. Le standard de l'IETF en la matière est IPsec. Il est le complément naturel du protocole L2TP.

Réseau d'entreprise utilisant INTERNET à la place de liaisons spécialisées ou d'ATM privé et qui, grâce à des techniques puissantes d'authentification et de cryptage garantit un certain degré de confidentialité.

**VPN IP -** Réseaux privés virtuels utilisés pour des accès distants ou l'interconnexion de sites. Ils utilisent l'infrastructure publique Internet (IP) ou le réseau privé IP d'un opérateur via des tunnels et permettent de donner la priorité aux flux d'applications critiques (messagerie, transfert de fichiers...). La sécurité des informations transmises est garantie par un chiffrement et déchiffrement des données aux extrémités du réseau.

**VRRP -** Virtual Router Redundancy Protocol - Gère le basculement automatique d'une plate-forme à une autre au sein d'une installation redondante.

**VSAT -** Very Small Aperture Terminal - Terminal d'émission-réception par satellite de petite dimension. Il permet d'échanger des données à bas ou moyens débits en utilisant une fraction étroite de la capacité totale du satellite. Intéressant dans le cas de sites très dispersés sur une grande étendue ou pour traverser les frontières.

Station terrienne comportant une antenne de petite dimension, destinée à communiquer avec des stations analogues par l'intermédiaire d'un satellite, sous la commande d'une station pivot.

**VTHD - (réseau VTHD) -** Réseau Vraiment Très Haut Débit - Développé pour contrer l'Internet 2 américain, il a été inauguré à l'INRIA en mai dernier. Créé par un consortium qui désire développer de nouvelles applications, construire un réseau performant pour les universités et transférer rapidement les technologies vers les industries.

**Vulnérabilité -** Faille au niveau des procédures de sécurité, de la conception ou la mise en œuvre du réseau, pouvant être exploitée pour contourner la politique de sécurité d'une entreprise.

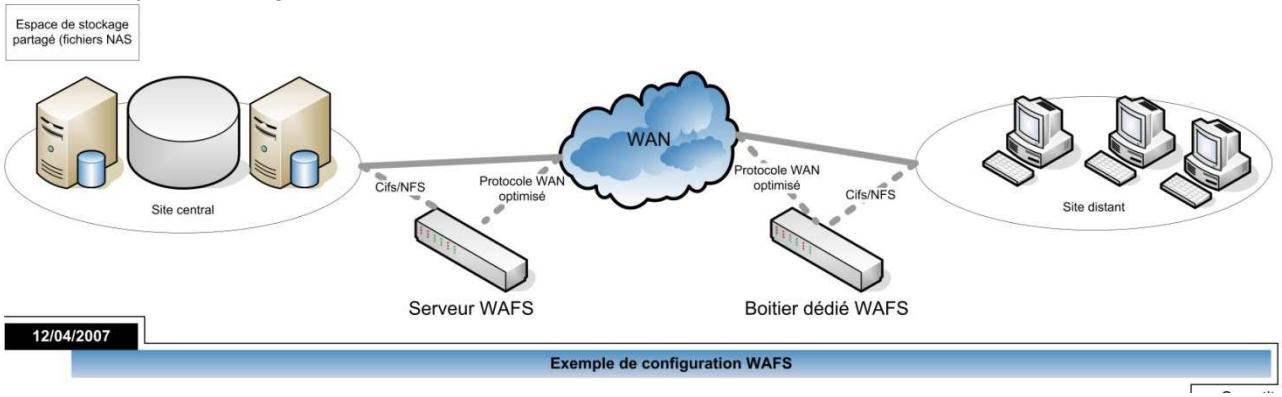
# W

**W3C -** World Wide Web Consortium - Organisme fondé en 1994 par Tim Berners-Lee et chargé de la standardisation sur Internet. Son objectif est la mise au point de normes et de protocoles ouverts et libres, dans un souci d'interopérabilité maximale.

**WAFS -** Wide Area File Services - Technique de virtualisation de fichiers pour réseaux étendus - Pour limiter les phénomènes de latence, la fiabilité aléatoire des réseaux étendus et les liens congestionnés, la technologie WAFS apporte des éléments de réponse en assurant le stockage de fichiers sur un équipement NAS partagé sur le site central et des équipements sur les sites distants.

Une architecture WAFS se décompose en deux éléments : Un serveur sur le site central et un boitier dédié sur le site distant. Chaque élément communique avec les stations clientes et les serveurs de fichiers via un protocole normalisé (ex CIFS ou NFS). Les échanges entres éléments constitutifs du système WAFS se font via un protocole dédié, optimisé pour les WAN, le tout associé à certaines techniques d'optimisation pour limiter les phénomènes ci-avant énumérés.

Voir l'exemple de configuration WAFS ci-dessous :




**WAN -** Wide Area Network - Réseau fédérateur de taille supérieure à celle d'une métropole ou encore Réseau étendu qui englobe des sites géographiquement éloignés les uns des autres. L'expression est peu précise, l'étendue d'un tel réseau pouvant correspondre à quelques bâtiments, à une ville ou à une région. Elle sert surtout pour désigner tout réseau dépassant l'étendue d'un seul établissement physique et constitué par l'interconnexion de plusieurs réseaux élémentaires.

**WAP -** (Wireless Access Protocol): navigateur en format HDML (Handheld Device Markup Language), version allégée de HTML. Protocole permettant un accès à des services interactifs de type Internet, adapté aux contraintes actuelles des réseaux mobiles.

Le WAP est un protocole permettant de faire converser le monde GSM et le monde Internet. Il permet d'adapter le langage Internet à des petits terminaux en allégeant le langage de présentation des données. Ce protocole est développé au sein du WAP forum, fondé en décembre 1997 par Nokia, Ericsson, Motorola et Unwired Planet, qui ont décidé de mettre en commun leur savoir-faire pour faire émerger un standard. Rallié aujourd'hui par près de 90 sociétés au plan mondial (opérateurs, éditeurs de logiciels, constructeurs, etc.), le Wap Forum spécifie le format du contenu Internet ainsi que les protocoles d'accès aux services en ligne depuis les mobiles.

Cette spécification fait l'objet d'un large consensus auprès des acteurs du marché des services en ligne mobile, favorisant ainsi l'émergence d'une norme. La version 1.0 a été délivrée en avril 1998.

Pour en savoir plus : http://www.wapforum.org

**WAPECS -** Concept de plateforme universelle d'accès radio.

**WATTC -** Worldwide Administration Telegraph and Telephone Conference - Conférence mondiale, dans le cadre de l'UIT, des représentants des administrations et des opérateurs des télécommunications. Elle vise actuellement à traduire dans le domaine des télécommunications des orientations du GATT visant à faciliter la commercialisation des services de télécommunications et à alléger le poids des administrations nationales.

**WAV -** Format de sauvegarde pour les signaux sonores, généralement aussi l'extension de fichier pour les fichiers son (*.wav) d'origine Windows.

**WCDMA -** Wideband Code Division Multiple Access - Le concept W-CDMA utilise une technique d'étalement de spectre par séquence directe. Tous les utilisateurs émettent sur un même canal radioélectrique à large bande, mais ils sont distingués par une séquence d'étalement pseudo-aléatoire, appelée code et connue du récepteur. Le débit maximal supporté par un seul code est de 384 kbit/sec. Pour les services à plus haut débit, plusieurs codes sont alloués à un même utilisateur et transmis simultanément sur le même canal radio (par exemple, cinq codes sont nécessaires pour supporter un débit de 2 Mbit/sec). Voir CDMA.

Le WCDMA utilise la bande de fréquence de l'UMTS.

Une variante du WCDMA utilise la bande des 900 MHz. Ceci permet d'obtenir une meilleure couverture mobile à haut débit en zone rurale, en réduisant le nombre de stations terrestres nécessaires. La longueur d'onde plus courte offre aussi une meilleure pénétration des ondes à travers les murs. Des expérimentations sont en cours (février 2006) en France.

**WDM -** Wavelength Division Multiplexing, ou Multiplexage en longueur d'onde. La fibre optique peut transporter plusieurs canaux numériques (de 4 à plusieurs dizaines longueurs d'onde) à haut débit (de 8 Mbit/s à 40 Gbit/s) dans une fenêtre de 1450 à 1650 mm. Lorsque le nombre de canaux par fibre est élevé, on parle de Dense WDM (DWDM). Si l'espace fréquentiel entre canaux est faible, on parle de Thin WDM (TWDM). Voir multiplexage par répartition en longueur d'onde.

Le multiplexage en longueur d'onde consiste à utiliser sur une même fibre optique, plusieurs longueurs d'ondes de manière à accroître de manière souple et économique le débit global transporté. Dès a présent, des équipements permettent de mettre en oeuvre des liaisons a des débits supérieurs a 100 Gbits/s tandis que certains laboratoires de recherches mettent au point des équipements capables d'atteindre des débits supérieurs au Tbits/s.

La technologie WDM est né au début des années 90 de l'idée d'injecter simultanément dans la même fibre optique plusieurs trains de signaux numériques à la même vitesse de modulation, mais chacun a une longueur d'onde distincte.

La norme IUT G692 a défini un peigne de longueurs d'onde autorisées dans la fenêtre de transmission 1530-1565 nm. Elle normalise l'espacement en nanomètre ou en GigaHertz entre deux longueurs d'onde permises de la fenêtre : 200 GHz ou 1,6 nm ou 100 GHz ou 0,8 nm.

La technologie WDM est dite dense (DWDM) lorsque l'espacement utilisé est égal ou inférieur à 100 GHz. Des systèmes à 50 GHz ou à 25 GHz ont déjà été testés.

Les systèmes commercialisés aujourd'hui comportent 4, 8, 16, 32 ou 80 canaux optiques, ce qui permet d'obtenir des débits de 200 Gbps en prenant un débit par canal de 2,5 Gbps. Pour fixer les idées, un système à 16 canaux de 2,5 Gbps permet de transmettre 500 000 conversations téléphoniques sur une seule fibre…

**WEB CALL CENTER -** Technologique permettant de faire collaborer des applications en environnement Web / centre d'appels. Cette technologie permet d'offrir au client différents services mis à sa disposition sur le site Internet de l'entreprise. Ces services peuvent être regroupés selon deux grandes familles : les services de collaboration synchrone et les services de collaboration asynchrone :

Fonctionnalités apportées :

Pour les fonctions synchrone (qui demandent donc une réponse immédiate ou peu tardive à la demande du client) :

- Click to talk : sous la forme d'un bouton inséré dans certaines pages du site Web, l'utilisateur a la possibilité d'entrer directement en relation avec un conseiller clientèle (un télé conseiller dans ce cas ), se trouvant dans un centre d'appel. Pour le conseiller l'appel est reçu de la même façon qu'un coup de fil provenant du réseau téléphonique, à cela près qu'il disposera de plus d'informations sur le client et sa demande grâce à l'utilisation de formulaires électroniques à remplir sur le site. Pour bénéficier de ce genre de fonctionnalités, le client devra disposer d'un ordinateur multimédia capable de gérer les contraintes de la voix sur IP, de même pour le centre d'appels qui devra donc être capable de recevoir et émettre de la voix sous forme de paquets.
- Chat : l'internaute a la possibilité de dialoguer en direct par écrit avec un conseiller du centre de contact. Cette fonction est aisément implémentable, car déjà utilisée dans de nombreux "chat room "sur Internet. L'avantage pour le client est de pouvoir conserver une trace écrite de la réponse du conseiller.
- Borne interactive : après la voix sur Internet, l'étape suivante sera bien évidemment l'ajout de l'image à la parole. Là encore de nombreuses contraintes technologiques devront être résolues avant de pouvoir bénéficier de cette fonction. Néanmoins, l'utilisation de la visioconférence, de moins bonne qualité que la vidéo conférence, est à ce jour possible plus facilement.

Les services de collaboration asynchrones (qui demandent donc une réponse moins immédiate ou différée à la demande du client ):

- Call me back : le centre d'appels reçoit une demande d'appel qui sera routée et traitée lorsqu'un télé conseiller se rendra disponible.
- E-mail : Dans ce cas, la problématique est tout autre : il s'agit d'être garant bien évidemment sur le délai de réponse (qui se mesure au moins en heures et non plus en secondes comme c'est le cas pour un appel téléphonique) et de s'assurer d'autre part de la qualité de la réponse, puisqu'il s'agit dans ce cas de figure d'une réponse écrite faite à un client de l'entreprise.

**WECA -** En dehors des organismes de normalisation, les principaux acteurs de l'industrie du sans fil se sont réunis au sein de la WECA (Wireless Ethernet Compatibility Alliance). La mission de la WECA est de certifier l'interopérabilité et la compatibilité inter fournisseurs des équipements pour réseaux sans fil IEEE 802.11HR, ainsi que de promouvoir ce standard auprès des Grands Comptes, des PME et du grand public. La WECA regroupe des fabricants de semi-conducteurs pour WLAN, des fournisseurs de WLAN, des fabricants d'ordinateurs et des éditeurs de logiciels. On retiendra entre autres 3Com, Aironet, Apple, Breezecom, Cabletron, Compaq, Dell, Fujitsu, IBM, Intersil, Lucent Technologies, No Wires Needed, Nokia, Samsung, Symbol Technologies, Wayport et Zoom.

**WEP -** Protocole de sécurité défini dans la norme 802.11b afin de protéger les couches "physique" et "liaison" du modèle OSI. La couche physique de communication de 802.11 est l'air ambiant : quiconque se trouve dans une zone couverte par un point d'accès peut donc intercepter les échanges. Le protocole WEP chiffre les échanges pour protéger les données transitant sur le WLAN. Cependant, il est considéré comme peu sûr et a été régulièrement cassé.

L'algorithme WEP est un générateur de nombres pseudo aléatoires initialisé par une clef secrète partagée. Le générateur de nombres pseudo aléatoires ressort une séquence de clefs de bits pseudo aléatoires, égales en longueur au paquet le plus large possible, qui, combiné avec des paquets entrants ou sortants produit le paquet transmis par la voie des airs. Cet algorithme est utilisé en WLAN, norme 802.11.

L'algorithme WEP est un simple algorithme basé sur l'algorithme RC4 de RSA, qui a les propriétés suivantes

- Raisonnablement fort : l'attaque par force brute de cet algorithme est difficile par le fait que chaque trame est envoyée avec un vecteur d'initialisation qui relance le générateur de nombres pseudo aléatoires.
- Auto synchronisation : l'algorithme se resynchronise pour chaque message. Ceci est nécessaire pour travailler en mode non connecté, où les paquets peuvent être perdus, comme dans tout réseau local.

**White List (WL) -** (anti-spam) - Cette liste blanche recense les sites, usagers, domaines qui, pour des raisons privées ou professionnelles, ne doivent en aucun cas être filtrés par l'anti-spam ou condamnés par la RBL. La WL est prioritaire sur la Black List (RBL). Une validation trop "généraliste" peut laisser passer des pollutions provenant d'un domaine théoriquement "ami".

**WHO -** World Health Organisation (Organisation Mondiale de la Santé).

**Wi-Fi -** Wireless Fidelity - ASFI en français (accès sans fil à l'internet) - Wi-Fi est aujourd'hui promu par l'alliance WECA (Wireless Ethernet Compatibility Alliance). Il promet donc un débit de 11 Mbits par seconde, de 50 à 100 mètres. Des évolutions sont d'ores et déjà à l'ordre du jour: 802.11g affiche 54 Mbps sur la bande de fréquences des 2,4 Ghz; 802.11a également mais sur des fréquences de 5 Ghz. (voir WLAN)

Certification d'interopérabilité décernée à des produits fondés sur 802.11 par la Wifi Alliance (une organisation industrielle) mais aussi label pour les équipements conformes à la norme 802.11b établie par l'IEEE pour le WLAN.

Le Wi-Fi est un protocole de communication permettant des échanges de données sans fil sur de courtes distances, de l'ordre de dizaines de mètres et à des débits pouvant aller jusqu'à 54Mbit/s. Ce protocole catalogué "802.11" par l'organisation de standardisation IEEE se trouve dans différentes variantes, différenciées par une lettre ("a", "b", "e", "g", "i") suivant les débits, la qualité de service ou le niveau de sécurité.

**WiFimax -** Système propriétaire dérivé de la technologie Hiperlan, développé par la société Nomotech dans la Manche. Cette technologie radio couvre aujourd'hui plusieurs départements Français (Manche, Moselle…).

**WiMAX -** Worldwide Interoperability for Microwave Access - Standard de l'IEEE sous le code 802.16 - Protocole utilisé pour développer de nouveaux réseaux métropolitains sans fil (WMAN). Le WiMAX offre des débits jusqu'à 70 Mbits/seconde sur une portée de 50 kms (transport voix et vidéo). Utilisé dans le raccordement du client final au réseau haut débit sur les derniers kilomètres, il est une alternative à l'ADSL et au câble. Il permet aussi de relier les Hotspots Wi-Fi 802.11 à Internet. WiMAX utilise les bandes de fréquence comprises entre 2 et 11 GHz (à l'origine dans la bande des 10 à 66 GHz avec un débit potentiel de 134 Mbits / seconde).

Sur le marché français (et métropolitain), cette technologie sera utilisée dans un premier temps comme une alternative aux équipements de BLR qui fonctionnaient dans la bande des 26 GHz et imposaient une vue directe entre émetteur et récepteur. WiMAX permet en effet de s'affranchir de cette "ligne de vue" grâce aux bandes de fréquence plus basses.

Des fabricants, dont Intel, ont adhéré à cette technologie, ce qui devrait rapidement déboucher sur une commercialisation d'ordinateurs dotées de puces WiMAX permettant d'accéder à un réseau en tout lieu.

Protocole de communication sans fil destiné à établir des connexions sur de plus longues distances qu'avec le Wi-Fi (de l'ordre de kilomètres, voire jusqu'à 50 km en théorie) et en plus grand nombre simultanément (quelques centaines contre quelques dizaines seulement pour le Wi-Fi). Ce protocole baptisé "IEEE 802.16" n'est pas destiné à l'usage individuel, mais plutôt à l'interconnexion de réseaux Wi-Fi (alias "hotspots") à l'échelle d'une ville ou d'une agglomération. C'est le moyen idéal pour faire rayonner un accès Internet haut débit dans une commune rurale, dans une zone industrielle, là où l'ADSL déclare forfait.

**WINS -** Windows Internet Naming Service - Permet à des clients de sous-réseaux IP différents de s'enregistrer dynamiquement et de naviguer sur le réseau sans recourir au broadcast.

Les systèmes d'exploitation de Microsoft utilisent des noms NetBIOS pour les communications sur le réseau. Par conséquent, ces clients requièrent une méthode pour résoudre les noms NetBIOS en adresses IP. WINS permet d'enregistrer les noms de machines NetBIOS et les résoudre en adresses IP. WINS est l'implémentation NetBIOS de Microsoft. Il hérite donc des limites et fonctionnalités de NetBIOS :

- Les noms NetBIOS ont une longueur de 16 octets,
- L'espace de noms NetBIOS n'a qu'un niveau : réseau à plat, ce qui signifie que les noms NetBIOS ne peuvent être utilisés qu'une fois sur le réseau.

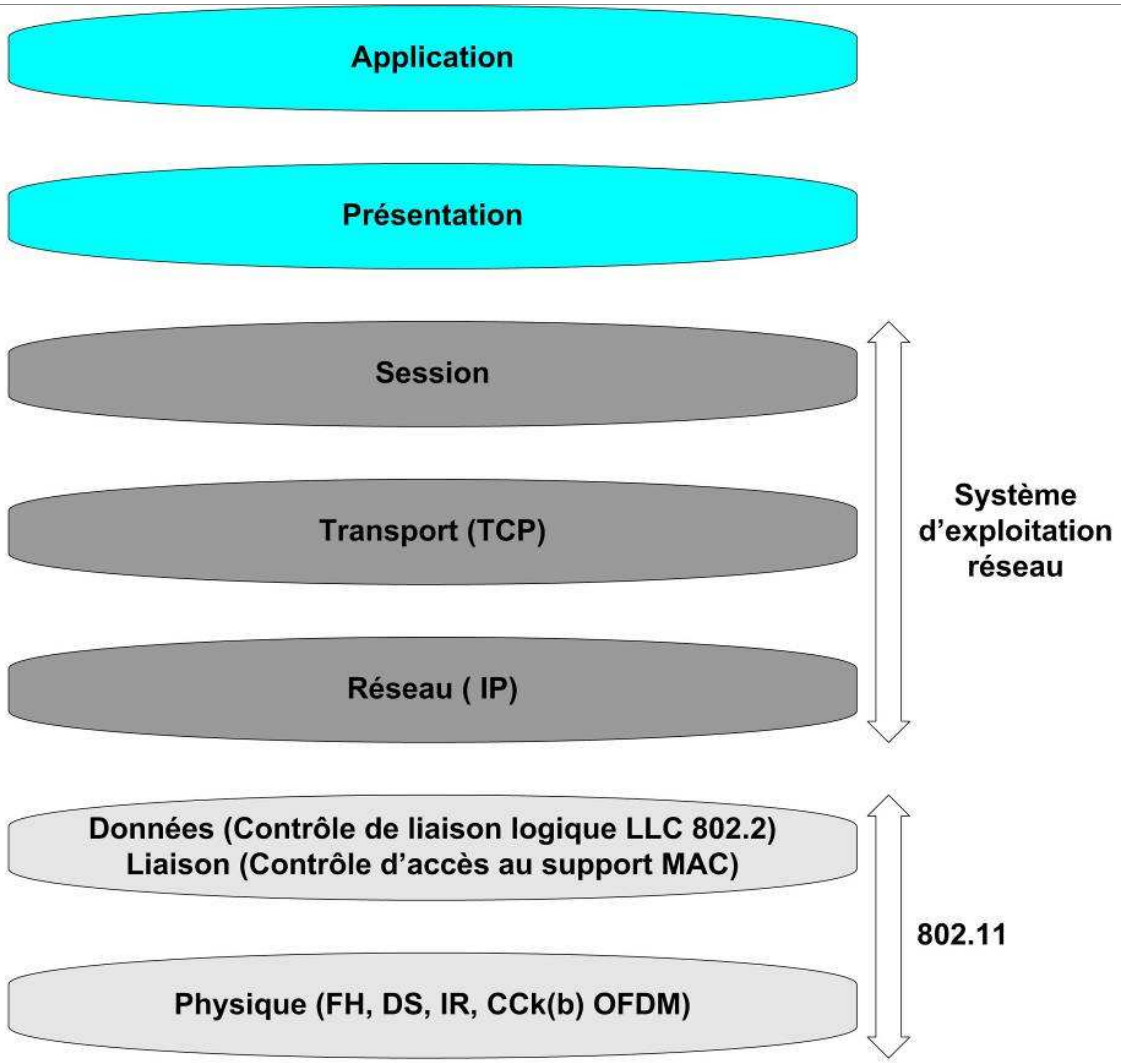
WINS est dynamique, chaque client démarrant envoie ses informations (nom, adresse et groupe de travail) au serveur WINS. Il est possible d'entrer des correspondances IP/noms NetBIOS statiquement sur un client Windows en passant par le fichier Lmhosts (similaire au fichier hosts.txt des premiers systèmes Unix avant l'apparition de DNS).

Le service WINS a une grande utilité car il réduit le trafic de diffusion en permettant aux clients de résoudre les noms NetBIOS par son intermédiaire au lieu d'émettre en diffusion (broadcast).

**WLAN -** Wireless Local Area Network - Réseau local sans fil. Il existe plusieurs technologies et normes. Le partage et les échanges d'informations se font via la voie des airs, sans être physiquement connecté par un fil. Pour les réseaux sans fil, les normes les plus usités sont les normes 802.11b, 802.11a et 802.11g (en attente de normalisation).

Le WLAN 802.11 et les couches OSI :

La spécification WLAN IEEE 802.11 et l'ensemble de ses déclinaisons (802.11a, 802.11b, 802.11g) ne porte que les deux premières couches ISO. Le gros du travail concerne surtout la couche physique (la couche 1), et seule la première moitié de la couche 2 est concernée. En effet, la partie LLC 802.2 de la couche 2 est conservée.




La spécification 802.11 n'intervient qu'au niveau 1 et 2 des couches ISO (Physique et données)

Les trois couches physiques définies à l'origine par 802.11 incluaient deux techniques radios à étalement de spectre et une spécification d'infrarouge diffus. Les standards radios fonctionnent sur la bande ISM des 2,4 GHz. Ces fréquences sont reconnues par les organismes réglementaires internationaux tels que la FCC (Etats-Unis), l'ETSI (Europe) et le MKK (Japon) pour utilisation sans licence.

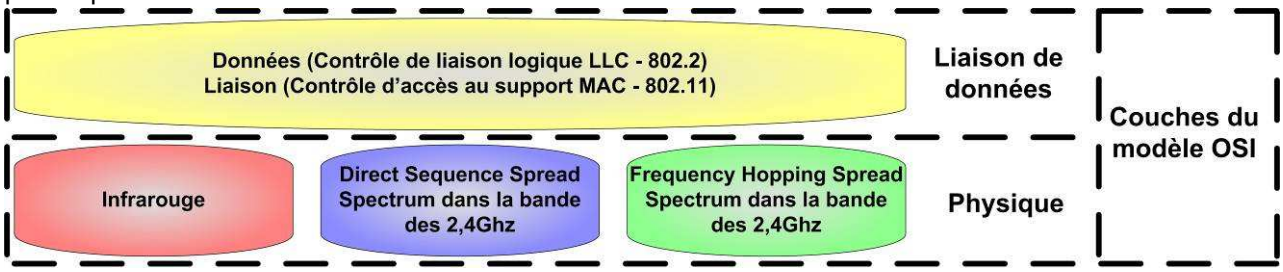
Seule la technique DSSS a été retenue en 802.11HR, puisque le saut de fréquence ne peut pas à la fois supporter les hauts débits et se conformer aux réglementations actuelles de la FCC. En conséquence, les systèmes 802.11HR seront interopérables avec les systèmes DSSS 802.11 à 1 et 2 Mbps, mais ils ne fonctionneront pas avec les systèmes FHSS 802.11 à 1 et 2 Mbps.

Le standard 802.11 DSSS original spécifie un shipping sur 11 bits (baptisé séquence Barker) pour le codage des données. Chaque séquence de 11 chips représente un seul bit de données (1 ou 0) et est converti en forme d'onde (ou symbole) émissible. Ces symboles sont transmis à la vitesse de 1 MSps (1 million de symboles par seconde) par la technique BPSK (Binary Phase Shift Keying). Dans le cas d'un débit de 2 Mbps, une technique plus sophistiquée, baptisée QPSK (Quadrature Phase Shift Keying), permet de doubler le débit de BPSK par l'optimisation de l'utilisation de la bande radio.

Pour augmenter le débit dans le cadre du standard 802.11HR, des techniques de codage évoluées sont mises en œuvre. Plutôt que de se cantonner aux deux séquences Barker sur 11 bits, la norme définit la technique CCK (Complementary Code Keying), qui consiste en un ensemble de 64 mots de 8 bits chacun. Les propriétés mathématiques spécifiques d'un tel ensemble de mots permettent de les distinguer correctement les uns des autres par le récepteur, même en présence de bruit et d'interférences (p. ex. les interférences causées par la réception de multiples réflexions radio dans un bâtiment). Le débit de 5,5 Mbps utilise la technique CCK pour coder 4 bits par porteuse, tandis que le mode 11 Mbps encode 8 bits par porteuse. Les deux modes font appel à la technique de modulation QPSK et signalent à 1,375 MSps. C'est de cette manière qu'il est possible d'atteindre ces débits supérieurs.

Pour supporter les environnements plus bruyants et étendre la portée des équipements, les WLAN

802.11HR utilisent la variation dynamique du débit (dynamic rate shifting), qui permet d'ajuster les taux de transmission automatiquement pour compenser les variations du canal radio. Dans une situation idéale, les utilisateurs se connectent à un taux de 11 Mbps plein. Cependant, lorsque les équipements sont déplacés au delà de leur portée optimale pour un débit de 11 Mbps, ou en cas d'interférences conséquentes, les équipements 802.11HR transmettent à des vitesses inférieures, redescendant en 5,5, puis 2 et enfin 1 Mbps. De la même façon, si le périphérique revient dans un rayon compatible avec des transmissions plus rapides, la vitesse de la connexion s'accélère automatiquement. La variation dynamique du débit est un mécanisme de couche physique transparent à la fois pour l'utilisateur et pour les couches supérieures de la pile de protocoles.




La couche de liaison de données de 802.11 se compose de deux sous-couches :

- Le contrôle de la liaison logique (Logical Link Control, ou LLC),
- Le contrôle d'accès au support (Media Access Control, ou MAC).

Le standard 802.11 utilise la LLC 802.2 et l'adressage sur 48 bits, tout comme les autres LAN 802, simplifiant ainsi le pontage entre les réseaux sans fil et filaires. Le contrôle d'accès au support est en revanche propre aux WLAN.

Le 802.11 MAC est très proche de 802.3 dans sa conception : il est conçu pour supporter de multiples utilisateurs sur un support partagé en faisant détecter le support par l'expéditeur avant d'y accéder.

La couche MAC définit deux méthodes d'accès différentes, la Distributed Coordination Function et la Point Coordination Function.

Dans un WLAN 802.11, la détection des collisions est impossible du fait de ce qu'on appelle le problème "near/far". Pour détecter une collision, une station doit être capable de transmettre et d'écouter en même temps. Or, dans les systèmes radio, il ne peut y avoir transmission et écoute simultanées (sauf à en augmenter le coût de façon exponentiel).

