Réseaux CPL par la pratique

Avec trois études de cas : réseau domestique, réseau d'entreprise et réseau de desserte de collectivité locale

Xavier Carcelle

EYROLLES

Réseaux CPL
par la pratique

Xavier Carcelle

Avec la contribution
de Davor Males et Guy Pujolle,
et la collaboration de Olivier Salvatori

EYROLLES

CHEZ LE MÊME ÉDITEUR

Autres ouvrages sur les réseaux

D. MALES, G. PUJOLLE. – **Wi-Fi par la pratique**.
N°11409, 2e édition, 2004, 420 pages.

G. PUJOLLE, *et al*. – **Sécurité Wi-Fi**.
N°11528, 2004, 242 pages.

J. NOZICK. – **Guide du câblage universel**.
Logements et bureaux - Nouvelle norme NF C 15-100 - Prises universelles RJ 45.
N°11758, 2e édition, 2006, 110 pages.

G. PUJOLLE. – **Les Réseaux**.
N°11987, 5e édition, 2004, 1 120 pages (édition semi-poche).

K. AL AGHA, G. PUJOLLE, G.VIVIER. – **Réseaux de mobiles et réseaux sans fil**.
N°11018, 2001, 490 pages.

P. MÜHLETHALER. – **802.11 et les réseaux sans fil**.
N°11154, 2002, 304 pages.

N. AGOULMINE, O. CHERKAOUI. – **Pratique de la gestion de réseau**.
N°11259, 2003, 280 pages.

J.-L. MÉLIN. – **Qualité de service sur IP**.
N°9261, 2001, 368 pages.

Ouvrages sur la sécurité réseau

S. BORDERES. – **Authentification réseau avec Radius**.
N°12007, 2006, 300 pages.

J. STEINBERG, T. SPEED, adapté par B. SONNTAG. – **SSL VPN**. *Accès web et extranets sécurisés*.
N°11933, 2006, 220 pages.

L. LEVIER, C. LLORENS. – **Tableaux de bord de la sécurité réseau**.
N°11973, 2e édition, 2006, 582 pages.

B. BOUTHERIN, B. DELAUNAY. – **Sécuriser un réseau Linux**.
N°11960, 3e édition, 2007, 250 pages.

F. IA, O. MÉNAGER. – **Optimiser et sécuriser son trafic IP**.
N°11274, 2004, 396 pages.

S. MCCLURE, J. SCAMBRAY, G. KURTZ. – **Halte aux hackers**.
N°25486, 4e édition, 2003, 762 pages.

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

© Groupe Eyrolles, 2006, ISBN : 2-212-11930-5, ISBN 13 : 978-2-212-11930-5

Mise en page : TyPAO
Dépôt légal : novembre 2006
N° d'éditeur : 7373
Imprimé en France

À Françoise

Remerciements

Mes remerciements vont tout d'abord aux éditions Eyrolles pour leur soutien et leur confiance dans l'écriture de ce livre. Je tiens à remercier plus particulièrement Olivier Salvatori pour son aide et son important travail de relecture, qui ont été une grande source de motivation pour moi.

Je tiens à remercier ensuite Michel Goldberg pour son apport et son expertise précieuse, qui m'ont permis d'écrire le premier chapitre, consacré au monde de la normalisation. Je remercie également Diego Santaren pour son soutien indéfectible et sa précieuse relecture.

Je remercie enfin Davor Males et Guy Pujolle, qui m'ont non seulement inspiré dans l'écriture de ce livre mais également guidé et apporté leur expertise reconnue.

Finalement, je tiens à remercier Yves Nouailhetas de la société Dévolo et Serge Brachet de la société Oxance pour leurs précieuses aides.

Table des matières

PARTIE II

Pratique des CPL

Avant-propos

Depuis l'apparition des premiers produits CPL, au début des années 2000, les technologies des courants porteurs en ligne ont beaucoup évolué pour aboutir à une technologie performante. Aujourd'hui, les CPL ont atteint leur maturité et offrent des performances semblables à celles des autres technologies de réseaux locaux, mais avec une facilité de déploiement incomparable.

Grâce aux CPL, il est devenu facile de diffuser n'importe quel type de données dans l'ensemble d'un bâtiment, y compris les services de vidéo IP proposés par les FAI dans leurs offres les plus récentes. Rappelons que ces offres visent à proposer de plus en plus d'applications IP sur tous types de terminaux utilisant des interfaces Ethernet pour communiquer avec les autres terminaux et avec Internet.

L'absence actuelle de standard IEEE pose la technologie HomePlug comme un standard de fait, en raison de la grande quantité d'équipements déjà déployés dans le monde et des perspectives de croissance de cette technologie désormais mature. Un groupe de travail de l'IEEE devrait mettre au point d'ici peu un standard CPL performant, sécurisé et respectueux des perturbations électromagnétiques susceptibles d'affecter les autres équipements de télécommunications. D'ores et déjà, les problèmes d'interférences avec des bandes de fréquences utilisées, par exemple, par les radioamateurs sont techniquement résolus par des mécanismes d'allocation intelligente des sous-bandes de fréquences communes.

Les équipements CPL vont continuer à se développer dans un avenir proche pour intégrer de plus en plus d'interfaces (Wi-Fi, Ethernet, câble TV, etc.) afin de répondre aux besoins des ingénieurs réseau d'offrir une plus grande connectivité des terminaux environnants.

Organisation de l'ouvrage

Cet ouvrage présente les technologies CPL dans leur ensemble, des points de vue aussi bien théorique que pratique, et s'étend jusqu'aux conseils d'installation de réseaux CPL à destination des particuliers, des professionnels comme des collectivités locales.

L'auteur et ses contributeurs se sont efforcés de transmettre avec pédagogie tout ce qu'il leur a paru nécessaire de comprendre pour maîtriser les techniques utilisées par les CPL,

technologies à la frontière entre les réseaux électriques et les réseaux informatiques. Abondamment illustré, l'ouvrage s'accompagne de nombreuses études de cas destinées à aider les installateurs à résoudre les problèmes pratiques de mise en œuvre de réseaux CPL.

Le livre est découpé en treize chapitres, regroupés en deux parties :

– **Chapitre 1. Introduction.** Ce premier chapitre couvre l'historique des technologies CPL et présente les travaux des différents groupes de travail (alliances, groupes industriels, etc.) ayant présidé à leur développement.

- **Première partie. Théorie des CPL.** Cette partie se penche sur les caractéristiques des réseaux électriques et informatiques et détaille les différentes fonctionnalités proposées dans les CPL pour acheminer l'information sous toutes ses formes à l'utilisateur.

  – **Chapitre 2. Architecture.** Ce chapitre décrit les caractéristiques des réseaux électriques, en s'efforçant de les situer dans les modèles communément utilisés en télécommunications.

  – **Chapitre 3. Fonctionnalités.** L'ensemble des fonctionnalités permettant d'offrir des communications optimales sur un réseau électrique sont inventoriées dans ce chapitre.

  – **Chapitre 4. Sécurité.** Les CPL ne souffrent pas des mêmes problèmes de sécurité que les réseaux Wi-Fi. Ils n'en mettent pas moins en œuvre un certain nombre de mécanismes de sécurisation des données.

  – **Chapitre 5. Trames.** La description complète des blocs d'informations transitant sur un réseau électrique est fournie dans ce chapitre.

- **Deuxième partie. Pratique des CPL.** Cette partie couvre l'ensemble des implémentations pratiques des CPL, depuis le contexte des réseaux locaux domestiques ou professionnels jusqu'à celui des réseaux de desserte des collectivités locales.

  – **Chapitre 6. Applications.** Les développements récents des offres d'accès Internet des FAI visent à fournir des applications de plus en plus complètes (voix, données, images, flux vidéo haute définition) et exigeantes en terme de débit comme de sécurité. Ce chapitre montre comment les réseaux CPL répondent dès à présent à ces nouvelles exigences.

  – **Chapitre 7. Équipements.** Le choix d'équipements CPL adaptés aux besoins demande une bonne connaissance des différentes fonctionnalités implémentées dans les terminaux CPL tels que passerelles, filtres, répéteurs et injecteurs, complétés d'équipements réseau classiques. Ce chapitre indique les bons critères de choix en fonction des différentes contraintes d'installation.

  – **Chapitre 8. Installation.** Il est important de configurer les équipements correctement avant de les installer. Ce chapitre détaille les problématiques d'installation les plus courantes afin d'optimiser le placement des équipements CPL au sein du réseau électrique.

– **Chapitre 9. Configuration.** Ce chapitre décrit les étapes de configuration des équipements sous plusieurs plates-formes (Windows, Linux, FreeBSD) et pour différents types de technologies CPL.

– **Chapitre 10. CPL domestique.** Les particuliers désirant installer un réseau CPL dans leur habitation trouveront dans ce chapitre tout ce qu'ils ont besoin de connaître en matière de critères de choix des appareils ou de conseils d'installation et de configuration.

– **Chapitre 11. CPL d'entreprise.** Depuis la PME jusqu'à l'entreprise disposant de plusieurs bâtiments industriels, les professionnels trouveront dans ce chapitre le détail des étapes nécessaires à l'utilisation optimale du réseau électrique comme infrastructure de réseau local.

– **Chapitre 12. CPL de collectivité locale.** Ce chapitre se penche sur le cas particulier des collectivités locales qui souhaitent pallier les difficultés d'acheminement de l'accès à Internet dans des zones mal ou non desservies. Ce chapitre apporte les éléments de compréhension des problématiques et principes d'architecture et de gestion de projet des réseaux de desserte utilisant comme support le réseau électrique public.

– **Chapitre 13. CPL hybride.** Ce dernier chapitre de l'ouvrage met en perspective les CPL vis-à-vis des autres technologies réseau et montre comment tirer le meilleur parti des différentes technologies de réseau local pour bâtir des architectures hybrides mêlant CPL, Wi-Fi, Ethernet câblé, câble TV et RTC (réseau téléphonique commuté).

À qui s'adresse l'ouvrage

Cet ouvrage intéressera tous ceux qui souhaitent en savoir plus sur les CPL mais vise en particulier les catégories de lecteurs suivantes :

- Particuliers qui souhaitent installer un réseau CPL dans leur domicile, principalement pour diffuser les services offerts par les fournisseurs d'accès à Internet.
- Architectes, ingénieurs ou administrateurs réseau, qui envisagent de choisir les CPL comme technologie pour construire leur réseau de petite, moyenne ou grande taille ou pour les installer en complément de réseaux existants.
- Électriciens désireux de s'initier à une technologie située au cœur de leur métier. Situées à la frontière de l'électricité et des télécommunications, les technologies CPL constituent pour ces professionnels une opportunité d'étendre leur activité .
- Étudiants désirant compléter leur formation réseau par un aperçu des techniques de transmission de données sur le réseau électrique.
- Décideurs, qui pourront comprendre tout l'intérêt des CPL en remplacement ou complément des autres technologies réseau.

Parcours de lecture

Ce livre comportant deux parties distinctes, une partie théorique, qui entre dans les moindres détails des technologies CPL, et une partie pratique, qui donne des conseils d'installation de réseaux CPL, les parcours de lecture recommandés suivant le profil du lecteur peuvent être les suivants :

- Le particulier intéressé par les aspects pratiques de la mise en œuvre de réseaux CPL pourra commencer par le choix des équipements, au chapitre 7, puis poursuivre par leur installation, au chapitre 8, leur configuration, au chapitre 9, et leur mise en œuvre sur le réseau électrique, au chapitre 10.
- L'architecte réseau sera plus particulièrement intéressé par le chapitre 11 présentant la mise en œuvre d'un vaste réseau CPL dans un hôtel (similaire au cas d'un campus ou d'une entreprise).
- L'étudiant en réseau et télécoms trouvera aux chapitres 1 à 5 les éléments théoriques nécessaires à sa formation et à la compréhension des technologies CPL.
- Le décideur pourra se reporter au chapitre 1 pour une vision d'ensemble des travaux de standardisation en cours des réseaux CPL. Le chapitre 7 lui donnera en outre une idée des prix des équipements CPL et des coûts comparés des différentes technologies de réseaux locaux.
- L'électricien comprendra au travers des chapitres 10, 11 et 12, illustrés de nombreux exemples pratiques, les étapes de constitution d'un réseau CPL de petite, moyenne ou grande taille. La nécessité de recourir à des professionnels habilités à intervenir sur un réseau électrique place les électriciens au cœur des déploiements CPL.

1

Introduction

Les CPL (courants porteurs en ligne) sont une technologie d'accès à haut débit, qui utilise le réseau électrique moyenne et basse tension pour fournir des services de télécommunications.

Producteurs et distributeurs d'énergie électrique ont depuis longtemps utilisé le réseau électrique pour contrôler le réseau et le piloter à distance à bas débit.

De nos jours, un producteur ou un distributeur d'électricité ne peut ignorer la normalisation. Il est intéressant de remarquer que c'est en raison du déploiement des réseaux électriques, de leur interconnexion et du nombre sans cesse croissant d'appareils électriques, que les premiers organismes de normalisation réseau sont apparus, à l'image de la CEI (Commission électrotechnique internationale).

Les technologies CPL

La technique des CPL n'est pas récente dans son principe. Dès 1838, en Angleterre, Edward Davy a proposé une solution permettant de mesurer à distance les niveaux de batterie des sites éloignés du système télégraphique entre Londres et Liverpool. En 1897, il présentait le premier brevet (British Patent N° 24833) d'une technique de mesure à distance des compteurs du réseau électrique communiquant sur les câbles électriques.

Appelés Ripple Control, les premiers systèmes CPL ont été élaborés puis déployés sur les réseaux électriques moyenne tension et basse tension en 1950. La fréquence porteuse était alors comprise entre 100 Hz et 1 kHz. Il s'agissait d'établir des communications monodirectionnelles *via* des signaux de commande pour l'allumage et l'extinction à distance des éclairages publics ou encore pour des changements tarifaires.

Les premiers systèmes industriels sont apparus en France en 1960 sous le nom de Pulsadis. Les puissances mises en jeu avoisinaient la centaine de kilovoltampères (kVA).

Ce n'est qu'ensuite qu'apparurent les premiers systèmes CPL de la bande dite Cenélec, s'étendant de 3 à 148,5 kHz et permettant des communications bidirectionnelles sur le réseau électrique BT (basse tension) afin, par exemple, de pratiquer des relevés de compteurs (télérelève), ainsi que bon nombre d'applications relevant du domaine de la domotique (alarme d'intrusion, détection d'incendie, détection fuite de gaz, etc.). Les puissances injectées étaient beaucoup moins importantes que les précédentes, puisque réduites à des niveaux de l'ordre d'une centaine de milliwatts.

L'expression « courants porteurs en ligne », communément abrégée CPL, est apparue à la fin de la Seconde Guerre mondiale, en 1945. À l'époque, beaucoup de lignes téléphoniques et électriques étaient détruites, mais il restait davantage de lignes électriques d'infrastructure que de lignes téléphoniques. Pour des besoins de communication, des systèmes ont été conçus afin de transmettre des données sur les câbles haute tension ou moyenne tension, en s'inspirant des télérelèves déjà effectuées sur les lignes électriques.

La figure 1.1 illustre l'évolution des technologies CPL classées par débit depuis le début des années 1990.

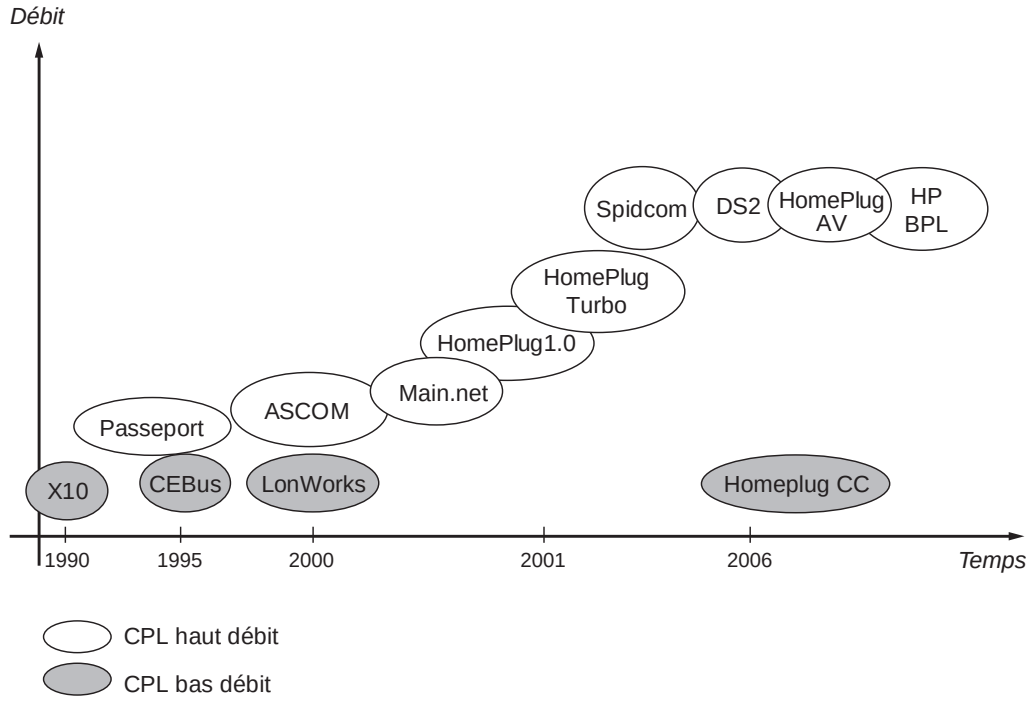


Figure 1.1

Technologies CPL bas et haut débits

Organismes de normalisation

Cette section présente les différents organismes de normalisation ainsi que les notions de normes et de standards que nous allons expliciter.

Il existe une différence entre une norme et un standard. Une norme correspond à un document issu d'un organisme international, tel que l'ISO (International Standardization Organization). Un standard est issu d'un organisme national, tel que l'IEEE américain, ou d'une communauté d'États, comme l'ETSI.

La normalisation s'effectue donc aux niveaux national, européen et international. Chaque comité de normalisation est responsable de un ou plusieurs domaines de normalisation.

La CEI (Commission électrotechnique internationale) et le Cenélec (Comité européen de normalisation en électrotechnique) sont chargés de l'électrotechnique et l'ETSI (European Telecommunications Standards Institute) des télécommunications.

L'ISO et le CEN (Comité européen de normalisation) couvrent tous les autres domaines d'activité.

Les termes « norme harmonisée » sont utilisés dans le contexte des directives européennes dites Nouvelle Approche pour désigner des normes européennes adoptées selon les orientations générales convenues entre la Commission européenne et les organismes de normalisation, dans le cadre d'un mandat octroyé par la Commission après consultation des États membres.