Pour prendre en compte cette différence, le standard 802.11 fait appel à un protocole légèrement modifié, baptisé CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), ou à la fonction DCF (Distributed Coordination Function).

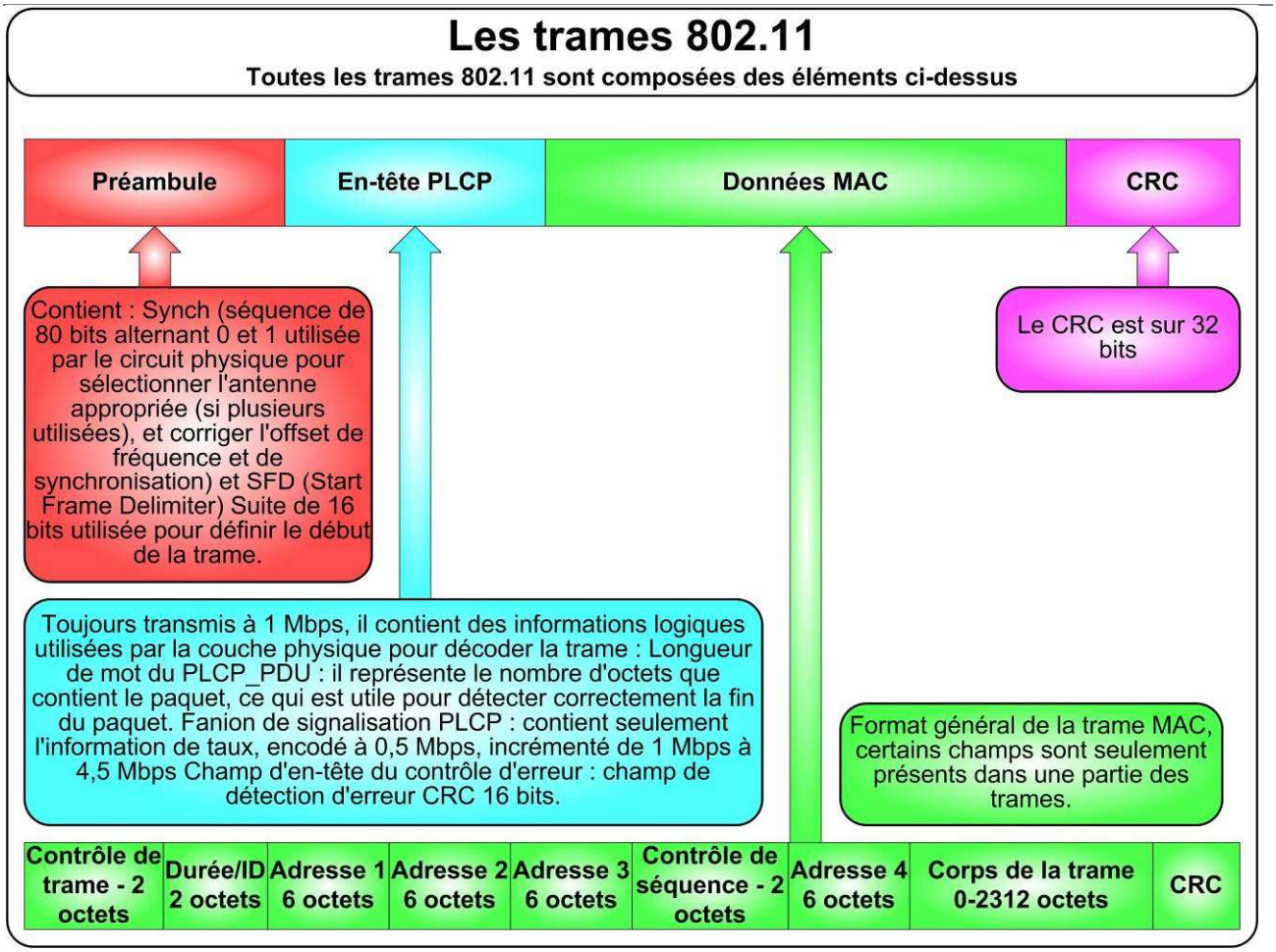
Autre spécificité de la couche MAC du sans fil : celui du "nœud caché", où deux stations situées de chaque côté d'un point d'accès peuvent entendre toutes les deux une activité du point d'accès, mais pas de l'autre station, problème généralement lié aux distances ou à la présence d'un obstacle. Pour résoudre ce problème, le standard 802.11 définit sur la couche MAC un protocole optionnel de type RTS/CTS (Request to Send/Clear to Send). Lorsque cette fonction est utilisée, une station émettrice transmet un RTS et attend que le point d'accès réponde par un CTS. Toutes les stations du réseau peuvent entendre le point d'accès, aussi le CTS leur permet-il de retarder toute transmission prévue, la station émettrice pouvant alors transmettre et recevoir son accusé de réception sans aucun risque de collision. Du fait que le protocole RTS/CTS ajoute à la charge du réseau en réservant temporairement le support, il est généralement réservé aux plus gros paquets, dont la retransmission s'avérerait lourde du point de vue de la bande passante.

Enfin, la couche MAC 802.11 offre deux autres caractéristiques de robustesse : les sommes de contrôle CRC et la fragmentation des paquets. Pour chaque paquet, une somme de contrôle est calculée et rattachée afin d'assurer que les données n'ont pas été corrompues durant leur transit. La fragmentation des paquets permet de casser les gros paquets en unités de plus petite taille lorsqu'ils sont transmis par radio, ce qui s'avère particulièrement utile dans les environnements très congestionnés ou lorsque les interférences posent problème, puisque les gros paquets courent plus de risque d'être corrompus.

Les principaux types de trames :

- Les trames de données, utilisées pour la transmission des données,
- Les trames de contrôle, utilisées pour contrôler l'accès au support (eg. RTS, CTS, ACK),
- Les trames de gestion, transmises de la même façon que les trames de données pour l'échange d'informations de gestion, mais qui ne sont pas transmises aux couches supérieures.

Chacun de ces trois types est subdivisé en différents sous-types, selon leurs fonctions spécifiques.




L'itinérance :

L'itinérance (roaming) est le processus de mouvement d'une cellule vers une autre sans fermer la connexion. Cette fonction est similaire au "handover" des téléphones portables, avec deux différences majeures :

- Sur un LAN, qui est basé sur des paquets, la transition d'une cellule à une autre doit être faite entre deux transmissions de paquets, contrairement à la téléphonie où la transition peut subvenir au cours d'une conversation. Ceci rend le roaming plus facile dans les LAN, mais…
- Dans un système vocal, une déconnexion temporaire peut ne pas affecter la conversation, alors que dans un environnement de paquets, les performances seront considérablement réduites à cause de la retransmission qui sera exécutée par les protocoles des couches supérieures.

Le standard 802.11 ne définit pas comment le roaming est fait, mais en définit cependant les règles de base. Celles-ci comprennent l'écoute active ou passive, le processus de réassociation, où une station qui passe d'un Point d'Accès à un autre sera associée au nouveau Point d'Accès

Si le standard 802.11HR définit la manière dont une station s'associe aux points d'accès, il ne définit pas la manière dont les points d'accès suivent l'utilisateur dans ses déplacements, soit sur la couche 2 entre deux points d'accès d'un même sous-réseau, soit sur la couche 3 lorsque l'utilisateur change de sous-réseau et de routeur.

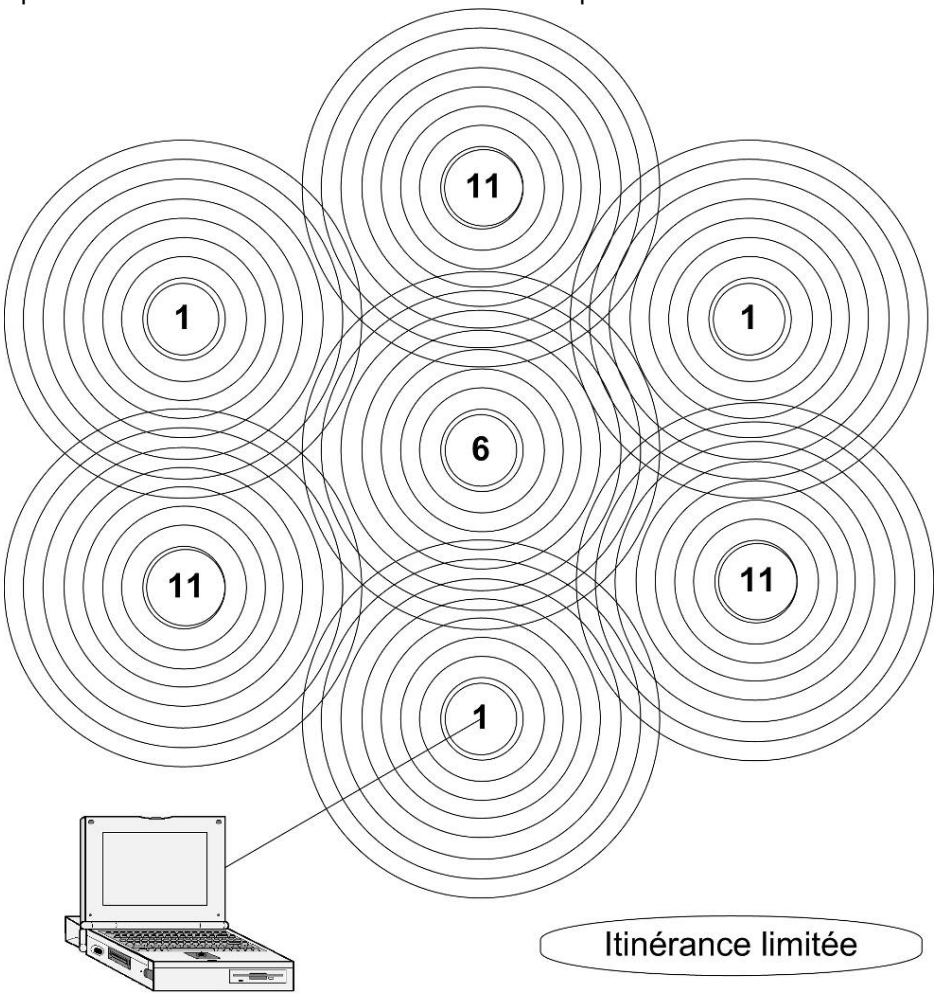
Le premier problème est pris en charge par des protocoles de communication inter-points d'accès propriétaires, dont les performances sont très variables. Si le protocole n'est pas efficace, il existera un risque de perte de paquets lorsque l'utilisateur passera d'un point d'accès à un autre. A terme, la WECA et l'IEEE définiront probablement des standards en ce domaine.

Le deuxième problème est géré par les mécanismes d'itinérance de niveau 3. Le plus fréquent d'entre eux est Mobile IP, baptisé RFC 2002 par l'IETF (Internet Engineering Task Force). Mobile IP fonctionne en définissant un point d'accès comme "agent domestique" pour chaque utilisateur.

Lorsqu'une station sans fil sort de sa zone d'origine et passe dans une nouvelle zone, le nouveau point d'accès demande à la station quelle est sa zone d'origine. Une fois celle-ci localisée, un paquet est transmis automatiquement entre les deux points d'accès pour garantir que l'adresse IP de l'utilisateur est préservée et qu'il est en mesure de recevoir de manière transparente ses données. Mobile IP n'est pas finalisé, aussi les fournisseurs peuvent-ils encore proposer des protocoles propriétaires, basés sur des techniques similaires, pour assurer que le trafic IP suivra un utilisateur entre des portions du réseau séparées par un routeur (p. ex. entre d'un bâtiment à un autre).

Une alternative incomplète mais pratique au problème de l'itinérance de niveau 3 consiste à utiliser le protocole DHCP (Dynamic Host Configuration Protocol) sur le réseau. DHCP permet à tout utilisateur qui éteint ou met en veille son ordinateur portable avant de passer sur un nouveau réseau d'obtenir automatiquement une nouvelle adresse IP lors du rallumage de la machine.

Une telle réassociation se produit en général lorsque la station s'est éloignée du point d'accès original, entraînant par conséquent un affaiblissement du signal. Elle peut aussi intervenir du fait d'un changement dans les caractéristiques radios du bâtiment, ou de l'augmentation du trafic réseau sur le point d'accès original. Dans ce dernier cas, la fonction sert à l'équilibrage des charges, puisqu'elle distribue la charge totale du WLAN plus efficacement sur l'infrastructure sans fil disponible.




Ce processus d'association/réassociation dynamique aux points d'accès permet à l'administrateur du réseau de créer une couverture très étendue en faisant se chevaucher de multiples cellules 802.11HR sur l'ensemble du bâtiment ou du campus. Pour ce faire, le responsable informatique utilisera la fonction de "réutilisation des canaux," en prenant soin de configurer chaque point d'accès sur des canaux DSSS 802.11 différents de ceux utilisés par les points d'accès contigus. Alors qu'il existe 14 canaux à recouvrement partiel pour les DSSS 802.11, seuls trois d'entre eux sont totalement isolés. Ces trois canaux sont les mieux adaptés à une couverture multicellulaire.

Lorsque les rayons d'action de deux points d'accès se chevauchent alors qu'ils sont configurés sur un même canal ou sur des canaux se recouvrant partiellement, des interférences sont susceptibles de se produire entre les deux, avec pour conséquence un rétrécissement de la bande passante utilisable sur la zone de chevauchement.

Point sur la réglementation Française :

Le cadre réglementaire français de l'utilisation des solutions de réseaux sans fil est établi par l'Autorité de Régulation des Télécoms (ART).

Pour la bande des 2.4GHZ :

Le cadre général autorise l'utilisation à l'intérieur, sur la bande 2400-2446,5MHz avec une puissance maximale de 10mW et sur la bande de 2446.5MHz-2483.5MHz avec une puissance de 100mW. A l'extérieur, sur la bande 2446,5-2483,5 MHz avec une puissance limitée à 100mW avec accord.

Dans tous les départements (les limitations départementales ont été annulées au cours de l'été 2003 - site Internet de l'ART), les RLANs sont autorisés à l'intérieur des bâtiments avec une puissance maximale de 100mW sur toute la bande 2400MHz-2483,5MHz. à l'extérieur des bâtiments avec une puissance maximale

de 100mW sur la partie 2400-2454MHz et avec une puissance maximale de 10mW sur la partie 2454-2483MHz.

Pour la bande des 5GHZ :

L'ART autorise l'utilisation d'une partie de la bande de fréquences des 5GHz pour les RLANs intégrant des solutions 802.11a supportant les fonctions DFS (Dynamic Frequency Selection) et TPC (Transmit Power Control). Seule la bande 5150-5350MHz est autorisée en France pour une utilisation intérieure avec une puissance limitée à 200mW en mode Infrastructure.

La sécurité :

La sécurité devrait être le premier souci de ceux qui déploient les réseaux locaux sans fil. Le comité 802.11 a apporté une première solution en élaborant un processus appelé WEP (Wired Equivalent Privacy).

Le principal, pour les utilisateurs, est d'être sûr qu'un intrus ne pourra pas :

- Accéder aux ressources du réseau en utilisant le même équipement sans fil,
- Capturer le trafic du réseau sans fil (écoute clandestine).
- Prévenir l'accès aux ressources du réseau. Ceci est obtenu en utilisant un mécanisme d'authentification où une station est obligée de prouver sa connaissance d'une clef, ce qui est similaire à la sécurité sur réseaux câblés, dans le sens où l'intrus doit entrer dans les lieux (en utilisant une clef physique) pour connecter son poste au réseau câblé.
- Ecoute clandestine. L'écoute clandestine est bloquée par l'utilisation de l'algorithme WEP qui est un générateur de nombres pseudo aléatoires initialisé par une clef secrète partagée.

Installer un réseau sans fil sans le sécuriser, c'est permettre à des personnes non autorisées d'écouter et d'accéder aux informations circulant sur le réseau. Voici les mesures minimales à prendre pour la sécurité des bornes d'accès:

- Supprimer la configuration par défaut du point d'accès en modifiant l'identifiant réseau (SSID) et la clé Wep par défaut.
- Protéger les services d'administration disponibles sur l'interface sans fil en changeant le mot de passe.
- Mettre en place le filtrage des adresses MAC ayant le droit de communiquer avec le point.
- Gérer la puissance d'émission des points d'accès, s'ils le permettent, pour éviter de diffuser les informations dans des zones non désirées.

Mais ces mesures ne sont pas toujours suffisantes et de nouveaux protocoles de sécurité apparaissent : Au niveau de l'authentification, le protocole 802.lx utilise EAP. Au niveau encryptage, vous pouvez distribuer des certificats automatiquement et changer les clés d'encryptage. De plus, le protocole TKIP peut également être implémenté avec pour points forts : des clés WEP dynamiques différentes à chaque session, des vecteurs d'initialisation sur 48 bits, le contrôle d'intégrité des données et des en têtes.

Au niveau global, quelques règles de mise en œuvre "type" pour sécuriser une extension d'un réseau local vers du sans-fil :

- Toujours isoler les réseaux filaires des réseaux sans-fils par un FireWall (les points d'accès ne devraient pas être connectés directement au réseau filaire) et sécuriser les points d'accès comme précédemment expliqué.
- Implémenter des tunnels RPV en IPSEC sur les liaisons radio.
- Contrôler la zone d'émission et limiter la portée des ondes au seul bâtiment. A cet effet, des compétences sur la transmission radio peuvent être utiles.
- Masquer le nom du réseau sans fil, pour en faire un réseau "fantôme", alors invisible pour tout utilisateur non autorisé.
- Mettre en œuvre une politique d'authentification des utilisateurs utilisant des processus cryptés (Radius en Chap par exemple, ou authentification forte avec Cryptage type SecurID et durée de vie très courte de la fenêtre d'authentification).

Rester synchronisé :

Les stations doivent rester synchronisées. Ceci est nécessaire pour garder la synchronisation au cours des sauts, ou pour d'autres fonctions comme l'économie d'énergie. Sur une même cellule, ceci est obtenu car toutes les stations synchronisent leur horloge avec l'horloge du Point d'Accès en utilisant le mécanisme suivant :

Le Point d'Accès transmet périodiquement des trames appelées "trames balise ". Ces trames contiennent la valeur de l'horloge du Point d'accès au moment de la transmission (notons que c'est le moment où la transmission à réellement lieu, et non quand la transmission est mise à la suite des transmissions à faire. Puisque la trame balise est transmise selon les règles du CSMA, la transmission pourrait être différée significativement).

Les stations réceptrices vérifient la valeur de leur horloge au moment de la réception, et la corrige pour rester synchronisées avec l'horloge du Point d'Accès. Ceci évite des dérives d'horloge qui pourraient causer la perte de la synchronisation au bout de quelques heures de fonctionnement.

L'installation d'un réseau :

Avant d'installer un réseau sans fil, il faut retenir certains points :

On peut installer 3 types de réseau :

- En architecture Ad-Hoc (les clients communiquent les uns avec les autres directement),
- En architecture Infrastructure (les communications des clients passent par un point d'accès),
- En mode point à point ou point à multipoint (le point d'accès sert de pont entre plusieurs réseaux).

Un point d'accès peut supporter au maximum une trentaine de clients

Les distances dépendent de l'environnement. S'il n'y a pas d'obstacle, la distance est plus grande, mais le taux de transfert est inversement proportionnel à la distance. La présence de parties métalliques accentue ces phénomènes.

La présence d'autres éléments utilisant les ondes radios sur la même bande de fréquences (micro-onde, ...) peuvent perturber les communications.

Un point d'accès suffit pour quelques postes équipés de cartes sans fil. Si le signal est faible, il est possible de rajouter une antenne omnidirectionnelle (en 802.11b). Si le nombre de clients augmente, il faut rajouter un ou plusieurs points d'accès. Attention : si les zones de couvertures des points d'accès se chevauchent, il est préférable de ne pas leur attribuer le même canal.

Pour relier 2 réseaux distants de plusieurs mètres, il suffit d'installer un point d'accès configuré en mode pont sur chacun des réseaux. Si les réseaux sont de type sans fil, il faut rajouter un point d'accès sur chaque réseau local pour permettre la communication des clients sans fil. Si la distance entre les deux réseaux est importante, il est possible de rajouter une antenne sur chacun des ponts. Les antennes doivent être identiques pour une performance optimale.

Pour augmenter la portée d'un point d'accès, il est possible d'utiliser le mode répéteur des points d'accès pour relier plusieurs points d'accès sans utiliser de câble Ethernet et ainsi augmenter la portée du réseau sans fil.

Les avantages des WLAN comprennent :

- Une mobilité génératrice de gains de productivité, avec un accès en temps réel aux informations, quel que soit le lieu où se situe l'utilisateur, pour une prise de décision plus rapide et plus efficace,
- Une installation plus économique du réseau dans les endroits difficiles à câbler, bâtiments anciens et structures en béton armé,
- Un coût d'appartenance inférieur (particulièrement dans les environnements dynamiques nécessitant des transformations fréquentes) grâce au coût minime du câblage et de l'installation par poste et par utilisateur,
- Les WLAN libèrent l'utilisateur de sa dépendance à l'égard des accès câblés au backbone, lui offrant un accès permanent et omniprésent. Cette liberté de mouvement offre de nombreux avantages dans de nombreux types d'environnements de travail tels que :
- Accès immédiat entre le lit d'hôpital et les informations concernant le patient pour les médecins et le personnel hospitalier,
- Un accès réseau simple et en temps réel pour les consultants et les auditeurs sur site, Un accès étendu aux bases de données pour les chefs de service nomades, directeurs de chaîne de fabrication, contrôleurs de gestion ou ingénieurs du bâtiment,
- Une configuration simplifiée du réseau avec un recours minime au personnel informatique pour les installation temporaires telles que stands de foire, d'exposition ou salles de conférence,
- Un accès plus rapide aux informations client pour les fournisseurs de services et détaillants, résultant en un meilleur service et une satisfaction supérieure,
- Un accès omniprésent au réseau pour les administrateurs, pour le support et le dépannage sur site,
- Un accès en temps réel pour les réunions des groupes d'étude et des liens de recherche pour les étudiants.

**WLL -** Wireless Local Loop - Boucle locale utilisant une technologie radio (sans fil) d'accès à l'abonné.

**WML -** Wireless Markup Language - Ce langage permet aux sites Internet d'adapter l'information à l'écran et aux capacités limitées des téléphones mobiles.

**Workflow -** Gestion optimisée des flux et du traitement suivi de l'information.

**WPA -** Wi-Fi Protected Access - Mécanisme de sécurité avec chiffrement sur 128 bits. Ce mécanisme présenté fin avril 2003 vient remplacer le mécanisme WEP. Employant le protocole TKIP (renouvellement de clé en cours de communication) et intégrant l'authentification (via le protocole 802.1x) avec EAP (Extensible Authentification Protocole). Modèle de sécurisation de Wi-Fi basé sur des standards.

**WPAN -** Wireless Personnal Area Network - Le WPAN est un réseau sans fil individuel. Très en vogue avec le développement de Bluetooth, ces réseaux devraient, avec le temps, augmenter leurs débits et leurs portées pour devenir de véritables concurrents des WLAN.

Les deux noms qui sortent du lot des WPAN sont Bluetooth et HomeRF.

Home Radio Frequency est une norme basée sur 802.11b et DECT. Elle permet indifféremment de faire transiter des flux audio ou des données. La norme autorise des portées de 50 mètres sans utiliser d'amplificateur.

De même que Bluetooth, HomeRF travaille au niveau physique dans la bande des 2,4 GHz, avec la technologie FHSS, à raison de 50 sauts de fréquence par seconde. Le débit nominal est de 1,6 Mbps (soit 1 Mbps réel), mais les débits peuvent atteindre 10 Mbps dans la version 2.

**WSCL -** Web Services Conversation Language - Langage définissant les règles de dialogue entre services web. WSCL décrit précisément leurs interactions respectives et leur ordre d'exécution.

**WSDL -** Web Services Description Language - Langage de description des services web dérivé de XML.

**WSFL -** Web Service Flow Language - Dialecte d'orchestration des services web, proposé par IBM. Utilisé pour décrire les scénarios d'enchaînement de composants.

**WSUI -** Web Services User Interface - Langage de description de l'interface utilisateur d'un service web.

**WWW -** World Wide Web - Toile d'araignée mondiale constituée par l'ensemble des serveurs Web sur l'Internet.


A partir de 1989, au CERN (Suisse), Tim Berners-Lee ainsi que Robert Cailliau (et quelques autres personnes du CERN) seront les co-créateurs du World Wide Web. Ils y voient là l'opportunité de lier le principe d'hypertexte avec Internet.

Ensuite, en 1990, seront développées les trois principales technologies du web : les adresses web, le Hypertext Transfer Protocol (HTTP) et le Hypertext Markup Language (HTML) et dans le même temps le premier navigateur web et éditeur web et le premier serveur HTTP.

# X

**X -** Préfixe utilisé par le CCITT pour identifier ses avis et recommandations dans le domaine des réseaux de données. Exemple = X25, X400…

**X.500 -** Norme de l'ISO et du CCITT, qui définit le moteur de base de données d'un annuaire électronique et le module d'interrogation de ces données. Cette norme établit des règles de nommage pour les éléments contenus dans cet annuaire, les protocoles pour y accéder (dont DAP) et les moyens d'authentification de l'utilisateur.

La norme X.500 se base sur le modèle OSI. Tous les protocoles de cette norme appartiennent à la couche 7.

Les annuaires X.500 ont été normalisé par l'organisme de l'UITT. La série X.500 de cet organisme s'efforce de définir les annuaires, leurs services, leurs méthodes d'accès et leurs protocoles. Voici les principales normes qui définissent les Systèmes Ouverts d'Annuaires selon l'UIT-T :

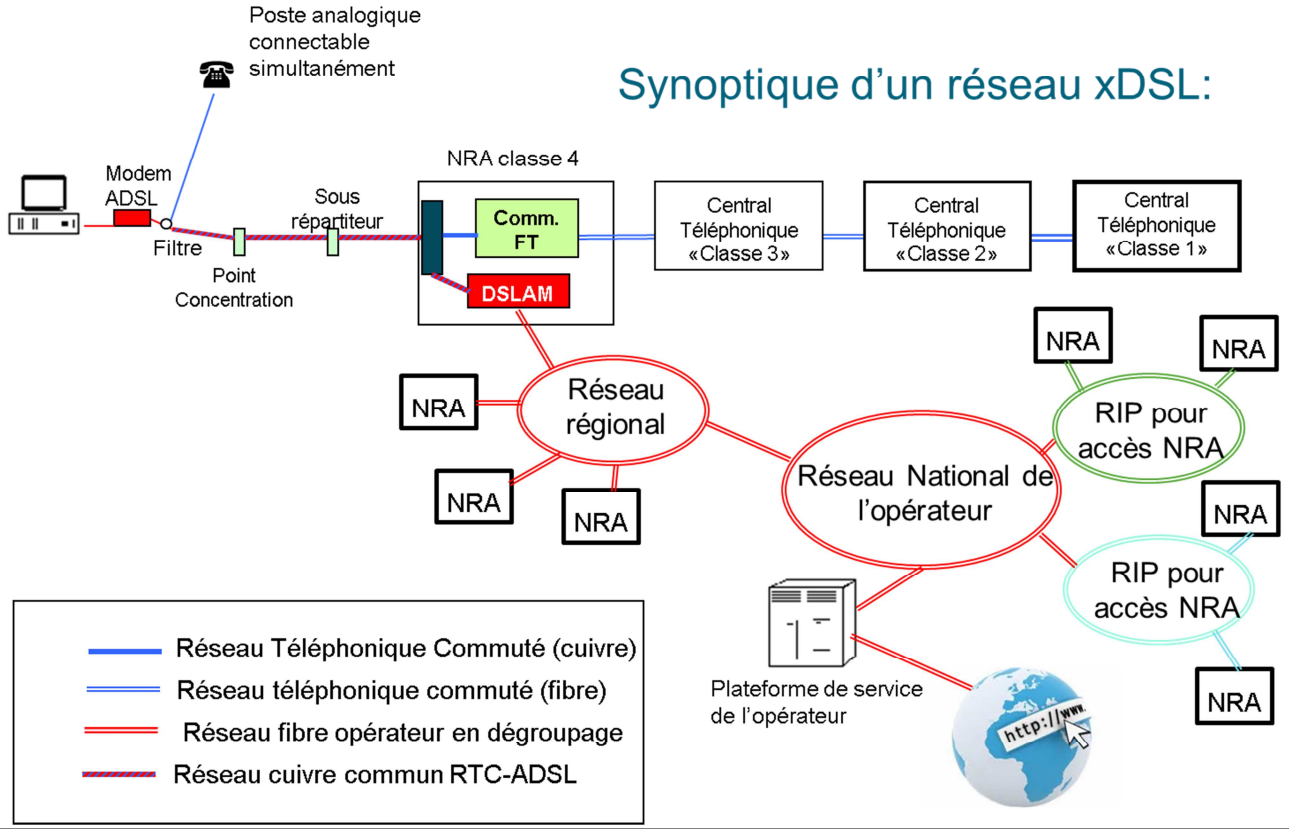
- X.500 : Aperçu des annuaires, concepts, modèles et services
- X.501 : Les modèles d'annuaires
- X.509 : l'Authentification des annuaires
- X.511 : Les services d'annuaires
- X.518 : Les annuaires distribués
- X.519 : Les protocoles
- X.525 : La réplication d'annuaires

**X25 -** Le protocole X25 définit l'interface entre un ETTD (Equipement Terminal de Traitement des Données) et un ETCD (Equipement Terminal de Circuit de Données). Il a été adopté par le CCITT en septembre 1976. On entend souvent par X25 l'ensemble des protocoles liés à X25 et qui couvre les couches 1 à 3 du modèle OSI. Pourtant, le terme X25 désigne uniquement le niveau 3 ou niveau paquet transporté entre les champs d'information des trames LAPB.

**X25-3** - X25 PLP - Packet Level Protocol - Protocole de niveau 3 de X25 (voir X25)

**XDSL -** Ensemble des technologies DSL permettant d'obtenir des hauts débits de transmission de signaux numériques, de l'ordre de plusieurs mégabits par seconde, sur les câbles traditionnellement utilisés pour la téléphonie analogique.

Il existe différentes normes de transmissions de données à haut débit regroupées sous cette appellation générique, on trouve notamment : ADSL (Asymmetric Digital Subscriber Line ou réseau de raccordement numérique asymétrique), SDSL (Symmetric Digital Subscriber Line ou réseau de raccordement numérique à débit symétrique), RADSL et VDSL.



**XKMS -** XML Key Management Specification - Protocole dont l'objectif est de faciliter l'intégration d'une infrastructure à clé publique (PKI) dans les applications de commerce électronique. XKMS est compatible avec les standards WSDL et Soap.

**XLANG -** Langage permettant de décrire en XML des processus collaboratifs de type services web. II est intégré à l'outil BizTalk Server de Microsoft.

**XLL -** (Extensible Link Language) - Langage permettant de spécifier des liens externes ou internes à un document XML et de gérer des liens avec les bases de données.

**XMLA -** XML for Analysis - En 2001, le comité XMLA a défini les spécifications permettant aux développeurs d'incorporer la business intelligence dans leurs services web. Le protocole XMLA est fondé sur les standards Internet ouverts HTTP, XML et Soap. Cette spécification standardisera les requêtes Olap à l'aide de Soap.

**XML-Dsig -** XML Signature - Normalisé au mois d'avril 2002 par le W3C, il vise à authentifier la signature d'un document par différents utilisateurs. Il décrit, à l'aide de son vocabulaire, les multiples signataires d'une partie de document XML ou de son ensemble. Ce dialecte assure l'intégrité de ces signatures multiples.

**XMLQuery -** Langage de requête XML, susceptible de remplacer SQL et les OQL (Object Query Language) utilisés dans les bases de données objet.

**Xmodem -** Un des premiers protocoles asynchrones de transfert de fichiers doit son succès à sa simplicité mais aussi au fait qu'il a été très tôt utilisé dans le domaine public. Ce protocole non propriétaire peut transférer tout type de données, texte ou binaires. Il découpe le fichier en blocs de 128 octets, y compris le dernier bloc. De ce fait, le fichier reçu peut avoir une taille supérieure de 127 octets par rapport au fichier "source".

**X-On/X-Off -** Méthode de contrôle simple d'une communication de données dans laquelle le terminal réactive la ligne chaque fois qu'il est prêt à émettre et la désactive chaque fois qu'il n'a pas de données disponibles.

**X-Open -** Association internationale ayant pour objet le développement concret d'architectures informatiques ouvertes et multi constructeurs, en s'appuyant sur les normes officielles aussi bien que sur des normes de facto.

**XQL -** XML Query Lanquage - Langage d'interrogation destiné à générer des requêtes dans une base de données XML.

**XSD -** XML Schema Definition - Les schémas permettent de décrire la structure d'un document XML, mais avec une précision accrue par rapport aux DTD, notamment au niveau du type des données contenues. Contrairement aux DTD, les schémas respecteront la syntaxe de XML.

**XSL -** (Extensible Style Langage) - Langage de style utilisé pour transformer des données XML en HTML ou vers d'autres formats de présentation.

**XSL -** XML Stylesheet Lanquage - Standard du W3C basé sur XML permettant de construire des feuilles de style. L'association d'une feuille de style à un document XML normalise la présentation des données.

**X-Windows -** Interface d'écran, utilisant largement le graphique et les fenêtres multiples, développée par le MIT (Massachussets Institute of Technology). Elle est devenue une norme de base pour les écrans dans le monde des stations de travail. Elle ne définit pas la présentation de l'écran définitif, mais les principales notions permettant de construire un écran à fenêtre. Avec X-Windows, une fenêtre peut être affectée à la visualisation d'une tâche se déroulant sur une autre machine d'un réseau.

# Y

**Ymodem -** Version perfectionnée de Xmodem, corrige les défauts de Xmodem en autorisant la transmission des paquets de 1024 octets, améliorant ainsi les performances du transfert. Le premier enregistrement contient le nom du fichier, sa taille et la date de la dernière modification. Un mécanisme de contrôle par redondance (CRC) codé sur 16 bits protège chaque bloc.

# Z

**ZAA -** Zone à Autonomie d'Acheminement - Sur le réseau de France Télécom, à chaque catégorie de commutateur correspond une zone technique qui représente le nombre d'abonnés desservis par un ou plusieurs commutateurs d'un niveau donné. La ZAA : (zone à autonomie d'acheminement) correspond au CAA ; la ZT (zone de transit) au CT.

**ZLE** - Zone Locale Elargie - Zone (souvent de la taille d'un département) d'au moins 150 000 abonnés au téléphone à l'intérieur de laquelle le tarif local est appliqué

**ZLT -** Zone Locale de Tri - L'opérateur de boucle locale n'achemine vers le transporteur choisi par l'appelant que les appels destinés à des appelés extérieurs à la zone locale de tri ; il conserve et achemine lui-même les appels internes à la zone locale de tri, quelle que soit la séquence de numérotation composée par l'appelant. En France, la zone locale de tri correspond le plus souvent au département.

Le territoire français a été décomposé en un ensemble de zones locales de tri. Chaque département constitue une ZLT. Deux exceptions: Paris et sa petite couronne et les deux départements corses forment une seule ZLT.

**Zmodem -** Autre version améliorée des protocoles Xmodem et Ymodem, autorise les reprises de transfert en cas d'incident.

**Zone arrière** - en FTTH - (du point de mutualisation, du NRO, du SRO,…) La zone arrière peut se définir comme la zone géographique qui est « couverte par l'équipement d'infrastructure concerné. Dans le cas d'un point de mutualisation, il s'agit de l'ensemble des logements que peut desservir le point de mutualisation concerné. Dans le cas de la zone d'emprise d'un NRO, il s'agit de l'ensembles des adresses déservies par le NRO.

**ZONE ASFI -** Espace dont la fréquentation importante par le public justifie la mise à disposition de services radioélectriques temporaires ou permanents, notamment un accès sans fil à l'internet. Des exemples sont des centres de congrès, hôtels, manifestations sportives, gares, aéroports.

**Zone blanche -** Terme utilisée pour désigner un territoire privé de service ADSL ou de téléphonie mobile**.**

**Zone grise -** Terme utilisé pour désigner un territoire avec un service ADSL de qualité moindre ne permettant pas d'accéder aux services dits de hauts débits (<2Mbits/s).

**Zone très dense -** Zone à forte concentration de population.

Le mode de détermination de la liste de communes des zones très denses est le suivant (selon ARCEP) :

- Un premier ensemble est constitué des unités urbaines (communes ou ensemble de communes) de France métropolitaine dont la population est de plus de 250 000 habitants.
- Un deuxième ensemble est délimité en ne retenant que les unités urbaines du premier ensemble pour lesquelles la proportion de logements en grands immeubles, c'est-à dire dans les immeubles de plus de 12 logements, est d'au moins 20%.
- Un troisième ensemble est délimité en retenant, au sein des unités urbaines constituant le second ensemble:
    - Les communes centres
    - Les communes périphériques pour lesquelles la proportion de logements en grands immeubles, c'est-à-dire dans les immeubles de plus de 12 logements, est d'au moins 50% ;

**Zone d'ombre -** En Transmission radio - Phénomène perturbant le déploiement du service, dû à la réflexion des ondes millimétriques par des obstacles (végétation, murs, collines). Autour de ces zones, les utilisateurs ne reçoivent pas de signal direct.

**ZT -** Zone de Transit - Voir ZAA - Le territoire métropolitain est divisé en 18 zones de transit (ZT) qui correspondent aux zones de transit du réseau interurbain de France Télécom pour l'entreprise. Ces ZT recoupent, à quelques nuances près, les départements, mais ne coïncident pas toujours avec les régions.

Chaque ZT est desservie par des points de raccordement de fournisseurs d'accès de service téléphonique au public (PRF) pour les détenteurs d'une licence L34-1. Ces PRF sont nommés points de raccordement d'opérateur (PRO) pour les détenteurs d'une licence L33-1.

Il existe à l'heure actuelle 69 PRF sur le territoire métropolitain dont la position a été déterminée à partir de l'architecture du réseau de FT et de prévisions d'implantation d'opérateurs concurrents.

Raccordement pour les détenteurs d'une licence L33-1

L'ARCEP a imposé une solution qui permet aux nouveaux opérateurs de se connecter à deux niveaux:

• raccordement à un commutateur d'abonnés de FT: Cela permet d'écouler le trafic terminal destiné aux abonnés raccordés directement à ce commutateur et de collecter le trafic des clients de l'opérateur longue distance qui y sont directement raccordés.

• raccordement à un PRO: L'ensemble des trafics d'accès direct est apporté par l'opérateur à un PRO situé dans la ZT de l'abonné. L'opérateur longue distance prend livraison à un PRO de tout le trafic d'accès indirect qui lui est destiné.

Raccordement pour les détenteurs d'une licence L34-1

Les détenteurs de cette licence ne peuvent se raccorder qu'à un PRF.

**ZTA -** Zone de Télécommunications Avancées - Lieu géographique dans lequel sont regroupés des moyens d'Accès à des systèmes de communications de grande capacité accessibles à plusieurs utilisateurs (réseau en fibre optique, antennes satellites...). Souvent synonyme de Téléport.

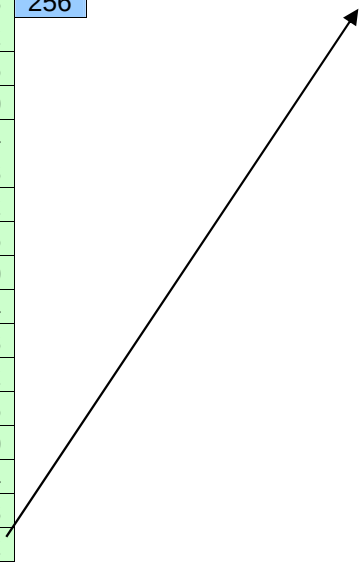
# Annexes

**Tableau de conversion numérique → binaire**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 00000001 | 43 | 00101011 | 85 | 01010101 | 127 | 01111111 | 169 | 10101001 | 211 | 11010011 |
| 2 | 00000010 | 44 | 00101100 | 86 | 01010110 | 128 | 10000000 | 170 | 10101010 | 212 | 11010100 |
| 3 | 00000011 | 45 | 00101101 | 87 | 01010111 | 129 | 10000001 | 171 | 10101011 | 213 | 11010101 |
| 4 | 00000100 | 46 | 00101110 | 88 | 01011000 | 130 | 10000010 | 172 | 10101100 | 214 | 11010110 |
| 5 | 00000101 | 47 | 00101111 | 89 | 01011001 | 131 | 10000011 | 173 | 10101101 | 215 | 11010111 |
| 6 | 00000110 | 48 | 00110000 | 90 | 01011010 | 132 | 10000100 | 174 | 10101110 | 216 | 11011000 |
| 7 | 00000111 | 49 | 00110001 | 91 | 01011011 | 133 | 10000101 | 175 | 10101111 | 217 | 11011001 |
| 8 | 00001000 | 50 | 00110010 | 92 | 01011100 | 134 | 10000110 | 176 | 10110000 | 218 | 11011010 |
| 9 | 00001001 | 51 | 00110011 | 93 | 01011101 | 135 | 10000111 | 177 | 10110001 | 219 | 11011011 |
| 10 | 00001010 | 52 | 00110100 | 94 | 01011110 | 136 | 10001000 | 178 | 10110010 | 220 | 11011100 |
| 11 | 00001011 | 53 | 00110101 | 95 | 01011111 | 137 | 10001001 | 179 | 10110011 | 221 | 11011101 |
| 12 | 00001100 | 54 | 00110110 | 96 | 01100000 | 138 | 10001010 | 180 | 10110100 | 222 | 11011110 |
| 13 | 00001101 | 55 | 00110111 | 97 | 01100001 | 139 | 10001011 | 181 | 10110101 | 223 | 11011111 |
| 14 | 00001110 | 56 | 00111000 | 98 | 01100010 | 140 | 10001100 | 182 | 10110110 | 224 | 11100000 |
| 15 | 00001111 | 57 | 00111001 | 99 | 01100011 | 141 | 10001101 | 183 | 10110111 | 225 | 11100001 |
| 16 | 00010000 | 58 | 00111010 | 100 | 01100100 | 142 | 10001110 | 184 | 10111000 | 226 | 11100010 |
| 17 | 00010001 | 59 | 00111011 | 101 | 01100101 | 143 | 10001111 | 185 | 10111001 | 227 | 11100011 |
| 18 | 00010010 | 60 | 00111100 | 102 | 01100110 | 144 | 10010000 | 186 | 10111010 | 228 | 11100100 |
| 19 | 00010011 | 61 | 00111101 | 103 | 01100111 | 145 | 10010001 | 187 | 10111011 | 229 | 11100101 |
| 20 | 00010100 | 62 | 00111110 | 104 | 01101000 | 146 | 10010010 | 188 | 10111100 | 230 | 11100110 |
| 21 | 00010101 | 63 | 00111111 | 105 | 01101001 | 147 | 10010011 | 189 | 10111101 | 231 | 11100111 |
| 22 | 00010110 | 64 | 01000000 | 106 | 01101010 | 148 | 10010100 | 190 | 10111110 | 232 | 11101000 |
| 23 | 00010111 | 65 | 01000001 | 107 | 01101011 | 149 | 10010101 | 191 | 10111111 | 233 | 11101001 |
| 24 | 00011000 | 66 | 01000010 | 108 | 01101100 | 150 | 10010110 | 192 | 11000000 | 234 | 11101010 |
| 25 | 00011001 | 67 | 01000011 | 109 | 01101101 | 151 | 10010111 | 193 | 11000001 | 235 | 11101011 |
| 26 | 00011010 | 68 | 01000100 | 110 | 01101110 | 152 | 10011000 | 194 | 11000010 | 236 | 11101100 |
| 27 | 00011011 | 69 | 01000101 | 111 | 01101111 | 153 | 10011001 | 195 | 11000011 | 237 | 11101101 |
| 28 | 00011100 | 70 | 01000110 | 112 | 01110000 | 154 | 10011010 | 196 | 11000100 | 238 | 11101110 |
| 29 | 00011101 | 71 | 01000111 | 113 | 01110001 | 155 | 10011011 | 197 | 11000101 | 239 | 11101111 |
| 30 | 00011110 | 72 | 01001000 | 114 | 01110010 | 156 | 10011100 | 198 | 11000110 | 240 | 11110000 |
| 31 | 00011111 | 73 | 01001001 | 115 | 01110011 | 157 | 10011101 | 199 | 11000111 | 241 | 11110001 |
| 32 | 00100000 | 74 | 01001010 | 116 | 01110100 | 158 | 10011110 | 200 | 11001000 | 242 | 11110010 |
| 33 | 00100001 | 75 | 01001011 | 117 | 01110101 | 159 | 10011111 | 201 | 11001001 | 243 | 11110011 |
| 34 | 00100010 | 76 | 01001100 | 118 | 01110110 | 160 | 10100000 | 202 | 11001010 | 244 | 11110100 |
| 35 | 00100011 | 77 | 01001101 | 119 | 01110111 | 161 | 10100001 | 203 | 11001011 | 245 | 11110101 |
| 36 | 00100100 | 78 | 01001110 | 120 | 01111000 | 162 | 10100010 | 204 | 11001100 | 246 | 11110110 |
| 37 | 00100101 | 79 | 01001111 | 121 | 01111001 | 163 | 10100011 | 205 | 11001101 | 247 | 11110111 |
| 38 | 00100110 | 80 | 01010000 | 122 | 01111010 | 164 | 10100100 | 206 | 11001110 | 248 | 11111000 |
| 39 | 00100111 | 81 | 01010001 | 123 | 01111011 | 165 | 10100101 | 207 | 11001111 | 249 | 11111001 |
| 40 | 00101000 | 82 | 01010010 | 124 | 01111100 | 166 | 10100110 | 208 | 11010000 | 250 | 11111010 |
| 41 | 00101001 | 83 | 01010011 | 125 | 01111101 | 167 | 10100111 | 209 | 11010001 | 251 | 11111011 |
| 42 | 00101010 | 84 | 01010100 | 126 | 01111110 | 168 | 10101000 | 210 | 11010010 | 252 | 11111100 |
| | | | | | | | | | | | |
| | | | | 253 | 11111101 | 254 | 11111110 | | | | |

**Tableau de sous-adressage IPv4**

| Masque (OSPF) | 0 | 1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 |
|---|---|---|---|---|---|---|---|---|---|
| Masque adresse IP | 255 | 254 | 252 | 248 | 240 | 224 | 192 | 128 | 0 |
| Nb bit masque | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Nb Subnet total | 0 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Nb Subnet Utilisable | -2 | 126 | 62 | 30 | 14 | 6 | 2 | 0 | -1 |
| Taille Totale | 2 | 1 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |
| Taille Utilisable | -2 | -1 | 2 | 6 | 14 | 30 | 62 | 126 | 254 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 1 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |
| | | | 8 | 16 | 32 | 64 | 128 | 256 | |
| | | | 12 | 24 | 48 | 96 | 192 | | |
| | | | 16 | 32 | 64 | 128 | 256 | | |
| | | | 20 | 40 | 80 | 160 | | | |
| | | | 24 | 48 | 96 | 192 | | | |
| | | | 28 | 56 | 112 | 224 | | | |
| | | | 32 | 64 | 128 | 256 | | | |
| | | | 36 | 72 | 144 | | | | |
| | | | 40 | 80 | 160 | | | | |
| | | | 44 | 88 | 176 | | | | |
| | | | 48 | 96 | 192 | | | | |
| | | | 52 | 104 | 208 | | | | |
| | | | 56 | 112 | 224 | | | | |
| | | | 60 | 120 | 240 | | | | |
| | | | 64 | 128 | 256 | | | | |
| | | | 68 | 136 | | | | | |
| | | | 72 | 144 | | | | | |
| | | | 76 | 152 | | | | | |
| | | | 80 | 160 | | | | | |
| | | | 84 | 168 | | | | | |
| | | | 88 | 176 | | | | | |
| | | | 92 | 184 | | | | | |
| | | | 96 | 192 | | | | | |
| | | | 100 | 200 | | | | | |
| | | | 104 | 208 | | | | | |
| | | | 108 | 216 | | | | | |
| | | | 112 | 224 | | | | | |
| | | | 116 | 232 | | | | | |
| | | | 120 | 240 | | | | | |
| | | | 124 | 248 | | | | | |
| | | | 128 | 256 | | | | | |
| | | | 132 | | | | | | 196 |
| | | | 136 | | | | | | 200 |
| | | | 140 | | | | | | 204 |
| | | | 144 | | | | | | 208 |
| | | | 148 | | | | | | 212 |
| | | | 152 | | | | | | 216 |
| | | | 156 | | | | | | 220 |
| | | | 160 | | | | | | 224 |
| | | | 164 | | | | | | 228 |
| | | | 168 | | | | | | 232 |
| | | | 172 | | | | | | 236 |
| | | | 176 | | | | | | 240 |
| | | | 180 | | | | | | 244 |
| | | | 184 | | | | | | 248 |
| | | | 188 | | | | | | 252 |
| | | | 192 | | | | | | 256 |



## Trace complète Radius (authentification et accounting)

```
User-Name = "herve@siris-maquette.fr" [flags = 0x00014500]
    CHAP-Password = "\0x01\0xe7\0xb1\0xa17m\0xd1w\0x994k\0x06t\0x03\0xd0\0xe0\0xf3" [flags = 0x00004500]
    NAS-IP-Address = 62.8.8.2 [flags = 0x00014500]
    Service-Type = Framed [flags = 0x00014600]
    Framed-Protocol = PPP [flags = 0x00014600]
    Framed-Compression = None [flags = 0x00004400]
    NAS-Port-Type = Async [flags = 0x00014500]
    NAS-Port = 1318913 [flags = 0x00014500]
    Port-Limit = 0 [flags = 0x00004600]
    Called-Station-Id = "860020304" [flags = 0x00014500]
    Calling-Station-Id = "170203005" [flags = 0x00014500]
    Acct-Session-Id = "0417405229" [flags = 0x00014500]
    NAS-Identifier = "AAPA2000" [flags = 0x00014500]
get_radrequest: Request from c0a8a278 (192.168.162.120[4798]) access, id = 16, len = 150
    Framed-Protocol = PPP [flags = 0x00014600]
    Framed-Compression = None [flags = 0x00004400]
    Port-Limit = 0 [flags = 0x00004600]
    Service-Type = Framed [flags = 0x00014600]
send_reply: Authentication: 16/2 'herve@siris-maquette.fr' via 192.168.162.120 from AAPA2000 port 1318913 $"0417405229" PPP
    User-Name = "herve@siris-maquette.fr" [flags = 0x00014500]
    Acct-Delay-Time = 0 [flags = 0x00014500]
    Acct-Session-Id = "0417405229" [flags = 0x00014500]
    Acct-Status-Type = Start [flags = 0x00014500]
    Acct-Authentic = RADIUS [flags = 0x00014500]
    Service-Type = 0 [flags = 0x00014600]
    Framed-IP-Address = 62.8.7.145 [flags = 0x00014600]
    Called-Station-Id = "860020304" [flags = 0x00014500]
    Calling-Station-Id = "170203005" [flags = 0x00014500]
    NAS-IP-Address = 62.8.8.2 [flags = 0x00014500]
    NAS-Port-Type = Async [flags = 0x00014500]
    NAS-Port = 1318913 [flags = 0x00014500]
    Tunnel-Type = L2TP [flags = 0x00014600]
    Tunnel-Medium-Type = IP [flags = 0x00014600]
    Tunnel-Client-EndPoint = "siris-ras" [flags = 0x00014400]
    Tunnel-Server-EndPoint = "62.8.7.145" [flags = 0x00014400]
    NAS-Identifier = "AAPA2000" [flags = 0x00014500]
    User-Id = "herve" [flags = 0x00014400]
    User-Realm = "siris-maquette.fr" [flags = 0x00014400]
    Proxy-State = "0" [flags = 0x00014000]
get_radrequest: Request from c0a8a241 (192.168.162.65[32939]) acct-req, id = 111, len = 201
send_reply: Accounting: 111/4 'herve@siris-maquette.fr' via 192.168.162.65 from AAPA2000 port 1318913 $"0417405229" 0 Start
    NAS-IP-Address = 192.168.161.80 [flags = 0x00014500]
    NAS-Port = 1 [flags = 0x00014500]
    NAS-Port-Type = Virtual [flags = 0x00014500]
    User-Name = "herve@siris-maquette.fr" [flags = 0x00014500]
    CHAP-Password = "\0x01\0xe7\0xb1\0xa17m\0xd1w\0x994k\0x06t\0x03\0xd0\0xe0\0xf3" [flags = 0x00004500]
    Service-Type = Framed [flags = 0x00014600]
    Framed-Protocol = PPP [flags = 0x00014600]
    NAS-Identifier = "HG01_MAQUETTE_NANTERRE" [flags = 0x00014500]
get_radrequest: Request from c0a8a278 (192.168.162.120[4798]) access, id = 17, len = 118
    Framed-Protocol = PPP [flags = 0x00014600]
    Service-Type = Framed [flags = 0x00014600]
send_reply: Authentication: 17/3 'herve@siris-maquette.fr' via 192.168.162.120 from HG01_MAQUETTE_NANTERRE port 1 PPP
    NAS-IP-Address = 192.168.161.80 [flags = 0x00014500]
    NAS-Port = 1 [flags = 0x00014500]
    NAS-Port-Type = Virtual [flags = 0x00014500]
    User-Name = "herve@siris-maquette.fr" [flags = 0x00014500]
    Acct-Status-Type = Start [flags = 0x00014500]
    Acct-Authentic = RADIUS [flags = 0x00014500]
    Service-Type = Framed [flags = 0x00014600]
    Acct-Session-Id = "00000083" [flags = 0x00014500]
    Framed-Protocol = PPP [flags = 0x00014600]
    Acct-Delay-Time = 0 [flags = 0x00014500]
    NAS-Identifier = "HG01_MAQUETTE_NANTERRE" [flags = 0x00014500]
    User-Id = "herve" [flags = 0x00014400]
    User-Realm = "siris-maquette.fr" [flags = 0x00014400]
    Proxy-State = "0" [flags = 0x00014000]
get_radrequest: Request from c0a8a241 (192.168.162.65[32939]) acct-req, id = 120, len = 156
send_reply: Accounting: 120/5 'herve@siris-maquette.fr' via 192.168.162.65 from HG01_MAQUETTE_NANTERRE port 1 $"00000083" PPP Start
    User-Name = "herve@siris-maquette.fr" [flags = 0x00014500]
    Acct-Delay-Time = 1 [flags = 0x00014500]
    Acct-Session-Id = "0417405229" [flags = 0x00014500]
    Acct-Status-Type = Stop [flags = 0x00014500]
    Acct-Authentic = RADIUS [flags = 0x00014500]
    Service-Type = 0 [flags = 0x00014600]
    Framed-IP-Address = 62.8.7.145 [flags = 0x00014600]
    Called-Station-Id = "860020304" [flags = 0x00014500]
    Calling-Station-Id = "170203005" [flags = 0x00014500]
    NAS-IP-Address = 62.8.8.2 [flags = 0x00014500]
    NAS-Port-Type = Async [flags = 0x00014500]
    NAS-Port = 1318913 [flags = 0x00014500]
    Tunnel-Type = L2TP [flags = 0x00014600]
    Tunnel-Medium-Type = IP [flags = 0x00014600]
    Tunnel-Client-EndPoint = "siris-ras" [flags = 0x00014400]
    Tunnel-Server-EndPoint = "62.8.7.145" [flags = 0x00014400]
    Acct-Terminate-Cause = NAS-Request [flags = 0x00014500]
    Cisco-Disconnect-Cause = Lost-carrier [flags = 0x00014400]
    Acct-Session-Time = 0 [flags = 0x00014500]
    Acct-Input-Packets = 67 [flags = 0x00014500]
    Acct-Output-Packets = 40 [flags = 0x00014500]
    Acct-Input-Octets = 5250 [flags = 0x00014500]
    Acct-Output-Octets = 3155 [flags = 0x00014500]
    NAS-Identifier = "AAPA2000" [flags = 0x00014500]
    User-Id = "herve" [flags = 0x00014400]
    User-Realm = "siris-maquette.fr" [flags = 0x00014400]
    Proxy-State = "0" [flags = 0x00014000]
get_radrequest: Request from c0a8a241 (192.168.162.65[32939]) acct-req, id = 252, len = 249
send_reply: Accounting: 252/6 'herve@siris-maquette.fr' via 192.168.162.65 from AAPA2000 port 1318913 $"0417405229" 0 Stop/NAS-Reque
st
    NAS-IP-Address = 192.168.161.80 [flags = 0x00014500]
    NAS-Port = 1 [flags = 0x00014500]
    NAS-Port-Type = Virtual [flags = 0x00014500]
    User-Name = "herve@siris-maquette.fr" [flags = 0x00014500]
    Acct-Status-Type = Stop [flags = 0x00014500]
    Acct-Authentic = RADIUS [flags = 0x00014500]
    Service-Type = Framed [flags = 0x00014600]
    Acct-Session-Id = "00000083" [flags = 0x00014500]
    Framed-Protocol = PPP [flags = 0x00014600]
    Framed-IP-Address = 194.183.205.246 [flags = 0x00014600]
    Acct-Terminate-Cause = Lost-Carrier [flags = 0x00014500]
    Acct-Input-Octets = 5173 [flags = 0x00014500]
    Acct-Output-Octets = 3424 [flags = 0x00014500]
    Acct-Input-Packets = 64 [flags = 0x00014500]
    Acct-Output-Packets = 36 [flags = 0x00014500]
    Acct-Session-Time = 39 [flags = 0x00014500]
    Acct-Delay-Time = 0 [flags = 0x00014500]
    NAS-Identifier = "HG01_MAQUETTE_NANTERRE" [flags = 0x00014500]
    Cisco-Disconnect-Cause = DCD-Detected-Then-Inactive [flags = 0x00014400]
    User-Id = "herve" [flags = 0x00014400]
    User-Realm = "siris-maquette.fr" [flags = 0x00014400]
    Proxy-State = "0" [flags = 0x00014000]
```

```
get_radrequest: Request from c0a8a241 (192.168.162.65[32939]) acct-req, id = 253, len = 210
send_reply: Accounting: 253/7 'herve@siris-maquette.fr' via 192.168.162.65 from HG01_MAQUETTE_NANTERRE port 1 $"00000083" PPP/194.183.205.246
Stop/Lost-Carrier
```

## TCP/IP V4 - Liste des numéros de Ports

PORT NUMBERS
Les numéros de ports sont divisés en 3 groupes :

- Les Ports connus (Well Known Ports) dont la valeur va de 0 à 1023,
- Les ports enregistrés (Registered Ports) dont la valeur va de 1024 à 49151,
- Les ports dynamiques et/ou privés (Dynamic and/or Private Ports) dont la valeur va de 49152 à 65535