La figure 1.2 illustre les champs d'activité de chaque comité de normalisation en charge des technologies CPL.

	Electrotechnique et électricité	Autres secteurs	Télécommunications
International	***CEI*** Commission électrotechnique internationale	***ISO*** Organisation internationale de standardisation	***ITU*** Union internationale des télécommunications
Europe	***CENELEC*** Comité européen de normalisation électrotechnique	***CEN*** Comité européen de normalisation	***ETSI*** European Telecommunications Standards Institute
France	***UTE*** Union technique de l'électricité et de la communication	***AFNOR*** Association française de normalisation	***AFNOR (CF ETSI)*** Comité français de l'ETSI

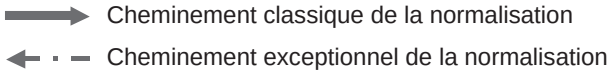


Figure 1.2

Organismes de normalisation en charge des technologies CPL

Selon l'ISO, une norme désigne « tout document destiné à une application répétitive, approuvé par un organisme reconnu de normalisation et mis à la disposition du public ».

L'Afnor complète cette définition de la façon suivante : « Une norme est une donnée de référence résultant d'un choix collectif raisonné en vue de servir de base d'action pour la solution de problèmes répétitifs. »

Rappelons que, par rapport au domaine réglementaire, une norme ne fait que définir méthodes et règles et qu'elle n'est pas obligatoire, contrairement à une réglementation.

Comme indiqué précédemment, pour l'Europe, le cadre réglementaire est fixé par les directives Nouvelle Approche, qui énumèrent les exigences essentielles auxquelles le produit doit satisfaire. Les normes européennes harmonisées, lorsque leurs prescriptions sont vérifiées, garantissent une présomption de conformité à ces exigences essentielles.

L'importance des normes harmonisées est illustrée par le marquage CE. Ce marquage, véritable passeport de libre circulation des produits en Europe, correspond à une déclaration du fabricant indiquant que son produit satisfait aux exigences essentielles des directives européennes qui le concernent.

Les équipements CPL doivent satisfaire aux exigences des directives CEM (compatibilité électromagnétique) et BT (basse tension).

Il convient toujours de distinguer les travaux concernant le « produit » et ceux relatifs au système, le « réseau » dans le cas des CPL. À ce jour, les travaux sur le produit amendent la publication internationale CISPR 22, tandis que ceux qui concernent le réseau, sont exclusivement européens et traités au Joint Working Group Cenélec/ETSI.

Ces travaux visent à disposer d'une norme réseau harmonisée suite au mandat M 313 donné par la Commission européenne au Cenélec et à l'ETSI. Cette norme ne cherche pas à limiter le déploiement des réseaux filaires, mais à limiter leurs émissions perturbatrices.

Après cinq années de recherche d'un consensus, constatant la quasi-impossibilité de définir des limites au rayonnement des réseaux filaires, il a été décidé d'abandonner l'idée de publication de cette norme réseau, et les travaux se sont concentrés sur la norme produit.

Entre-temps, la Commission a publié en avril 2006 une recommandation définissant un cadre juridique à la demande de l'ensemble de la communauté CPL. Ce texte recommande aux pays membres de lever toute barrière au déploiement des réseaux CPL, en contrepartie de l'engagement des installateurs, fabricants de matériel et fournisseurs d'accès Internet à respecter les exigences de la directive CEM et à utiliser toute méthode de mitigation à distance en cas de perturbation avérée sur une fréquence donnée.

Au Cenélec, les CPL sont suivis par les comités (TC) et sous-comités (SC) techniques suivantes :

- TC 205, « Systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) » ;
- SC 205 A, « Systèmes de communication par le réseau électrique basse tension » ;
- TC 210, « Compatibilité électromagnétique (CEM) », miroir du CISPR.

Extraits de la recommandation européenne du 6 avril 2005

1. Les États membres appliquent les conditions et principes suivants à la fourniture de systèmes publics de communication à large bande par courant porteur.
2. Sans préjudice des dispositions des points 3 à 5, les États membres lèvent tous les obstacles réglementaires injustifiés, pour les entreprises de service public notamment, au déploiement de systèmes de communication à large bande par courant porteur et à la fourniture de services de communication électroniques à l'aide de ces systèmes.
3. En attendant que des normes permettant d'établir la présomption de conformité des systèmes de communication par courant porteur aient été harmonisées en vertu de la directive 89/336/CEE, les États membres considèrent comme conforme à cette directive tout système de communication par courant porteur qui :
   - Est constitué d'un équipement conforme à la directive et utilisé aux fins auxquelles il est destiné.
   - Est installé et exploité selon les règles de l'art prévues pour satisfaire aux exigences essentielles de la directive.

   La documentation relative aux règles de l'art doit être tenue la disposition des autorités nationales compétentes aux fins d'inspection aussi longtemps que le système est exploité.
4. Lorsqu'il est établi qu'un système de communication par courant porteur provoque des interférences néfastes qui ne peuvent être supprimées par les parties concernées, les autorités compétentes de l'État membre demandent une attestation de conformité du système et, le cas échéant, procèdent à une évaluation.
5. Si l'évaluation conduit à établir la non-conformité du système de communication par courant porteur, les autorités compétentes imposent des mesures d'exécution proportionnées, non discriminatoires et transparentes afin d'assurer la conformité.
6. En cas de conformité du système de communication par courant porteur mais de persistance des interférences, les autorités compétentes de l'État membre doivent envisager de prendre des mesures particulières conformément à l'article 6 de la directive 89/336/CEE de façon proportionnée, non discriminatoire et transparente.
7. Les États membres rendent compte régulièrement au comité des communications du déploiement et de l'exploitation des systèmes de communication par courant porteur sur leur territoire. Ces comptes rendus doivent contenir toutes les données pertinentes concernant les niveaux de perturbation (y compris des relevés de mesures, les niveaux correspondants de signal injecté et toutes les autres données utiles à l'établissement d'une norme européenne harmonisée), les problèmes d'interférences et les mesures d'exécution relatives aux systèmes de communication par courant porteur. Le premier de ces comptes rendus est prévu le 31 décembre 2005.
8. Les États membres sont destinataires de la présente recommandation.

Fait à Bruxelles, le 6 avril 2005 par la Commission, Viviane REDING, membre de la Commission.

Le sous-comité « produit » SC 205 A a pour mission de « préparer des normes harmonisées pour les systèmes de communication utilisant les lignes d'alimentation électrique basse tension ou le câblage des immeubles comme support de transmission et utilisant des fréquences supérieures à 3 kHz et jusqu'à 30 MHz. Cette tâche inclut l'attribution des bandes de fréquences pour la transmission du signal sur le réseau basse tension ».

Par respect pour le principe de non-duplication des travaux avec la CEI, les travaux sur la norme *produit* sont plus ou moins en attente dans ce sous-comité.

La figure 1.3 illustre les différents liens entre les acteurs (organismes, consortiums, États, Commission européenne, etc.) travaillant sur des normes et standards relatifs aux CPL en Europe, en particulier l'IEC (CEI en français), le Cenélec et l'ETSI.

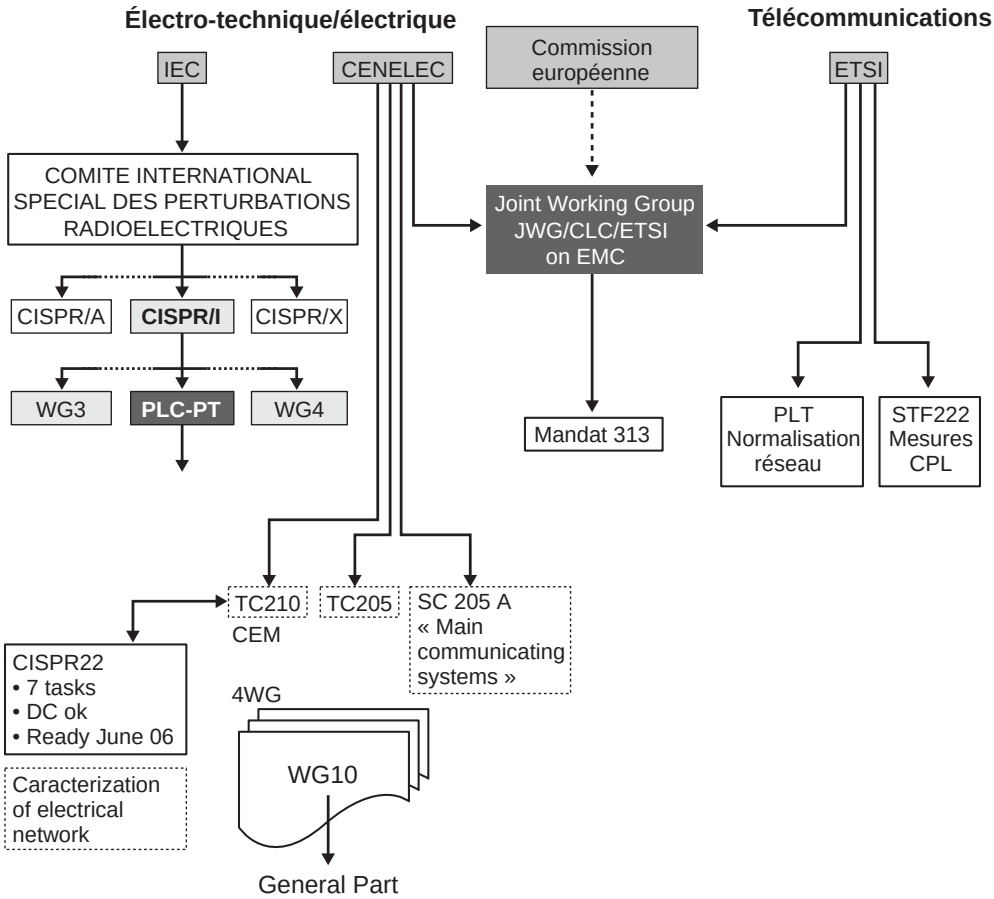


Figure 1.3

Acteurs de la normalisation CPL

Consortiums et associations

Outre les organismes et institutions précédentes, certaines associations et consortiums jouent un rôle de « prénormalisation », voire de standardisation, pour les CPL, notamment les trois acteurs majeurs HomePlug, l'IEEE et le consortium Opera. En Europe, le lobbying en faveur des CPL a été mené par le PUA et le PLC Forum.

La figure 1.4 illustre les rôles de chacun des acteurs impliqués dans cette prénormalisation des CPL.

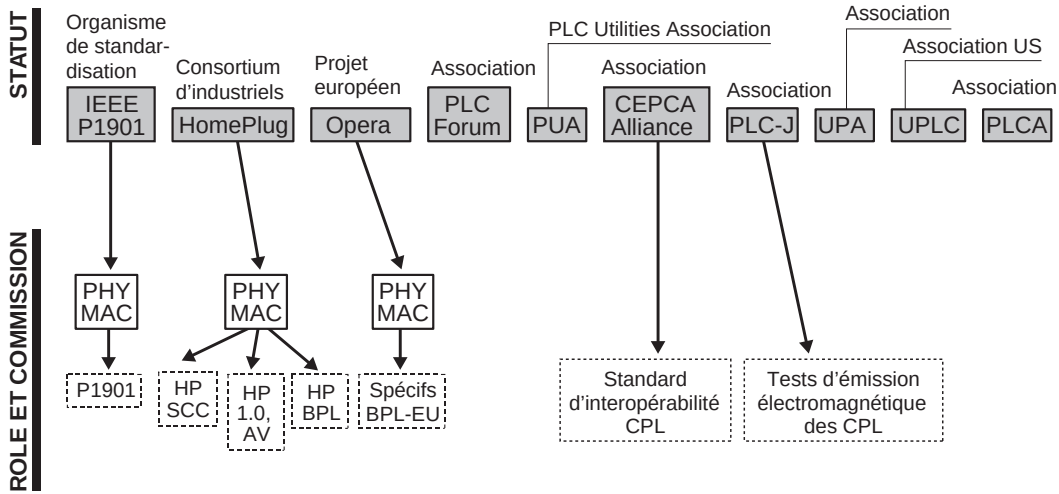


Figure 1.4

Consortiums et associations relatifs aux CPL

HomePlug Alliance

L'alliance HomePlug regroupe des industriels couvrant aussi bien la technologie que les services CPL afin de développer les spécifications HomePlug (HomePlug 1.0, HomePlug AV et HomePlug BPL).

Aujourd'hui, seule la spécification HomePlug 1.0 est finalisée et implémentée dans de nombreux produits du marché.

IEEE (Institute of Electrical and Electronics Engineers)

L'IEEE, une organisation à but non lucratif, est la plus grande association professionnelle internationale technique et une des principales autorités de secteurs aussi variés que les systèmes aérospatiaux, les ordinateurs et les télécommunications, les technologies biomédicales, l'énergie électrique ou l'électronique grand public.

L'IEEE diffuse à ses membres des informations, mais aussi des ressources et des services techniques et professionnels. Pour stimuler l'intérêt pour les métiers liés à la technologie, l'IEEE propose également des services à ses membres étudiants dans le monde entier.

Une autre partie importante des partenaires de l'IEEE est constituée de prospects, personnes physiques et morales, qui achètent ses produits et participent à ses conférences et symposiums.

Opera

Le consortium Opera compte trente-six partenaires originaires de divers pays européens et d'Israël. Tous les organismes et associations impliqués dans le développement de la technologie CPL sont représentés dans le consortium, depuis les services publics jusqu'aux opérateurs de télécommunications, en passant par les fabricants de chipsets et de modems, les industriels et consultants et les universités.

Ce regroupement de profils différents et de compétences variées contribue à la réussite des objectifs du consortium.

L'objectif stratégique d'Opera est d'« offrir le service de l'accès à haut débit à tous les citoyens européens, en utilisant l'infrastructure la plus universelle, le réseau CPL ». Opera effectue pour cela la recherche et le développement, ainsi que les opérations de démonstration et de dissémination au niveau européen, afin de vaincre tout obstacle résiduel et de permettre aux opérateurs de CPL de fournir à chaque citoyen européen les services d'accès à haut débit à un coût concurrentiel.

Les principales missions d'Opera sont les suivantes :

- amélioration générale des systèmes CPL basse et moyenne tension (débit, facilité de mise en œuvre, etc.) ;
- développement de solutions optimales pour la connexion des réseaux CPL aux réseaux backbone ;
- standardisation des systèmes CPL.

PUA (PLC Utilities Alliance)

La PUA est une alliance créée à Madrid le 21 janvier 2002 autour de services publics européens desservant plus de cent millions de clients.

Ses membres actuels sont les suivants :

- EDF (Électricité de France), France
- Endesa Net Factory, Espagne
- Enel Distribuzione, Italie
- Iberdrola, Espagne
- EDP (Electricidade de Portugal), Portugal
- EEF (Entreprises électriques fribourgeoises), Suisse
- Unión Fenosa, Espagne

PLC Forum

Le PLC Forum est un organisme international créé au début des années 2000 à partir de la fusion de deux associations.

Il développe ses activités en coordination avec les autres organismes travaillant sur les CPL.

Vers une normalisation de la technologie CPL

Toute normalisation est un processus lent. Cela n'a rien d'étonnant si l'on considère qu'elle exige le consensus des membres du groupe de travail considéré avant de prendre une quelconque décision.

Si cette démarche a prouvé son efficacité dans la plupart des domaines industriels, elle est peut-être moins adaptée aux technologies de l'information, pour lesquelles les standards devraient viser davantage à satisfaire les besoins immédiats.

Futur standard IEEE

Début juin 2005, le comité de direction de l'IEEE a validé la création d'un projet de standard CPL sous le titre « IEEE P1901 Draft Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications ».

Le standard concernera les équipements CPL haut débit (supérieur à 100 Mbit/s au niveau de la couche physique), dans la gamme de fréquences inférieure à 100 MHz, et adressera les techniques d'accès et les réseaux intérieurs. Il s'attachera en outre à définir les mécanismes de coexistence et d'interopérabilité entre les différents équipements CPL ainsi que la qualité du service offert et la confidentialité des données.

La quasi-totalité des acteurs des CPL font partie de ce projet, notamment ceux récapitulés au tableau 1.1.

Tableau 1.1 Principaux acteurs de la standardisation IEEE des CPL

Advanced Communications Networks SA	Mitsubishi Electric Corporation
Ambient Corporation	Mitsubishi Materials Corp.
Arkados, Inc.	Panasonic Corporation
CEPCA Administration	Pioneer Corporation
Conexant Systems, Inc.	PUA
Corinex Communications Corporation	RadioShack
Current Technologies	Schneider Electric Powerline Communications
DS2	SiConnect
Duke Power	Sony Corporation
Earthlink	Spidcom Technologies
HomePlug Powerline Alliance	Sumitomo Electric Industries, Ltd
IBM	Texas Instruments
IBEC (International Broadband Electric Communications), Inc.	TEPCO
Intel	Toyo Network Systems Co., Ltd
Intellon Corporation	Universal Powerline Association
Itochu Corporation	Xeline
	Yamaha

Future norme d'interopérabilité

Pour faire face à la multiplicité des spécifications et technologies CPL présentes dans les réseaux électriques domestiques, professionnels et publics, une norme d'interopérabilité est en cours d'élaboration.

Le support de communication qu'est le réseau électrique étant partagé, ces différentes technologies cohabitent sur les câbles électriques dans les mêmes bandes de fréquences. Les différents acteurs du CPL travaillent donc de concert au sein de l'IEEE et du CEPCA (Consumer Electronics Powerline Communication Alliance) afin de les rendre interopérables.

Avantages et inconvénients des CPL

Comme tout système viable, les CPL présentent des avantages par rapport aux technologies concurrentes, mais également des inconvénients.

Parmi les inconvénients, citons en premier lieu l'immaturité relative des produits concernant « l'outdoor » (réseaux extérieurs) et l'« access » (réseaux d'accès). Dans le cas du haut débit, le problème est essentiellement lié à la compatibilité électromagnétique et au respect des contraintes d'émission.

Les principaux avantages des CPL sont les suivants :

- utilisation du réseau électrique existant, ce qui implique une couverture potentielle de la totalité du pays considéré ;
- déploiement rapide ;
- pas de câblage supplémentaire ;
- méthode de cryptage robuste.

Partie I

Théorie des CPL

Cette partie traite essentiellement de la spécification HomePlug. Issue de l'alliance industrielle du même nom, HomePlug se focalise sur deux axes principaux, la couche physique, qui s'occupe de la transmission de l'information sur le support électrique, et la couche liaison de données, qui définit l'architecture et les mécanismes à mettre en œuvre pour permettre cette transmission sur le réseau dans les meilleures conditions possibles.

Depuis la finalisation de HomePlug 1.0, deux nouvelles versions sont apparues, qui améliorent la vitesse de transmission, la sécurité et la qualité de service.