Les "ports connus" sont contrôlés et assignés par l’IANA. Sur la plupart des systèmes, les "ports connus" ne peuvent être utilisés que par les processus système (un par un processus de l’utilisateur root) ou par les processus d’utilisateurs disposant des privilèges adéquat.

| Keyword | Decimal | Description | References |
|---|---|---|---|
| | 0/tcp | Reserved | |
| | 0/udp | Reserved | |
| tcpmux | 1/tcp | TCP Port Service Multiplexer | |
| tcpmux | 1/udp | TCP Port Service Multiplexer | |
| compressnet | 2/tcp | Management Utility | |
| compressnet | 2/udp | Management Utility | |
| compressnet | 3/tcp | Compression Process | |
| compressnet | 3/udp | Compression Process | |
| # | 4/tcp | Unassigned | |
| # | 4/udp | Unassigned | |
| rje | 5/tcp | Remote Job Entry | |
| rje | 5/udp | Remote Job Entry | |
| # | 6/tcp | Unassigned | |
| # | 6/udp | Unassigned | |
| echo | 7/tcp | Echo | |
| echo | 7/udp | Echo | |
| # | 8/tcp | Unassigned | |
| # | 8/udp | Unassigned | |
| discard | 9/tcp | Discard | |
| discard | 9/udp | Discard | |
| # | 10/tcp | Unassigned | |
| # | 10/udp | Unassigned | |
| systat | 11/tcp | Active Users | |
| systat | 11/udp | Active Users | |
| # | 12/tcp | Unassigned | |
| # | 12/udp | Unassigned | |
| daytime | 13/tcp | Daytime | |
| daytime | 13/udp | Daytime | |
| # | 14/tcp | Unassigned | |
| # | 14/udp | Unassigned | |
| # | 15/tcp | Unassigned [was netstat] | |
| # | 15/udp | Unassigned | |
| # | 16/tcp | Unassigned | |
| # | 16/udp | Unassigned | |
| qotd | 17/tcp | Quote of the Day | |
| qotd | 17/udp | Quote of the Day | |
| msp | 18/tcp | Message Send Protocol | |
| msp | 18/udp | Message Send Protocol | |
| chargen | 19/tcp | Character Generator | |
| chargen | 19/udp | Character Generator | |
| ftp-data | 20/tcp | File Transfer [Default Data] | |
| ftp-data | 20/udp | File Transfer [Default Data] | |
| ftp | 21/tcp | File Transfer [Control] | |
| ftp | 21/udp | File Transfer [Control] | |
| ssh | 22/tcp | SSH Remote Login Protocol | |
| ssh | 22/udp | SSH Remote Login Protocol | |
| telnet | 23/tcp | Telnet | |
| telnet | 23/udp | Telnet | |
| | 24/tcp | any private mail system | |
| | 24/udp | any private mail system | |
| smtp | 25/tcp | Simple Mail Transfer | |
| smtp | 25/udp | Simple Mail Transfer | |
| # | 26/tcp | Unassigned | |
| # | 26/udp | Unassigned | |
| nsw-fe | 27/tcp | NSW User System FE | |
| nsw-fe | 27/udp | NSW User System FE | |
| # | 28/tcp | Unassigned | |
| # | 28/udp | Unassigned | |
| msg-icp | 29/tcp | MSG ICP | |
| msg-icp | 29/udp | MSG ICP | |
| # | 30/tcp | Unassigned | |
| # | 30/udp | Unassigned | |
| msg-auth | 31/tcp | MSG Authentication | |
| msg-auth | 31/udp | MSG Authentication | |
| # | 32/tcp | Unassigned | |
| # | 32/udp | Unassigned | |
| dsp | 33/tcp | Display Support Protocol | |
| dsp | 33/udp | Display Support Protocol | |
| # | 34/tcp | Unassigned | |
| # | 34/udp | Unassigned | |
| | 35/tcp | any private printer server | |
| | 35/udp | any private printer server | |
| # | 36/tcp | Unassigned | |
| # | 36/udp | Unassigned | |
| time | 37/tcp | Time | |
| time | 37/udp | Time | |
| rap | 38/tcp | Route Access Protocol | |
| rap | 38/udp | Route Access Protocol | |
| rlp | 39/tcp | Resource Location Protocol | |
| rlp | 39/udp | Resource Location Protocol | |
| # | 40/tcp | Unassigned | |
| # | 40/udp | Unassigned | |
| graphics | 41/tcp | Graphics | |
| graphics | 41/udp | Graphics | |
| name | 42/tcp | Host Name Server | |
| name | 42/udp | Host Name Server | |
| nameserver | 42/tcp | Host Name Server | |
| nameserver | 42/udp | Host Name Server | |
| nicname | 43/tcp | Who Is | |
| nicname | 43/udp | Who Is | |
| mpm-flags | 44/tcp | MPM FLAGS Protocol | |
| mpm-flags | 44/udp | MPM FLAGS Protocol | |
| mpm | 45/tcp | Message Processing Module [recv] | |
| mpm | 45/udp | Message Processing Module [recv] | |
| mpm-snd | 46/tcp | MPM [default send] | |
| mpm-snd | 46/udp | MPM [default send] | |
| ni-ftp | 47/tcp | NI FTP | |
| ni-ftp | 47/udp | NI FTP | |
| auditd | 48/tcp | Digital Audit Daemon | |
| auditd | 48/udp | Digital Audit Daemon | |
| tacacs | 49/tcp | Login Host Protocol (TACACS) | |
| tacacs | 49/udp | Login Host Protocol (TACACS) | |
| re-mail-ck | 50/tcp | Remote Mail Checking Protocol | |
| re-mail-ck | 50/udp | Remote Mail Checking Protocol | |
| la-maint | 51/tcp | IMP Logical Address Maintenance | |
| la-maint | 51/udp | IMP Logical Address Maintenance | |
| xns-time | 52/tcp | XNS Time Protocol | |
| xns-time | 52/udp | XNS Time Protocol | |
| domain | 53/tcp | Domain Name Server | |
| domain | 53/udp | Domain Name Server | |
| xns-ch | 54/tcp | XNS Clearinghouse | |
| xns-ch | 54/udp | XNS Clearinghouse | |
| isi-gl | 55/tcp | ISI Graphics Language | |
| isi-gl | 55/udp | ISI Graphics Language | |
| xns-auth | 56/tcp | XNS Authentication | |
| xns-auth | 56/udp | XNS Authentication | |
| | 57/tcp | any private terminal access | |
| | 57/udp | any private terminal access | |
| xns-mail | 58/tcp | XNS Mail | |
| xns-mail | 58/udp | XNS Mail | |
| | 59/tcp | any private file service | |
| | 59/udp | any private file service | |
| | 60/tcp | Unassigned | |
| | 60/udp | Unassigned | |
| ni-mail | 61/tcp | NI MAIL | |
| ni-mail | 61/udp | NI MAIL | |
| acas | 62/tcp | ACA Services | |
| acas | 62/udp | ACA Services | |
| whois++ | 63/tcp | whois++ | |
| whois++ | 63/udp | whois++ | |
| covia | 64/tcp | Communications Integrator (CI) | |
| covia | 64/udp | Communications Integrator (CI) | |
| tacacs-ds | 65/tcp | TACACS-Database Service | |
| tacacs-ds | 65/udp | TACACS-Database Service | |
| sql*net | 66/tcp | Oracle SQL*NET | |
| sql*net | 66/udp | Oracle SQL*NET | |
| bootps | 67/tcp | Bootstrap Protocol Server | |
| bootps | 67/udp | Bootstrap Protocol Server | |
| bootpc | 68/tcp | Bootstrap Protocol Client | |
| bootpc | 68/udp | Bootstrap Protocol Client | |
| tftp | 69/tcp | Trivial File Transfer | |
| tftp | 69/udp | Trivial File Transfer | |
| gopher | 70/tcp | Gopher | |
| gopher | 70/udp | Gopher | |
| netrjs-1 | 71/tcp | Remote Job Service | |
| netrjs-1 | 71/udp | Remote Job Service | |
| netrjs-2 | 72/tcp | Remote Job Service | |
| netrjs-2 | 72/udp | Remote Job Service | |
| netrjs-3 | 73/tcp | Remote Job Service | |
| netrjs-3 | 73/udp | Remote Job Service | |
| netrjs-4 | 74/tcp | Remote Job Service | |
| netrjs-4 | 74/udp | Remote Job Service | |
| | 75/tcp | any private dial out service | |
| | 75/udp | any private dial out service | |
| deos | 76/tcp | Distributed External Object Store | |
| deos | 76/udp | Distributed External Object Store | |
| | 77/tcp | any private RJE service | |
| | 77/udp | any private RJE service | |
| vettcp | 78/tcp | vettcp | |
| vettcp | 78/udp | vettcp | |
| finger | 79/tcp | Finger | |
| finger | 79/udp | Finger | |
| http | 80/tcp | World Wide Web HTTP | |
| http | 80/udp | World Wide Web HTTP | |
| www | 80/tcp | World Wide Web HTTP | |
| www | 80/udp | World Wide Web HTTP | |
| www-http | 80/tcp | World Wide Web HTTP | |
| www-http | 80/udp | World Wide Web HTTP | |
| hosts2-ns | 81/tcp | HOSTS2 Name Server | |
| hosts2-ns | 81/udp | HOSTS2 Name Server | |
| xfer | 82/tcp | XFER Utility | |
| xfer | 82/udp | XFER Utility | |
| mit-ml-dev | 83/tcp | MIT ML Device | |
| mit-ml-dev | 83/udp | MIT ML Device | |
| ctf | 84/tcp | Common Trace Facility | |
| ctf | 84/udp | Common Trace Facility | |
| mit-ml-dev | 85/tcp | MIT ML Device | |
| mit-ml-dev | 85/udp | MIT ML Device | |
| mfcobol | 86/tcp | Micro Focus Cobol | |
| mfcobol | 86/udp | Micro Focus Cobol | |
| | 87/tcp | any private terminal link | |
| | 87/udp | any private terminal link | |
| kerberos | 88/tcp | Kerberos | |
| kerberos | 88/udp | Kerberos | |
| su-mit-tg | 89/tcp | SU/MIT Telnet Gateway | |
| su-mit-tg | 89/udp | SU/MIT Telnet Gateway | |
| dnsix | 90/tcp | DNSIX Securit Attribute Token Map | |
| dnsix | 90/udp | DNSIX Securit Attribute Token Map | |
| mit-dov | 91/tcp | MIT Dover Spooler | |
| mit-dov | 91/udp | MIT Dover Spooler | |
| npp | 92/tcp | Network Printing Protocol | |
| npp | 92/udp | Network Printing Protocol | |
| dcp | 93/tcp | Device Control Protocol | |
| dcp | 93/udp | Device Control Protocol | |
| objcall | 94/tcp | Tivoli Object Dispatcher | |
| objcall | 94/udp | Tivoli Object Dispatcher | |
| supdup | 95/tcp | SUPDUP | |
| supdup | 95/udp | SUPDUP | |
| dixie | 96/tcp | DIXIE Protocol Specification | |
| dixie | 96/udp | DIXIE Protocol Specification | |
| swift-rvf | 97/tcp | Swift Remote Virtural File Protocol | |
| swift-rvf | 97/udp | Swift Remote Virtural File Protocol | |
| tacnews | 98/tcp | TAC News | |
| tacnews | 98/udp | TAC News | |
| metagram | 99/tcp | Metagram Relay | |
| metagram | 99/udp | Metagram Relay | |
| newacct | 100/tcp | [unauthorized use] | |
| hostname | 101/tcp | NIC Host Name Server | |
| hostname | 101/udp | NIC Host Name Server | |
| iso-tsap | 102/tcp | ISO-TSAP Class 0 | |
| iso-tsap | 102/udp | ISO-TSAP Class 0 | |
| gppitnp | 103/tcp | Genesis Point-to-Point Trans Net | |
| gppitnp | 103/udp | Genesis Point-to-Point Trans Net | |
| acr-nema | 104/tcp | ACR-NEMA Digital Imag. & Comm. 300 | |
| acr-nema | 104/udp | ACR-NEMA Digital Imag. & Comm. 300 | |
| cso | 105/tcp | CCSO name server protocol | |
| cso | 105/tcp | CCSO name server protocol | |
| csnet-ns | 105/tcp | Mailbox Name Nameserver | |
| csnet-ns | 105/udp | Mailbox Name Nameserver | |
| 3com-tsmux | 106/tcp | 3COM-TSMUX | |
| 3com-tsmux | 106/udp | 3COM-TSMUX | |
| rtelnet | 107/tcp | Remote Telnet Service | |
| rtelnet | 107/udp | Remote Telnet Service | |
| snagas | 108/tcp | SNA Gateway Access Server | |
| snagas | 108/udp | SNA Gateway Access Server | |
| pop2 | 109/tcp | Post Office Protocol - Version 2 | |
| pop2 | 109/udp | Post Office Protocol - Version 2 | |
| pop3 | 110/tcp | Post Office Protocol - Version 3 | |
| pop3 | 110/udp | Post Office Protocol - Version 3 | |
| sunrpc | 111/tcp | SUN Remote Procedure Call | |
| sunrpc | 111/udp | SUN Remote Procedure Call | |
| mcidas | 112/tcp | McIDAS Data Transmission Protocol | |
| mcidas | 112/udp | McIDAS Data Transmission Protocol | |
| ident | 113/tcp | | |
| auth | 113/tcp | Authentication Service | |
| auth | 113/udp | Authentication Service | |
| audionews | 114/tcp | Audio News Multicast | |
| audionews | 114/udp | Audio News Multicast | |
| sftp | 115/tcp | Simple File Transfer Protocol | |
| sftp | 115/udp | Simple File Transfer Protocol | |
| ansanotify | 116/tcp | ANSA REX Notify | |
| ansanotify | 116/udp | ANSA REX Notify | |
| uucp-path | 117/tcp | UUCP Path Service | |
| uucp-path | 117/udp | UUCP Path Service | |

```
sqlserv         118/tcp    SQL Services
sqlserv         118/udp    SQL Services
nntp            119/tcp    Network News Transfer Protocol
nntp            119/udp    Network News Transfer Protocol
cfdptkt         120/tcp    CFDPTKT
cfdptkt         120/udp    CFDPTKT
erpc            121/tcp    Encore Expedited Remote Pro.Call
erpc            121/udp    Encore Expedited Remote Pro.Call
smakynet        122/tcp    SMAKYNET
smakynet        122/udp    SMAKYNET
ntp             123/tcp    Network Time Protocol
ntp             123/udp    Network Time Protocol
ansatrader      124/tcp    ANSA REX Trader
ansatrader      124/udp    ANSA REX Trader
locus-map       125/tcp    Locus PC-Interface Net Map Ser
locus-map       125/udp    Locus PC-Interface Net Map Ser
unitary         126/tcp    Unisys Unitary Login
unitary         126/udp    Unisys Unitary Login
locus-con       127/tcp    Locus PC-Interface Conn Server
locus-con       127/udp    Locus PC-Interface Conn Server
gss-xlicen      128/tcp    GSS X License Verification
gss-xlicen      128/udp    GSS X License Verification
pwdgen          129/tcp    Password Generator Protocol
pwdgen          129/udp    Password Generator Protocol
cisco-fna       130/tcp    cisco FNATIVE
cisco-fna       130/udp    cisco FNATIVE
cisco-tna       131/tcp    cisco TNATIVE
cisco-tna       131/udp    cisco TNATIVE
cisco-sys       132/tcp    cisco SYSMAINT
cisco-sys       132/udp    cisco SYSMAINT
statsrv         133/tcp    Statistics Service
statsrv         133/udp    Statistics Service
ingres-net      134/tcp    INGRES-NET Service
ingres-net      134/udp    INGRES-NET Service
epmap           135/tcp    DCE endpoint resolution
epmap           135/udp    DCE endpoint resolution
profile         136/tcp    PROFILE Naming System
profile         136/udp    PROFILE Naming System
netbios-ns      137/tcp    NETBIOS Name Service
netbios-ns      137/udp    NETBIOS Name Service
netbios-dgm     138/tcp    NETBIOS Datagram Service
netbios-dgm     138/udp    NETBIOS Datagram Service
netbios-ssn     139/tcp    NETBIOS Session Service
netbios-ssn     139/udp    NETBIOS Session Service
emfis-data      140/tcp    EMFIS Data Service
emfis-data      140/udp    EMFIS Data Service
emfis-cntl      141/tcp    EMFIS Control Service
emfis-cntl      141/udp    EMFIS Control Service
bl-idm          142/tcp    Britton-Lee IDM
bl-idm          142/udp    Britton-Lee IDM
imap            143/tcp    Internet Message Access Protocol
imap            143/udp    Internet Message Access Protocol
news            144/tcp    NewS
news            144/udp    NewS
uaac            145/tcp    UAAC Protocol
uaac            145/udp    UAAC Protocol
iso-tp0         146/tcp    ISO-IP0
iso-tp0         146/udp    ISO-IP0
iso-ip          147/tcp    ISO-IP
iso-ip          147/udp    ISO-IP
jargon          148/tcp    Jargon
jargon          148/udp    Jargon
aed-512         149/tcp    AED 512 Emulation Service
aed-512         149/udp    AED 512 Emulation Service
sql-net         150/tcp    SQL-NET
sql-net         150/udp    SQL-NET
hems            151/tcp    HEMS
hems            151/udp    HEMS
bftp            152/tcp    Background File Transfer Program
bftp            152/udp    Background File Transfer Program
sgmp            153/tcp    SGMP
sgmp            153/udp    SGMP
netsc-prod      154/tcp    NETSC
netsc-prod      154/udp    NETSC
netsc-dev       155/tcp    NETSC
netsc-dev       155/udp    NETSC
sqlsrv          156/tcp    SQL Service
sqlsrv          156/udp    SQL Service
knet-cmp        157/tcp    KNET/VM Command/Message Protocol
knet-cmp        157/udp    KNET/VM Command/Message Protocol
pcmail-srv      158/tcp    PCMail Server
pcmail-srv      158/udp    PCMail Server
nss-routing     159/tcp    NSS-Routing
nss-routing     159/udp    NSS-Routing
sgmp-traps      160/tcp    SGMP-TRAPS
sgmp-traps      160/udp    SGMP-TRAPS
snmp            161/tcp    SNMP
snmp            161/udp    SNMP
snmptrap        162/tcp    SNMPTRAP
snmptrap        162/udp    SNMPTRAP
cmip-man        163/tcp    CMIP/TCP Manager
cmip-man        163/udp    CMIP/TCP Manager
cmip-agent      164/tcp    CMIP/TCP Agent
smip-agent      164/udp    CMIP/TCP Agent
xns-courier     165/tcp    Xerox
xns-courier     165/udp    Xerox
s-net           166/tcp    Sirius Systems
s-net           166/udp    Sirius Systems
namp            167/tcp    NAMP
namp            167/udp    NAMP
rsvd            168/tcp    RSVD
rsvd            168/udp    RSVD
send            169/tcp    SEND
send            169/udp    SEND
print-srv       170/tcp    Network PostScript
print-srv       170/udp    Network PostScript
multiplex       171/tcp    Network Innovations Multiplex
multiplex       171/udp    Network Innovations Multiplex
cl/1            172/tcp    Network Innovations CL/1
cl/1            172/udp    Network Innovations CL/1
xyplex-mux      173/tcp    Xyplex
xyplex-mux      173/udp    Xyplex
mailq           174/tcp    MAILQ
mailq           174/udp    MAILQ
vmnet           175/tcp    VMNET
vmnet           175/udp    VMNET
genrad-mux      176/tcp    GENRAD-MUX
genrad-mux      176/udp    GENRAD-MUX
xdmcp           177/tcp    X Display Manager Control Protocol
xdmcp           177/udp    X Display Manager Control Protocol
nextstep        178/tcp    NextStep Window Server
NextStep        178/udp    NextStep Window Server
bgp             179/tcp    Border Gateway Protocol
bgp             179/udp    Border Gateway Protocol
ris             180/tcp    Intergraph
ris             180/udp    Intergraph
unify           181/tcp    Unify
unify           181/udp    Unify
audit           182/tcp    Unisys Audit SITP
audit           182/udp    Unisys Audit SITP
ocbinder        183/tcp    OCBinder
ocbinder        183/udp    OCBinder
ocserver        184/tcp    OCServer
ocserver        184/udp    OCServer
remote-kis      185/tcp    Remote-KIS
remote-kis      185/udp    Remote-KIS
kis             186/tcp    KIS Protocol
kis             186/udp    KIS Protocol
aci             187/tcp    Application Communication Interface
aci             187/udp    Application Communication Interface
mumps           188/tcp    Plus Five's MUMPS
mumps           188/udp    Plus Five's MUMPS
qft             189/tcp    Queued File Transport
qft             189/udp    Queued File Transport
gacp            190/tcp    Gateway Access Control Protocol
cacp            190/udp    Gateway Access Control Protocol
prospero        191/tcp    Prospero Directory Service
prospero        191/udp    Prospero Directory Service
osu-nms         192/tcp    OSU Network Monitoring System
osu-nms         192/udp    OSU Network Monitoring System
srmp            193/tcp    Spider Remote Monitoring Protocol
srmp            193/udp    Spider Remote Monitoring Protocol
irc             194/tcp    Internet Relay Chat Protocol
irc             194/udp    Internet Relay Chat Protocol
dn6-nlm-aud     195/tcp    DNSIX Network Level Module Audit
dn6-nlm-aud     195/udp    DNSIX Network Level Module Audit
dn6-smm-red     196/tcp    DNSIX Session Mgt Module Audit Redir
dn6-smm-red     196/udp    DNSIX Session Mgt Module Audit Redir
dls             197/tcp    Directory Location Service
dls             197/udp    Directory Location Service
dls-mon         198/tcp    Directory Location Service Monitor
dls-mon         198/udp    Directory Location Service Monitor
smux            199/tcp    SMUX
smux            199/udp    SMUX
src             200/tcp    IBM System Resource Controller
src             200/udp    IBM System Resource Controller
at-rtmp         201/tcp    AppleTalk Routing Maintenance
at-rtmp         201/udp    AppleTalk Routing Maintenance
at-nbp          202/tcp    AppleTalk Name Binding
at-nbp          202/udp    AppleTalk Name Binding
at-3            203/tcp    AppleTalk Unused
at-3            203/udp    AppleTalk Unused
at-echo         204/tcp    AppleTalk Echo
at-echo         204/udp    AppleTalk Echo
at-5            205/tcp    AppleTalk Unused
at-5            205/udp    AppleTalk Unused
at-zis          206/tcp    AppleTalk Zone Information
at-zis          206/udp    AppleTalk Zone Information
at-7            207/tcp    AppleTalk Unused
at-7            207/udp    AppleTalk Unused
at-8            208/tcp    AppleTalk Unused
at-8            208/udp    AppleTalk Unused
qmtp            209/tcp    The Quick Mail Transfer Protocol
qmtp            209/udp    The Quick Mail Transfer Protocol
z39.50          210/tcp    ANSI Z39.50
z39.50          210/udp    ANSI Z39.50
914c/g          211/tcp    Texas Instruments 914C/G Terminal
914c/g          211/udp    Texas Instruments 914C/G Terminal
anet            212/tcp    ATEXSSTR
anet            212/udp    ATEXSSTR
ipx             213/tcp    IPX
ipx             213/udp    IPX
vmpwscs         214/tcp    VM PWSCS
vmpwscs         214/udp    VM PWSCS
softpc          215/tcp    Insignia Solutions
softpc          215/udp    Insignia Solutions
CAIlic          216/tcp    Computer Associates Int'l License Server
CAIlic          216/udp    Computer Associates Int'l License Server
dbase           217/tcp    dBASE Unix
dbase           217/udp    dBASE Unix
mpp             218/tcp    Netix Message Posting Protocol
mpp             218/udp    Netix Message Posting Protocol
uarps           219/tcp    Unisys ARPs
uarps           219/udp    Unisys ARPs
imap3           220/tcp    Interactive Mail Access Protocol v3
imap3           220/udp    Interactive Mail Access Protocol v3
fln-spx         221/tcp    Berkeley rlogind with SPX auth
fln-spx         221/udp    Berkeley rlogind with SPX auth
rsh-spx         222/tcp    Berkeley rshd with SPX auth
rsh-spx         222/udp    Berkeley rshd with SPX auth
cdc             223/tcp    Certificate Distribution Center
cdc             223/udp    Certificate Distribution Center
#               224-241    Reserved
direct          242/tcp    Direct
direct          242/udp    Direct
sur-meas        243/tcp    Survey Measurement
sur-meas        243/udp    Survey Measurement
dayna           244/tcp    Dayna
dayna           244/udp    Dayna
link            245/tcp    LINK
link            245/udp    LINK
dsp3270         246/tcp    Display Systems Protocol
dsp3270         246/udp    Display Systems Protocol
#               247-255    Reserved
rap             256/tcp    RAP
rap             256/udp    RAP
set             257/tcp    Secure Electronic Transaction
set             257/udp    Secure Electronic Transaction
yak-chat        258/tcp    Yak Winsock Personal Chat
yak-chat        258/udp    Yak Winsock Personal Chat
esro-gen        259/tcp    Efficient Short Remote Operations
esro-gen        259/udp    Efficient Short Remote Operations
openport        260/tcp    Openport
openport        260/udp    Openport
naming-iiop-ssl 261/tcp    IIOP Naming Service (SSL)
naming-iiop-ssl 261/udp    IIOP Naming Service (SSL)
arcisdms        262/tcp    Arcisdms
arcisdms        262/udp    Arcisdms
hdap            263/tcp    HDAP
hdap            263/udp    HDAP
#               264-279    Unassigned
http-mgmt       280/tcp    http-mgmt
http-mgmt       280/udp    http-mgmt
personal-link   281/tcp    Personal Link
personal-link   281/udp    Personal Link
cableport-ax    282/tcp    Cable Port A/X
```

| | | |
|---|---|---|
| cableport-ax | 282/udp | Cable Port A/X |
| # | 283-308 | Unassigned |
| entrusttime | 309/tcp | EntrustTime |
| entrusttime | 309/udp | EntrustTime |
| # | 310-343 | Unassigned |
| pdap | 344/tcp | Prospero Data Access Protocol |
| pdap | 344/udp | Prospero Data Access Protocol |
| pawserv | 345/tcp | Perf Analysis Workbench |
| pawserv | 345/udp | Perf Analysis Workbench |
| zserv | 346/tcp | Zebra server |
| zserv | 346/udp | Zebra server |
| fatserv | 347/tcp | Fatmen Server |
| fatserv | 347/udp | Fatmen Server |
| csi-sgwp | 348/tcp | Cabletron Management Protocol |
| csi-sgwp | 348/udp | Cabletron Management Protocol |
| mftp | 349/tcp | mftp |
| mftp | 349/udp | mftp |
| matip-type-a | 350/tcp | MATIP Type A |
| matip-type-a | 350/udp | MATIP Type A |
| matip-type-b | 351/tcp | MATIP Type B |
| matip-type-b | 351/udp | MATIP Type B |
| # | 352-370 | Unassigned |
| clearcase | 371/tcp | Clearcase |
| clearcase | 371/udp | Clearcase |
| ulistproc | 372/tcp | ListProcessor |
| ulistproc | 372/udp | ListProcessor |
| legent-1 | 373/tcp | Legent Corporation |
| legent-1 | 373/udp | Legent Corporation |
| legent-2 | 374/tcp | Legent Corporation |
| legent-2 | 374/udp | Legent Corporation |
| hassle | 375/tcp | Hassle |
| hassle | 375/udp | Hassle |
| nip | 376/tcp | Amiga Envoy Network Inquiry Proto |
| nip | 376/udp | Amiga Envoy Network Inquiry Proto |
| tnETOS | 377/tcp | NEC Corporation |
| tnETOS | 377/udp | NEC Corporation |
| dsETOS | 378/tcp | NEC Corporation |
| dsETOS | 378/udp | NEC Corporation |
| is99c | 379/tcp | TIA/EIA/IS-99 modem client |
| is99c | 379/udp | TIA/EIA/IS-99 modem client |
| is99s | 380/tcp | TIA/EIA/IS-99 modem server |
| is99s | 380/udp | TIA/EIA/IS-99 modem server |
| hp-collector | 381/tcp | hp performance data collector |
| hp-collector | 381/udp | hp performance data collector |
| hp-managed-node | 382/tcp | hp performance data managed node |
| hp-managed-node | 382/udp | hp performance data managed node |
| hp-alarm-mgr | 383/tcp | hp performance data alarm manager |
| hp-alarm-mgr | 383/udp | hp performance data alarm manager |
| arns | 384/tcp | A Remote Network Server System |
| arns | 384/udp | A Remote Network Server System |
| ibm-app | 385/tcp | IBM Application |
| ibm-app | 385/udp | IBM Application |
| asa | 386/tcp | ASA Message Router Object Def. |
| asa | 386/udp | ASA Message Router Object Def. |
| aurp | 387/tcp | Appletalk Update-Based Routing Pro. |
| aurp | 387/udp | Appletalk Update-Based Routing Pro. |
| unidata-ldm | 388/tcp | Unidata LDM Version 4 |
| unidata-ldm | 388/udp | Unidata LDM Version 4 |
| ldap | 389/tcp | Lightweight Directory Access Protocol |
| ldap | 389/udp | Lightweight Directory Access Protocol |
| uis | 390/tcp | UIS |
| uis | 390/udp | UIS |
| synotics-relay | 391/tcp | SynOptics SNMP Relay Port |
| synotics-relay | 391/udp | SynOptics SNMP Relay Port |
| synotics-broker | 392/tcp | SynOptics Port Broker Port |
| synotics-broker | 392/udp | SynOptics Port Broker Port |
| dis | 393/tcp | Data Interpretation System |
| dis | 393/udp | Data Interpretation System |
| embl-ndt | 394/tcp | EMBL Nucleic Data Transfer |
| embl-ndt | 394/udp | EMBL Nucleic Data Transfer |
| netcp | 395/tcp | NETscout Control Protocol |
| netcp | 395/udp | NETscout Control Protocol |
| netware-ip | 396/tcp | Novell Netware over IP |
| netware-ip | 396/udp | Novell Netware over IP |
| mptn | 397/tcp | Multi Protocol Trans. Net. |
| mptn | 397/udp | Multi Protocol Trans. Net. |
| kryptolan | 398/tcp | Kryptolan |
| kryptolan | 398/udp | Kryptolan |
| iso-tsap-c2 | 399/tcp | ISO Transport Class 2 Non-Control over TCP |
| iso-tsap-c2 | 399/udp | ISO Transport Class 2 Non-Control over TCP |
| work-sol | 400/tcp | Workstation Solutions |
| work-sol | 400/udp | Workstation Solutions |
| ups | 401/tcp | Uninterruptible Power Supply |
| ups | 401/udp | Uninterruptible Power Supply |
| genie | 402/tcp | Genie Protocol |
| genie | 402/udp | Genie Protocol |
| decap | 403/tcp | decap |
| decap | 403/udp | decap |
| nced | 404/tcp | nced |
| nced | 404/udp | nced |
| ncld | 405/tcp | ncld |
| ncld | 405/udp | ncld |
| imsp | 406/tcp | Interactive Mail Support Protocol |
| imsp | 406/udp | Interactive Mail Support Protocol |
| timbuktu | 407/tcp | Timbuktu |
| timbuktu | 407/udp | Timbuktu |
| prm-sm | 408/tcp | Prospero Resource Manager Sys. Man. |
| prm-sm | 408/udp | Prospero Resource Manager Sys. Man. |
| prm-nm | 409/tcp | Prospero Resource Manager Node Man. |
| prm-nm | 409/udp | Prospero Resource Manager Node Man. |
| decladebug | 410/tcp | DECLadebug Remote Debug Protocol |
| decladebug | 410/udp | DECLadebug Remote Debug Protocol |
| rmt | 411/tcp | Remote MT Protocol |
| rmt | 411/udp | Remote MT Protocol |
| synoptics-trap | 412/tcp | Trap Convention Port |
| synoptics-trap | 412/udp | Trap Convention Port |
| smsp | 413/tcp | SMSP |
| smsp | 413/udp | SMSP |
| infoseek | 414/tcp | InfoSeek |
| infoseek | 414/udp | InfoSeek |
| bnet | 415/tcp | BNet |
| bnet | 415/udp | BNet |
| silverplatter | 416/tcp | Silverplatter |
| silverplatter | 416/udp | Silverplatter |
| onmux | 417/tcp | Onmux |
| onmux | 417/udp | Onmux |
| hyper-g | 418/tcp | Hyper-G |
| hyper-g | 418/udp | Hyper-G |
| ariel1 | 419/tcp | Ariel |
| ariel1 | 419/udp | Ariel |
| smpte | 420/tcp | SMPTE |
| smpte | 420/udp | SMPTE |
| ariel2 | 421/tcp | Ariel |
| ariel2 | 421/udp | Ariel |
| ariel3 | 422/tcp | Ariel |
| ariel3 | 422/udp | Ariel |
| opc-job-start | 423/tcp | IBM Operations Planning and Control Start |
| opc-job-start | 423/udp | IBM Operations Planning and Control Start |
| opc-job-track | 424/tcp | IBM Operations Planning and Control Track |
| opc-job-track | 424/udp | IBM Operations Planning and Control Track |
| icad-el | 425/tcp | ICAD |
| icad-el | 425/udp | ICAD |
| smartsdp | 426/tcp | smartsdp |
| smartsdp | 426/udp | smartsdp |
| svrloc | 427/tcp | Server Location |
| svrloc | 427/udp | Server Location |
| ocs_cmu | 428/tcp | OCS_CMU |
| ocs_cmu | 428/udp | OCS_CMU |
| ocs_amu | 429/tcp | OCS_AMU |
| ocs_amu | 429/udp | OCS_AMU |
| utmpsd | 430/tcp | UTMPSD |
| utmpsd | 430/udp | UTMPSD |
| utmpcd | 431/tcp | UTMPCD |
| utmpcd | 431/udp | UTMPCD |
| iasd | 432/tcp | IASD |
| iasd | 432/udp | IASD |
| nnsp | 433/tcp | NNSP |
| nnsp | 433/udp | NNSP |
| mobileip-agent | 434/tcp | MobileIP-Agent |
| mobileip-agent | 434/udp | MobileIP-Agent |
| mobilip-mn | 435/tcp | MobilIP-MN |
| mobilip-mn | 435/udp | MobilIP-MN |
| dna-cml | 436/tcp | DNA-CML |
| dna-cml | 436/udp | DNA-CML |
| comscm | 437/tcp | comscm |
| comscm | 437/udp | comscm |
| dsfgw | 438/tcp | dsfgw |
| dsfgw | 438/udp | dsfgw |
| dasp | 439/tcp | dasp |
| dasp | 439/udp | dasp |
| sgcp | 440/tcp | sgcp |
| sgcp | 440/udp | sgcp |
| decvms-sysmgt | 441/tcp | decvms-sysmgt |
| decvms-sysmgt | 441/udp | decvms-sysmgt |
| cvc_hostd | 442/tcp | cvc_hostd |
| cvc_hostd | 442/udp | cvc_hostd |
| https | 443/tcp | https  MCom |
| https | 443/udp | https  MCom |
| snpp | 444/tcp | Simple Network Paging Protocol |
| snpp | 444/udp | Simple Network Paging Protocol |
| microsoft-ds | 445/tcp | Microsoft-DS |
| microsoft-ds | 445/udp | Microsoft-DS |
| ddm-rdb | 446/tcp | DDM-RDB |
| ddm-rdb | 446/udp | DDM-RDB |
| ddm-dfm | 447/tcp | DDM-RFM |
| ddm-dfm | 447/udp | DDM-RFM |
| ddm-byte | 448/tcp | DDM-BYTE |
| ddm-byte | 448/udp | DDM-BYTE |
| as-servermap | 449/tcp | AS Server Mapper |
| as-servermap | 449/udp | AS Server Mapper |
| tserver | 450/tcp | TServer |
| tserver | 450/udp | TServer |
| sfs-smp-net | 451/tcp | Cray Network Semaphore server |
| sfs-smp-net | 451/udp | Cray Network Semaphore server |
| sfs-config | 452/tcp | Cray SFS config server |
| sfs-config | 452/udp | Cray SFS config server |
| creativeserver | 453/tcp | CreativeServer |
| creativeserver | 453/udp | CreativeServer |
| contentserver | 454/tcp | ContentServer |
| contentserver | 454/udp | ContentServer |
| creativepartnr | 455/tcp | CreativePartnr |
| creativepartnr | 455/udp | CreativePartnr |
| macon-tcp | 456/tcp | macon-tcp |
| macon-udp | 456/udp | macon-udp |
| scohelp | 457/tcp | scohelp |
| scohelp | 457/udp | scohelp |
| appleqtc | 458/tcp | apple quick time |
| appleqtc | 458/udp | apple quick time |
| ampr-rcmd | 459/tcp | ampr-rcmd |
| ampr-rcmd | 459/udp | ampr-rcmd |
| skronk | 460/tcp | skronk |
| skronk | 460/udp | skronk |
| datasurfsrv | 461/tcp | DataRampSrv |
| datasurfsrv | 461/udp | DataRampSrv |
| datasurfsrvsec | 462/tcp | DataRampSrvSec |
| datasurfsrvsec | 462/udp | DataRampSrvSec |
| alpes | 463/tcp | alpes |
| alpes | 463/udp | alpes |
| kpasswd | 464/tcp | kpasswd |
| kpasswd | 464/udp | kpasswd |
| ssmtp | 465/tcp | ssmtp |
| ssmtp | 465/udp | ssmtp |
| digital-vrc | 466/tcp | digital-vrc |
| digital-vrc | 466/udp | digital-vrc |
| mylex-mapd | 467/tcp | mylex-mapd |
| mylex-mapd | 467/udp | mylex-mapd |
| photuris | 468/tcp | proturis |
| photuris | 468/udp | proturis |
| rcp | 469/tcp | Radio Control Protocol |
| rcp | 469/udp | Radio Control Protocol |
| scx-proxy | 470/tcp | scx-proxy |
| scx-proxy | 470/udp | scx-proxy |
| mondex | 471/tcp | Mondex |
| mondex | 471/udp | Mondex |
| ljk-login | 472/tcp | ljk-login |
| ljk-login | 472/udp | ljk-login |
| hybrid-pop | 473/tcp | hybrid-pop |
| hybrid-pop | 473/udp | hybrid-pop |
| tn-tl-w1 | 474/tcp | tn-tl-w1 |
| tn-tl-w2 | 474/udp | tn-tl-w2 |
| tcpnethaspsrv | 475/tcp | tcpnethaspsrv |
| tcpnethaspsrv | 475/tcp | tcpnethaspsrv |
| tn-tl-fd1 | 476/tcp | tn-tl-fd1 |
| tn-tl-fd1 | 476/udp | tn-tl-fd1 |
| ss7ns | 477/tcp | ss7ns |
| ss7ns | 477/udp | ss7ns |
| spsc | 478/tcp | spsc |
| spsc | 478/udp | spsc |
| iafserver | 479/tcp | iafserver |
| iafserver | 479/udp | iafserver |
| iafdbase | 480/tcp | iafdbase |
| iafdbase | 480/udp | iafdbase |
| ph | 481/tcp | Ph service |
| ph | 481/udp | Ph service |
| bgs-nsi | 482/tcp | bgs-nsi |
| bgs-nsi | 482/udp | bgs-nsi |

```
ulpnet          483/tcp    ulpnet
ulpnet          483/udp    ulpnet
integra-sme     484/tcp    Integra Software Management Environment
integra-sme     484/udp    Integra Software Management Environment
powerburst      485/tcp    Air Soft Power Burst
powerburst      485/udp    Air Soft Power Burst
avian           486/tcp    avian
avian           486/udp    avian
saft            487/tcp    saft
saft            487/udp    saft
gss-http        488/tcp    gss-http
gss-http        488/udp    gss-http
nest-protocol   489/tcp    nest-protocol
nest-protocol   489/udp    nest-protocol
micom-pfs       490/tcp    micom-pfs
micom-pfs       490/udp    micom-pfs
go-login        491/tcp    go-login
go-login        491/udp    go-login
ticf-1          492/tcp    Transport Independent Convergence for FNA
ticf-1          492/udp    Transport Independent Convergence for FNA
ticf-2          493/tcp    Transport Independent Convergence for FNA
ticf-2          493/udp    Transport Independent Convergence for FNA
pov-ray         494/tcp    POV-Ray
pov-ray         494/udp    POV-Ray
intecourier     495/tcp    intecourier
intecourier     495/udp    intecourier
pim-rp-disc     496/tcp    PIM-RP-DISC
pim-rp-disc     496/udp    PIM-RP-DISC
dantz           497/tcp    dantz
dantz           497/udp    dantz
siam            498/tcp    siam
siam            498/udp    siam
iso-ill         499/tcp    ISO ILL Protocol
iso-ill         499/udp    ISO ILL Protocol
isakmp          500/tcp    isakmp
isakmp          500/udp    isakmp
stmf            501/tcp    STMF
stmf            501/udp    STMF
asa-appl-proto  502/tcp    asa-appl-proto
asa-appl-proto  502/udp    asa-appl-proto
intrinsa        503/tcp    Intrinsa
intrinsa        503/udp    Intrinsa
citadel         504/tcp    citadel
citadel         504/udp    citadel
mailbox-lm      505/tcp    mailbox-lm
mailbox-lm      505/udp    mailbox-lm
ohimsrv         506/tcp    ohimsrv
ohimsrv         506/udp    ohimsrv
crs             507/tcp    crs
crs             507/udp    crs
xvttp           508/tcp    xvttp
xvttp           508/udp    xvttp
snare           509/tcp    snare
snare           509/udp    snare
fcp             510/tcp    FirstClass Protocol
fcp             510/udp    FirstClass Protocol
mynet           511/tcp    mynet-as
mynet           511/udp    mynet-as
exec               512/tcp     remote process execution; authentication
performed using
#                          passwords and UNIX loppgin names
comsat          512/udp
biff             512/udp    used by mail system to notify users of new
mail received; currently
#                           receives messages only from processes on the
same machine
login                513/tcp      remote login a la telnet; automatic
authentication performed
#                                based on priviledged port numbers and
distributed data bases which
#                          identify "authentication domains"
who              513/udp    maintains data bases showing who's logged in
to machines on a local
#                          net and the load average of the machine
shell                514/tcp       cmd  /  like  exec,  but  automatic
authentication
#                          is performed as for login server
syslog          514/udp
printer         515/tcp    spooler
printer         515/udp    spooler
videotex        516/tcp    videotex
videotex        516/udp    videotex
talk               517/tcp     like tenex link, but across machine -
unfortunately, doesn't
#                          use link protocol (this is actually just a
rendezvous port from
#                          which a tcp connection is established)
talk               517/udp     like tenex link, but across machine -
unfortunately, doesn't
#                             use link protocol (this is actually just a
rendezvous port from
#                          which a tcp connection is established)
ntalk           518/tcp
ntalk           518/udp
utime           519/tcp    unixtime
utime           519/udp    unixtime
efs             520/tcp    extended file name server
router           520/udp    local routing process (on site);uses variant
of Xerox NS routing
#                          information protocol
ripng           521/tcp    ripng
ripng           521/udp    ripng
ulp             522/tcp    ULP
ulp             522/udp    ULP
ibm-db2         523/tcp    IBM-DB2
ibm-db2         523/tcp    IBM-DB2
ncp             524/tcp    NCP
ncp             524/udp    NCP
timed           525/tcp    timeserver
timed           525/udp    timeserver
tempo            526/tcp    newdate
tempo            526/udp    newdate
stx             527/tcp    Stock IXChange
stx             527/udp    Stock IXChange
custix          528/tcp    Customer IXChange
custix          528/udp    Customer IXChange
irc-serv        529/tcp    IRC-SERV
irc-serv        529/tcp    IRC-SERV
courier         530/tcp    rpc
courier         530/udp    rpc
conference      531/tcp    chat
conference      531/udp    chat
netnews         532/tcp    readnews
netnews         532/udp    readnews
netwall         533/tcp    for emergency broadcasts
netwall         533/udp    for emergency broadcasts
mm-admin        534/tcp    MegaMedia Admin
mm-admin        534/udp    MegaMedia Admin
iiop            535/tcp    iiop
iiop            535/udp    iiop
opalis-rdv      536/tcp    opalis-rdv
opalis-rdv      536/udp    opalis-rdv
nmsp            537/tcp    Networked Media Streaming Protocol
nmsp            537/udp    Networked Media Streaming Protocol
gdomap          538/tcp    gdomap
gdomap          538/udp    gdomap
apertus-ldp     539/tcp    Apertus Technologies Load Determination
apertus-ldp     539/udp    Apertus Technologies Load Determination
uucp            540/tcp    uucpd
uucp            540/udp    uucpd
uucp-rlogin     541/tcp    uucp-rlogin
uucp-rlogin     541/udp    uucp-rlogin
commerce        542/tcp    commerce
commerce        542/udp    commerce
klogin          543/tcp
klogin          543/udp
kshell          544/tcp    krcmd
kshell          544/udp    krcmd
appleqtcsrvr    545/tcp    appleqtcsrvr
appleqtcsrvr    545/udp    appleqtcsrvr
dhcpv6-client   546/tcp    DHCPv6 Client
dhcpv6-client   546/udp    DHCPv6 Client
dhcpv6-server   547/tcp    DHCPv6 Server
dhcpv6-server   547/udp    DHCPv6 Server
afpovertcp      548/tcp    AFP over TCP
afpovertcp      548/udp    AFP over TCP
idfp            549/tcp    IDFP
idfp            549/udp    IDFP
new-rwho        550/tcp    new-who
new-rwho        550/udp    new-who
cybercash       551/tcp    cybercash
cybercash       551/udp    cybercash
deviceshare     552/tcp    deviceshare
deviceshare     552/udp    deviceshare
pirp            553/tcp    pirp
pirp            553/udp    pirp
rtsp            554/tcp    Real Time Stream Control Protocol
rtsp            554/udp    Real Time Stream Control Protocol
dsf             555/tcp
dsf             555/udp
remotefs        556/tcp    rfs server
remotefs        556/udp    rfs server
openvms-sysipc  557/tcp    openvms-sysipc
openvms-sysipc  557/udp    openvms-sysipc
sdnskmp         558/tcp    SDNSKMP
sdnskmp         558/udp    SDNSKMP
teedtap         559/tcp    TEEDTAP
teedtap         559/udp    TEEDTAP
rmonitor        560/tcp    rmonitord
rmonitor        560/udp    rmonitord
monitor         561/tcp
monitor         561/udp
chshell         562/tcp    chcmd
chshell         562/udp    chcmd
snews           563/tcp    snews
snews           563/udp    snews
9pfs            564/tcp    plan 9 file service
9pfs            564/udp    plan 9 file service
whoami          565/tcp    whoami
whoami          565/udp    whoami
streettalk      566/tcp    streettalk
streettalk      566/udp    streettalk
banyan-rpc      567/tcp    banyan-rpc
banyan-rpc      567/udp    banyan-rpc
ms-shuttle      568/tcp    microsoft shuttle
ms-shuttle      568/udp    microsoft shuttle
ms-rome         569/tcp    microsoft rome
ms-rome         569/udp    microsoft rome
meter           570/tcp    demon
meter           570/udp    demon
meter           571/tcp    udemon
meter           571/udp    udemon
sonar           572/tcp    sonar
sonar           572/udp    sonar
banyan-vip      573/tcp    banyan-vip
banyan-vip      573/udp    banyan-vip
ftp-agent       574/tcp    FTP Software Agent System
ftp-agent       574/udp    FTP Software Agent System
vemmi           575/tcp    VEMMI
vemmi           575/udp    VEMMI
ipcd            576/tcp    ipcd
ipcd            576/udp    ipcd
vnas            577/tcp    vnas
vnas            577/udp    vnas
ipdd            578/tcp    ipdd
ipdd            578/udp    ipdd
decbsrv         579/tcp    decbsrv
decbsrv         579/udp    decbsrv
sntp-heartbeat  580/tcp    SNTP HEARTBEAT
sntp-heartbeat  580/udp    SNTP HEARTBEAT
bdp             581/tcp    Bundle Discovery Protocol
bdp             581/udp    Bundle Discovery Protocol
#               582-599    Unassigned
ipcserver       600/tcp    Sun IPC server
ipcserver       600/udp    Sun IPC server
urm             606/tcp    Cray Unified Resource Manager
urm             606/udp    Cray Unified Resource Manager
nqs             607/tcp    nqs
nqs             607/udp    nqs
sift-uft        608/tcp    Sender-Initiated/Unsolicited File Transfer
sift-uft        608/udp    Sender-Initiated/Unsolicited File Transfer
npmp-trap       609/tcp    npmp-trap
npmp-trap       609/udp    npmp-trap
npmp-local      610/tcp    npmp-local
npmp-local      610/udp    npmp-local
npmp-gui        611/tcp    npmp-gui
npmp-gui        611/udp    npmp-gui
hmmp-ind        612/tcp    HMMP Indication
hmmp-ind        612/udp    HMMP Indication
hmmp-op         613/tcp    HMMP Operation
hmmp-op         613/udp    HMMP Operation
sshell          614/tcp    SSLshell
sshell          614/udp    SSLshell
sco-inetmg      615/tcp    Internet Configuration Manager
sco-inetmgr     615/udp    Internet Configuration Manager
sco-sysmgr      616/tcp    SCO System Administration Server
```

```
sco-sysmgr      616/udp    SCO System Administration Server
sco-dtmgr       617/tcp    SCO Desktop Administration Server
sco-dtmgr       617/udp    SCO Desktop Administration Server
dei-icda        618/tcp    DEI-ICDA
dei-icda        618/udp    DEI-ICDA
digital-evm     619/tcp    Digital EVM
digital-evm     619/udp    Digital EVM
sco-websrvrmgr  620/tcp    SCO WebServer Manager
sco-websrvrmgr  620/udp    SCO WebServer Manager
#               621-632    Unassigned
servstat        633/tcp    Service Status update (Sterling Software)
servstat        633/udp    Service Status update (Sterling Software)
ginad           634/tcp    ginad
ginad           634/udp    ginad
rlzdbase        635/tcp    RLZ DBase
rlzdbase        635/udp    RLZ DBase
ssl-ldap        636/tcp    ssl-ldap
ssl-ldap        636/udp    ssl-ldap
lanserver       637/tcp    lanserver
lanserver       637/udp    lanserver
#               638-665    Unassigned
mdqs            666/tcp
mdqs            666/udp
doom            666/tcp    doom Id Software
doom            666/udp    doom Id Software
disclose        667/tcp    campaign contribution disclosures -
disclose        667/udp    campaign contribution disclosures -
mecomm          668/tcp    MeComm
mecomm          668/udp    MeComm
meregister      669/tcp    MeRegister
meregister      669/udp    MeRegister
vacdsm-sws      670/tcp    VACDSM-SWS
vacdsm-sws      670/udp    VACDSM-SWS
vacdsm-app      671/tcp    VACDSM-APP
vacdsm-app      671/udp    VACDSM-APP
vpps-qua        672/tcp    VPPS-QUA
vpps-qua        672/udp    VPPS-QUA
cimplex         673/tcp    CIMPLEX
cimplex         673/udp    CIMPLEX
acap            674/tcp    ACAP
acap            674/udp    ACAP
#               674-703    Unassigned
elcsd           704/tcp    errlog copy/server daemon
elcsd           704/udp    errlog copy/server daemon
agent           705/tcp    AgentX
agentx          705/udp    AgentX
#               706-708    Unassigned
entrust-kmsh    709/tcp    Entrust Key Management Service Handler
entrust-kmsh    709/udp    Entrust Key Management Service Handler
entrust-ash     710/tcp    Entrust Administration Service Handler
entrust-ash     710/udp    Entrust Administration Service Handler
#               711-728    Unassigned
netviewdm1      729/tcp    IBM NetView DM/6000 Server/Client
netviewdm1      729/udp    IBM NetView DM/6000 Server/Client
netviewdm2      730/tcp    IBM NetView DM/6000 send/tcp
netviewdm2      730/udp    IBM NetView DM/6000 send/tcp
netviewdm3      731/tcp    IBM NetView DM/6000 receive/tcp
netviewdm3      731/udp    IBM NetView DM/6000 receive/tcp
netgw           741/tcp    netGW
netgw           741/udp    netGW
netrcs          742/tcp    Network based Rev. Cont. Sys.
netrcs          742/udp    Network based Rev. Cont. Sys.
flexlm          744/tcp    Flexible License Manager
flexlm          744/udp    Flexible License Manager
fujitsu-dev     747/tcp    Fujitsu Device Control
fujitsu-dev     747/udp    Fujitsu Device Control
ris-cm          748/tcp    Russell Info Sci Calendar Manager
ris-cm          748/udp    Russell Info Sci Calendar Manager
kerberos-adm    749/tcp    kerberos administration
kerberos-adm    749/udp    kerberos administration
rfile           750/tcp
loadav          750/udp
kerberos-iv     750/udp    kerberos version iv
pump            751/tcp
pump            751/udp
qrh             752/tcp
qrh             752/udp
rrh             753/tcp
rrh             753/udp
tell            754/tcp    send
tell            754/udp    send
nlogin          758/tcp
nlogin          758/udp
con             759/tcp
con             759/udp
ns              760/tcp
ns              760/udp
rxe             761/tcp
rxe             761/udp
quotad          762/tcp
quotad          762/udp
cycleserv       763/tcp
cycleserv       763/udp
omserv          764/tcp
omserv          764/udp
webster         765/tcp
webster         765/udp
phonebook       767/tcp    phone
phonebook       767/udp    phone
vid             769/tcp
vid             769/udp
cadlock         770/tcp
cadlock         770/udp
rtip            771/tcp
rtip            771/udp
cycleserv2      772/tcp
cycleserv2      772/udp
submit          773/tcp
notify          773/udp
rpasswd         774/tcp
acmaint_dbd     774/udp
entomb          775/tcp
acmaint_transd  775/udp
wpages          776/tcp
wpages          776/udp
wpgs            780/tcp
wpgs            780/udp
concert         786/tcp    Concert
concert         786/udp    Concert
#               787-799    Unassigned
mdbs_daemon     800/tcp
mdbs_daemon     800/udp
device          801/tcp
device          801/udp
iclcnet-locate  886/tcp    ICL coNETion locate server
iclcnet-locate  886/udp    ICL coNETion locate server
iclcnet_svinfo  887/tcp    ICL coNETion server info
iclcnet_svinfo  887/udp    ICL coNETion server info
accessbuilder   888/tcp    AccessBuilder
accessbuilder   888/udp    AccessBuilder
#               889-910    Unassigned
xact-backup     911/tcp    xact-backup
xact-backup     911/tcp    xact-backup
#               912-990    Unassigned
nas             991/tcp    Netnews Administration System
nas             991/udp    Netnews Administration System
#               992-994    Unassigned
spop3           995/tcp    SSL based POP3
spop3           995/udp    SSL based POP3
vsinet          996/tcp    vsinet
vsinet          996/udp    vsinet
maitrd          997/tcp
maitrd          997/udp
busboy          998/tcp
puparp          998/udp
garcon          999/tcp
applix          999/udp    Applix ac
puprouter       999/tcp
puprouter       999/udp
cadlock        1000/tcp
ock            1000/udp
#              1001-1022    Unassigned
               1023/tcp     Reserved
               1023/udp     Reserved
```

NUMEROS DE PORTS ENREGISTRES (REGISTERED PORT NUMBERS)
Les ports enregistrés ne sont pas contôlés par l'IANA. Sur la majorité des systems, les ports enregistrés peuvent être utilisés par des utilisateurs ou des processus standards, sans autorités particulière.