Afin d'améliorer la transmission, la couche physique utilise les meilleurs mécanismes de codage, de modulation et de correction d'erreur, offrant de la sorte une excellente connectivité entre équipements et de bonnes vitesses de transmission. Ces dernières sont respectivement, pour HomePlug 1.0, Turbo et AV, de 14 Mbit/s, 85 Mbit/s et 200 Mbit/s, permettant aux CPL d'entrer en concurrence avec les réseaux Ethernet et Wi-Fi.

La couche liaison de données met en œuvre un ensemble de mécanismes permettant l'envoi des données sous forme de paquets IP dans les meilleures conditions tout en optimisant les performances. Les techniques d'accès au réseau que définit cette couche régissent les performances du réseau.

Des améliorations apportées aux versions successives de la spécification HomePlug ont modifié cette couche en vue de permettre une gestion optimisée de la qualité de service *via* des processus d'allocation de temps de transmission répartis (TDMA) ainsi qu'une gestion efficace de l'architecture réseau des équipements CPL *via* une hiérarchisation des trames de données. La qualité de service est un élément essentiel de la transmission de trafic en temps réel, telles la voix ou la vidéo.

Concernant la sécurité, la technologie CPL se démarque de Wi-Fi, en ce qu'elle affiche une certaine immunité aux attaques du fait de la difficulté d'accès au support physique. Cette immunité est encore renforcée par l'implémentation de cryptages DES et AES des trames échangées sur le support électrique ainsi que par des techniques d'intégrité du réseau, qui permettent de gérer les équipements autorisés à participer au réseau CPL.

2

Architecture

CPL, ou courants porteurs en ligne, est le nom générique d'une technologie réseau utilisant les câbles électriques, issue de nombreux travaux de recherche sur les transmissions de données haut débit sur le support électrique.

L'architecture des réseaux CPL est comparable à maints égards à celle des réseaux filaires, mais également à celle des réseaux Wi-Fi, comme nous le verrons dans ce chapitre.

HomePlug a été la première spécification CPL à offrir un débit compris entre 1 et 5 Mbit/s. Elle a en outre implémenté de nouveaux mécanismes pour raccorder des équipements réseau, que nous allons détailler de manière précise.

Une autre caractéristique de cette spécification est qu'elle évolue en permanence. De nombreuses améliorations ont permis d'accroître les débits, qui restent toujours partagés, et d'ajouter de nombreuses fonctionnalités, comme la qualité de service ou la sécurité. L'alliance HomePlug est pour l'instant le seul standard CPL de fait, mais des projets de standardisation sont en cours, comme nous l'avons vu au chapitre 1, aussi bien au niveau de l'ETSI que de l'IEEE.

Ce chapitre présente l'architecture générale des réseaux CPL et en détaille les deux couches essentielles, la couche physique et la couche liaison de données.

Architecture des réseaux électriques

La technologie CPL, en anglais PLC (Power Line Communications), vise à transmettre des données sur un câble électrique. Ce câble fait donc office de support (couche PHY du modèle OSI) de la transmission des données. Contrairement à d'autres supports de communication, comme les câbles Ethernet, coaxiaux, fibre optique, etc., ce rôle de support de transmission des données n'est pas la fonction principale du câble électrique.

Le transport des données doit donc s'ajouter à celui de l'énergie électrique (en France et en Europe 200 V/50 Hz, aux États-Unis et au Japon 100 V/60 Hz) dans les câbles permettant d'alimenter les équipements électriques en énergie à partir du réseau public d'électricité.

Les réseaux électriques sont découpés en différentes catégories selon leur niveau de tension, comme indiqué au tableau 2.1.

Tableau 2.1 Niveaux de tension électrique

Appellation actuelle	Ancienne appellation (toujours d'usage)	Niveaux de tension usuels en France
HTB	Très Haute Tension (THT)	400 000 V 225 000 V
	Haute Tension (HT)	90 000 V 65 000 V
HTA	Moyenne Tension (MT)	20 000 V
BT	Basse Tension (BT)	380 V (triphasé) 220 V (monophasé)

Cette classification des réseaux électriques en niveaux de tension permet de séparer les rôles de chacun des acteurs des réseaux électriques en terme de responsabilité sur ces réseaux.

À l'image du réseau téléphonique commuté (RTC) de France Télécom, le réseau de distribution électrique est composé d'un « central » électrique et d'un réseau de desserte jusqu'à l'abonné. Ce réseau s'appuie sur une architecture en étoile, chaque branche de l'étoile étant le câble téléphonique reliant l'abonné au central.

Dans le réseau RTC, le central téléphonique sert « d'aiguilleur » entre le trafic IP venant des modems des abonnés sur la bande de fréquences 20 kHz-1,1 MHz et les communications téléphoniques classiques sur la bande de fréquences 300 kHz-3 300 kHz. Du point de vue de la modélisation réseau, le central téléphonique fait office de commutateur Ethernet et de routeur IP vers la liaison à plus haut débit de la dorsale IP *(voir figure 2.1)*.

Dans le réseau de distribution électrique, appelé EGS (Électricité Gaz Services), du nom de l'entité d'EDF qui opère la distribution en gaz et en électricité de ses 26 millions d'abonnés, c'est le transformateur MT/BT qui fait le lien entre le réseau MT et les réseaux de desserte et de distribution, dont chacun alimente en moyenne 200 compteurs EDF d'abonnés *(voir figure 2.2)*. Le transformateur MT/BT peut être vu comme le concentrateur Ethernet du réseau EGS et comme la passerelle vers la dorsale IP grâce à des liens de transit IP haut débit.

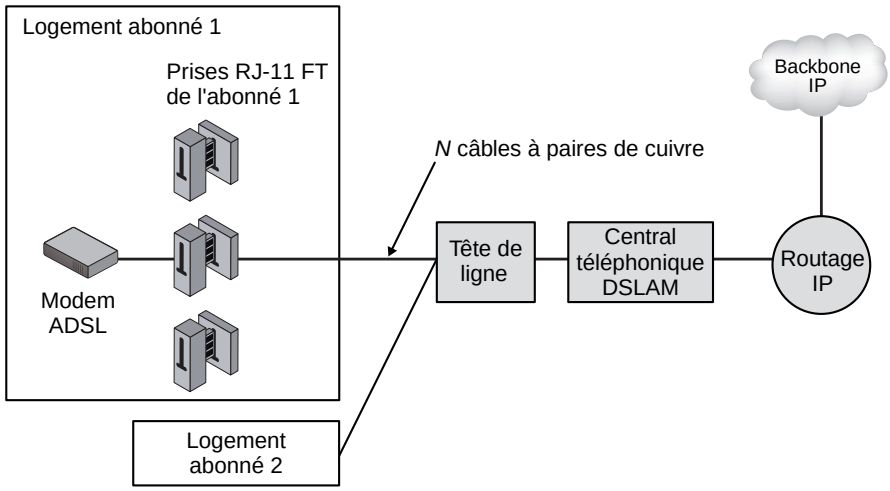


Figure 2.1

Architecture simplifiés du réseau téléphonique commuté

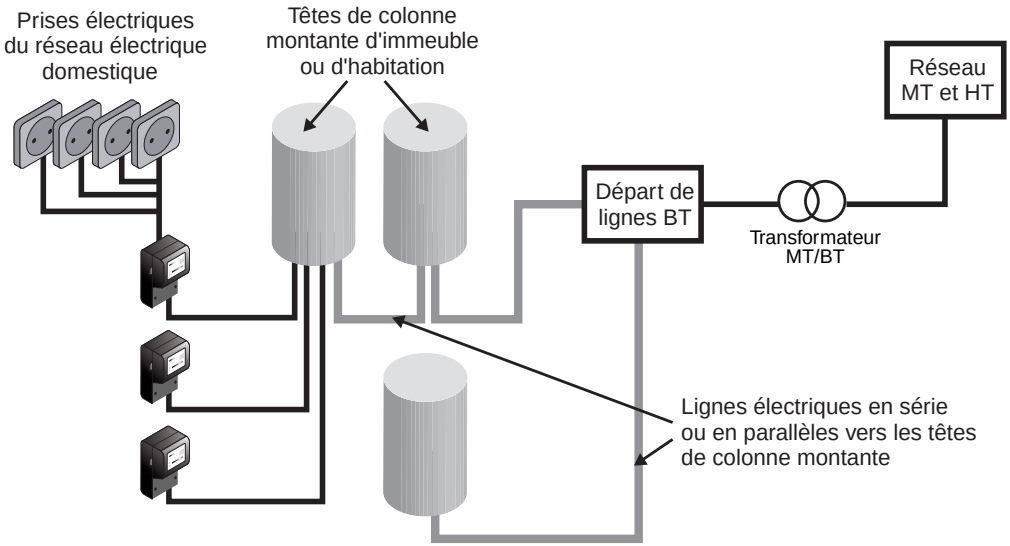


Figure 2.2

Architecture simplifiée du réseau de distribution électrique

En terme de responsabilité, chaque partie du réseau électrique est opérée par des entités distinctes, auxquelles revient la charge de l'alimentation et du transport électrique, ainsi que, le cas échéant, du transport de données pour les réseaux CPL.

La figure 2.3 illustre cette distinction des responsabilités à l'égard des différentes parties du réseau électrique national.

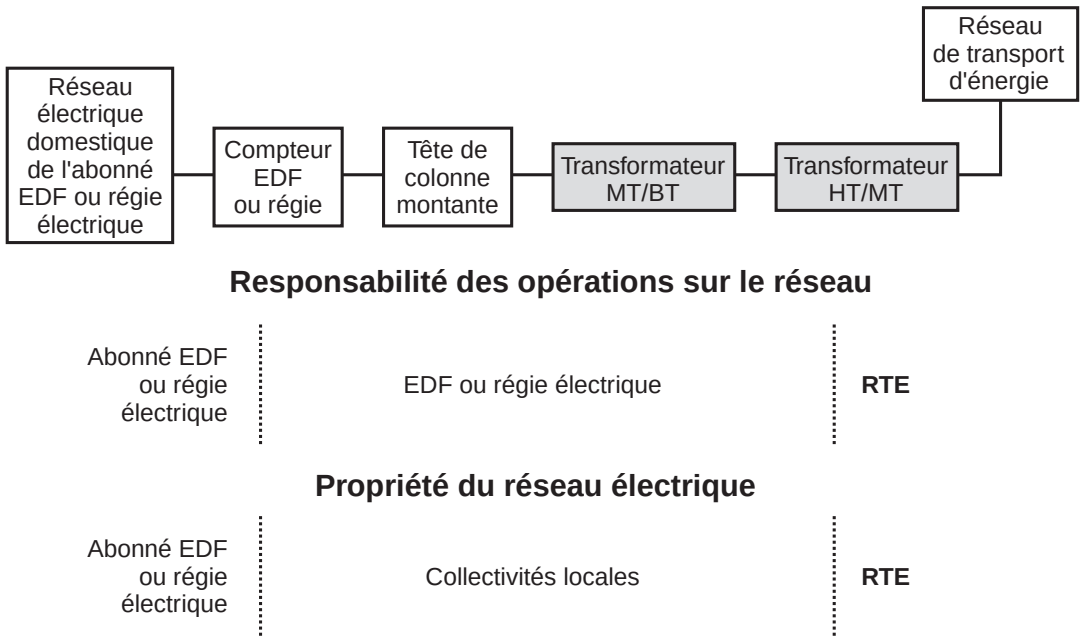


Figure 2.3
Responsabilités des opérations sur le réseau électrique

Caractéristiques du câble électrique

Le support de communication utilisé dans les technologies CPL est le câble électrique, qui n'est pas, au départ, conçu pour transporter des données, et dont les caractéristiques physiques sont avant tout adaptées au transport du signal 220 V/Hz.

Cette section présente un certain nombre de ces propriétés physiques afin de faire mieux comprendre les capacités (avantages et limitations) qu'offre ce support à la transmission de données.

Impédance

Un câble électrique présente une impédance Z (valeur absolue des composantes résistives, inductives et capacitives des éléments du réseau électrique), qui, n'est pas fixe. Les équipements branchés et débranchés en permanence sur le câble électrique modifient l'impédance du câble, rendant difficile une modélisation du support de communication et donc du canal de transmission.

Par principe, un équipement électrique peut être branché ou débranché du réseau à tout moment, engendrant une modification de l'impédance globale du réseau électrique. De plus, cet appareil peut subir une modification de sa propre impédance en fonction de son mode de fonctionnement, de sa vitesse de fonctionnement, de son état de vieillissement, de sa conception, etc.

Des études ont montré que l'impédance des équipements électriques BT varie classiquement entre 10 Ω et 1 kΩ.

Capacité et inductance

Les différents équipements qui sont connectés sur le réseau électrique ont chacun une certaine capacité et une certaine inductance vis-à-vis du courant électrique qui circule sur le circuit 220 V alternatif à la fréquence de 50 Hz.

L'*inductance* (L), aussi appelée bobine ou self, d'un circuit ou d'un dipôle électrique est une valeur qui traduit le flux d'induction créé par le courant électrique traversant ce circuit. Le déplacement de charges électriques dans un matériau de susceptibilité magnétique (μ) non nulle crée un champ magnétique (H) et une induction magnétique (B).

Dans le cas d'un matériau qui se limite à une surface circonscrite, typiquement un câble électrique, le champ magnétique provenant du courant qui traverse ce circuit crée un flux d'induction. L'inductance peut être propre au circuit ou mutuelle avec un autre circuit électrique.

L'inductance vis-à-vis du champ magnétique (ϕ) et du courant électrique (I) peut être exprimée par la formule :

$$L = \frac{\phi}{1}$$

En régime sinusoïdal (cas du courant électrique 220 V/50 Hz), cette équation est exprimée en valeurs efficaces par la loi d'Ohm, en fonction de la tension (U), du courant électrique (I) et de la fréquence (f) :

$$L = \frac{U}{2\pi f I} \text{ (exprimée en henry)}$$

La *capacité* (C), aussi appelée condensateur ou capacitance, d'un circuit électrique est une valeur qui traduit l'énergie potentielle stockée dans un champ électrique constitué de deux plaques conductrices séparées se faisant face et de charge électrique opposée.

Cette énergie potentielle, ou capacité, est proportionnelle à la charge électrique stockée par le dipôle électrique constitué de ces deux plaques. Cette charge électrique peut être également exprimée en flux électrique (ϕ) et associée au potentiel électrique entre les deux plaques du dipôle :

$$C = \frac{\phi}{V} \text{ (exprimée en coulomb)}$$

En régime sinusoïdal (cas du courant électrique 220 V/50 Hz), cette équation est exprimée en valeurs efficaces par la loi d'Ohm, en fonction de la tension (*U*), du courant électrique (*I*) et de la fréquence (*f*) :

$$C = \frac{I}{2\pi fI} \text{ (exprimée en farad)}$$

L'*impédance* (Z) d'un circuit électrique est composée d'une partie résistive (R), d'une partie inductive (L) et d'une partie capacitive (C), qui le caractérisent complètement du point de vue électrique.

Ces caractéristiques influent sur le comportement global du réseau électrique en fonction des niveaux de courant électrique circulant dans ce réseau. Du point de vue informatique, ces caractéristiques se traduisent par une modélisation particulière de la couche physique afin d'obtenir la meilleure qualité possible du canal de transmission.

L'impédance peut s'exprimer en valeurs complexes par la loi d'Ohm comme la somme de ses composantes résistives, inductives et capacitives, *j* exprimant la partie imaginaire d'un nombre complexe :

$$Z = R + jL2\pi f + \frac{1}{C2\pi f} \text{(exprimée en ohm pour la valeur absolue)}$$

L'ensemble des impédances des différents circuits électriques traversés par le courant électrique forme donc un réseau complexe d'impédances en série et en parallèle, qui peuvent être connectées et déconnectées en permanence du réseau. De plus, ces différentes impédances induisent des champs magnétiques et électriques mutuels, qui se traduisent par des courants électriques proportionnels les uns par rapport aux autres. Du point de vue du canal de transmission, cette caractéristique peut se révéler étonnante, comme nous le verrons.

Les caractéristiques inductives et capacitives modifiant en permanence le canal de transmission physique, cela nécessite une optimisation et une consolidation des techniques de transmission CPL.

Bruits et perturbations électromagnétiques

Le canal de transmission récolte un certain bruit des différents équipements électriques connectés ou à proximité du câble électrique.

Les différents types de bruits qui peuvent être perçus sur et autour du câble électrique sont les suivants :

- bruits impulsionnels dus aux arrêts/démarrages des appareils électriques ;
- bruits blancs à large bande, dont la densité spectrale de puissance est la même pour toutes les fréquences ;

- bruits périodiques à plusieurs fréquences ;
- bruits harmoniques, composés des multiples fréquences utilisés par les équipements électriques branchés sur le réseau et qui sont, par exemple, des multiples de 50 Hz (300, 600, etc.).

Ces bruits sont exprimés globalement par le rapport signal sur bruit, ou SNR (Signal to Noise Ratio), généralement mesuré en décibels (dB).

En plus des bruits sur le support électrique, les appareils électriques connectés ou déconnectés du réseau électrique mais à proximité du câble électrique engendrent un certain nombre de perturbations sur le canal de transmission. Ce sujet technique fort complexe est appelé CEM (compatibilité électromagnétique), ou EMC (Electro-Magnetic Compatibility).

Du point de vue de la CEM, chaque appareil électrique alimenté en énergie est générateur de perturbations électromagnétiques conduites, c'est-à-dire transportées sur le câble électrique, ou induites, c'est-à-dire émises dans l'environnement radio de l'équipement perturbateur.

De nombreux groupes de travail du Cenélec (européen) et de la CEI (international) ont mis en place des règles fixant les limites des perturbations autorisées pour chaque classe d'équipement électrique, y compris les équipements CPL. De leur côté, les organismes de standardisation et de normalisation des télécommunications ETSI (européen) et ITU (international) travaillent sur les seuils de perturbation afin d'optimiser le canal de transmission et les techniques de traitement du signal à mettre en œuvre pour obtenir les meilleures performances des CPL. L'IEEE travaille également sur ces sujets pour optimiser la couche physique du modèle ISO.

Le groupe de travail ISRIC (International Special Radio Interference Committee) Working Group 3 a fixé les limites de perturbations autorisées des appareils électriques CPL dans la bande 150 kHz-30 MHz.

Les perturbations CEM reçues et provoquées par les CPL font l'objet de nombreux autres travaux et études en vue d'harmoniser les niveaux d'émission de chaque appareil et d'obtenir un canal de transmission efficace avec ces niveaux d'émission.

Atténuation

De même que le signal radio subit une atténuation de sa puissance en fonction de la distance parcourue par les ondes ou que le signal DSL s'atténue le long du câble à paires de cuivres du RTC, le signal électrique perd de sa puissance en fonction de la distance parcourue.