Port Assignments:

```
Keyword         Decimal    Description                    References
-------         -------    -----------                    ----------
                1024/tcp   Reserved
                1024/udp   Reserved
blackjack       1025/tcp   network blackjack
blackjack       1025/udp   network blackjack
iad1            1030/tcp   BBN IAD
iad1            1030/udp   BBN IAD
iad2            1031/tcp   BBN IAD
iad2            1031/udp   BBN IAD
iad3            1032/tcp   BBN IAD
iad3            1032/udp   BBN IAD
neod1           1047/tcp   Sun's NEO Object Request Broker
neod1           1047/udp   Sun's NEO Object Request Broker
neod2           1048/tcp   Sun's NEO Object Request Broker
neod2           1048/udp   Sun's NEO Object Request Broker
nim             1058/tcp   nim
nim             1058/udp   nim
nimreg          1059/tcp   nimreg
nimreg          1059/udp   nimreg
instl_boots     1067/tcp   Installation Bootstrap Proto. Serv.
instl_boots     1067/udp   Installation Bootstrap Proto. Serv.
instl_bootc     1068/tcp   Installation Bootstrap Proto. Cli.
instl_bootc     1068/udp   Installation Bootstrap Proto. Cli.
socks           1080/tcp   Socks
socks           1080/udp   Socks
ansoft-lm-1     1083/tcp   Anasoft License Manager
ansoft-lm-1     1083/udp   Anasoft License Manager
ansoft-lm-2     1084/tcp   Anasoft License Manager
ansoft-lm-2     1084/udp   Anasoft License Manager
nfsd-status     1110/tcp   Cluster status info
nfsd-keepalive  1110/udp   Client status info
murray          1123/tcp   Murray
murray          1123/udp   Murray
nfa             1155/tcp   Network File Access
nfa             1155/udp   Network File Access
lupa            1212/tcp   lupa
lupa            1212/udp   lupa
nerv            1222/tcp   SNI R&D network
nerv            1222/udp   SNI R&D network
hermes          1248/tcp
hermes          1248/udp
#               1249-1312  Unassigned
bmc_patroldb    1313/tcp   BMC_PATROLDB
bmc-patroldb    1313/udp   BMC_PATROLDB
pdps            1314/tcp   Photoscript Distributed Printing System
pdps            1314/udp   Photoscript Distributed Printing System
#               1315-1344  Unassigned
vpjp            1345/tcp   VPJP
vpjp            1345/udp   VPJP
alta-ana-lm     1346/tcp   Alta Analytics License Manager
alta-ana-lm     1346/udp   Alta Analytics License Manager
bbn-mmc         1347/tcp   multi media conferencing
bbn-mmc         1347/udp   multi media conferencing
bbn-mmx         1348/tcp   multi media conferencing
bbn-mmx         1348/udp   multi media conferencing
sbook           1349/tcp   Registration Network Protocol
sbook           1349/udp   Registration Network Protocol
editbench       1350/tcp   Registration Network Protocol
editbench       1350/udp   Registration Network Protocol
equationbuilder 1351/tcp   Digital Tool Works (MIT)
equationbuilder 1351/udp   Digital Tool Works (MIT)
lotusnote       1352/tcp   Lotus Note
lotusnote       1352/udp   Lotus Note
relief          1353/tcp   Relief Consulting
relief          1353/udp   Relief Consulting
rightbrain      1354/tcp   RightBrain Software
rightbrain      1354/udp   RightBrain Software
intuitive edge  1355/tcp   Intuitive Edge
intuitive edge  1355/udp   Intuitive Edge
cuillamartin    1356/tcp   CuillaMartin Company
cuillamartin    1356/udp   CuillaMartin Company
pegboard        1357/tcp   Electronic PegBoard
pegboard        1357/udp   Electronic PegBoard
connlcli        1358/tcp   CONNLCLI
connlcli        1358/udp   CONNLCLI
ftsrv           1359/tcp   FTSRV
ftsrv           1359/udp   FTSRV
mimer           1360/tcp   MIMER
mimer           1360/udp   MIMER
linx            1361/tcp   LinX
linx            1361/udp   LinX
#                          Steffen Schilke <---none--->
timeflies       1362/tcp   TimeFlies
timeflies       1362/udp   TimeFlies
```

| | | |
|---|---|---|
| ndm-requester | 1363/tcp | Network DataMover Requester |
| ndm-requester | 1363/udp | Network DataMover Requester |
| ndm-server | 1364/tcp | Network DataMover Server |
| ndm-server | 1364/udp | Network DataMover Server |
| adapt-sna | 1365/tcp | Network Software Associates |
| adapt-sna | 1365/udp | Network Software Associates |
| netware-csp | 1366/tcp | Novell NetWare Comm Service Platform |
| netware-csp | 1366/udp | Novell NetWare Comm Service Platform |
| dcs | 1367/tcp | DCS |
| dcs | 1367/udp | DCS |
| screencast | 1368/tcp | ScreenCast |
| screencast | 1368/udp | ScreenCast |
| gv-us | 1369/tcp | GlobalView to Unix Shell |
| gv-us | 1369/udp | GlobalView to Unix Shell |
| us-gv | 1370/tcp | Unix Shell to GlobalView |
| us-gv | 1370/udp | Unix Shell to GlobalView |
| fc-cli | 1371/tcp | Fujitsu Config Protocol |
| fc-cli | 1371/udp | Fujitsu Config Protocol |
| fc-ser | 1372/tcp | Fujitsu Config Protocol |
| fc-ser | 1372/udp | Fujitsu Config Protocol |
| chromagrafx | 1373/tcp | Chromagrafx |
| chromagrafx | 1373/udp | Chromagrafx |
| molly | 1374/tcp | EPI Software Systems |
| molly | 1374/udp | EPI Software Systems |
| bytex | 1375/tcp | Bytex |
| bytex | 1375/udp | Bytex |
| ibm-pps | 1376/tcp | IBM Person to Person Software |
| ibm-pps | 1376/udp | IBM Person to Person Software |
| cichlid | 1377/tcp | Cichlid License Manager |
| cichlid | 1377/udp | Cichlid License Manager |
| elan | 1378/tcp | Elan License Manager |
| elan | 1378/udp | Elan License Manager |
| dbreporter | 1379/tcp | Integrity Solutions |
| dbreporter | 1379/udp | Integrity Solutions |
| telesis-licman | 1380/tcp | Telesis Network License Manager |
| telesis-licman | 1380/udp | Telesis Network License Manager |
| apple-licman | 1381/tcp | Apple Network License Manager |
| apple-licman | 1381/udp | Apple Network License Manager |
| udt_os | 1382/tcp | |
| udt_os | 1382/udp | |
| gwha | 1383/tcp | GW Hannaway Network License Manager |
| gwha | 1383/udp | GW Hannaway Network License Manager |
| os-licman | 1384/tcp | Objective Solutions License Manager |
| os-licman | 1384/udp | Objective Solutions License Manager |
| atex_elmd | 1385/tcp | Atex Publishing License Manager |
| atex_elmd | 1385/udp | Atex Publishing License Manager |
| checksum | 1386/tcp | CheckSum License Manager |
| checksum | 1386/udp | CheckSum License Manager |
| cadsi-lm | 1387/tcp | Computer Aided Design Software Inc LM |
| cadsi-lm | 1387/udp | Computer Aided Design Software Inc LM |
| objective-dbc | 1388/tcp | Objective Solutions DataBase Cache |
| objective-dbc | 1388/udp | Objective Solutions DataBase Cache |
| iclpv-dm | 1389/tcp | Document Manager |
| iclpv-dm | 1389/udp | Document Manager |
| iclpv-sc | 1390/tcp | Storage Controller |
| iclpv-sc | 1390/udp | Storage Controller |
| iclpv-sas | 1391/tcp | Storage Access Server |
| iclpv-sas | 1391/udp | Storage Access Server |
| iclpv-pm | 1392/tcp | Print Manager |
| iclpv-pm | 1392/udp | Print Manager |
| iclpv-nls | 1393/tcp | Network Log Server |
| iclpv-nls | 1393/udp | Network Log Server |
| iclpv-nlc | 1394/tcp | Network Log Client |
| iclpv-nlc | 1394/udp | Network Log Client |
| iclpv-wsm | 1395/tcp | PC Workstation Manager software |
| iclpv-wsm | 1395/udp | PC Workstation Manager software |
| dvl-activemail | 1396/tcp | DVL Active Mail |
| dvl-activemail | 1396/udp | DVL Active Mail |
| audio-activmail | 1397/tcp | Audio Active Mail |
| audio-activmail | 1397/udp | Audio Active Mail |
| video-activmail | 1398/tcp | Video Active Mail |
| video-activmail | 1398/udp | Video Active Mail |
| cadkey-licman | 1399/tcp | Cadkey License Manager |
| cadkey-licman | 1399/udp | Cadkey License Manager |
| cadkey-tablet | 1400/tcp | Cadkey Tablet Daemon |
| cadkey-tablet | 1400/udp | Cadkey Tablet Daemon |
| goldleaf-licman | 1401/tcp | Goldleaf License Manager |
| goldleaf-licman | 1401/udp | Goldleaf License Manager |
| prm-sm-np | 1402/tcp | Prospero Resource Manager |
| prm-sm-np | 1402/udp | Prospero Resource Manager |
| prm-nm-np | 1403/tcp | Prospero Resource Manager |
| prm-nm-np | 1403/udp | Prospero Resource Manager |
| igi-lm | 1404/tcp | Infinite Graphics License Manager |
| igi-lm | 1404/udp | Infinite Graphics License Manager |
| ibm-res | 1405/tcp | IBM Remote Execution Starter |
| ibm-res | 1405/udp | IBM Remote Execution Starter |
| netlabs-lm | 1406/tcp | NetLabs License Manager |
| netlabs-lm | 1406/udp | NetLabs License Manager |
| dbsa-lm | 1407/tcp | DBSA License Manager |
| dbsa-lm | 1407/udp | DBSA License Manager |
| sophia-lm | 1408/tcp | Sophia License Manager |
| sophia-lm | 1408/udp | Sophia License Manager |
| here-lm | 1409/tcp | Here License Manager |
| here-lm | 1409/udp | Here License Manager |
| hiq | 1410/tcp | HiQ License Manager |
| hiq | 1410/udp | HiQ License Manager |
| af | 1411/tcp | AudioFile |
| af | 1411/udp | AudioFile |
| innosys | 1412/tcp | InnoSys |
| innosys | 1412/udp | InnoSys |
| innosys-acl | 1413/tcp | Innosys-ACL |
| innosys-acl | 1413/udp | Innosys-ACL |
| ibm-mqseries | 1414/tcp | IBM MQSeries |
| ibm-mqseries | 1414/udp | IBM MQSeries |
| dbstar | 1415/tcp | DBStar |
| dbstar | 1415/udp | DBStar |
| novell-lu6.2 | 1416/tcp | Novell LU6.2 |
| novell-lu6.2 | 1416/udp | Novell LU6.2 |
| timbuktu-srv1 | 1417/tcp | Timbuktu Service 1 Port |
| timbuktu-srv1 | 1417/udp | Timbuktu Service 1 Port |
| timbuktu-srv2 | 1418/tcp | Timbuktu Service 2 Port |
| timbuktu-srv2 | 1418/udp | Timbuktu Service 2 Port |
| timbuktu-srv3 | 1419/tcp | Timbuktu Service 3 Port |
| timbuktu-srv3 | 1419/udp | Timbuktu Service 3 Port |
| timbuktu-srv4 | 1420/tcp | Timbuktu Service 4 Port |
| timbuktu-srv4 | 1420/udp | Timbuktu Service 4 Port |
| gandalf-lm | 1421/tcp | Gandalf License Manager |
| gandalf-lm | 1421/udp | Gandalf License Manager |
| autodesk-lm | 1422/tcp | Autodesk License Manager |
| autodesk-lm | 1422/udp | Autodesk License Manager |
| essbase | 1423/tcp | Essbase Arbor Software |
| essbase | 1423/udp | Essbase Arbor Software |
| hybrid | 1424/tcp | Hybrid Encryption Protocol |
| hybrid | 1424/udp | Hybrid Encryption Protocol |
| zion-lm | 1425/tcp | Zion Software License Manager |
| zion-lm | 1425/udp | Zion Software License Manager |
| sais | 1426/tcp | Satellite-data Acquisition System 1 |
| sais | 1426/udp | Satellite-data Acquisition System 1 |
| mloadd | 1427/tcp | mloadd monitoring tool |
| mloadd | 1427/udp | mloadd monitoring tool |
| informatik-lm | 1428/tcp | Informatik License Manager |
| informatik-lm | 1428/udp | Informatik License Manager |
| nms | 1429/tcp | Hypercom NMS |
| nms | 1429/udp | Hypercom NMS |
| tpdu | 1430/tcp | Hypercom TPDU |
| tpdu | 1430/udp | Hypercom TPDU |
| rgtp | 1431/tcp | Reverse Gossip Transport |
| rgtp | 1431/udp | Reverse Gossip Transport |
| blueberry-lm | 1432/tcp | Blueberry Software License Manager |
| blueberry-lm | 1432/udp | Blueberry Software License Manager |
| ms-sql-s | 1433/tcp | Microsoft-SQL-Server |
| ms-sql-s | 1433/udp | Microsoft-SQL-Server |
| ms-sql-m | 1434/tcp | Microsoft-SQL-Monitor |
| ms-sql-m | 1434/udp | Microsoft-SQL-Monitor |
| ibm-cics | 1435/tcp | IBM CICS |
| ibm-cics | 1435/udp | IBM CICS |
| saism | 1436/tcp | Satellite-data Acquisition System 2 |
| saism | 1436/udp | Satellite-data Acquisition System 2 |
| tabula | 1437/tcp | Tabula |
| tabula | 1437/udp | Tabula |
| eicon-server | 1438/tcp | Eicon Security Agent/Server |
| eicon-server | 1438/udp | Eicon Security Agent/Server |
| eicon-x25 | 1439/tcp | Eicon X25/SNA Gateway |
| eicon-x25 | 1439/udp | Eicon X25/SNA Gateway |
| eicon-slp | 1440/tcp | Eicon Service Location Protocol |
| eicon-slp | 1440/udp | Eicon Service Location Protocol |
| cadis-1 | 1441/tcp | Cadis License Management |
| cadis-1 | 1441/udp | Cadis License Management |
| cadis-2 | 1442/tcp | Cadis License Management |
| cadis-2 | 1442/udp | Cadis License Management |
| ies-lm | 1443/tcp | Integrated Engineering Software |
| ies-lm | 1443/udp | Integrated Engineering Software |
| marcam-lm | 1444/tcp | Marcam  License Management |
| marcam-lm | 1444/udp | Marcam  License Management |
| proxima-lm | 1445/tcp | Proxima License Manager |
| proxima-lm | 1445/udp | Proxima License Manager |
| ora-lm | 1446/tcp | Optical Research Associates License Manager |
| ora-lm | 1446/udp | Optical Research Associates License Manager |
| apri-lm | 1447/tcp | Applied Parallel Research LM |
| apri-lm | 1447/udp | Applied Parallel Research LM |
| oc-lm | 1448/tcp | OpenConnect License Manager |
| oc-lm | 1448/udp | OpenConnect License Manager |
| peport | 1449/tcp | PEport |
| peport | 1449/udp | PEport |
| dwf | 1450/tcp | Tandem Distributed Workbench Facility |
| dwf | 1450/udp | Tandem Distributed Workbench Facility |
| infoman | 1451/tcp | IBM Information Management |
| infoman | 1451/udp | IBM Information Management |
| gtegsc-lm | 1452/tcp | GTE Government Systems License Man |
| gtegsc-lm | 1452/udp | GTE Government Systems License Man |
| genie-lm | 1453/tcp | Genie License Manager |
| genie-lm | 1453/udp | Genie License Manager |
| interhdl_elmd | 1454/tcp | interHDL License Manager |
| interhdl_elmd | 1454/udp | interHDL License Manager |
| esl-lm | 1455/tcp | ESL License Manager |
| esl-lm | 1455/udp | ESL License Manager |
| dca | 1456/tcp | DCA |
| dca | 1456/udp | DCA |
| valisys-lm | 1457/tcp | Valisys License Manager |
| valisys-lm | 1457/udp | Valisys License Manager |
| nrcabq-lm | 1458/tcp | Nichols Research Corp. |
| nrcabq-lm | 1458/udp | Nichols Research Corp. |
| proshare1 | 1459/tcp | Proshare Notebook Application |
| proshare1 | 1459/udp | Proshare Notebook Application |
| proshare2 | 1460/tcp | Proshare Notebook Application |
| proshare2 | 1460/udp | Proshare Notebook Application |
| ibm_wrless_lan | 1461/tcp | IBM Wireless LAN |
| ibm_wrless_lan | 1461/udp | IBM Wireless LAN |
| world-lm | 1462/tcp | World License Manager |
| world-lm | 1462/udp | World License Manager |
| nucleus | 1463/tcp | Nucleus |
| nucleus | 1463/udp | Nucleus |
| msl_lmd | 1464/tcp | MSL License Manager |
| msl_lmd | 1464/udp | MSL License Manager |
| pipes | 1465/tcp | Pipes Platform |
| pipes | 1465/udp | Pipes Platform  mfarlin@peerlogic.com |
| oceansoft-lm | 1466/tcp | Ocean Software License Manager |
| oceansoft-lm | 1466/udp | Ocean Software License Manager |
| csdmbase | 1467/tcp | CSDMBASE |
| csdmbase | 1467/udp | CSDMBASE |
| csdm | 1468/tcp | CSDM |
| csdm | 1468/udp | CSDM |
| aal-lm | 1469/tcp | Active Analysis Limited License Manager |
| aal-lm | 1469/udp | Active Analysis Limited License Manager |
| uaiact | 1470/tcp | Universal Analytics |
| uaiact | 1470/udp | Universal Analytics |
| csdmbase | 1471/tcp | csdmbase |
| csdmbase | 1471/udp | csdmbase |
| csdm | 1472/tcp | csdm |
| csdm | 1472/udp | csdm |
| openmath | 1473/tcp | OpenMath |
| openmath | 1473/udp | OpenMath |
| telefinder | 1474/tcp | Telefinder |
| telefinder | 1474/udp | Telefinder |
| taligent-lm | 1475/tcp | Taligent License Manager |
| taligent-lm | 1475/udp | Taligent License Manager |
| clvm-cfg | 1476/tcp | clvm-cfg |
| clvm-cfg | 1476/udp | clvm-cfg |
| ms-sna-server | 1477/tcp | ms-sna-server |
| ms-sna-server | 1477/udp | ms-sna-server |
| ms-sna-base | 1478/tcp | ms-sna-base |
| ms-sna-base | 1478/udp | ms-sna-base |
| dberegister | 1479/tcp | dberegister |
| dberegister | 1479/udp | dberegister |
| pacerforum | 1480/tcp | PacerForum |
| pacerforum | 1480/udp | PacerForum |
| airs | 1481/tcp | AIRS |
| airs | 1481/udp | AIRS |
| miteksys-lm | 1482/tcp | Miteksys License Manager |
| miteksys-lm | 1482/udp | Miteksys License Manager |
| afs | 1483/tcp | AFS License Manager |
| afs | 1483/udp | AFS License Manager |
| confluent | 1484/tcp | Confluent License Manager |
| confluent | 1484/udp | Confluent License Manager |
| lansource | 1485/tcp | LANSource |
| lansource | 1485/udp | LANSource |