Il est important de prendre en compte cette caractéristique du câble électrique pour implémenter un réseau CPL. Nous détaillons au chapitre 8 les paramètres à configurer

pour offrir les meilleures performances au réseau CPL, ces dernières variant grandement en fonction de la portée et de l'atténuation du signal.

Les différences d'impédances sur le réseau électrique provoquent des effets tels que les multitrajets, qui entraînent des « notches », ou pics d'amplitude du signal CPL, importants à certaines fréquences. Dans un habitat domestique, l'atténuation du signal sur le câble électrique est de l'ordre de 20 à 60 dB, en fonction de la charge réseau.

L'atténuation minimale de l'ensemble compteur/disjoncteurs est de 30 dB pour un équipement émettant un signal à une fréquence supérieure à 20 MHz. Pour les fréquences situées en dessous de 20 MHz, la valeur moyenne de l'atténuation est d'environ 50 dB. Un coupleur CPL de bonne qualité permet toutefois de réduire l'atténuation de 10 à 15 dB pour certaines fréquences.

La fréquence du signal d'un modem HomePlug 1.0 étant comprise entre 4 et 25 MHz, la densité spectrale de sa puissance est de – 50 dBm/Hz. Nous reviendrons sur les conséquences de cette valeur au chapitre 8.

Le tableau 2.2 récapitule quelques valeurs d'atténuation pour les principaux équipements du réseau électrique.

Tableau 2.2 Atténuation des principaux équipements électriques d'un réseau électrique

Équipement électrique	Atténuation	Commentaire
Compteur électromécanique	15 dB	Les compteurs électromécaniques atténuent le signal CPL mais ne le bloquent pas, si bien que le signal CPL se propage hors du réseau électrique privé.
Compteur électronique	15 dB	Idem
Disjoncteur	5 dB	S'il traverse un trop grand nombre de disjoncteurs pour relier deux équipements CPL, le signal CPL risque d'être trop atténué.
Multiprise	10 dB	La qualité de fabrication de la multiprise influe énormément sur l'atténuation. Il faut donc éviter de brancher les équipements CPL sur des multiprises.
Compteur électronique + disjoncteurs	20 à 30 dB	L'ensemble compteur + disjoncteurs n'atténue pas assez le signal pour empêcher qu'il se propage hors du réseau électrique privé d'un appartement ou d'une entreprise.
Compteur électromécanique + disjoncteurs	30 dB	Au-dessus de 20 MHz
	50 dB	En dessous de 20 MHz

Les différences mesures effectuées indiquent que, dans un réseau de distribution basse tension, l'atténuation moyenne du signal est de l'ordre de 50 dB/km.

Couplage entre phases

Un signal électrique alternatif à haute fréquence circulant dans un câble électrique provoque un champ électromagnétique, appelé *couplage,* à proximité de ce câble.

Le couplage est appelé diaphonique lorsque l'induction concerne deux câbles d'un même réseau électrique et tellurique lorsqu'elle s'effectue entre des câbles de deux réseaux électriques différents.

Réponse fréquentielle

Selon la nature des câbles électriques (matériau, constitution, âge, etc.), la réponse du câble, c'est-à-dire sa capacité à propager le signal, aux signaux HF diffère notablement.

Nous détaillons les conséquences de cette caractéristique sur la mise en place d'un réseau CPL au chapitre 8 et montrons comment la prendre en compte dans le choix de la topologie réseau et celui des câbles électriques.

Sensibilité des interfaces

Les équipements électriques sont constitués d'interfaces analogiques, qui permettent leur couplage au support électrique (inductif ou capacitif). Dans le cas des CPL, ces interfaces permettent en outre la transmission du signal numérique sur les câbles électriques.

Selon les composants électroniques utilisés, l'interface analogique présente une certaine « sensibilité », qui influe sur sa capacité à transmettre le signal CPL sans trop de dégradation. Cette sensibilité est modélisée par une impédance entre le câble électrique et les circuits numériques de l'équipement.

Modélisation des réseaux électriques

La modélisation d'un réseau électrique permet d'anticiper les phénomènes qui se produisent lors de la transmission des données (perturbations, perte de liens, etc.) et d'en proposer une représentation susceptible d'aider à l'ingénierie du réseau.

La modélisation des réseaux électriques, qu'ils soient domestiques, d'entreprise ou publics (dans le cas des réseaux de distribution électrique) est un sujet technique difficile, qui exige de prendre en compte de nombreux paramètres (topologie, nature des câbles, perturbations, équipements branchés sur le réseau, heures de la journée, etc.).

Comme il n'existe pas d'outil de modélisation complet des réseaux électriques, l'ingénierie des réseaux CPL de télécommunications se limite à modéliser la couche physique de transport du signal CPL.

Les mesures effectuées sur les réseaux électriques ont permis de quantifier l'impédance moyenne d'une ligne électrique dans les fréquences hautes du type de celle utilisées par les équipements CPL.

La figure 2.4 illustre la courbe de l'impédance exprimée en ohm (impédance en valeur absolue) en fonction de la fréquence. Cette impédance varie de 50 à 150 ohms pour les fréquences des CPL.

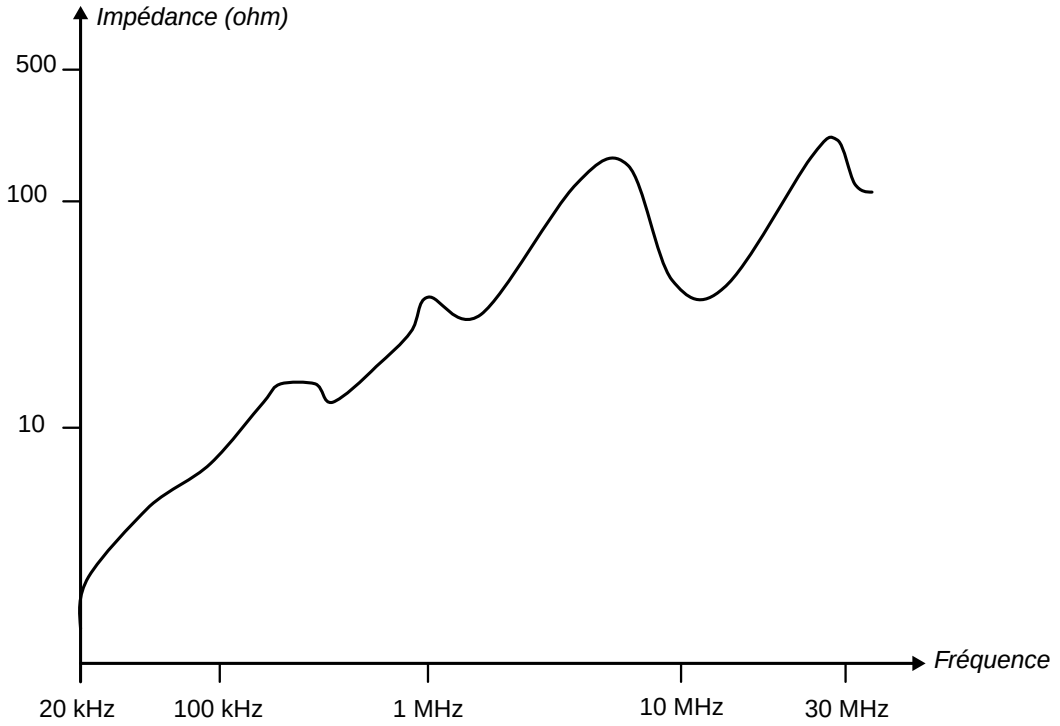


Figure 2.4

Impédances moyennes d'une ligne électrique en fonction de la fréquence

Les travaux de Nicholson et Malak ont permis d'exprimer l'impédance moyenne d'une ligne électrique par la formule :

$$Z_c = \sqrt{\frac{L}{C}}$$

Où

L = $\mu H/m$ (inductance linéaire de la ligne électrique)

C = $\mu F/m$ (capacitance linéaire de la ligne électrique)

Les travaux de Downey et Sutterlin ont permis de modéliser le circuit électrique équivalent d'une ligne électrique. Ce circuit, composé de résistances, d'inductances et de capacitances peut être schématisé comme illustré à la figure 2.5.

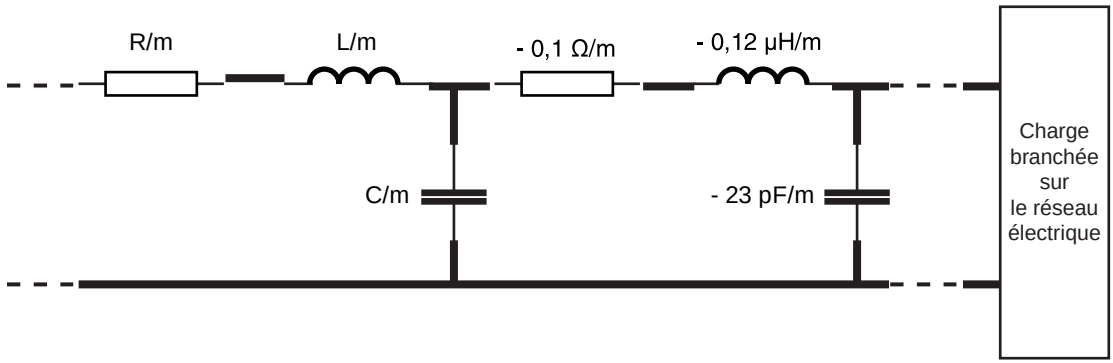


Figure 2.5
Circuit schématique d'une ligne électrique selon le modèle de Downey et Sutterlin

L'impédance d'une ligne électrique est décrite par l'équation suivante :

$$Z = R() + s \times L \text{ (exprimée en ohm)}$$

où R est la résistance du câble électrique en fonction de la fréquence du signal qui se propage dans le câble, s la section du câble électrique et L l'inductance de la ligne électrique.

L'impédance dépend de la charge branchée sur la ligne électrique, c'est-à-dire des équipements électriques (tels que séchoirs électriques, lampes halogènes, etc.) branchés sur le réseau, avec leur impédance propre.

Ces éléments de modélisation des réseaux électriques permettent de donner des ordres de grandeur des valeurs caractéristiques des réseaux électriques influant sur le transport des signaux CPL.

Modélisation des équipements électriques sur le réseau

De la même manière qu'il est difficile de modéliser des réseaux électriques, il est difficile de modéliser les équipements électriques branchés sur le réseau électrique. Ces équipements de toutes sortes sont en effet branchés et débranchés de manière aléatoire, modifiant la charge du réseau en permanence.

De plus, les caractéristiques de ces équipements changent au cours de leur vie, des heures de la journée, de leur fréquence d'utilisation, etc., rendant parfois peu fiable cette modélisation.

À l'exception d'EMTP, qui permet de modéliser l'ensemble d'un réseau électrique avec ses différents câbles en fonction de la topologie, il n'existe guère d'outil susceptible de faciliter l'ingénierie et la compréhension des comportements des signaux CPL sur les câbles électriques.

Le Cenélec travaille toutefois à la mise au point d'un projet destiné à faciliter la modélisation des réseaux électriques domestiques.

Architecture à média partagé

Nous verrons aux chapitres 10, 11 et 12, consacrés à l'installation de réseaux CPL domestiques, d'entreprise et de collectivités locales, que les topologies des réseaux électriques peuvent être vues comme des médias partagés entre tous les équipements au travers desquels se propagent les différents signaux CPL transportant les données échangées entre les terminaux d'un réseau local.

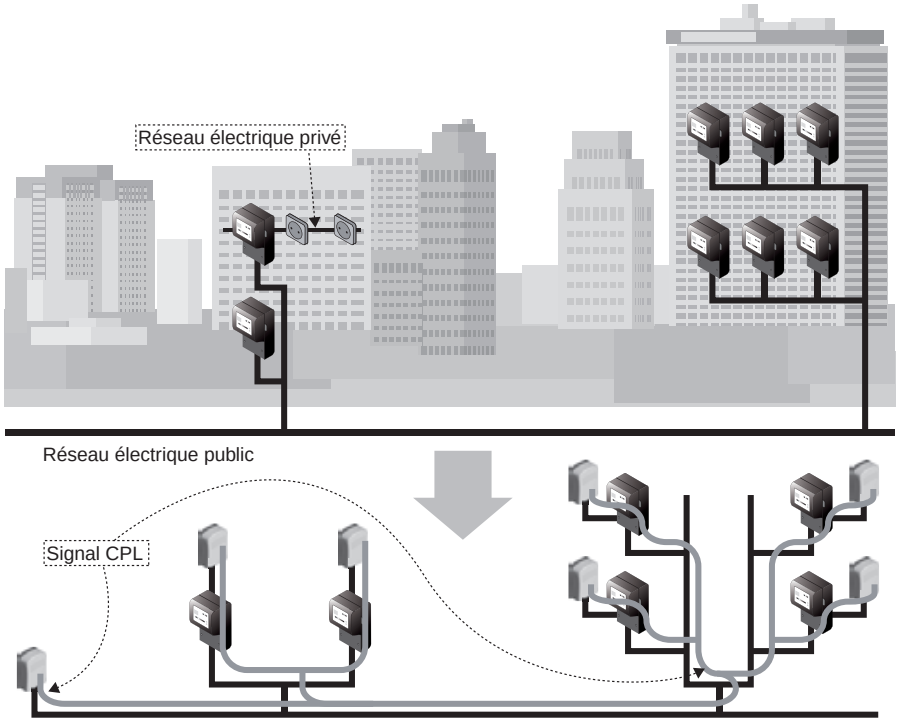
Nous distinguons dans cette section les réseaux dits « publics », qui fournissent l'électricité aux particuliers, entreprises et collectivités, et les réseaux dits « privés », constitués par les réseaux de distribution de l'électricité d'un bâtiment depuis les compteurs jusqu'à l'ensemble des prises du bâtiment. Nous verrons que la notion de média partagé est équivalente pour ces deux types de réseaux.

Réseaux publics

On appelle réseau électrique public, un réseau de distribution qui alimente les bâtiments, appartements, immeubles et entreprises d'un quartier, d'une agglomération ou d'une collectivité locale. Ce réseau est public dans la mesure où quiconque peut souscrire un abonnement pour être alimenté par la régie électrique locale ou par un fournisseur tel qu'EDF.

La figure 2.6 illustre schématiquement un réseau électrique public alimentant six compteurs électriques, derrière lesquels se trouvent des équipements CPL connectés au réseau

Figure 2.6
Réseau électrique public et média partagé



électrique privé de l'habitation. Selon les types de topologie du réseau électrique public (étoile, anneau, etc.), le média est plus ou moins partagé entre tous les compteurs en fonction des ramifications du réseau.

Sur cette figure, deux ramifications électriques aboutissent à plusieurs compteurs et aux équipements CPL. Le signal CPL se propage entre les différents équipements connectés au réseau électrique tout le long de ces ramifications, incluant les ensembles compteur + disjoncteurs, aux atténuations du signal près. Cela permet de voir le réseau électrique comme un bus de données, auquel les équipements CPL sont « connectés » de part et d'autre.

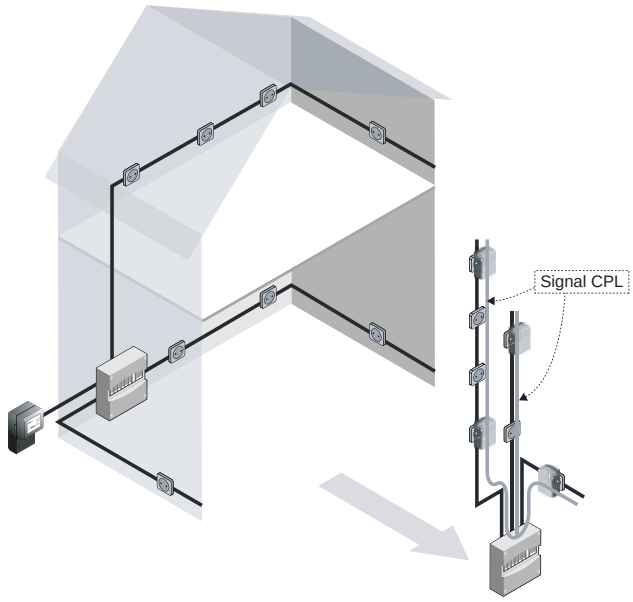
Réseaux privés

Un réseau électrique privé se situe derrière le compteur d'alimentation du réseau électrique public et ne concerne, en terme de responsabilité, que les occupants de l'habitation (appartement, maison, bureau, usine, etc.).

La topologie de ce type de réseau, contrairement à celle des réseaux électriques publics, ne dispose pas de règles d'ingénierie bien définies et peut être spécifique à chaque installation (ajout de parties de réseau ou de tableaux électriques, topologie en série, etc.). Néanmoins, toutes les ramifications du réseau partent généralement de l'ensemble compteur + tableau électrique, et le signal CPL circule dans l'ensemble des ramifications en repassant par le tableau électrique.

La figure 2.7 illustre un exemple de réseau électrique simplifié, avec trois ramifications depuis le tableau électrique. À droite de la figure, le signal CPL se propage entre les différentes prises afin de connecter les équipements CPL. Cet exemple montre que le réseau électrique privé peut être vu comme un média partagé de type bus de données.

Figure 2.7
Réseau électrique privé et média partagé



Analogie avec le concentrateur réseau

Les deux exemples précédents de réseaux électriques public et privé démontrent que tout type de réseau électrique peut être vu comme un vaste bus de données sur lequel se connectent les équipements CPL du réseau.

En terme d'équipement de télécommunications, l'analogie la plus évidente est celle d'un concentrateur, ou hub, dont les différents équipements CPL connectés au réseau électrique représenteraient les différents ports Ethernet.

La figure 2.8 illustre schématiquement cette analogie.

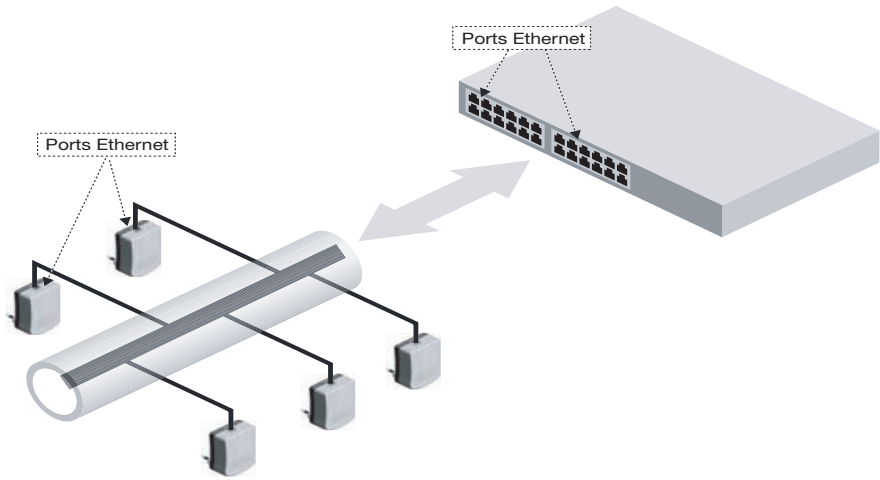


Figure 2.8
Analogie des réseaux CPL avec un concentrateur réseau

Notions de répéteurs

Comme nous le verrons au chapitre 7, dédié aux équipements CPL, il peut être nécessaire de répéter le signal afin d'agrandir sa zone de couverture et de connecter davantage d'équipements.

Lorsque le signal CPL est trop atténué pour pouvoir être interprété par les équipements CPL du réseau, l'équipement répéteur le réamplifie et le régénère le long du câble électrique.

Il existe deux types de répéteurs de signal permettant d'agrandir la couverture réseau :

- Les répéteurs « physiques », qui amplifient réellement le signal et le réémettent le long de la ligne électrique. Cette répétition est dite « physique », car elle intervient sur le signal physique lui-même et non sur les trames logiques. Ce type de répéteur ne diminue donc pas la bande passante de l'ensemble du réseau CPL.

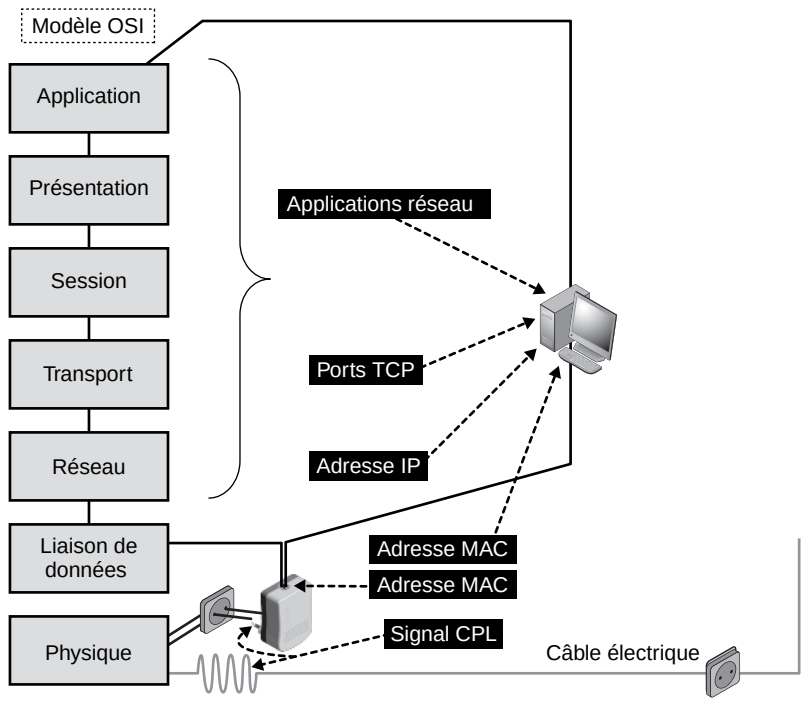
- Les répéteurs « logiques », qui répètent le signal au niveau des trames de données. Ce type de répéteur est constitué de deux équipements CPL reliés par leur interface Ethernet, l'un des équipements étant connecté à un segment du réseau électrique et l'autre au segment du réseau électrique inaccessible par le signal CPL du fait d'une atténuation trop importante. Ce type de répéteur divise par deux la bande passante de l'ensemble du réseau CPL puisqu'il produit deux réseaux logiques distincts sur le même réseau électrique.

Architecture en couches

Le modèle OSI (Open Systems Interconnection) en couches offre une base commune à la description de tout réseau informatique. Ce modèle comporte sept couches, dont chacune décrit un protocole indépendant des autres couches et fournit un service à la couche supérieure et demande des services de la couche inférieure.

Dans le cadre de ce modèle, les réseaux CPL se situent au niveau des couches 1 (physique) et 2 (liaison de données) pour fournir un service de connexion Ethernet aux couches supérieures.

Figure 2.9
Place des technologies CPL dans le modèle OSI



La figure 2.9 illustre la place des technologies CPL dans le modèle OSI. La couche 1 (physique) est constituée logiquement par le câble électrique sur lequel circule le signal

CPL. L'équipement CPL fournit à un terminal (classiquement un PC) un service de connexion Ethernet au niveau de la couche 2 (liaison de données) au moyen d'un adressage MAC et d'une connectique RJ-45. Le terminal utilise les services du réseau CPL pour accéder aux services des couches supérieures (IP, TCP, HTTP, etc.).

La couche physique

La couche physique des technologies CPL est constituée par le câble électrique et plus généralement par les réseaux électriques. La technique utilisée pour transporter le signal CPL sur ce support consiste à ajouter aux 220 V/50 Hz du circuit électrique un signal modulé de faible amplitude autour d'une fréquence centrale dite « fréquence porteuse » *F*.

La couche physique consiste en ce signal modulé (nous détaillons les techniques de modulation au chapitre 3) de faible amplitude, transporté sur les câbles électriques à une fréquence déterminée par la technologie CPL considérée et la réglementation en vigueur.

La figure 2.10 illustre la somme des signaux CPL et 220 V/50 Hz qui se superposent sur les câbles électriques pour constituer la couche physique des réseaux CPL.

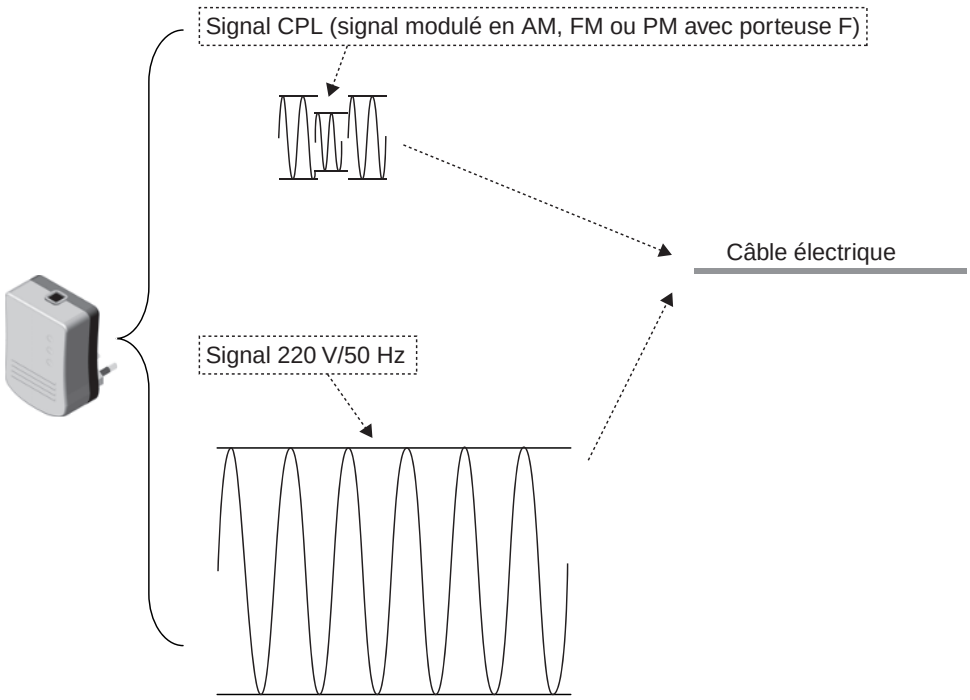


Figure 2.10

Somme du signal CPL modulé et du signal électrique 220 V/50 Hz

Les bandes de fréquences

Le signal CPL étant un signal modulé en amplitude, fréquence ou phase autour d'une fréquence porteuse *F*, il est nécessaire de mettre en place des règles d'utilisation de chaque bande de fréquences entre 0 et quelques dizaines de gigahertz par le biais d'organismes de régulation nationaux ou européens.

Deux bandes de fréquences sont allouées aux technologies CPL :

- 3 à 148 kHz pour les CPL dits bas débit ;
- 2 à 20 MHz pour les CPL dits haut débit.

La figure 2.11 illustre la place des fréquences CPL relativement à d'autres technologies réseau.

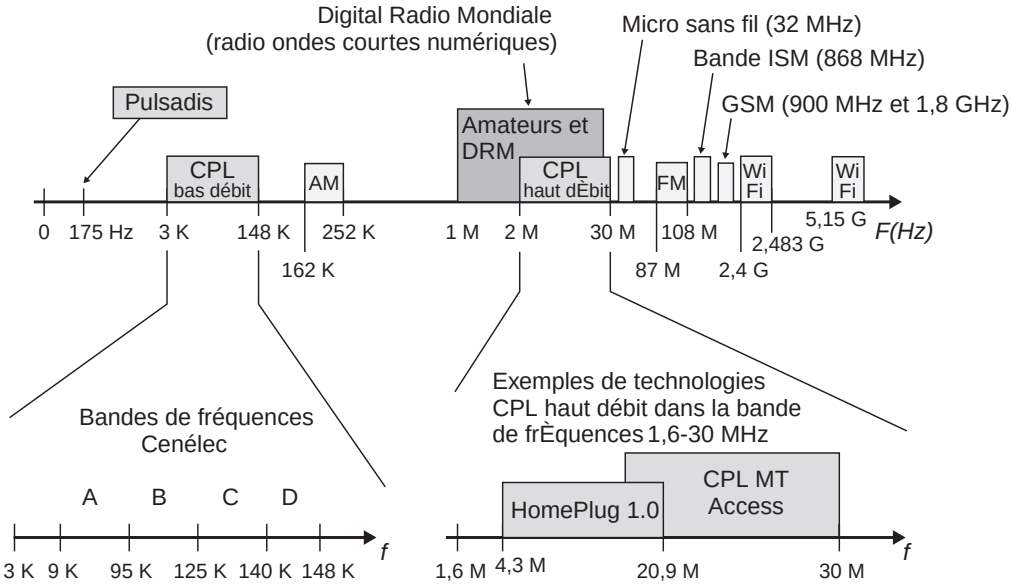


Figure 2.11

Bandes de fréquences utilisées par les réseaux CPL

3

Fonctionnalités

Ce chapitre présente les fonctionnalités des réseaux CPL. Les technologies utilisées dans ces réseaux sont assez simples pour être intégrées sur une puce unique et permettre la réalisation de composants à très bas coût. Elles resteront d'actualité jusqu'à l'arrivée de nouvelles interfaces CPL permettant d'augmenter le débit des équipements.

Les fonctionnalités des CPL tirent parti de nombreux développements technologiques des réseaux fixes, notamment l'ADSL, Wi-Fi, Ethernet, etc. La composante électrique des CPL nécessite pour sa part de recourir à des technologies permettant de fiabiliser le lien CPL, qui constitue le principal point faible de ce type de réseau.

Les principales fonctionnalités des CPL sont les suivantes :

- Le mode réseau, qui permet de gérer l'organisation du réseau et les communications entre les différents équipements CPL.
- Le mode de gestion des trames CPL, notamment la fragmentation et le réassemblage, qui permet de pallier le problème de la transmission d'importants volumes de données.
- La technique d'accès au média, qui inclue la synchronisation des équipements du réseau et la gestion des priorités.
- La qualité de service, qui autorise la transmission des données de type voix ou vidéo dans les environnements CPL.

Fonctionnalités du mode réseau

Une des fonctionnalités importantes des réseaux CPL est le mode réseau, qui permet de gérer l'ensemble des équipements CPL d'un même réseau.

Un réseau étant, par définition, constitué de plusieurs équipements qui échangent des données, il est nécessaire de mettre en place une gestion de ces échanges afin qu'ils soient organisés et optimisés.

Il existe plusieurs manières d'organiser un réseau. Les différentes technologies CPL utilisent un des trois modes réseau suivants :

- Mode maître-esclave. Peut être comparé à un réseau IP de type client-serveur, dans lequel un équipement maître gère les échanges entre les équipements CPL du réseau. Les esclaves peuvent s'échanger des données entre eux selon la gestion du maître.
- Mode pair-à-pair. Peut être comparé à un réseau IP de type peer-to-peer, où tous les équipements CPL du réseau jouent le même rôle et ont le même niveau hiérarchique. Ces équipements peuvent échanger les uns avec les autres sans être contrôlés par un équipement maître.
- Mode centralisé. Mélange des deux précédents, dans lequel un équipement centralisateur est responsable de la gestion du réseau et des échanges entre équipements CPL. Les autres équipements peuvent également échanger entre eux sans avoir à passer par le centralisateur.

Les principaux avantages et inconvénients de ces trois modes sont récapitulés au tableau 3.1.

Tableau 3.1 Avantages et inconvénients des modes maître-esclave, pair-à-pair et centralisé

Mode	Avantage	Inconvénient
Maître-esclave	– Administration centralisée – Rôle de passerelle pour le réseau CPL – Gestion des niveaux de QoS (TDMA) – Gestion des rôles de chaque équipement – Hiérarchisation des réseaux CPL et IP – Supervision du réseau facilitée	– Besoin de redondance – Points de faiblesse en matière de sécurité – Encombrement possible de la bande passante – Configuration plus complexe
Pair-à-pair	– Distribution de la bande passante – Distribution des tables de routage CPL au niveau physique – Facilité de déploiement	– Pas de hiérarchisation du réseau – Faible définition de la passerelle CPL
Centralisé	– Administration centralisée – Seul le trafic d'administration passe par le coordinateur.	– Point de faiblesse sur le centralisateur – Besoin du coordinateur pour la gestion des trames TDMA

Le mode maître-esclave

Le mode maître-esclave permet d'utiliser la logique du réseau électrique – composé d'un compteur électrique en tête de réseau, considéré comme un maître du réseau électrique, et de ses disjoncteurs et départs, considérés comme des esclaves de ces disjoncteurs –, sur lequel s'appuie le réseau CPL pour son support physique, et de placer l'équipement dit maître sur la partie en tête de réseau et les équipements esclaves sur les différents brins du réseau.

Dans le cas de réseaux CPL sur les réseaux électriques MT ou BT publics, les principales fonctionnalités attendues du maître sont les suivantes :

- Gestion des connexions sécurisées des différents équipements esclaves. Chacun des équipements appartient à un réseau logique privé, grâce à un canal de connexion dédié sur le support électrique, qui fait office de support partagé. Les trames CPL circulent donc librement sur les différents brins du réseau électrique.

- Gestion de la qualité de service (QoS) des liens physiques CPL entre les esclaves et le maître par le biais de différentes méthodes d'analyse du niveau physique (niveau signal sur bruit dans chaque sous-bande de fréquences, calcul des nombres de bits/Hz transmissibles, etc.). Cette gestion de la QoS est assurée par une table de qualité des différents liens, située au niveau du maître CPL.

- Possibilité de créer des VLAN ou des liens interéquipement esclaves *via* une administration centralisée des clés de cryptage aux niveaux physique et éventuellement logique.

- Supervision des équipements afin d'intégrer des outils d'administration réseau IP (de type pile SNMP) en amont du réseau CPL selon une architecture plus complète de réseau IP.

- Gestion de la redondance avec d'autres équipements maîtres.

L'équipement maître intègre ainsi toute l'intelligence du réseau CPL, offrant une gestion optimisée de l'architecture *via* des interfaces embarquées ou déportées, accessibles depuis des protocoles standards, généralement HTTP ou IP, avec des piles SNMP mises à jour en permanence en fonction des fluctuations du réseau électrique.

Pour le cas des réseaux CPL sur les réseaux électriques BT domestiques (appartement, maison, PME, hôpital, hôtel, école, etc.), les fonctionnalités attendues des différents équipements CPL maîtres – il peut y en avoir plusieurs sur le réseau électrique afin de constituer une architecture logique distincte ou de répéter les signaux CPL – sont les suivantes :

- Gestion des niveaux de qualité des liaisons CPL entre les équipements esclaves et l'équipement maître, ainsi qu'entre équipements esclaves.

- Gestion de la QoS par le biais des paramètres de bande passante utile (au niveau de la couche TCP), de la jitte et de la latence.
- Gestion de connexions sécurisées au moyen de clés de cryptage pour chaque réseau logique afin d'assurer un isolement logique de chaque équipement CPL esclave, par exemple, dans une architecture d'hôtel ou de résidence universitaire. Cette fonctionnalité permet de détecter automatiquement des équipements nouvellement branchés ou les équipements déjà branchés.
- Gestion de la redondance entre équipements maîtres afin de garantir le bon fonctionnement de l'ensemble de l'architecture CPL à des débits atteignant 200 Mbit/s, et davantage encore dans les années à venir, au niveau physique.

Le tableau 3.2 récapitule les principales fonctions attendues de l'équipement CPL maître et les solutions techniques correspondantes.

Tableau 3.2 Fonctions attendues de l'équipement maître et solutions techniques correspondantes

Fonction	Solution technique
Collision des trames	CSMA/CA
Multiplexage temporel	TDMA
Table d'états des liaisons physiques	Table dite Tone Map
Synchronisation des trames au réseau 50 Hz	Passage par zéro
SNR dans chaque sous-bande de fréquences	Écoute des niveaux de bruit
Supervision de la couche MAC	Trames et FEC
Trames de supervision	Mode beacon et régionalisation beacon

Le mode pair-à-pair

La théorie des réseaux de télécommunications s'est beaucoup appuyée sur le principe de la hiérarchisation des équipements réseau. Ce principe a été remis en cause avec l'avènement des architectures de type *ad-hoc,* que ce soit dans les réseaux sans fil ou les réseaux d'échange de fichiers sur Internet, dits peer-to-peer, ou pair-à-pair. Les réseaux décentralisés offrent de nombreux avantages par rapport aux réseaux hiérarchisés ou en mode maître-esclave.

Dans l'architecture CPL en mode pair-à-pair illustrée à la figure 3.1, les équipements CPL jouent tous le même rôle et échangent en permanence un certain nombre de paramètres afin de maintenir la cohérence du réseau. Dans le cas de HomePlug 1.0, ils échangent et mettent à jour des informations localement.