| | | |
|---|---|---|
| nms_topo_serv | 1486/tcp | nms_topo_serv |
| nms_topo_serv | 1486/udp | nms_topo_serv |
| localinfosrvr | 1487/tcp | LocalInfoSrvr |
| localinfosrvr | 1487/udp | LocalInfoSrvr |
| docstor | 1488/tcp | DocStor |
| docstor | 1488/udp | DocStor |
| dmdocbroker | 1489/tcp | dmdocbroker |
| dmdocbroker | 1489/udp | dmdocbroker |
| insitu-conf | 1490/tcp | insitu-conf |
| insitu-conf | 1490/udp | insitu-conf |
| anynetgateway | 1491/tcp | anynetgateway |
| anynetgateway | 1491/udp | anynetgateway |
| stone-design-1 | 1492/tcp | stone-design-1 |
| stone-design-1 | 1492/udp | stone-design-1 |
| netmap_lm | 1493/tcp | netmap_lm |
| netmap_lm | 1493/udp | netmap_lm |
| ica | 1494/tcp | ica |
| ica | 1494/udp | ica |
| cvc | 1495/tcp | cvc |
| cvc | 1495/udp | cvc |
| liberty-lm | 1496/tcp | liberty-lm |
| liberty-lm | 1496/udp | liberty-lm |
| rfx-lm | 1497/tcp | rfx-lm |
| rfx-lm | 1497/udp | rfx-lm |
| watcom-sql | 1498/tcp | Watcom-SQL |
| watcom-sql | 1498/udp | Watcom-SQL |
| fhc | 1499/tcp | Federico Heinz Consultora |
| fhc | 1499/udp | Federico Heinz Consultora |
| vlsi-lm | 1500/tcp | VLSI License Manager |
| vlsi-lm | 1500/udp | VLSI License Manager |
| saiscm | 1501/tcp | Satellite-data Acquisition System 3 |
| saiscm | 1501/udp | Satellite-data Acquisition System 3 |
| shivadiscovery | 1502/tcp | Shiva |
| shivadiscovery | 1502/udp | Shiva |
| imtc-mcs | 1503/tcp | Databeam |
| imtc-mcs | 1503/udp | Databeam |
| evb-elm | 1504/tcp | EVB Software Engineering License Manager |
| evb-elm | 1504/udp | EVB Software Engineering License Manager |
| funkproxy | 1505/tcp | Funk Software, Inc. |
| funkproxy | 1505/udp | Funk Software, Inc. |
| utcd | 1506/tcp | Universal Time daemon (utcd) |
| utcd | 1506/udp | Universal Time daemon (utcd) |
| symplex | 1507/tcp | symplex |
| symplex | 1507/udp | symplex |
| diagmond | 1508/tcp | diagmond |
| diagmond | 1508/udp | diagmond |
| robcad-lm | 1509/tcp | Robcad, Ltd. License Manager |
| robcad-lm | 1509/udp | Robcad, Ltd. License Manager |
| mvx-lm | 1510/tcp | Midland Valley Exploration Ltd. Lic. Man. |
| mvx-lm | 1510/udp | Midland Valley Exploration Ltd. Lic. Man. |
| 3l-l1 | 1511/tcp | 3l-l1 |
| 3l-l1 | 1511/udp | 3l-l1 |
| wins | 1512/tcp | Microsoft's Windows Internet Name Service |
| wins | 1512/udp | Microsoft's Windows Internet Name Service |
| fujitsu-dtc | 1513/tcp | Fujitsu Systems Business of America, Inc |
| fujitsu-dtc | 1513/udp | Fujitsu Systems Business of America, Inc |
| fujitsu-dtcns | 1514/tcp | Fujitsu Systems Business of America, Inc |
| fujitsu-dtcns | 1514/udp | Fujitsu Systems Business of America, Inc |
| ifor-protocol | 1515/tcp | ifor-protocol |
| ifor-protocol | 1515/udp | ifor-protocol |
| vpad | 1516/tcp | Virtual Places Audio data |
| vpad | 1516/udp | Virtual Places Audio data |
| vpac | 1517/tcp | Virtual Places Audio control |
| vpac | 1517/udp | Virtual Places Audio control |
| vpvd | 1518/tcp | Virtual Places Video data |
| vpvd | 1518/udp | Virtual Places Video data |
| vpvc | 1519/tcp | Virtual Places Video control |
| vpvc | 1519/udp | Virtual Places Video control |
| atm-zip-office | 1520/tcp | atm zip office |
| atm-zip-office | 1520/udp | atm zip office |
| ncube-lm | 1521/tcp | nCube License Manager |
| ncube-lm | 1521/udp | nCube License Manager |
| ricardo-lm | 1522/tcp | Ricardo North America License Manager |
| ricardo-lm | 1522/udp | Ricardo North America License Manager |
| cichild-lm | 1523/tcp | cichild |
| cichild-lm | 1523/udp | cichild |
| ingreslock | 1524/tcp | ingres |
| ingreslock | 1524/udp | ingres |
| orasrv | 1525/tcp | oracle |
| orasrv | 1525/udp | oracle |
| prospero-np | 1525/tcp | Prospero Directory Service non-priv |
| prospero-np | 1525/udp | Prospero Directory Service non-priv |
| pdap-np | 1526/tcp | Prospero Data Access Prot non-priv |
| pdap-np | 1526/udp | Prospero Data Access Prot non-priv |
| tlisrv | 1527/tcp | oracle |
| tlisrv | 1527/udp | oracle |
| mciautoreg | 1528/tcp | micautoreg |
| mciautoreg | 1528/udp | micautoreg |
| coauthor | 1529/tcp | oracle |
| coauthor | 1529/udp | oracle |
| rap-service | 1530/tcp | rap-service |
| rap-service | 1530/udp | rap-service |
| rap-listen | 1531/tcp | rap-listen |
| rap-listen | 1531/udp | rap-listen |
| miroconnect | 1532/tcp | miroconnect |
| miroconnect | 1532/udp | miroconnect |
| virtual-places | 1533/tcp | Virtual Places Software |
| virtual-places | 1533/udp | Virtual Places Software |
| micromuse-lm | 1534/tcp | micromuse-lm |
| micromuse-lm | 1534/udp | micromuse-lm |
| ampr-info | 1535/tcp | ampr-info |
| ampr-info | 1535/udp | ampr-info |
| ampr-inter | 1536/tcp | ampr-inter |
| ampr-inter | 1536/udp | ampr-inter |
| sdsc-lm | 1537/tcp | isi-lm |
| sdsc-lm | 1537/udp | isi-lm |
| 3ds-lm | 1538/tcp | 3ds-lm |
| 3ds-lm | 1538/udp | 3ds-lm |
| intellistor-lm | 1539/tcp | Intellistor License Manager |
| intellistor-lm | 1539/udp | Intellistor License Manager |
| rds | 1540/tcp | rds |
| rds | 1540/udp | rds |
| rds2 | 1541/tcp | rds2 |
| rds2 | 1541/udp | rds2 |
| gridgen-elmd | 1542/tcp | gridgen-elmd |
| gridgen-elmd | 1542/udp | gridgen-elmd |
| simba-cs | 1543/tcp | simba-cs |
| simba-cs | 1543/udp | simba-cs |
| aspeclmd | 1544/tcp | aspeclmd |
| aspeclmd | 1544/udp | aspeclmd |
| vistium-share | 1545/tcp | vistium-share |
| vistium-share | 1545/udp | vistium-share |
| abbaccuray | 1546/tcp | abbaccuray |
| abbaccuray | 1546/udp | abbaccuray |
| laplink | 1547/tcp | laplink |
| laplink | 1547/udp | laplink |
| axon-lm | 1548/tcp | Axon License Manager |
| axon-lm | 1548/udp | Axon License Manager |
| shivahose | 1549/tcp | Shiva Hose |
| shivasound | 1549/udp | Shiva Sound |
| 3m-image-lm | 1550/tcp | Image Storage license manager 3M Company |
| 3m-image-lm | 1550/udp | Image Storage license manager 3M Company |
| hecmtl-db | 1551/tcp | HECMTL-DB |
| hecmtl-db | 1551/udp | HECMTL-DB |
| pciarray | 1552/tcp | pciarray |
| pciarray | 1552/udp | pciarray |
| sna-cs | 1553/tcp | sna-cs |
| sna-cs | 1553/udp | sna-cs |
| caci-lm | 1554/tcp | CACI Products Company License Manager |
| caci-lm | 1554/udp | CACI Products Company License Manager |
| livelan | 1555/tcp | livelan |
| livelan | 1555/udp | livelan |
| ashwin | 1556/tcp | AshWin CI Tecnologies |
| ashwin | 1556/udp | AshWin CI Tecnologies |
| arbortext-lm | 1557/tcp | ArborText License Manager |
| arbortext-lm | 1557/udp | ArborText License Manager |
| xingmpeg | 1558/tcp | xingmpeg |
| xingmpeg | 1558/udp | xingmpeg |
| web2host | 1559/tcp | web2host |
| web2host | 1559/udp | web2host |
| asci-val | 1560/tcp | asci-val |
| asci-val | 1560/udp | asci-val |
| facilityview | 1561/tcp | facilityview |
| facilityview | 1561/udp | facilityview |
| pconnectmgr | 1562/tcp | pconnectmgr |
| pconnectmgr | 1562/udp | pconnectmgr |
| cadabra-lm | 1563/tcp | Cadabra License Manager |
| cadabra-lm | 1563/udp | Cadabra License Manager |
| pay-per-view | 1564/tcp | Pay-Per-View |
| pay-per-view | 1564/udp | Pay-Per-View |
| winddlb | 1565/tcp | WinDD |
| winddlb | 1565/udp | WinDD |
| corelvideo | 1566/tcp | CORELVIDEO |
| corelvideo | 1566/udp | CORELVIDEO |
| jlicelmd | 1567/tcp | jlicelmd |
| jlicelmd | 1567/udp | jlicelmd |
| tsspmap | 1568/tcp | tsspmap |
| tsspmap | 1568/udp | tsspmap |
| ets | 1569/tcp | ets |
| ets | 1569/udp | ets |
| orbixd | 1570/tcp | orbixd |
| orbixd | 1570/udp | orbixd |
| rdb-dbs-disp | 1571/tcp | Oracle Remote Data Base |
| rdb-dbs-disp | 1571/udp | Oracle Remote Data Base |
| chip-lm | 1572/tcp | Chipcom License Manager |
| chip-lm | 1572/udp | Chipcom License Manager |
| itscomm-ns | 1573/tcp | itscomm-ns |
| itscomm-ns | 1573/udp | itscomm-ns |
| mvel-lm | 1574/tcp | mvel-lm |
| mvel-lm | 1574/udp | mvel-lm |
| oraclenames | 1575/tcp | oraclenames |
| oraclenames | 1575/udp | oraclenames |
| moldflow-lm | 1576/tcp | moldflow-lm |
| moldflow-lm | 1576/udp | moldflow-lm |
| hypercube-lm | 1577/tcp | hypercube-lm |
| hypercube-lm | 1577/udp | hypercube-lm |
| jacobus-lm | 1578/tcp | Jacobus License Manager |
| jacobus-lm | 1578/udp | Jacobus License Manager |
| ioc-sea-lm | 1579/tcp | ioc-sea-lm |
| ioc-sea-lm | 1579/udp | ioc-sea-lm |
| tn-tl-r1 | 1580/tcp | tn-tl-r1 |
| tn-tl-r2 | 1580/udp | tn-tl-r2 |
| vmf-msg-port | 1581/tcp | vmf-msg-port |
| vmf-msg-port | 1581/udp | vmf-msg-port |
| msims | 1582/tcp | MSIMS |
| msims | 1582/udp | MSIMS |
| simbaexpress | 1583/tcp | simbaexpress |
| simbaexpress | 1583/udp | simbaexpress |
| tn-tl-fd2 | 1584/tcp | tn-tl-fd2 |
| tn-tl-fd2 | 1584/udp | tn-tl-fd2 |
| intv | 1585/tcp | intv |
| intv | 1585/udp | intv |
| ibm-abtact | 1586/tcp | ibm-abtact |
| ibm-abtact | 1586/udp | ibm-abtact |
| pra_elmd | 1587/tcp | pra_elmd |
| pra_elmd | 1587/udp | pra_elmd |
| triquest-lm | 1588/tcp | triquest-lm |
| triquest-lm | 1588/udp | triquest-lm |
| vqp | 1589/tcp | VQP |
| vqp | 1589/udp | VQP |
| gemini-lm | 1590/tcp | gemini-lm |
| gemini-lm | 1590/udp | gemini-lm |
| ncpm-pm | 1591/tcp | ncpm-pm |
| ncpm-pm | 1591/udp | ncpm-pm |
| commonspace | 1592/tcp | commonspace |
| commonspace | 1592/udp | commonspace |
| mainsoft-lm | 1593/tcp | mainsoft-lm |
| mainsoft-lm | 1593/udp | mainsoft-lm |
| sixtrak | 1594/tcp | sixtrak |
| sixtrak | 1594/udp | sixtrak |
| radio | 1595/tcp | radio |
| radio | 1595/udp | radio |
| radio-sm | 1596/tcp | radio-sm |
| radio-bc | 1596/udp | radio-bc |
| orbplus-iiop | 1597/tcp | orbplus-iiop |
| orbplus-iiop | 1597/udp | orbplus-iiop |
| picknfs | 1598/tcp | picknfs |
| picknfs | 1598/udp | picknfs |
| simbaservices | 1599/tcp | simbaservices |
| simbaservices | 1599/udp | simbaservices |
| issd | 1600/tcp | |
| issd | 1600/udp | |
| aas | 1601/tcp | aas |
| aas | 1601/udp | aas |
| inspect | 1602/tcp | inspect |
| inspect | 1602/udp | inspect |
| picodbc | 1603/tcp | pickodbc |
| picodbc | 1603/udp | pickodbc |
| icabrowser | 1604/tcp | icabrowser |
| icabrowser | 1604/udp | icabrowser |
| slp | 1605/tcp | Salutation Manager (Salutation Protocol) |
| slp | 1605/udp | Salutation Manager (Salutation Protocol) |
| slm-api | 1606/tcp | Salutation Manager (SLM-API) |
| slm-api | 1606/udp | Salutation Manager (SLM-API) |
| stt | 1607/tcp | stt |
| stt | 1607/udp | stt |

```
smart-lm        1608/tcp   Smart Corp. License Manager
smart-lm        1608/udp   Smart Corp. License Manager
isysg-lm        1609/tcp   isysg-lm
isysg-lm        1609/udp   isysg-lm
taurus-wh       1610/tcp   taurus-wh
taurus-wh       1610/udp   taurus-wh
ill             1611/tcp   Inter Library Loan
ill             1611/udp   Inter Library Loan
netbill-trans   1612/tcp   NetBill Transaction Server
netbill-trans   1612/udp   NetBill Transaction Server
netbill-keyrep  1613/tcp   NetBill Key Repository
netbill-keyrep  1613/udp   NetBill Key Repository
netbill-cred    1614/tcp   NetBill Credential Server
netbill-cred    1614/udp   NetBill Credential Server
netbill-auth    1615/tcp   NetBill Authorization Server
netbill-auth    1615/udp   NetBill Authorization Server
netbill-prod    1616/tcp   NetBill Product Server
netbill-prod    1616/udp   NetBill Product Server
nimrod-agent    1617/tcp   Nimrod Inter-Agent Communication
nimrod-agent    1617/udp   Nimrod Inter-Agent Communication
skytelnet       1618/tcp   skytelnet
skytelnet       1618/udp   skytelnet
xs-openstorage   1619/tcp  xs-openstorage
xs-openstorage   1619/udp  xs-openstorage
faxportwinport  1620/tcp   faxportwinport
faxportwinport  1620/udp   faxportwinport
softdataphone   1621/tcp   softdataphone
softdataphone   1621/udp   softdataphone
ontime          1622/tcp   ontime
ontime          1622/udp   ontime
jaleosnd        1623/tcp   jaleosnd
jaleosnd        1623/udp   jaleosnd
udp-sr-port     1624/tcp   udp-sr-port
udp-sr-port     1624/udp   udp-sr-port
svs-omagent     1625/tcp   svs-omagent
svs-omagent     1625/udp   svs-omagent
cncp            1636/tcp   CableNet Control Protocol
cncp            1636/udp   CableNet Control Protocol
cnap            1637/tcp   CableNet Admin Protocol
cnap            1637/udp   CableNet Admin Protocol
cnip            1638/tcp   CableNet Info Protocol
cnip            1638/udp   CableNet Info Protocol
cert-initiator  1639/tcp   cert-initiator
cert-initiator  1639/udp   cert-initiator
cert-responder  1640/tcp   cert-responder
cert-responder  1640/udp   cert-responder
invision        1641/tcp   InVision
invision        1641/udp   InVision
isis-am         1642/tcp   isis-am
isis-am         1642/udp   isis-am
isis-ambc       1643/tcp   isis-ambc
isis-ambc       1643/udp   isis-ambc
saiseh          1644/tcp   Satellite-data Acquisition System 4
datametrics     1645/tcp   datametrics
datametrics     1645/udp   datametrics
sa-msg-port     1646/tcp   sa-msg-port
sa-msg-port     1646/udp   sa-msg-port
rsap            1647/tcp   rsap
rsap            1647/udp   rsap
concurrent-lm   1648/tcp   concurrent-lm
concurrent-lm   1648/udp   concurrent-lm
inspect         1649/tcp   inspect
inspect         1649/udp   inspect
nkd             1650/tcp
nkd             1650/udp
shiva_confsrvr  1651/tcp   shiva_confsrvr
shiva_confsrvr  1651/udp   shiva_confsrvr
xnmp            1652/tcp   xnmp
xnmp            1652/udp   xnmp
alphatech-lm    1653/tcp   alphatech-lm
alphatech-lm    1653/udp   alphatech-lm
stargatealerts  1654/tcp   stargatealerts
stargatealerts  1654/udp   stargatealerts
dec-mbadmin     1655/tcp   dec-mbadmin
dec-mbadmin     1655/udp   dec-mbadmin
dec-mbadmin-h   1656/tcp   dec-mbadmin-h
dec-mbadmin-h   1656/udp   dec-mbadmin-h
fujitsu-mmpdc   1657/tcp   fujitsu-mmpdc
fujitsu-mmpdc   1657/udp   fujitsu-mmpdc
sixnetudr       1658/tcp   sixnetudr
sixnetudr       1658/udp   sixnetudr
sg-lm           1659/tcp   Silicon Grail License Manager
sg-lm           1659/udp   Silicon Grail License Manager
skip-mc-gikreq  1660/tcp   skip-mc-gikreq
skip-mc-gikreq  1660/udp   skip-mc-gikreq
netview-aix-1   1661/tcp   netview-aix-1
netview-aix-1   1661/udp   netview-aix-1
netview-aix-2   1662/tcp   netview-aix-2
netview-aix-2   1662/udp   netview-aix-2
netview-aix-3   1663/tcp   netview-aix-3
netview-aix-3   1663/udp   netview-aix-3
netview-aix-4   1664/tcp   netview-aix-4
netview-aix-4   1664/udp   netview-aix-4
netview-aix-5   1665/tcp   netview-aix-5
netview-aix-5   1665/udp   netview-aix-5
netview-aix-6   1666/tcp   netview-aix-6
netview-aix-6   1666/udp   netview-aix-6
netview-aix-7   1667/tcp   netview-aix-7
netview-aix-7   1667/udp   netview-aix-7
netview-aix-8   1668/tcp   netview-aix-8
netview-aix-8   1668/udp   netview-aix-8
netview-aix-9   1669/tcp   netview-aix-9
netview-aix-9   1669/udp   netview-aix-9
netview-aix-10  1670/tcp   netview-aix-10
netview-aix-10  1670/udp   netview-aix-10
netview-aix-11  1671/tcp   netview-aix-11
netview-aix-11  1671/udp   netview-aix-11
netview-aix-12  1672/tcp   netview-aix-12
netview-aix-12  1672/udp   netview-aix-12
proshare-mc-1   1673/tcp   Intel Proshare Multicast
proshare-mc-1   1673/udp   Intel Proshare Multicast
proshare-mc-2   1674/tcp   Intel Proshare Multicast
proshare-mc-2   1674/udp   Intel Proshare Multicast
pdp             1675/tcp   Pacific Data Products
pdp             1675/udp   Pacific Data Products
netcomm1        1676/tcp   netcomm1
netcomm2        1676/udp   netcomm2
groupwise       1677/tcp   groupwise
groupwise       1677/udp   groupwise
prolink         1678/tcp   prolink
prolink         1678/udp   prolink
darcorp-lm      1679/tcp   darcorp-lm
darcorp-lm      1679/udp   darcorp-lm
microcom-sbp    1680/tcp   microcom-sbp
microcom-sbp    1680/udp   microcom-sbp
sd-elmd         1681/tcp   sd-elmd
sd-elmd         1681/udp   sd-elmd
lanyon-lantern  1682/tcp   lanyon-lantern
lanyon-lantern  1682/udp   lanyon-lantern
ncpm-hip        1683/tcp   ncpm-hip
ncpm-hip        1683/udp   ncpm-hip
snaresecure     1684/tcp   SnareSecure
snaresecure     1684/udp   SnareSecure
n2nremote       1685/tcp   n2nremote
n2nremote       1685/udp   n2nremote
cvmon           1686/tcp   cvmon
cvmon           1686/udp   cvmon
nsjtp-ctrl      1687/tcp   nsjtp-ctrl
nsjtp-ctrl      1687/udp   nsjtp-ctrl
nsjtp-data      1688/tcp   nsjtp-data
nsjtp-data      1688/udp   nsjtp-data
firefox         1689/tcp   firefox
firefox         1689/udp   firefox
ng-umds         1690/tcp   ng-umds
ng-umds         1690/udp   ng-umds
empire-empuma   1691/tcp   empire-empuma
empire-empuma   1691/udp   empire-empuma
sstsys-lm       1692/tcp   sstsys-lm
sstsys-lm       1692/udp   sstsys-lm
rrirtr          1693/tcp   rrirtr
rrirtr          1693/udp   rrirtr
rrimwm          1694/tcp   rrimwm
rrimwm          1694/udp   rrimwm
rrilwm          1695/tcp   rrilwm
rrilwm          1695/udp   rrilwm
rrifmm          1696/tcp   rrifmm
rrifmm          1696/udp   rrifmm
rrisat          1697/tcp   rrisat
rrisat          1697/udp   rrisat
rsvp-encap-1    1698/tcp   RSVP-ENCAPSULATION-1
rsvp-encap-1    1698/udp   RSVP-ENCAPSULATION-1
rsvp-encap-2    1699/tcp   RSVP-ENCAPSULATION-2
rsvp-encap-2    1699/udp   RSVP-ENCAPSULATION-2
mps-raft        1700/tcp   mps-raft
mps-raft        1700/udp   mps-raft
l2f             1701/tcp   l2f
l2f             1701/udp   l2f
deskshare       1702/tcp   deskshare
deskshare       1702/udp   deskshare
hb-engine       1703/tcp   hb-engine
hb-engine       1703/udp   hb-engine
bcs-broker      1704/tcp   bcs-broker
bcs-broker      1704/udp   bcs-broker
slingshot       1705/tcp   slingshot
slingshot       1705/udp   slingshot
jetform         1706/tcp   jetform
jetform         1706/udp   jetform
vdmplay         1707/tcp   vdmplay
vdmplay         1707/udp   vdmplay
gat-lmd         1708/tcp   gat-lmd
gat-lmd         1708/udp   gat-lmd
centra          1709/tcp   centra
centra          1709/udp   centra
impera          1710/tcp   impera
impera          1710/udp   impera
pptconference   1711/tcp   pptconference
pptconference   1711/udp   pptconference
registrar       1712/tcp   resource monitoring service
registrar       1712/udp   resource monitoring service
conferencetalk  1713/tcp   ConferenceTalk
conferencetalk  1713/udp   ConferenceTalk
sesi-lm         1714/tcp   sesi-lm
sesi-lm         1714/udp   sesi-lm
houdini-lm      1715/tcp   houdini-lm
houdini-lm      1715/udp   houdini-lm
xmsg            1716/tcp   xmsg
xmsg            1716/udp   xmsg
fj-hdnet        1717/tcp   fj-hdnet
fj-hdnet        1717/udp   fj-hdnet
h323gatedisc    1718/tcp   h323gatedisc
h323gatedisc    1718/udp   h323gatedisc
h323gatestat    1719/tcp   h323gatestat
h323gatestat    1719/udp   h323gatestat
h323hostcall    1720/tcp   h323hostcall
h323hostcall    1720/udp   h323hostcall
caicci          1721/tcp   caicci
caicci          1721/udp   caicci
hks-lm          1722/tcp   HKS License Manager
hks-lm          1722/udp   HKS License Manager
pptp            1723/tcp   pptp
pptp            1723/udp   pptp
csbphonemaster  1724/tcp   csbphonemaster
csbphonemaster  1724/udp   csbphonemaster
iden-ralp       1725/tcp   iden-ralp
iden-ralp       1725/udp   iden-ralp
iberiagames     1726/tcp   IBERIAGAMES
iberiagames     1726/tcp   IBERIAGAMES
winddx          1727/tcp   winddx
winddx          1727/udp   winddx
telindus        1728/tcp   TELINDUS
telindus        1728/udp   TELINDUS
citynl          1729/tcp   CityNL License Management
citynl          1729/udp   CityNL License Management
roketz          1730/tcp   roketz
roketz          1730/udp   roketz
msiccp          1731/tcp   MSICCP
msiccp          1731/udp   MSICCP
proxim          1732/tcp   proxim
proxim          1732/udp   proxim
sipat           1733/tcp   sipat
sipat           1733/udp   sipat
cambertx-lm     1734/tcp   Camber Corporation License Management
cambertx-lm     1734/udp   Camber Corporation License Management
privatechat     1735/tcp   PrivateChat
privatechat     1735/udp   PrivateChat
street-stream   1736/tcp   street-stream
street-stream   1736/udp   street-stream
ultimad         1737/tcp   ultimad
ultimad         1737/udp   ultimad
gamegen1        1738/tcp   GameGen1
gamegen1        1738/udp   GameGen1
webaccess       1739/tcp   webaccess
webaccess       1739/udp   webaccess
encore          1740/tcp   encore
encore          1740/udp   encore
cisco-net-mgmt  1741/tcp   cisco-net-mgmt
```

```
cisco-net-mgmt  1741/udp   cisco-net-mgmt
3Com-nsd        1742/tcp   3Com-nsd
3Com-nsd        1742/udp   3Com-nsd
cinegrfx-lm     1743/tcp   Cinema Graphics License Manager
cinegrfx-lm     1743/udp   Cinema Graphics License Manager
ncpm-ft         1744/tcp   ncpm-ft
ncpm-ft         1744/udp   ncpm-ft
remote-winsock  1745/tcp   remote-winsock
remote-winsock  1745/udp   remote-winsock
ftrapid-1       1746/tcp   ftrapid-1
ftrapid-1       1746/udp   ftrapid-1
ftrapid-2       1747/tcp   ftrapid-2
ftrapid-2       1747/udp   ftrapid-2
oracle-em1      1748/tcp   oracle-em1
oracle-em1      1748/udp   oracle-em1
aspen-services  1749/tcp   aspen-services
aspen-services  1749/udp   aspen-services
sslp            1750/tcp   Simple Socket Library's PortMaster
sslp            1750/udp   Simple Socket Library's PortMaster
swiftnet        1751/tcp   SwiftNet
swiftnet        1751/udp   SwiftNet
lofr-lm         1752/tcp   Leap of Faith Research License Manager
lofr-lm         1752/udp   Leap of Faith Research License Manager
translogic-lm   1753/tcp   Translogic License Manager
translogic-lm   1753/udp   Translogic License Manager
oracle-em2      1754/tcp   oracle-em2
oracle-em2      1754/udp   oracle-em2
ms-streaming    1755/tcp   ms-streaming
ms-streaming    1755/udp   ms-streaming
capfast-lmd     1756/tcp   capfast-lmd
capfast-lmd     1756/udp   capfast-lmd
cnhrp           1757/tcp   cnhrp
cnhrp           1757/udp   cnhrp
tftp-mcast      1758/tcp   tftp-mcast
tftp-mcast      1758/udp   tftp-mcast
spss-lm         1759/tcp   SPSS License Manager
spss-lm         1759/udp   SPSS License Manager
www-ldap-gw     1760/tcp   www-ldap-gw
www-ldap-gw     1760/udp   www-ldap-gw
cft-0           1761/tcp   cft-0
cft-0           1761/udp   cft-0
cft-1           1762/tcp   cft-1
cft-1           1762/udp   cft-1
cft-2           1763/tcp   cft-2
cft-2           1763/udp   cft-2
cft-3           1764/tcp   cft-3
cft-3           1764/udp   cft-3
cft-4           1765/tcp   cft-4
cft-4           1765/udp   cft-4
cft-5           1766/tcp   cft-5
cft-5           1766/udp   cft-5
cft-6           1767/tcp   cft-6
cft-6           1767/udp   cft-6
cft-7           1768/tcp   cft-7
cft-7           1768/udp   cft-7
bmc-net-adm     1769/tcp   bmc-net-adm
bmc-net-adm     1769/udp   bmc-net-adm
bmc-net-svc     1770/tcp   bmc-net-svc
bmc-net-svc     1770/udp   bmc-net-svc
vaultbase       1771/tcp   vaultbase
vaultbase       1771/udp   vaultbase
essweb-gw       1772/tcp   EssWeb Gateway
essweb-gw       1772/udp   EssWeb Gateway
kmscontrol      1773/tcp   KMSControl
kmscontrol      1773/udp   KMSControl
global-dtserv   1774/tcp   global-dtserv
global-dtserv   1774/udp   global-dtserv
#               1775/tcp   femis
#                  1776/tcp    Federal Emergency Management Information
Systemfemis
#                  1776/udp    Federal Emergency Management Information
System
powerguardian   1777/tcp   powerguardian
powerguardian   1777/udp   powerguardian
prodigy-internet1778/tcp   prodigy-internet
prodigy-internet1778/udp   prodigy-internet
pharmasoft      1779/tcp   pharmasoft
pharmasoft      1779/udp   pharmasoft
dpkeyserv       1780/tcp   dpkeyserv
dpkeyserv       1780/udp   dpkeyserv
answersoft-lm   1781/tcp   answersoft-lm
answersoft-lm   1781/udp   answersoft-lm
hp-hcip         1782/tcp   hp-hcip
hp-hcip         1782/udp   hp-hcip
fjris           1783/tcp   Fujitsu Remote Install Service
fjris           1783/udp   Fujitsu Remote Install Service
finle-lm        1784/tcp   Finle License Manager
finle-lm        1784/udp   Finle License Manager
windlm          1785/tcp   Wind River Systems License Manager
windlm          1785/udp   Wind River Systems License Manager
funk-logger     1786/tcp   funk-logger
funk-logger     1786/udp   funk-logger
funk-license    1787/tcp   funk-license
funk-license    1787/udp   funk-license
psmond          1788/tcp   psmond
psmond          1788/udp   psmond
hello           1789/tcp   hello
hello           1789/udp   hello
nmsp            1790/tcp   Narrative Media Streaming Protocol
nmsp            1790/udp   Narrative Media Streaming Protocol
ea1             1791/tcp   EA1
ea1             1791/udp   EA1
ibm-dt-2        1792/tcp   ibm-dt-2
ibm-dt-2        1792/udp   ibm-dt-2
rsc-robot       1793/tcp   rsc-robot
rsc-robot       1793/udp   rsc-robot
cera-bcm        1794/tcp   cera-bcm
cera-bcm        1794/udp   cera-bcm
dpi-proxy       1795/tcp   dpi-proxy
dpi-proxy       1795/udp   dpi-proxy
vocaltec-admin  1796/tcp   Vocaltec Server Administration
vocaltec-admin  1796/udp   Vocaltec Server Administration
uma             1797/tcp   UMA
uma             1797/udp   UMA
etp             1798/tcp   Event Transfer Protocol
etp             1798/udp   Event Transfer Protocol
netrisk         1799/tcp   NETRISK
netrisk         1799/udp   NETRISK
ansys-lm        1800/tcp   ANSYS-License manager
ansys-lm        1800/udp   ANSYS-License manager
msmq            1801/tcp   Microsoft Message Que
msmq            1801/udp   Microsoft Message Que
concomp1        1802/tcp   ConComp1
concomp1        1802/udp   ConComp1
hp-hcip-gwy     1803/tcp   HP-HCIP-GWY
hp-hcip-gwy     1803/udp   HP-HCIP-GWY
enl             1804/tcp   ENL
enl             1804/udp   ENL
enl-name        1805/tcp   ENL-Name
enl-name        1805/udp   ENL-Name
musiconline     1806/tcp   Musiconline
musiconline     1806/udp   Musiconline
fhsp            1807/tcp   Fujitsu Hot Standby Protocol
fhsp            1807/udp   Fujitsu Hot Standby Protocol
oracle-vp2      1808/tcp   Oracle-VP2
oracle-vp2      1808/udp   Oracle-VP2
oracle-vp1      1809/tcp   Oracle-VP1
oracle-vp1      1809/udp   Oracle-VP1
jerand-lm       1810/tcp   Jerand License Manager
jerand-lm       1810/udp   Jerand License Manager
scientia-sdb    1811/tcp   Scientia-SDB
scientia-sdb    1811/udp   Scientia-SDB
radius          1812/tcp   RADIUS
radius          1812/udp   RADIUS
radius-acct     1813/tcp   RADIUS Accounting
radius-acct     1813/udp   RADIUS Accounting
tdp-suite       1814/tcp   TDP Suite
tdp-suite       1814/udp   TDP Suite
mmpft           1815/tcp   MMPFT
mmpft           1815/udp   MMPFT
#               1814-1817  Unassigned
etftp           1818/tcp   Enhanced Trivial File Transfer Protocol
etftp           1818/udp   Enhanced Trivial File Transfer Protocol
plato-lm        1819/tcp   Plato License Manager
plato-lm        1819/udp   Plato License Manager
mcagent         1820/tcp   mcagent
mcagent         1820/udp   mcagent
donnyworld      1821/tcp   donnyworld
donnyworld      1821/udp   donnyworld
es-elmd         1822/tcp   es-elmd
es-elmd         1822/udp   es-elmd
unisys-lm       1823/tcp   Unisys Natural Language License Manager
unisys-lm       1823/udp   Unisys Natural Language License Manager
metrics-pas     1824/tcp   metrics-pas
metrics-pas     1824/udp   metrics-pas
#               1825-1900  Unassigned
fjicl-tep-a     1901/tcp   Fujitsu ICL Terminal Emulator Program A
fjicl-tep-a     1901/udp   Fujitsu ICL Terminal Emulator Program A
fjicl-tep-b     1902/tcp   Fujitsu ICL Terminal Emulator Program B
fjicl-tep-b     1902/udp   Fujitsu ICL Terminal Emulator Program B
linkname        1903/tcp   Local Link Name Resolution
linkname        1903/udp   Local Link Name Resolution
fjicl-tep-c     1904/tcp   Fujitsu ICL Terminal Emulator Program C
fjicl-tep-c     1904/udp   Fujitsu ICL Terminal Emulator Program C
sugp            1905/tcp   Secure UP.Link Gateway Protocol
sugp            1905/udp   Secure UP.Link Gateway Protocol
tpmd            1906/tcp   TPortMapperReq
tpmd            1906/udp   TPortMapperReq
intrastar       1907/tcp   IntraSTAR
intrastar       1907/udp   IntraSTAR
dawn            1908/tcp   Dawn
dawn            1908/udp   Dawn
global-wlink    1909/tcp   Global World Link
global-wlink    1909/udp   Global World Link
#               1908-1910  Unassigned
mtp                1911/tcp    Starlight Networks Multimedia Transport
Protocol
mtp                1911/tcp    Starlight Networks Multimedia Transport
Protocol
#               1912       Unassigned
armadp          1913/tcp   armadp
armadp          1913/udp   armadp
elm-momentum    1914/tcp   Elm-Momentum
elm-momentum    1914/udp   Elm-Momentum
facelink        1915/tcp   FACELINK
facelink        1915/udp   FACELINK
persoft         1916/tcp   Persoft Persona
persoft         1916/udp   Persoft Persona
noagent         1917/tcp   nOAgent
noagent         1917/udp   nOAgent
can-nds         1918/tcp   Candle Directory Service - NDS
can-nds         1918/udp   Candle Directory Service - NDS
can-dch         1919/tcp   Candle Directory Service - DCH
can-dch         1919/udp   Candle Directory Service - DCH
can-ferret      1920/tcp   Candle Directory Service - FERRET
can-ferret      1920/udp   Candle Directory Service - FERRET
#               1921-1943  Unassigned
close-combat    1944/tcp   close-combat
close-combat    1944/udp   close-combat
dialogic-elmd   1945/tcp   dialogic-elmd
dialogic-elmd   1945/udp   dialogic-elmd
tekpls          1946/tcp   tekpls
tekpls          1946/udp   tekpls
hlserver        1947/tcp   hlserver
hlserver        1947/udp   hlserver
eye2eye         1948/tcp   eye2eye
eye2eye         1948/udp   eye2eye
ismaeasdaqlive  1949/tcp   ISMA Easdaq Live
ismaeasdaqlive  1949/udp   ISMA Easdaq Live
ismaeasdaqtest  1950/tcp   ISMA Easdaq Test
ismaeasdaqtest  1950/udp   ISMA Easdaq Test
bcs-lmserver    1951/tcp   bcs-lmserver
bcs-lmserver    1951/udp   bcs-lmserver
#               1952-1972  Unassigned
dlsrap          1973/tcp   Data Link Switching Remote Access Protocol
dlsrap          1973/udp   Data Link Switching Remote Access Protocol
#               1974-1984  Unassigned
foliocorp       1985/tcp   Folio Remote Server
foliocorp       1985/udp   Folio Remote Server
licensedaemon   1986/tcp   cisco license management
licensedaemon   1986/udp   cisco license management
tr-rsrb-p1      1987/tcp   cisco RSRB Priority 1 port
tr-rsrb-p1      1987/udp   cisco RSRB Priority 1 port
tr-rsrb-p2      1988/tcp   cisco RSRB Priority 2 port
tr-rsrb-p2      1988/udp   cisco RSRB Priority 2 port
tr-rsrb-p3      1989/tcp   cisco RSRB Priority 3 port
tr-rsrb-p3      1989/udp   cisco RSRB Priority 3 port
#PROBLEMS!==================================================
mshnet          1989/tcp   MHSnet system
mshnet          1989/udp   MHSnet system
#PROBLEMS!==================================================
stun-p1         1990/tcp   cisco STUN Priority 1 port
stun-p1         1990/udp   cisco STUN Priority 1 port
stun-p2         1991/tcp   cisco STUN Priority 2 port
stun-p2         1991/udp   cisco STUN Priority 2 port
stun-p3         1992/tcp   cisco STUN Priority 3 port
```

```
stun-p3         1992/udp   cisco STUN Priority 3 port
#PROBLEMS!==================================================
ipsendmsg       1992/tcp   IPsendmsg
ipsendmsg       1992/udp   IPsendmsg
#PROBLEMS!==================================================
snmp-tcp-port   1993/tcp   cisco SNMP TCP port
snmp-tcp-port   1993/udp   cisco SNMP TCP port
stun-port       1994/tcp   cisco serial tunnel port
stun-port       1994/udp   cisco serial tunnel port
perf-port       1995/tcp   cisco perf port
perf-port       1995/udp   cisco perf port
tr-rsrb-port    1996/tcp   cisco Remote SRB port
tr-rsrb-port    1996/udp   cisco Remote SRB port
gdp-port        1997/tcp   cisco Gateway Discovery Protocol
gdp-port        1997/udp   cisco Gateway Discovery Protocol
x25-svc-port    1998/tcp   cisco X.25 service (XOT)
x25-svc-port    1998/udp   cisco X.25 service (XOT)
tcp-id-port     1999/tcp   cisco identification port
tcp-id-port     1999/udp   cisco identification port
callbook        2000/tcp
callbook        2000/udp
dc              2001/tcp
wizard          2001/udp   curry
globe           2002/tcp
globe           2002/udp
mailbox         2004/tcp
emce            2004/udp   CCWS mm conf
berknet         2005/tcp
oracle          2005/udp
invokator       2006/tcp
raid-cc         2006/udp   raid
dectalk         2007/tcp
raid-am         2007/udp
conf            2008/tcp
terminaldb      2008/udp
news            2009/tcp
whosockami      2009/udp
search          2010/tcp
pipe_server     2010/udp
raid-cc         2011/tcp    raid
servserv        2011/udp
ttyinfo         2012/tcp
raid-ac         2012/udp
raid-am         2013/tcp
raid-cd         2013/udp
troff           2014/tcp
raid-sf         2014/udp
cypress         2015/tcp
raid-cs         2015/udp
bootserver      2016/tcp
bootserver      2016/udp
cypress-stat    2017/tcp
bootclient      2017/udp
terminaldb      2018/tcp
rellpack        2018/udp
whosockami      2019/tcp
about           2019/udp
xinupageserver  2020/tcp
xinupageserver  2020/udp
servexec        2021/tcp
xinuexpansion1  2021/udp
down            2022/tcp
xinuexpansion2  2022/udp
xinuexpansion3  2023/tcp
xinuexpansion3  2023/udp
xinuexpansion4  2024/tcp
xinuexpansion4  2024/udp
ellpack         2025/tcp
xribs           2025/udp
scrabble        2026/tcp
scrabble        2026/udp
shadowserver    2027/tcp
shadowserver    2027/udp
submitserver    2028/tcp
submitserver    2028/udp
device2         2030/tcp
device2         2030/udp
blackboard      2032/tcp
blackboard      2032/udp
glogger         2033/tcp
glogger         2033/udp
scoremgr        2034/tcp
scoremgr        2034/udp
imsldoc         2035/tcp
imsldoc         2035/udp
objectmanager   2038/tcp
objectmanager   2038/udp
lam             2040/tcp
lam             2040/udp
interbase       2041/tcp
interbase       2041/udp
isis            2042/tcp   isis
isis            2042/udp   isis
isis-bcast      2043/tcp   isis-bcast
isis-bcast      2043/udp   isis-bcast
rimsl           2044/tcp
rimsl           2044/udp
cdfunc          2045/tcp
cdfunc          2045/udp
sdfunc          2046/tcp
sdfunc          2046/udp
dls             2047/tcp
dls             2047/udp
dls-monitor     2048/tcp
dls-monitor     2048/udp
#PROBLEMS!==================================================
shilp           2049/tcp
shilp           2049/udp
#PROBLEMS!==================================================
nfs             2049/tcp   Network File System - Sun Microsystems
nfs             2049/udp   Network File System - Sun Microsystems
dlsrpn          2065/tcp   Data Link Switch Read Port Number
dlsrpn          2065/udp   Data Link Switch Read Port Number
dlswpn          2067/tcp   Data Link Switch Write Port Number
dlswpn          2067/udp   Data Link Switch Write Port Number
zephyr-srv      2102/tcp   Zephyr server
zephyr-srv      2102/udp   Zephyr server
zephyr-clt      2103/tcp   Zephyr serv-hm connection
zephyr-clt      2103/udp   Zephyr serv-hm connection
zephyr-hm       2104/tcp   Zephyr hostmanager
zephyr-hm       2104/udp   Zephyr hostmanager
minipay         2105/tcp   MiniPay
minipay         2105/udp   MiniPay
#               2106-2200  Unassigned
ats             2201/tcp   Advanced Training System Program
ats             2201/udp   Advanced Training System Program
imtc-map        2202/tcp   Int. Multimedia Teleconferencing Cosortium
imtc-map        2202/udp   Int. Multimedia Teleconferencing Cosortium
kali            2213/tcp   Kali
kali            2213/udp   Kali
unreg-ab1       2221/tcp   Allen-Bradley unregistered port
unreg-ab1       2221/udp   Allen-Bradley unregistered port
unreg-ab2       2222/tcp   Allen-Bradley unregistered port
unreg-ab2       2222/udp   Allen-Bradley unregistered port
inreg-ab3       2223/tcp   Allen-Bradley unregistered port
inreg-ab3       2223/udp   Allen-Bradley unregistered port
ivs-video       2232/tcp   IVS Video default
ivs-video       2232/udp   IVS Video default
infocrypt       2233/tcp   INFOCRYPT
infocrypt       2233/udp   INFOCRYPT
directplay      2234/tcp   DirectPlay
directplay      2234/udp   DirectPlay
sercomm-wlink   2235/tcp   Sercomm-WLink
sercomm-wlink   2235/udp   Sercomm-WLink
nani            2236/tcp   Nani
nani            2236/udp   Nani
optech-port1-lm 2237/tcp   Optech Port1 License Manager
optech-port1-lm 2237/udp   Optech Port1 License Manager
aviva-sna       2238/tcp   AVIVA SNA SERVER
aviva-sna       2238/udp   AVIVA SNA SERVER
imagequery      2239/tcp   Image Query
imagequery      2239/udp   Image Query
#               2240       Unassigned
ivsd            2241/tcp   IVS Daemon
ivsd            2241/udp   IVS Daemon
#               2242-2278  Unassigned
xmquery         2279/tcp   xmquery
xmquery         2279/udp   xmquery
lnvpoller       2280/tcp   LNVPOLLER
lnvpoller       2280/udp   LNVPOLLER
lnvconsole      2281/tcp   LNVCONSOLE
lnvconsole      2281/udp   LNVCONSOLE
lnvalarm        2282/tcp   LNVALARM
lnvalarm        2282/udp   LNVALARM
lnvstatus       2283/tcp   LNVSTATUS
lnvstatus       2283/udp   LNVSTATUS
lnvmaps         2284/tcp   LNVMAPS
lnvmaps         2284/udp   LNVMAPS
lnvmailmon      2285/tcp   LNVMAILMON
lnvmailmon      2285/udp   LNVMAILMON
nas-meterin     2286/tcp   NAS-Metering
nas-meterin     2286/udp   NAS-Metering
dna             2287/tcp   DNA
dna             2287/udp   DNA
netml           2288/tcp   NETML
netml           2288/udp   NETML
#               2289-2306  Unassigned
pehelp          2307/tcp   pehelp
pehelp          2307/udp   pehelp
#               2308-2400  Unassigned
cvspserver      2401/tcp   cvspserver
cvspserver      2401/udp   cvspserver
rtsserv         2500/tcp   Resource Tracking system server
rtsserv         2500/udp   Resource Tracking system server
rtsclient       2501/tcp   Resource Tracking system client
rtsclient       2501/udp   Resource Tracking system client
hp-3000-elnet   2564/tcp   HP 3000 NS/VT block mode telnet
netrek          2592/tcp   netrek
netrek          2592/udp   netrek
tqdata          2700/tcp   tqdata
tqdata          2700/udp   tqdata
#               Unasigned
www-dev         2784/tcp   world wide web - development
www-dev         2784/udp   world wide web - development
aic-n           2785/tcp   aic-np
aic-p           2785/udp   aic-np
aic-oncrpc      2786/tcp   aic-oncrpc - Destiny MCD database
aic-oncrpc      2786/udp   aic-oncrpc - Destiny MCD database
piccolo         2787/tcp   piccolo - Cornerstone Software
piccolo         2787/udp   piccolo - Cornerstone Software
fryeserv        2788/tcp   NetWare Loadable Module - Seagate Software
fryeserv        2788/udp   NetWare Loadable Module - Seagate Software
media-agent     2789/tcp   Media Agent
media-agen      2789/udp   Media Agent
#               2789-2907  Unasigned
mao             2908/tcp   mao
mao             2908/udp   mao
#               2909-2999  Unasigned
hbci            3000/tcp   HBCI
hbci            3000/udp   HBCI
redwood-broker  3001/tcp   Redwood Broker
redwood-broker  3001/udp   Redwood Broker
exlm-agent      3002/tcp   EXLM Agent
exlm-agent      3002/udp   EXLM Agent
#               3003-3009  Unassigned
gw              3010/tcp   Telerate Workstation
ping-pong       3010/udp   Telerate Workstation
trusted-web     3011/tcp   Trusted Web
trusted-web     3011/udp   Trusted Web
#               3012-3046  Unassigned
hlserver        3047/tcp   Fast Security HL Server
hlserver        3047/udp   Fast Security HL Server
pctrader        3048/tcp   Sierra Net PC Trader
pctrader        3048/udp   Sierra Net PC Trader
NSWS            3049/tcp
NSWS            3049/udp
vmodem          3141/tcp   VMODEM
vmodem          3141/udp   VMODEM
rdc-wh-eos      3142/tcp   RDC WH EOS
rdc-wh-eos      3142/udp   RDC WH EOS
seaview         3143/tcp   Sea View
seaview         3143/udp   Sea View
tarantella      3144/tcp   Tarantella
tarantella      3144/udp   Tarantella
csi-lfap        3145/tcp   CSI-LFAP
csi-lfap        3145/udp   CSI-LFAP
#               3146-3263  Unassigned
ccmail          3264/tcp   cc:mail/lotus
ccmail          3264/udp   cc:mail/lotus
dec-notes       3333/tcp   DEC Notes
dec-notes       3333/udp   DEC Notes
mapper-nodemgr  3984/tcp   MAPPER network node manager
mapper-nodemgr  3984/udp   MAPPER network node manager
mapper-mapethd  3985/tcp   MAPPER TCP/IP server
mapper-mapethd  3985/udp   MAPPER TCP/IP server
mapper-ws_ethd  3986/tcp   MAPPER workstation server
```

```
mapper-ws_ethd  3986/udp   MAPPER workstation server
bmap            3421/tcp   Bull Apprise portmapper
bmap            3421/udp   Bull Apprise portmapper
mira            3454/tcp   Apple Remote Access Protocol
prsvp           3455/tcp   RSVP Port
prsvp           3455/udp   RSVP Port
vat             3456/tcp   VAT default data
vat             3456/udp   VAT default data
vat-control     3457/tcp   VAT default control
vat-control     3457/udp   VAT default control
#               3458-3899  Unassigned
udt_os          3900/tcp   Unidata UDT OS
udt_os          3900/udp   Unidata UDT OS
netcheque       4008/tcp   NetCheque accounting
netcheque       4008/udp   NetCheque accounting
chimera-hwm     4009/tcp   Chimera HWM
chimera-hwm     4009/udp   Chimera HWM
#               4010-4131  Unassigned
nuts_dem        4132/tcp   NUTS Daemon
nuts_dem        4132/udp   NUTS Daemon
nuts_bootp      4133/tcp   NUTS Bootp Server
nuts_bootp      4133/udp   NUTS Bootp Server
nifty-hmi       4134/tcp   NIFTY-Serve HMI protocol
nifty-hmi       4134/udp   NIFTY-Serve HMI protocol
rwhois          4321/tcp   Remote Who Is
rwhois          4321/udp   Remote Who Is
unicall         4343/tcp   UNICALL
unicall         4343/udp   UNICALL
krb524          4444/tcp   KRB524
krb524          4444/udp   KRB524
# PROBLEM krb524 assigned the port,
# PROBLEM nv used it without an assignment
nv-video        4444/tcp   NV Video default
nv-video        4444/udp   NV Video default
upnotifyp       4445/tcp   UPNOTIFYP
upnotifyp       4445/udp   UPNOTIFYP
n1-fwp          4446/tcp   N1-FWP
n1-fwp          4446/udp   N1-FWP
n1-rmgmt        4447/tcp   N1-RMGMT
n1-rmgmt        4447/udp   N1-RMGMT
asc-slmd        4448/tcp   ASC Licence Manager
asc-slmd        4448/udp   ASC Licence Manager
arcryptoip      4449/tcp   ARCrypto IP
arcryptoip      4449/udp   ARCrypto IP
camp            4450/tcp   Camp
camp            4450/udp   Camp
ctisystemmsg    4451/tcp   CTI System Msg
ctisystemmsg    4451/udp   CTI System Msg
ctiprogramload  4452/tcp   CTI Program Load
ctiprogramload  4452/udp   CTI Program Load
nssalertmgr     4453/tcp   NSS Alert Manager
nssalertmgr     4453/udp   NSS Alert Manager
nssagentmgr     4454/tcp   NSS Agent Manager
nssagentmgr     4454/udp   NSS Agent Manager
#               4455-4499  Unassigned
sae-urn         4500/tcp   sae-urn
sae-urn         4500/udp   sae-urn
urn-x-cdchoice  4501/tcp   urn-x-cdchoice
urn-x-cdchoice  4501/udp   urn-x-cdchoice
rfa             4672/tcp   remote file access server
rfa             4672/udp   remote file access server
commplex-main   5000/tcp
commplex-main   5000/udp
commplex-link   5001/tcp
commplex-link   5001/udp
rfe             5002/tcp   radio free ethernet
rfe             5002/udp   radio free ethernet
claris-fmpro    5003/tcp   Claris FileMaker Pro
claris-fmpro    5003/udp   Claris FileMaker Pro
avt-profile-1   5004/tcp   avt-profile-1
avt-profile-1   5004/udp   avt-profile-1
avt-profile-2   5005/tcp   avt-profile-2
avt-profile-2   5005/udp   avt-profile-2
telelpathstart  5010/tcp   TelepathStart
telelpathstart  5010/udp   TelepathStart
telelpathattack 5011/tcp   TelepathAttack
telelpathattack 5011/udp   TelepathAttack
zenginkyo-1     5020/tcp   zenginkyo-1
zenginkyo-1     5020/udp   zenginkyo-1
zenginkyo-2     5021/tcp   zenginkyo-2
zenginkyo-2     5021/udp   zenginkyo-2
mmcc            5050/tcp   multimedia conference control tool
mmcc            5050/udp   multimedia conference control tool
rmonitor_secure 5145/tcp
rmonitor_secure 5145/udp
atmp            5150/tcp   Ascend Tunnel Management Protocol
atmp            5150/udp   Ascend Tunnel Management Protocol
aol             5190/tcp   America-Online
aol             5190/udp   America-Online
aol-1           5191/tcp   AmericaOnline1
aol-1           5191/udp   AmericaOnline1
aol-2           5192/tcp   AmericaOnline2
aol-2           5192/udp   AmericaOnline2
aol-3           5193/tcp   AmericaOnline3
aol-3           5193/udp   AmericaOnline3
padl2sim        5236/tcp
padl2sim        5236/udp
hacl-hb         5300/tcp   HA cluster heartbeat
hacl-hb         5300/udp   HA cluster heartbeat
hacl-gs         5301/tcp   HA cluster general services
hacl-gs         5301/udp   HA cluster general services
hacl-cfg        5302/tcp   HA cluster configuration
hacl-cfg        5302/udp   HA cluster configuration
hacl-probe      5303/tcp   HA cluster probing
hacl-probe      5303/udp   HA cluster probing
hacl-local      5304/tcp   HA Cluster Commands
hacl-local      5304/udp
hacl-test       5305/tcp   HA Cluster Test
hacl-test       5305/udp
excerpt         5400/tcp   Excerpt Search
excerpt         5400/udp   Excerpt Search
excerpts        5401/tcp   Excerpt Search Secure
excerpts        5401/udp   Excerpt Search Secure
personal-agent  5555/tcp   Personal Agent
personal-agent  5555/udp   Personal Agent
pcanywheredata  5631/tcp   pcANYWHEREdata
pcanywheredata  5631/udp   pcANYWHEREdata
pcanywherestat  5632/tcp   pcANYWHEREstat
pcanywherestat  5632/udp   pcANYWHEREstat
rrac            5678/tcp   Remote Replication Agent Connection
rrac            5678/udp   Remote Replication Agent Connection
dccm            5679/tcp   Direct Cable Connect Manager
dccm            5679/udp   Direct Cable Connect Manager
proshareaudio   5713/tcp   proshare conf audio
proshareaudio   5713/udp   proshare conf audio
prosharevideo   5714/tcp   proshare conf video
prosharevideo   5714/udp   proshare conf video
prosharedata    5715/tcp   proshare conf data
prosharedata    5715/udp   proshare conf data
prosharerequest 5716/tcp   proshare conf request
prosharerequest 5716/udp   proshare conf request
prosharenotify  5717/tcp   proshare conf notify
prosharenotify  5717/udp   proshare conf notify
openmail        5729/tcp   Openmail User Agent Layer
openmail        5729/udp   Openmail User Agent Layer
openmailg       5755/tcp   OpenMail Desk Gateway server
openmailg       5755/udp   OpenMail Desk Gateway server
x500ms          5757/tcp   OpenMail X.500 Directory Server
x500ms          5757/udp   OpenMail X.500 Directory Server
openmailns      5766/tcp   OpenMail NewMail Server
openmailns      5766/udp   OpenMail NewMail Server
s-openmail      5767/tcp   OpenMail Suer Agent Layer (Secure)
s-openmail      5767/udp   OpenMail Suer Agent Layer (Secure)
fcopy-server    5745/tcp   fcopy-server
fcopy-server    5745/udp   fcopy-server
x11             6000-6063/tcp   X Window System
x11             6000-6063/udp   X Window System
softcm          6110/tcp   HP SoftBench CM
softcm          6110/udp   HP SoftBench CM
spc             6111/tcp   HP SoftBench Sub-Process Control
spc             6111/udp   HP SoftBench Sub-Process Control
dtspcd          6112/tcp   dtspcd
dtspcd          6112/udp   dtspcd
backup-express  6123/tcp   Backup Express
backup-express  6123/udp   Backup Express
meta-corp       6141/tcp   Meta Corporation License Manager
meta-corp       6141/udp   Meta Corporation License Manager
aspentec-lm     6142/tcp   Aspen Technology License Manager
aspentec-lm     6142/udp   Aspen Technology License Manager
watershed-lm    6143/tcp   Watershed License Manager
watershed-lm    6143/udp   Watershed License Manager
statsci1-lm     6144/tcp   StatSci License Manager - 1
statsci1-lm     6144/udp   StatSci License Manager - 1
statsci2-lm     6145/tcp   StatSci License Manager - 2
statsci2-lm     6145/udp   StatSci License Manager - 2
lonewolf-lm     6146/tcp   Lone Wolf Systems License Manager
lonewolf-lm     6146/udp   Lone Wolf Systems License Manager
montage-lm      6147/tcp   Montage License Manager
montage-lm      6147/udp   Montage License Manager
ricardo-lm      6148/tcp   Ricardo North America License Manager
ricardo-lm      6148/udp   Ricardo North America License Manager
tal-pod         6149/tcp    tal-pod
tal-pod         6149/udp    tal-pod
crip            6253/tcp    CRIP
crip            6253/udp    CRIP
clariion-evr01  6389/tcp    clariion-evr01
clariion-evr01  6389/udp    clariion-evr01
skip-cert-recv  6455/tcp   SKIP Certificate Receive
skip-cert-send  6456/tcp   SKIP Certificate Send
xdsxdm          6558/tcp
xdsxdm          6558/udp
vocaltec-gold   6670/tcp   Vocaltec Global Online Directory
vocaltec-gold   6670/udp   Vocaltec Global Online Directory
vision_server   6672/tcp   vision_server
vision_server   6672/udp   vision_server
vision_elmd     6673/tcp   vision_elmd
vision_elmd     6673/udp   vision_elmd
ambit-lm        6831/tcp   ambit-lm
ambit-lm        6831/udp   ambit-lm
acmsoda         6969/tcp   acmsoda
acmsoda         6969/udp   acmsoda
afs3-fileserver 7000/tcp   file server itself
afs3-fileserver 7000/udp   file server itself
afs3-callback   7001/tcp   callbacks to cache managers
afs3-callback   7001/udp   callbacks to cache managers
afs3-prserver   7002/tcp   users & groups database
afs3-prserver   7002/udp   users & groups database
afs3-vlserver   7003/tcp   volume location database
afs3-vlserver   7003/udp   volume location database
afs3-kaserver   7004/tcp   AFS/Kerberos authentication service
afs3-kaserver   7004/udp   AFS/Kerberos authentication service
afs3-volser     7005/tcp   volume managment server
afs3-volser     7005/udp   volume managment server
afs3-errors     7006/tcp   error interpretation service
afs3-errors     7006/udp   error interpretation service
afs3-bos        7007/tcp   basic overseer process
afs3-bos        7007/udp   basic overseer process
afs3-update     7008/tcp   server-to-server updater
afs3-update     7008/udp   server-to-server updater
afs3-rmtsys     7009/tcp   remote cache manager service
afs3-rmtsys     7009/udp   remote cache manager service
ups-onlinet     7010/tcp   onlinet uninterruptable power supplies
ups-onlinet     7010/udp   onlinet uninterruptable power supplies
lazy-ptop       7099/tcp   lazy-ptop
lazy-ptop       7099/udp   lazy-ptop
font-service    7100/tcp   X Font Service
font-service    7100/udp   X Font Service
virprot-lm      7121/tcp   Virtual Prototypes License Manager
virprot-lm      7121/udp   Virtual Prototypes License Manager
clutild         7174/tcp   Clutild
clutild         7174/tcp   Clutild
fodms           7200/tcp   FODMS FLIP
fodms           7200/udp   FODMS FLIP
dlip            7201/tcp   DLIP
dlip            7201/udp   DLIP
winqedit        7395/tcp    winqedit
winqedit        7395/udp    winqedit
telops-lmd      7491/tcp    telops-lmd
telops-lmd      7491/udp    telops-lmd
pafec-lm        7511/tcp    pafec-lm
pafec-lm        7511/udp    pafec-lm
cbt             7777/tcp    cbt
cbt             7777/udp    cbt
accu-lmgr       7781/tcp    accu-lmgr
accu-lmgr       7781/udp    accu-lmgr
irdmi2          7999/tcp    iRDMI2
irdmi2          7999/udp    iRDMI2
irdmi           8000/tcp    iRDMI
irdmi           8000/udp    iRDMI
pro-ed          8032/tcp    ProEd
pro-ed          8032/udp    ProEd
npmp            8450/tcp    npmp
npmp            8450/udp    npmp
ddi-tcp-1       8888/tcp    NewsEDGE server TCP (TCP 1)
ddi-udp-1       8888/udp    NewsEDGE server UDP (UDP 1)
ddi-tcp-2       8889/tcp    Desktop Data TCP 1
```