Les principaux paramètres nécessaires aux équipements CPL sont les suivants :

- Qualité du lien CPL entre un équipement et tous les autres. Cette qualité est mesurée au niveau physique, de la même manière que les équipements radio mesurent la qualité

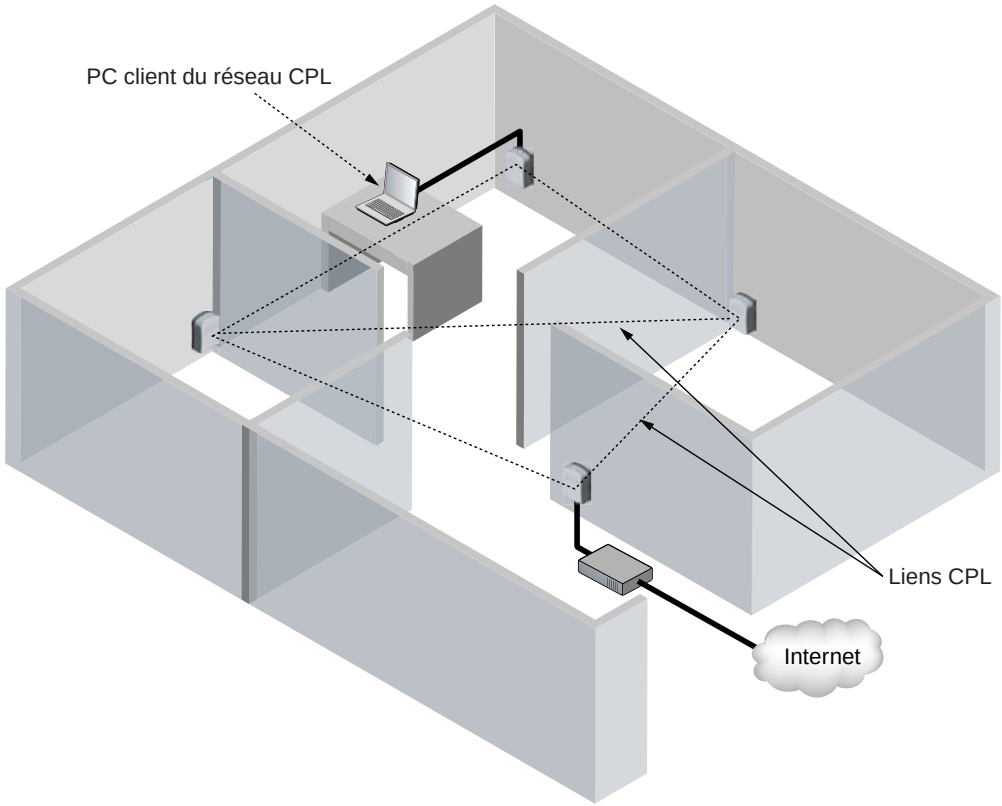


Figure 3.1
Architecture d'un réseau CPL en mode pair-à-pair

des liens radio pour évaluer les services disponibles dans les couches OSI supérieures, et ce au moyen d'une table, appelée Tone Map, mise à jour en permanence.

- Clés de cryptage EKS (Encryption Key Select) permettant de se connecter sur un réseau CPL et d'échanger avec les autres équipements. Les EKS sont au nombre de deux dans HomePlug 1.0 : DEK (Default Encryption Key) et NEK (Network Encryption Key). Nous reviendrons sur leurs caractéristiques au chapitre 4, dédié à la sécurité, et sur leur configuration au chapitre 9. Ces clés permettent de créer, sur un même réseau électrique, plusieurs réseaux CPL en mode pair-à-pair, sans communication de données interréseau. Ces réseaux utilisant le même réseau électrique, il est possible de réduire le débit de communication des données puisque la technologie CPL utilise l'ensemble de la bande de fréquences des 2-30 MHz.
- Sélection du mode de modulation et du type de FEC (Forward Error Correction) les mieux adaptés au vu des qualités des liens CPL. Dans le cas de HomePlug 1.0, les quatre modes possibles sont DQPSK 3/4 (Differential Quadrature Phase Shift

Keying), DQPSK 1/2, DBPSK 1/2 (Differential Binary PSK) et ROBO (Robust OFDM), qui permettent d'obtenir quatre types de débits de données.

- Priorité de chaque équipement CPL du réseau. Ce paramètre est marqué dans le champ VLAN des trames Ethernet pour chaque équipement CPL en fonction de sa configuration. Il permet d'établir une quasi-hiérarchisation du réseau, avec des équipements jouant le rôle de passerelle vers d'autres réseaux et d'autres jouant des rôles standards dans l'architecture.

Hiérarchisation des réseaux CPL HomePlug 1.0 par le biais des priorités

Au sein des trames Ethernet IEEE 802.3, il est possible de placer un champ VLAN, décrit dans le standard IEEE 802.1Q. Dans le cadre des réseaux CPL en mode pair-à-pair, ce champ permet de créer une quasi-hiérarchie entre les équipements CPL du même réseau. Le champ est codé sur 3 bits et peut donc prendre huit valeurs.

Le tableau 3.3 recense les quatre priorités CPL disponibles en fonction de la valeur du champ VLAN.

Tableau 3.3 Priorités CPL du champ VLAN

Priorité	Valeur du champ VLAN	Classe d'application
Priorité 3	7,6	VoIP (moins de 10 ms de temps de transmission)
Priorité 2	4,5	Video Over IP (moins de 100 ms de temps de transmission)
Priorité 1	2,3	Transfert de données brutes et trafic de contrôle
Priorité 0	0,1	Communication de données limitée

Il peut être utile de mettre en place une priorité plus importante sur un équipement CPL servant de passerelle vers un autre réseau IP ou étant relié à un équipement de type serveur, susceptible de recevoir beaucoup de trafic en provenance des autres équipements CPL du réseau connectés à des PC en mode client dudit serveur. On peut également imaginer plusieurs équipements CPL connectés à des téléphones IP sur le réseau et se mettant en priorité 4 afin d'offrir le meilleur temps de transmission pour les communications audio en temps réel.

Cette priorité est un des paramètres de configuration les plus importants des réseaux CPL en mode pair-à-pair, bien qu'il ne s'agisse que d'un paramètre « logique », n'agissant pas sur les liaisons CPL au niveau physique. Nous reviendrons sur ce paramètre au chapitre 9.

La figure 3.2 illustre l'architecture d'un réseau CPL en mode pair-à-pair, dans lequel ces quatre paramètres sont échangés en permanence par les équipements du réseau afin de maintenir l'homogénéité du réseau et une meilleure distribution du routage des trames Ethernet et de la bande passante.

Le mode pair-à-pair est largement utilisé dans les réseaux CPL au standard HomePlug 1.0, car il permet de créer rapidement des réseaux CPL dans lesquels chaque équipement crée des liaisons CPL avec les équipements branchés sur les autres prises du réseau électrique. Ce mode permet ainsi de créer un réseau *ad-hoc* CPL sur l'architecture électrique du bâtiment pour les besoins applicatifs du réseau LAN.

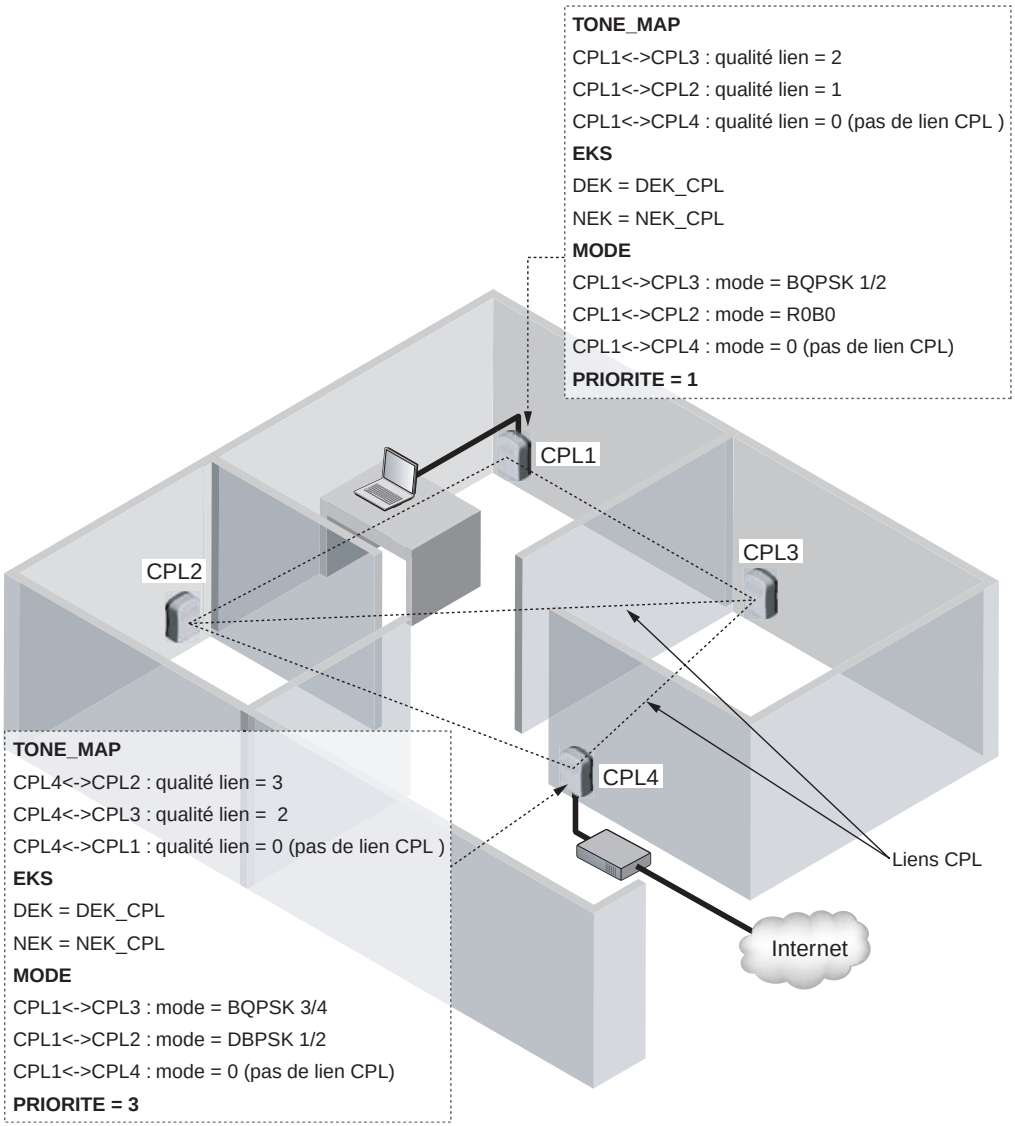


Figure 3.2

Échange de paramètres entre équipements d'un réseau CPL en mode pair-à-pair

La configuration et l'optimisation du réseau CPL dépendent des fonctionnalités attendues sur le réseau LAN et des besoins en terme d'architecture client-serveur afin de réaliser une architecture réaliste au regard des performances des technologies CPL.

La figure 3.3 illustre les différentes étapes d'organisation d'un réseau CPL en mode pair-à-pair, depuis les besoins en fonctionnalités jusqu'aux solutions techniques.

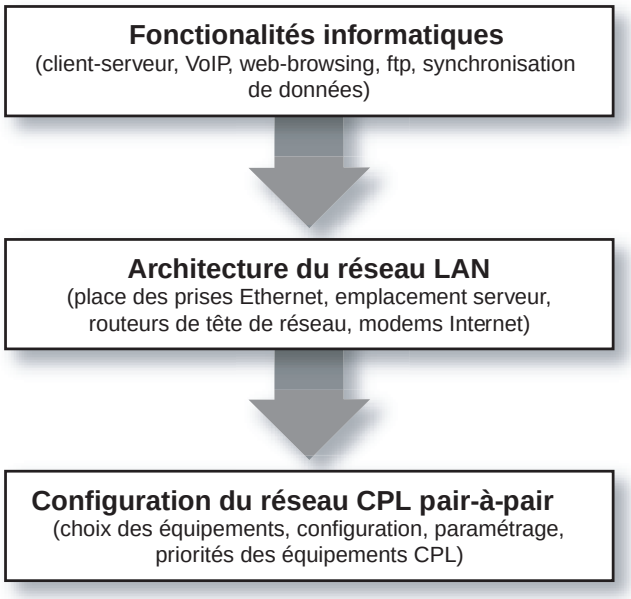


Figure 3.3
Organisation d'un réseau CPL en mode pair-à-pair

Le mode centralisé

L'architecture de la technologie CPL HomePlug AV n'est ni vraiment en mode pair-à-pair ni en mode maître-esclave. Elle met en jeu deux types d'équipements : des équipements de niveau hiérarchique similaire et un équipement centralisateur, comme l'illustre la figure 3.4.

L'équipement CCo (centralisateur) gère les allocations d'accès au média des différents équipements CPL qui veulent communiquer entre eux.

La communication des données entre les équipements CPL1 et CPL2 s'effectue de la façon suivante :

1. CPL1 et CPL2 mettent en place une estimation du canal de transmission (niveaux de modulation, niveau de codage d'erreur, etc.).
2. CPL1 et CPL2 informent CCo (CPL3) qu'ils veulent échanger des données.

3. CCo (CPL3) leur alloue un intervalle de temps pendant lequel ils ont accès au média.
4. CPL1 et CPL2 échangent leurs données directement, sans passer par CCo.

Si la gestion des accès au média est prise en charge par l'équipement centralisateur CCo, comme dans le mode maître-esclave, l'échange des données se déroule pour sa part directement entre les équipements, comme dans le mode pair-à-pair.

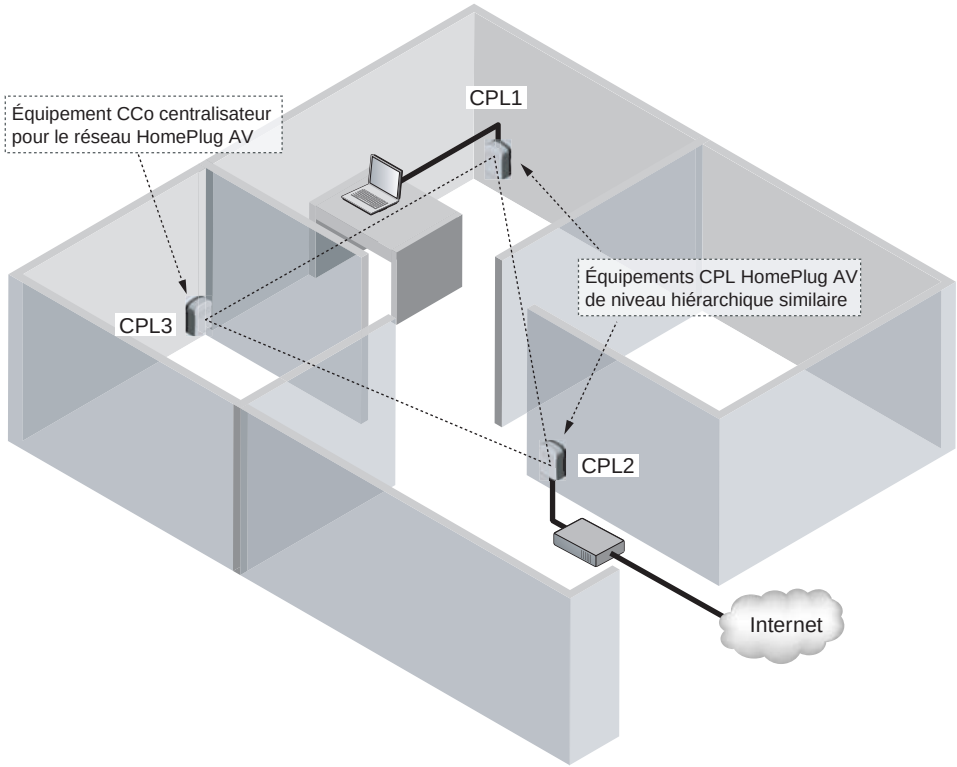


Figure 3.4
Architecture d'un réseau CPL en mode centralisé

Fonctionnalités du canal de transmission

Dans les CPL, le canal de transmission est le réseau électrique. N'étant pas conçu au départ pour supporter des applications réseau, il a fallu lui ajouter des fonctionnalités réseau afin d'implémenter correctement la couche liaison de données. Parmi celles-ci, l'accès au média et les processus de synchronisation des trames et de gestion des canaux de fréquences sur le câble électrique sont spécifiques des technologies CPL.

Techniques d'accès au média par la méthode CSMA/CA

Le CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) est une technique dite d'accès aléatoire avec écoute de la porteuse, qui permet d'écouter le support de transmission avant tout envoi de données. Le CSMA évite que plusieurs transmissions aient lieu sur un même support au même moment et réduit les collisions, sans toutefois les éviter complètement.

Dans Ethernet, le protocole CSMA/CD (Carrier Sense Multiple Access/Collision Detection) contrôle l'accès au support de chaque station et détecte et traite les collisions qui se produisent lorsque deux stations ou plus essayent de communiquer simultanément à travers le réseau.

Dans le cas des CPL, la détection des collisions n'est pas possible. En effet, pour détecter une collision, une station doit être capable d'écouter et de transmettre en même temps. Or, dans les systèmes CPL comme dans les systèmes radio, la transmission empêche la station d'écouter en même temps sur la fréquence d'émission. De ce fait, la station ne peut entendre les collisions. Comme une station ne peut écouter sa propre transmission, si une collision se produit, la station continue à transmettre la trame complète, entraînant une perte globale de performance du réseau.

Tenant compte de ces spécificités, les CPL utilisent un protocole légèrement modifié par rapport au CSMA/CD, appelé CSMA/CA. Le rôle du CSMA/CA n'est pas d'attendre qu'une collision se produise pour réagir, comme dans le CSMA/CD, mais de prévenir les collisions. Le CSMA/CA essaye donc de réduire le nombre de collisions en évitant qu'elles se produisent, sachant que la plus grande probabilité d'avoir une collision se situe lors de l'accès au support.

Pour éviter les collisions, le CSMA/CA fait appel à différentes techniques, telles que des mécanismes d'écoute du support introduits par les CPL, l'algorithme de back-off pour la gestion de l'accès multiple au support, un mécanisme optionnel de réservation, dont le rôle est de limiter le nombre de collisions en s'assurant que le support est libre, ainsi que l'utilisation de trames d'acquittement positif (ACQ)

Le CSMA/CA utilisé dans les CPL est légèrement modifié par rapport à celui mis en œuvre dans Wi-Fi. Le standard HomePlug spécifie l'utilisation d'une valeur indiquant le nombre de fois qu'une station n'a pu émettre par rapport aux autres stations CPL ayant la même priorité d'accès au média. Cette valeur, appelée DC (Deferral Counter), augmente lorsqu'une station n'a pu émettre, permettant d'ajuster l'utilisation du réseau à ce niveau de priorité.

La figure 3.5 illustre le fonctionnement de l'algorithme CSMA/CA dans son ensemble.

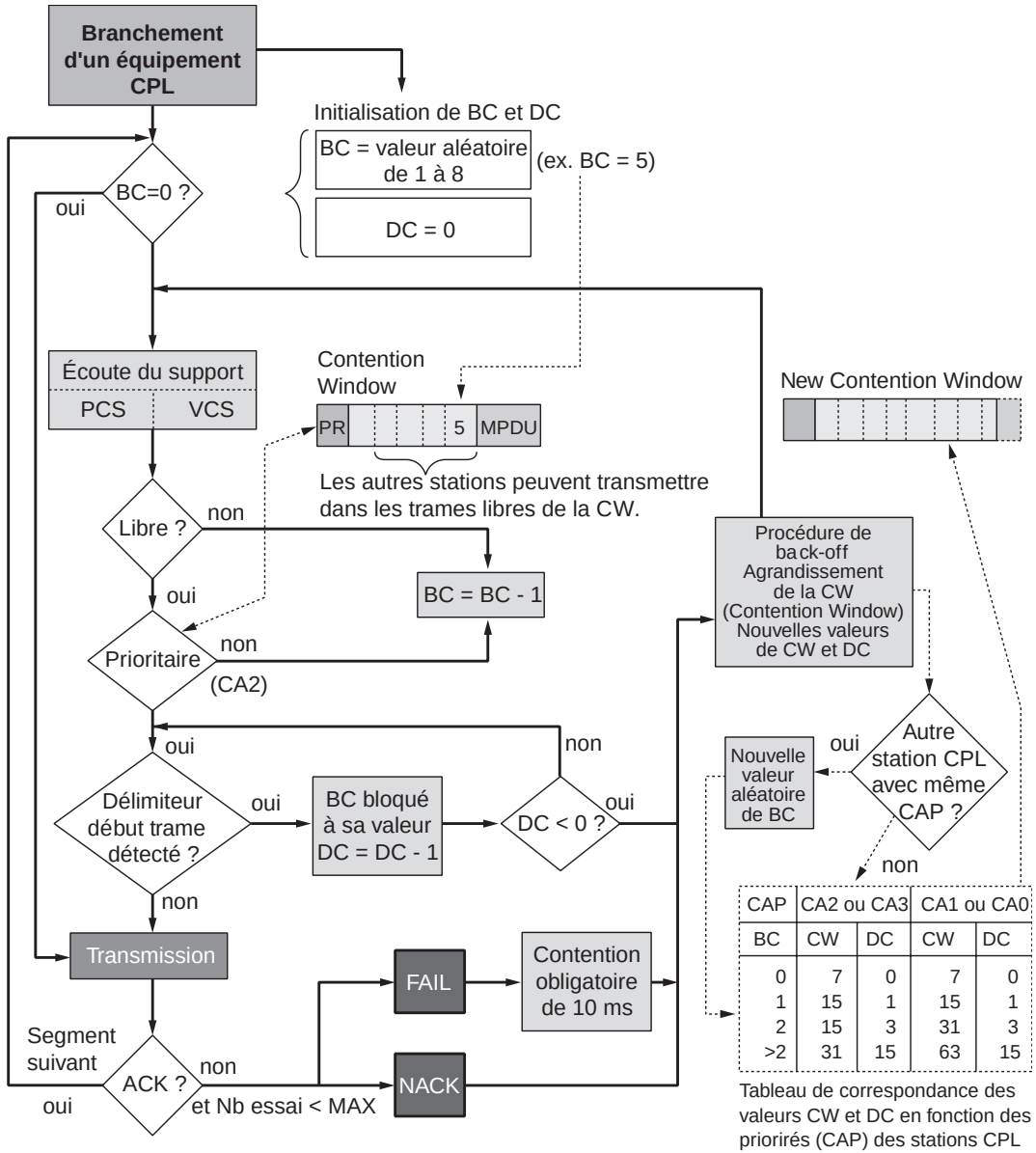


Figure 3.5

Fonctionnement du CSMA/CA dans HomePlug 1.0

Écoute du support

Dans les CPL, l'écoute du support se fait à la fois au niveau de la couche physique, avec le PCS (Physical Carrier Sense), et au niveau de la couche MAC, avec le VCS (Virtual Carrier Sense).

Le PCS permet de connaître l'état du support en détectant la présence d'autres stations CPL et en analysant les trames reçues, ou en écoutant l'activité sur le support grâce à la puissance relative du signal des différentes stations.

Le PCS s'appuie sur l'écoute de certaines trames reçues, les trames de préambule et les trames de priorité.

Le VCS ne permet pas vraiment l'écoute du support mais réserve le support par l'intermédiaire du PCS.

Deux types de mécanismes sont utilisés dans le VCS :

- la détection des champs de début de trame ;
- l'information d'attente de réponse fournie par les champs de contrôle de trame.

La figure 3.6 illustre ces deux techniques d'écoute du support avant la transmission de trames de données sur le réseau électrique.

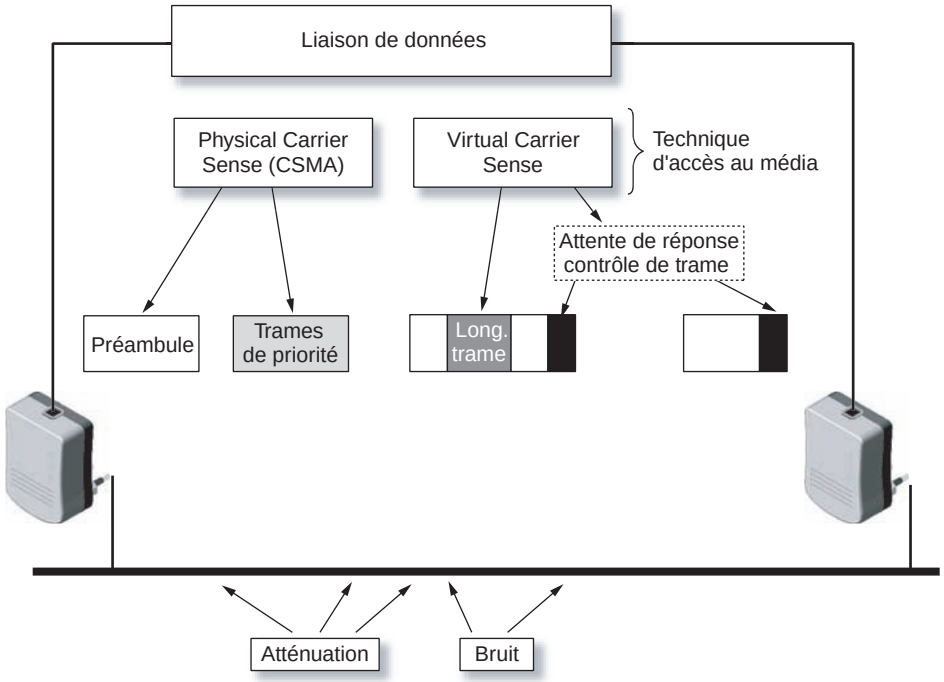


Figure 3.6
Écoute du support dans HomePlug 1.0

Accès au support

L'accès au support est contrôlé au moyen d'un mécanisme d'espacement entre deux trames appelé IFS (Inter-Frame Spacing). Cet espacement correspond à l'intervalle de temps entre la transmission de deux trames. Les intervalles IFS sont en fait des périodes d'inactivité sur le support de transmission, qui permettent de gérer l'accès au support pour les stations ainsi que d'instaurer un système de priorités lors d'une transmission.

Les valeurs des différents IFS dépendent de l'implémentation de la couche physique. Le standard HomePlug 1.0 définit trois types d'IFS :

- **CIFS (Contention distributed Inter-Frame Spacing).** Le CIFS est utilisé par les stations qui veulent accéder au support lorsqu'il est libre, entraînant la fin des autres transmissions pendant 35,84 µs. Le CIFS est suivi de la phase de résolution des priorités de chaque station.
- **RIFS (Response Inter-Frame Spacing).** Lorsqu'une station attend une réponse de la station destination, cette dernière attend un temps RIFS de 26 µs avant de transmettre sa réponse. Ce RIFS permet également aux stations de passer d'un mode émetteur à un mode récepteur.
- **EIFS (Extended Inter-Frame Spacing).** L'EIFS correspond au maximum de temps nécessaire à une station pour transmettre. Il correspond à la somme des temps d'écoulement de la trame de données en mode non-ROBO (Robust OFDM), avec ses différents délimiteurs, des intervalles de priorités, du CIFS, du RIFS et du EFG (End of Frame Gap), ce qui correspond à 1 695 µs. Le temps EIFS est également utilisé pour déterminer pendant combien de temps le support est occupé après une collision, ainsi que pour le processus de FEC (Forward Error Control), qui permet de vérifier si les données reçues ne sont pas erronées. En effet, la mesure de la longueur des trames n'est pas déterminée de manière complètement robuste dans l'écoute du support avec la méthode VCS.

Le tableau 3.4 récapitule les valeurs des IFS et du timeslot de HomePlug 1.0 et HomePlug AV.

Tableau 3.4 Valeurs des IFS et du timeslot selon la couche physique

	HomePlug 1.0	HomePlug AV
Timeslot	35,84 µs	35,84 µs
CIFS	35,84 µs	100 µs
RIFS	26 µs	30 à 160 µs 140 µs (par défaut)
EIFS	1 695 µs	2 920 µs
AIFS	-	30 µs
B2BIFS	-	85 µs

Tableau 3.4 Valeurs des IFS et du timeslot selon la couche physique *(suite)*

	HomePlug 1.0	HomePlug AV
BIFS	-	20 µs
CIFS AV	-	100 µs
RGIFS	-	80 µs

La version AV du standard HomePlug dispose d'un certain nombre d'IFS supplémentaires par rapport à la version 1.0 :

- **AIFS (Allocation Inter-Frame Spacing).** Utilisé pour séparer les zones d'allocation TDMA et CSMA/CA des services réservés au standard HomePlug AV.
- **B2BIFS (Beacon To Beacon Inter-Frame Spacing).** Utilisé pour séparer les différentes trames balises dans la zone d'allocation TDMA spécifique des trames balises HomePlug AV.
- **BIFS (Burst Inter-Frame Spacing).** Utilisé pour séparer les différentes trames MPDU dans le cas du mode de réseau de type *bursting*, avec un accès au support de type CSMA/CA.
- **CIFS AV (Contention distributed Inter-Frame Spacing version AV).** Utilisé par les stations qui veulent accéder au support afin de séparer les trames de transmission provenant de la station source et les trames de réponse provenant de la station destination.
- **RGIFS (Reverse Grant Inter-Frame Spacing).** Utilisé pour séparer les trames dans le mode réseau Reverse Grant, spécifique du standard HomePlug AV.

L'algorithme de back-off

Comme expliqué précédemment, le CPL utilise la méthode CSMA/CA pour contrôler l'accès au canal de transmission.

Puisque les collisions ne peuvent être détectées du fait de l'atténuation et du bruit sur le média électrique, lorsqu'une station CPL veut émettre, elle doit attendre jusqu'à ce que le média soit disponible pour l'émission. La station doit attendre qu'un IFS se libère pour un temps aléatoire, dit de *back-off*. Comme il n'y a aucune garantie qu'une collision ne se produise pas dans l'intervalle, la station source (émettrice) attend une trame d'acquittement positif (ACK) de la part de la station destination. La station destination émet une réponse de bonne réception si les données arrivent correctement. Cette réponse ACK est émise dans les prochains IFS disponibles.

Dans les CPL, le temps est découpé en intervalles, ou timeslots. Ces derniers sont gérés par un temporisateur appliqué aux transmissions et retransmissions des différentes stations afin de permettre à chacune des stations d'avoir la même probabilité d'accéder au support.

L'algorithme de back-off définit une fenêtre de contention CW (Contention Window), ou fenêtre de back-off. Ce paramètre correspond au nombre de timeslots qui peuvent être sélectionnées pour le calcul du timer de back-off.

Il est compris entre des valeurs CW_{min} et CW_{max} prédéfinies par le standard HomePlug. Appelé BC (Backoff Counter), ce nombre de timeslots est utilisé par la procédure de back-off lorsque le média n'est pas libre ou que la station source n'a pas reçu une trame ACK de la part de la station destination. Dès qu'une station veut transmettre des informations, elle écoute le support grâce au PCS défini précédemment.

Si le support est libre, elle retarde sa transmission en attendant un IFS. À l'expiration de l'IFS, et si le support est toujours libre, elle transmet directement sa trame, sans utiliser l'algorithme de back-off. Dans le cas contraire, le support étant occupé par une autre station, la station attend qu'il se libère, autrement dit diffère sa transmission.

Pour tenter d'accéder à nouveau au support, elle utilise l'algorithme de back-off. Si plusieurs stations attendent de transmettre, elles recourent toutes à l'algorithme de back-off. En effet, une station ne connaît pas le nombre de stations associées au réseau. Sans ce mécanisme, par lequel chaque station calcule potentiellement un temporisateur de back-off différent pour différer sa transmission, les stations entreraient directement en collision dès la libération du support.

Les stations calculent leur temporisateur, ou $T_{BACKOFF}$ selon la formule :

$$T_{BACKOFF} = Random(0,CW) \times \text{timeslot}$$

Random(0,*CW*) est une variable pseudo-aléatoire uniforme, comprise dans l'intervalle [0, $CW - 1$]. Le $T_{BACKOFF}$ correspond donc à un nombre de timeslot. Cet algorithme tire de manière aléatoire différentes valeurs de temporisateur pour chaque station.

La figure 3.7 illustre la variation de la fenêtre de contention (CW) et du compteur d'échec d'émission (DC) en fonction du nombre de retransmissions. Ces valeurs évoluent depuis une valeur initiale jusqu'à une valeur seuil, qui indique généralement un souci global du réseau sur lequel la station veut transmettre.

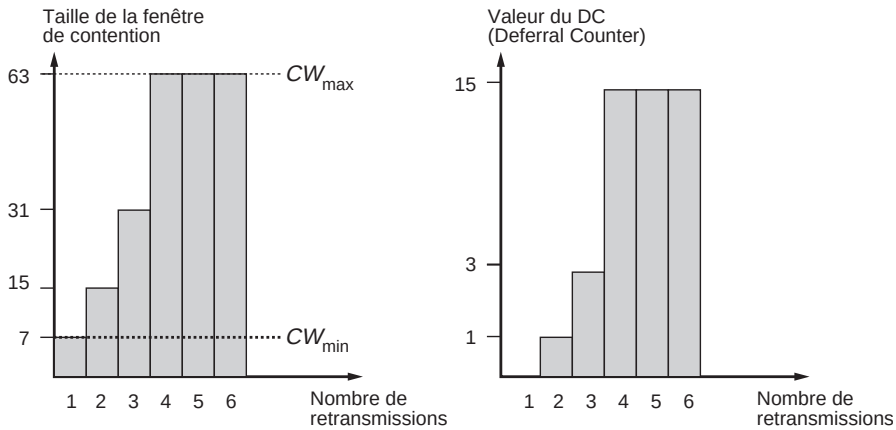


Figure 3.7

Variation de la taille de la fenêtre de contention en fonction de l'algorithme de back-off

Quand le support redevient libre, et après un CIFS et la phase de priorisation des trames, les stations vérifient que le support est toujours libre. Si tel est le cas, elles décrémentent leurs temporisateurs timeslot par timeslot jusqu'à ce que le temporisateur d'une station expire. Si le support est toujours libre, cette station transmet ses données, interdisant l'accès au support aux autres stations, lesquelles bloquent leurs temporisateurs.

La procédure de back-off peut être utilisée même lorsqu'il ne se produit pas de collision. Une station incrémente son BPC (Backoff Procedure Counter) dès qu'une collision est détectée ou lorsque le BPC atteint zéro. Pendant le back-off, si une autre station transmet d'abord, la station vérifie son DC (Defferal Counter) et le décrémente jusqu'à zéro. Après avoir décrémenté son DC, une station bloque son temporisateur à la valeur de BPC.

Une fois la transmission de la station terminée, les autres stations attendent toujours pendant un CIFS et la phase de priorité en vérifiant l'occupation du support avant et après le CIFS puis décrémentent à nouveau leurs temporisateurs là où elles l'avaient bloqué jusqu'à ce qu'une autre station transmette des données. Elles ne tirent toutefois pas de nouvelle valeur de temporisateur. En effet, comme elles ont déjà attendu pour accéder au support, elles ont plus de chance d'y accéder que les stations qui commencent leur tentative.

Si le DC atteint zéro, toutes les stations en attente de transmettre doivent passer par une procédure de back-off et reporter la transmission de leurs données.

Lors du calcul du temporisateur, il se peut que deux stations ou davantage tirent la même valeur de temporisateur, lequel expire donc en même temps, entraînant une émission simultanée sur le support et provoquant une collision. Après la procédure de back-off, les stations réinitialisent donc l'algorithme de back-off pour une nouvelle transmission si nécessaire, en obtenant une nouvelle valeur de *CW* et de DC. Si une station reçoit une trame de bonne réception (ACK), ces valeurs sont réinitialisées à leur valeur minimale.

Si *CW* et DC atteignent leur valeur maximale définie par le standard HomePlug 1.0, ces valeurs sont maintenues, même si le BPC est décrémenté.

Comme expliqué précédemment, lorsque l'algorithme est utilisé, les stations d'un même réseau ont la même probabilité d'accéder au support. Le seul inconvénient de cet algorithme est qu'il ne garantit aucun délai minimal. Il est donc difficile à utiliser dans le cadre d'applications temps réel telles que la voix ou la vidéo.

TDMA et l'accès au support dans HomePlug AV

L'algorithme CSMA/CA ne garantissant pas un délai minimal de transmission, le standard HomePlug AV, une extension de HomePlug 1.0, implémente une allocation des timeslots de transmission fondée sur le système d'accès au support TDMA (Time Division Multiple Access).

Ce système d'accès au support permet une allocation déterministe des temps de transmission de chaque station. Cette allocation est gérée par l'équipement CCo, qui coordonne les accès au support des différentes stations du réseau.

☞

La figure 3.8 illustre la répartition temporelle des espaces de temps dans la technique de multiplexage TDMA. On voit que la base de temps d'une trame transmise est divisée en blocs TDMA, correspondant à des espaces de temps dédiés aux communications entre deux stations. Pendant le bloc TDMA1, par exemple, seules les stations 1 et 2 communiquent entre elles. Cela garantit l'organisation temporelle des communications sur le réseau CPL.