| | | |
|---|---|---|
| ddi-udp-2 | 8889/udp | NewsEDGE server broadcast |
| ddi-tcp-3 | 8890/tcp | Desktop Data TCP 2 |
| ddi-udp-3 | 8890/udp | NewsEDGE client broadcast |
| ddi-tcp-4 | 8891/tcp | Desktop Data TCP 3: NESS application |
| ddi-udp-4 | 8891/udp | Desktop Data UDP 3: NESS application |
| ddi-tcp-5 | 8892/tcp | Desktop Data TCP 4: FARM product |
| ddi-udp-5 | 8892/udp | Desktop Date UDP 4: FARM product |
| ddi-tcp-6 | 8893/tcp | Desktop Data TCP 5: NewsEDGE/Web application |
| ddi-udp-6 | 8893/udp | Desktop Date UDP 5: NewsEDGE/Web application |
| ddi-tcp-7 | 8894/tcp | Desktop Data TCP 6: COAL application |
| ddi-udp-7 | 8894/udp | Desktop Date UDP 6: COAL application |
| cslistener | 9000/tcp | CSlistener |
| cslistener | 9000/udp | CSlistener |
| man | 9535/tcp | |
| man | 9535/udp | |
| sd | 9876/tcp | Session Director |
| sd | 9876/udp | Session Director |
| # | 9877-9991 | Unassigned |
| palace | 9992/tcp | Palace |
| palace | 9992/udp | Palace |
| palace | 9993/tcp | Palace |
| palace | 9993/udp | Palace |
| palace | 9994/tcp | Palace |
| palace | 9994/udp | Palace |
| palace | 9995/tcp | Palace |
| palace | 9995/udp | Palace |
| palace | 9996/tcp | Palace |
| palace | 9996/udp | Palace |
| palace | 9997/tcp | Palace |
| palace | 9997/udp | Palace |
| distinct32 | 9998/tcp | Distinct32 |
| distinct32 | 9998/udp | Distinct32 |
| distinct | 9999/tcp | distinct |
| distinct | 9999/udp | distinct |
| ndmp | 10000/tcp | Network Data Management Protocol |
| ndmp | 10000/udp | Network Data Management Protocol |
| tsaf | 12753/tcp | tsaf port |
| tsaf | 12753/udp | tsaf port |
| isode-dua | 17007/tcp | |
| isode-dua | 17007/udp | |
| biimenu | 18000/tcp | Beckman Instruments, Inc. |
| biimenu | 18000/udp | Beckman Instruments, Inc. |
| webphone | 21845/tcp | webphone |
| webphone | 21845/udp | webphone |
| netspeak-is | 21846/tcp | NetSpeak Corp. Directory Services |
| netspeak-is | 21846/udp | NetSpeak Corp. Directory Services |
| netspeak-cs | 21847/tcp | NetSpeak Corp. Connection Services |
| netspeak-cs | 21847/udp | NetSpeak Corp. Connection Services |
| netspeak-acd | 21848/tcp | NetSpeak Corp. Automatic Call Distribution |
| netspeak-acd | 21848/udp | NetSpeak Corp. Automatic Call Distribution |
| netspeak-cps | 21849/tcp | NetSpeak Corp. Credit Processing System |
| netspeak-cps | 21849/udp | NetSpeak Corp. Credit Processing System |
| wnn6 | 22273/tcp | wnn6 |
| wnn6 | 22273/udp | wnn6 |
| vocaltec-wconf | 22555/tcp | Vocaltec Web Conference |
| vocaltec-phone | 22555/udp | Vocaltec Internet Phone |
| aws-brf | 22800/tcp | Telerate Information Platform LAN |
| aws-brf | 22800/udp | Telerate Information Platform LAN |
| brf-gw | 22951/tcp | Telerate Information Platform WAN |
| brf-gw | 22951/udp | Telerate Information Platform WAN |
| icl-twobase1 | 25000/tcp | icl-twobase1 |
| icl-twobase1 | 25000/udp | icl-twobase1 |
| icl-twobase2 | 25001/tcp | icl-twobase2 |
| icl-twobase2 | 25001/udp | icl-twobase2 |
| icl-twobase3 | 25002/tcp | icl-twobase3 |
| icl-twobase3 | 25002/udp | icl-twobase3 |
| icl-twobase4 | 25003/tcp | icl-twobase4 |
| icl-twobase4 | 25003/udp | icl-twobase4 |
| icl-twobase5 | 25004/tcp | icl-twobase5 |
| icl-twobase5 | 25004/udp | icl-twobase5 |
| icl-twobase6 | 25005/tcp | icl-twobase6 |
| icl-twobase6 | 25005/udp | icl-twobase6 |
| icl-twobase7 | 25006/tcp | icl-twobase7 |
| icl-twobase7 | 25006/udp | icl-twobase7 |
| icl-twobase8 | 25007/tcp | icl-twobase8 |
| icl-twobase8 | 25007/udp | icl-twobase8 |
| icl-twobase9 | 25008/tcp | icl-twobase9 |
| icl-twobase9 | 25008/udp | icl-twobase9 |
| icl-twobase10 | 25009/tcp | icl-twobase10 |
| icl-twobase10 | 25009/udp | icl-twobase10 |
| vocaltec-hos | 25793/tcp | Vocaltec Address Server |
| vocaltec-hos | 25793/udp | Vocaltec Address Server |
| quake | 26000/tcp | quake |
| quake | 26000/tcp | quake |
| wnn6-ds | 26208/tcp | wnn6-ds |
| wnn6-ds | 26208/udp | wnn6-ds |
| dbbrowse | 47557/tcp | Databeam Corporation |
| dbbrowse | 47557/udp | Databeam Corporation |
| ap | 47806/tcp | ALC Protocol |
| ap | 47806/udp | ALC Protocol |
| bacnet | 47808/tcp | Building Automation and Control Networks |
| bacnet | 47808/udp | Building Automation and Control Networks |

DYNAMIC AND/OR PRIVATE PORTS

Les Ports dynamique et/ou privés sont compris entre les valeurs 49152 et 65535

REFERENCES

[RFC768] Postel, J., "User Datagram Protocol", STD 6, RFC 768,
USC/Information Sciences Institute, August 1980.

[RFC793] Postel, J., ed., "Transmission Control Protocol - DARPA
Internet Program Protocol Specification", STD 7, RFC 793,
USC/Information Sciences Institute, September 1981.

# Bibliographie

**Sites Internet en langue Française :**

http://lexique.reseaux.free.fr - Le site que j'ai développé pour le lexique que je rédige

www.arcep.fr - site de l'Autorité de Régulation des Télécommunications (ARCEP) - Site consulté régulièrement pour suivre les activités autour des différentes règlementations et recommandations.

http://www.commentcamarche.net- Site de vulgarisation informatique. Le site présente maintenant un profil plus axé « nouvelles technologies » mais on y trouve toujours un forum réseau très riche.

http://www.nic.fr : Association Française pour le Nommage Internet en Coopération chargée de l'attribution des noms de domaine en ".fr". Un site utile si l'on souhaite suivre certaines actualités autour de l'Internet en France

http://www.securiteinfo.com- Site permettant d'appréhender la sécurité Agence nationale de la sécurité des systèmes d'information.

http://www.ssi.gouv.fr- Serveur Thématique de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information - J'utilise ce site pour m'assurer de certaines « bonnes pratiques »

http://www.wireless-fr.org- site d'une organisation ayant pour but le développement d'un vaste réseau libre.

http://fr.wikipedia.org - Site de l'encyclopédie libre et modifiable.

**Sites en langue Anglaise :**

http://www.cert.org- Centre d'études sur la vulnérabilité de la sécurité d'Internet. Un site de référence pour bien démarrer dans la mise en œuvre d'une politique de sécurité.

http://www.cisco.com - site du constructeur/équipementier CISCO - Très utile pour accéder en ligne à la documentation des produits et à la documentation de l'IOS (Internetworking Operating System)

http://www.ripe.net - RIPE (Réseaux IP Européens) - Quelques outils en ligne très utiles pour diagnostiquer sur Internet, tracer une adresse ou des « annoncements »

**Bibliographie :**

*Dictionnaire Télécoms et Réseaux - Français : Anglais*, Dictem Paris, 1996 (épuisé).

*Dictionnaire Larousse de l'Informatique,* Larousse, 1981

*Dictionnaire Larousse de l'Informatique,* Larousse, 1988

Alexis, FERRERO, *Ethernet et ses évolutions*, Editions Addison-Wesley, 1999

Radia, PERLMAN, *Interconnexions Ponts et Routeurs,* Editions Addison-Wesley, 1994

*Internetworking Technology Overview* - Cisco Systems - DOC-ITO, 1993

*Internetworking Terms and Acronyms* - Cisco Systems - DOC-ITA, 1994

Gisèle, CIZAULT, *IPv6 : Théorie et pratique*, Editions O'REILLY, 1999

*L'anneau à jeton - Présentation technique,* IBM - Marketing Interne, 1991

Guy, PUJOLLE, *Les Réseaux Editions 2003*, Editions Eyrolles, 2003

Douglas, COMER, *TCP/IP Architecture, Protocoles, Applications - 3eme édition* - Editions DUNOD Informatiques, 2000

Xavier, LAGRANGE, Philippe, GODLEWSKI, Sami, TABBANE, *Réseaux GSM, 5eme Edition revue et corrigée*, Hermes Sciences Publications, 2005

Helmut TORNSDORF, Manfred TORNSDORF, *Le Grand Livre MS-DOS 5.0,* Editions Micro Application, 1991

Mathieu, NEBRA, *Concevez votre Site Web avec PHP et MYSQL,* Le Livre du Zéro, 2010

**Revues Utilisées / Veille technologique (revues consultées entre 1992 et 2010) :**

*01 Réseaux* - Groupe Tests - Mensuel

*Décision Informatique* - Groupe Tests - Hebdomadaire (ancien titre = *Décision Micro et Réseaux*)

*L'ordinateur Individuel* - Groupe tests - Mensuel

*Micro Hebdo* - Groupe Tests - Hebdomadaire

*Réseaux et Télécoms* - Network World - IDG Communications France - Mensuel

*Science et Vie Micro* - SVM - Mensuel

*Stratégie Télécoms et Multimédia* - Hebdomadaire