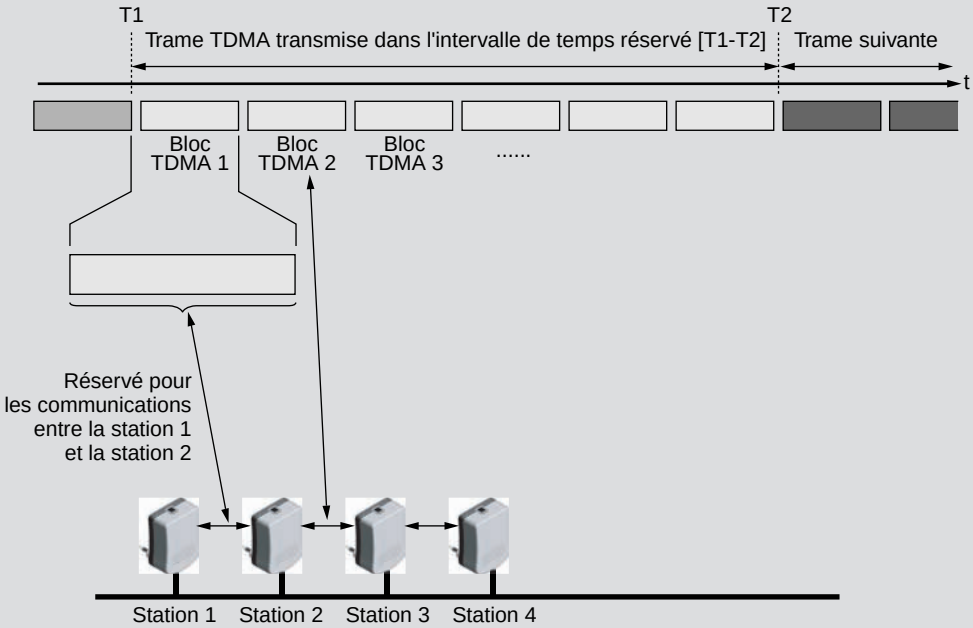


Figure 3.8

Répartition temporelle des espaces de temps TDMA d'une trame CPL

HomePlug AV spécifie donc des périodes temporelles déterminées, correspondant à deux périodes du signal électrique 220 V/50 Hz synchronisées sur des passages par zéro du signal. Ces zones temporelles TDMA sont divisées en plusieurs allocations temporelles déterminées et fixes. Une des allocations temporelles est réservée aux trames CSMA/CA et à l'échange de trames aux standards HomePlug 1.0 et HomePlug AV.

Exemple de transmission de données

Lorsqu'une station source veut transmettre des données à une station destination, elle vérifie que le support est libre. Si aucune activité n'est détectée pendant une période de temps correspondant à un CIFS, la station source attend la période de priorisation puis transmet ses données.

La figure 3.9 illustre le rôle des temporisateurs lors de la transmission d'une trame de données et de son acquittement.

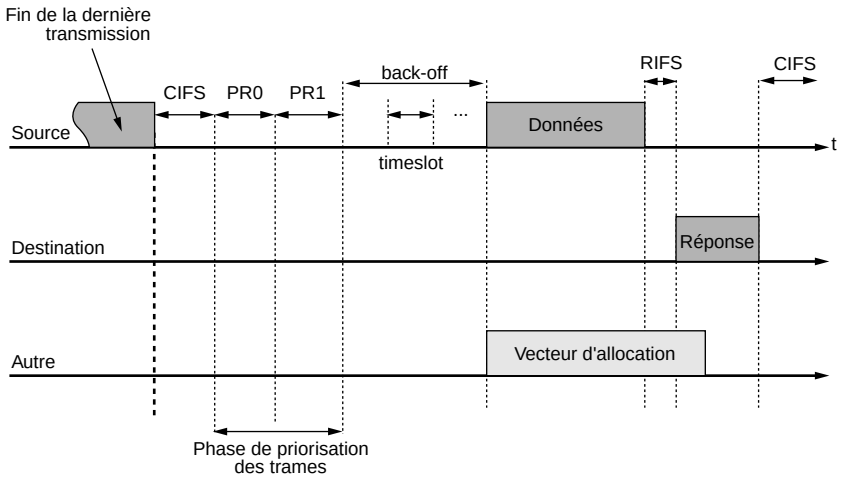


Figure 3.9

Rôle des temporisateurs dans la transmission des données

Si le support est occupé, la station attend qu'il se libère. Une fois le support libéré, la station attend pendant un CIFS puis, après avoir vérifié que le support est libre, initie l'algorithme de back-off pour retarder une fois encore sa transmission afin d'éviter toute collision. Lorsque le temporisateur de l'algorithme de back-off expire, et pour autant que le support soit libre, la station source transmet ses données vers la station destination.

Lorsque deux stations ou davantage accèdent en même temps au support, une collision se produit. Ces stations réutilisent en ce cas l'algorithme de back-off pour accéder au support. Si les données envoyées sont reçues correctement – la station destination vérifie pour le savoir le CRC de la trame de données –, la station concernée attend pendant un intervalle de temps RIFS et émet un ACK pour confirmer la bonne réception.

Si cet ACK n'est pas détecté par la station source ou si les données ne sont pas reçues correctement ou encore si l'ACK n'est pas reçu correctement, on suppose qu'une collision s'est produite, et la procédure de retransmission est initiée.

Le processus ARQ (Automatic Repeat reQuest)

Lorsqu'une station source transmet ses données sur le support, elle attend une trame d'acquittement de la part de la station destination. Cette trame est potentiellement suivie d'une procédure de retransmission des données non reçues ou erronées, appelée ARQ (Automatic Repeat reQuest).

La station destination peut renvoyer trois types de trames d'acquittement :

- **ACK.** La station destination a bien reçu les données contenues dans les trames, et ces dernières sont correctes.

- **NACK.** La station destination a bien reçu les données, mais certaines d'entre elles sont endommagées. Cette vérification s'effectue à l'aide de la valeur du CRC (Cyclic Redundancy Check). La station destination demande alors à la station source de renvoyer le segment de données endommagé.
- **FAIL.** Les données ne sont pas arrivées à la station destination, ou le tampon de celle-ci est plein et ne permet pas de les accueillir et de les traiter.

La figure 3.10 illustre, en représentation temporelle, les différents types de réponses d'acquittement dans le standard CPL HomePlug 1.0. Ce processus améliore la qualité de l'accès au support en permettant des échanges entre les stations sources et les stations destination.

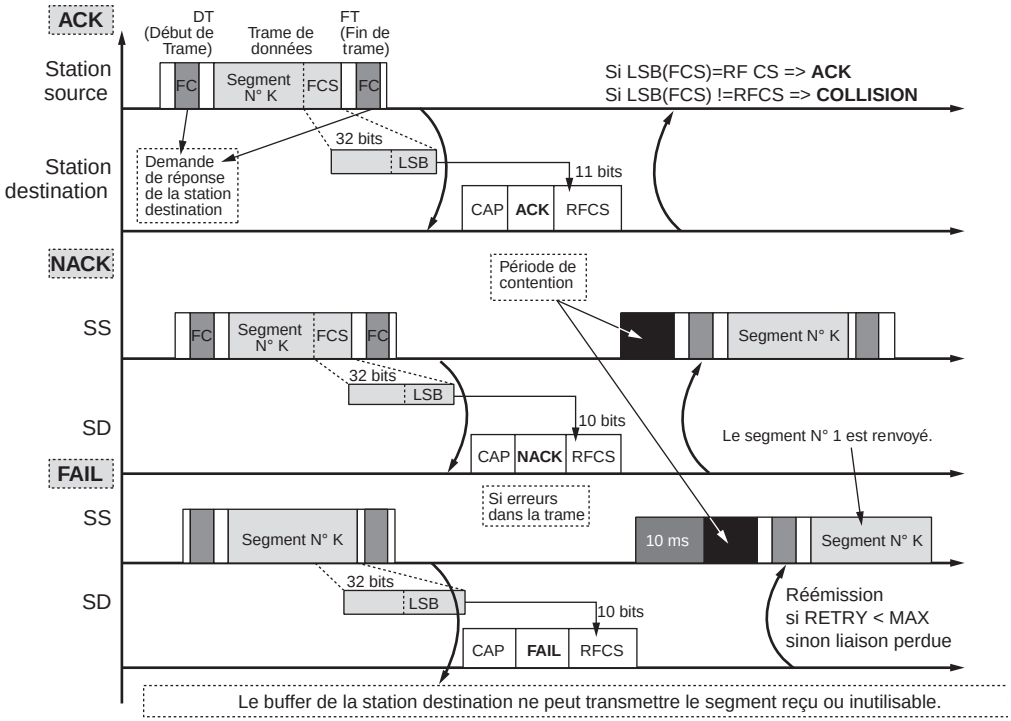


Figure 3.10

Trames d'acquittement dans le processus ARQ

Pour déterminer la trame de réponse qui va être renvoyée vers la station source, les stations source et destination utilisent un des champs présents dans la trame de données. Appelé FCS (Frame Check Sequence), ce champ permet de vérifier l'intégrité des données reçues par la station destination.

De la même manière, la station destination renvoie l'acquittement avec une partie de ce champ, le champ RFCS (Response FCS). Ce dernier permet à la station source de savoir

si les données ont été reçues correctement en comparant le FCS transmis et le RFCS reçu (*voir la figure 3.11*.)

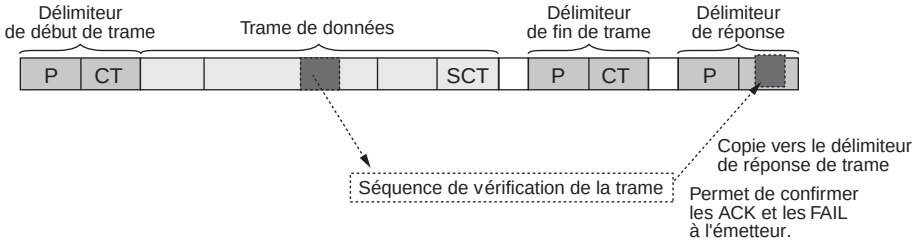


Figure 3.11

Vérification de la trame au moyen des champs FCS et RFCS dans le processus ARQ

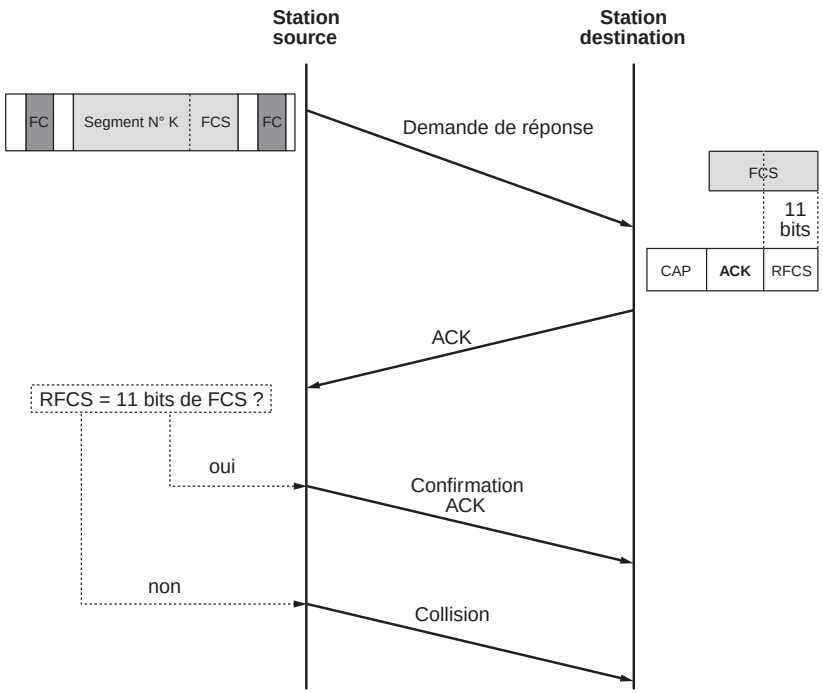
La réponse ACK

En cas d'acquittement de type ACK par la station source, la station destination lui renvoie une trame de réponse contenant le champ RFCS de la trame de données transmise par la station source. Ce champ permet à cette dernière de savoir si les données ont été correctement reçues par la station destination ou si une collision s'est produite, collision qui peut être à l'origine d'une corruption des données transmises sur le support.

La figure 3.12 illustre ce mécanisme d'acquittement dans le standard HomePlug 1.0.

Figure 3.12

Acquittement de type ACK dans HomePlug 1.0



La réponse NACK

En cas d'acquittement de type NACK, la station destination renvoie vers la station source une trame de réponse après une période de contention, afin d'indiquer que les données ont été endommagées lors de la transmission. La station source renvoie à son tour à la station destination une confirmation de l'acquittement NACK et retransmet le segment de la trame de données endommagé (*voir figure 3.13*).

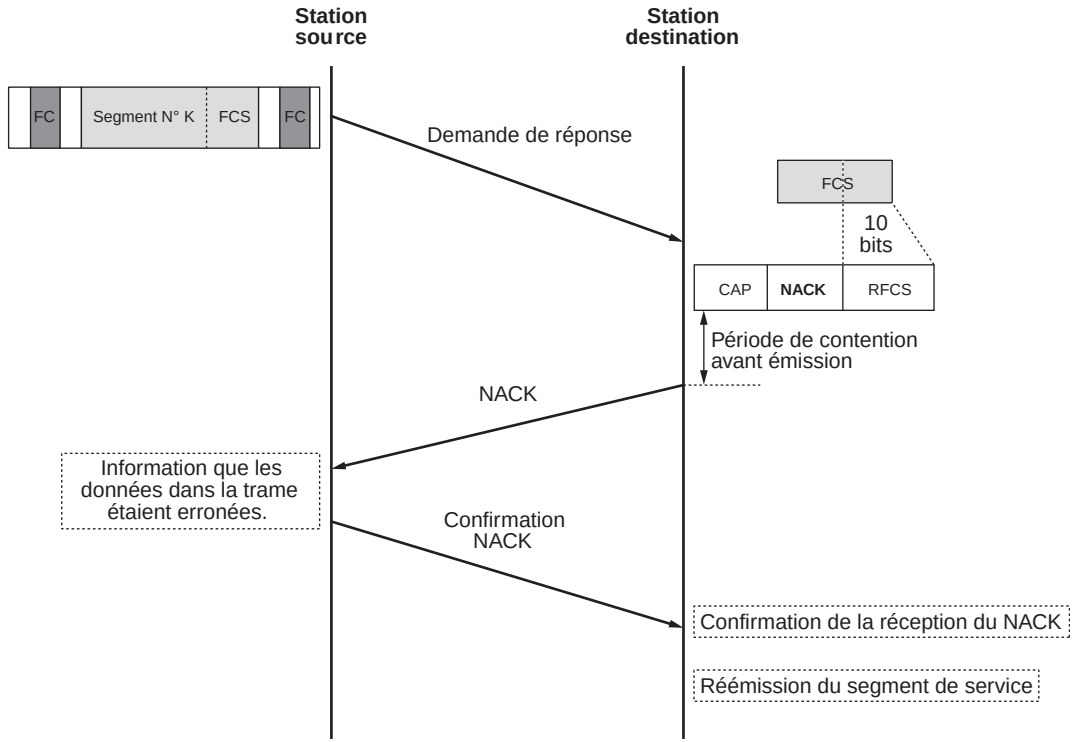


Figure 3.13

Acquittement de type NACK dans HomePlug 1.0

La réponse FAIL

La réponse FAIL indique que la station destination n'a pu utiliser la trame de données reçue du fait d'une collision ou d'une congestion du tampon de réception des données. En effet, la station destination ne peut prévoir le débit de données qu'elle va recevoir et peut se trouver dans la situation de ne pas pouvoir stocker toutes les données reçues.

Une période de contention propre aux réponses FAIL de 10 ms est obligatoire dans ce cas *(voir figure 3.14).*

La station destination enregistre le nombre de fois que le statut FAIL a été mis sur le segment. Si ce nombre dépasse un certain seuil, la station destination demande à la station source de renvoyer le bloc de services depuis le premier segment.

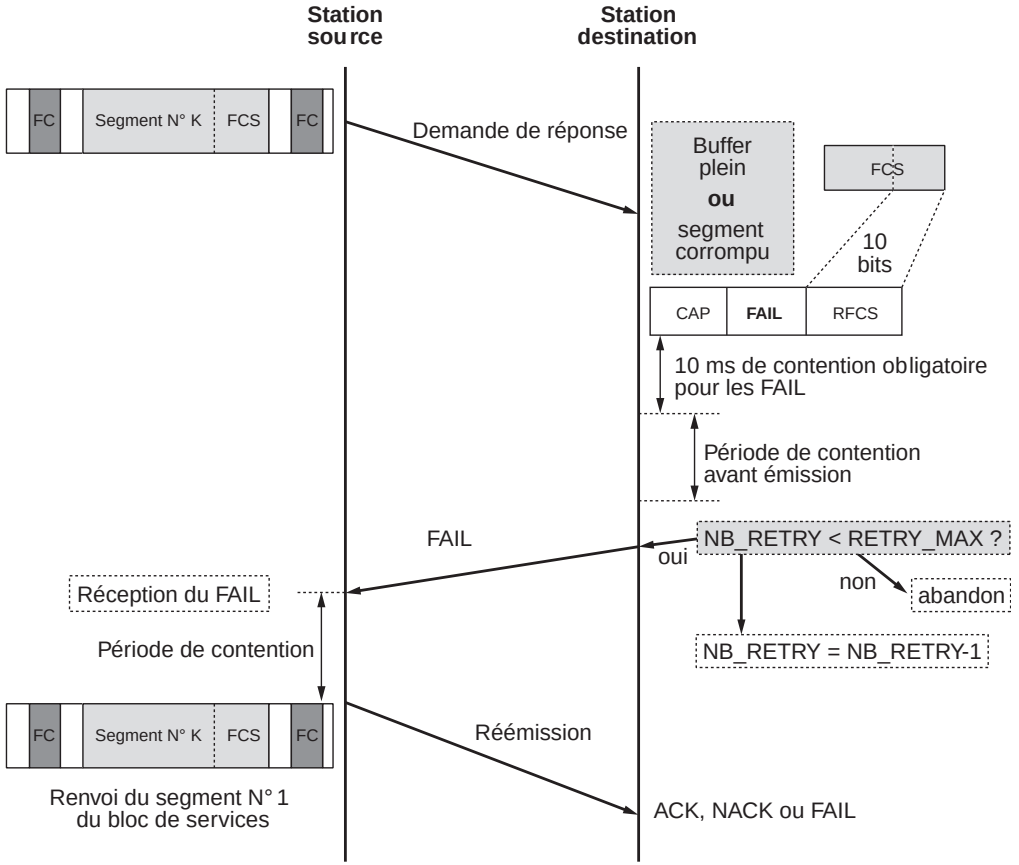


Figure 3.14
Réponse FAIL dans HomePlug 1.0

La réponse SACK dans HomePlug AV

Dans la version AV du standard HomePlug, une réponse supplémentaire, la réponse SACK (Selective ACK), a été ajoutée pour pallier le fait que les liaisons CPL entre deux stations ne sont pas forcément symétriques en terme de débit utile. Du fait des caractéristiques du réseau électrique, en effet, les transmissions de données ne subissent pas les mêmes influences dans un sens et dans l'autre. La réponse SACK est utilisée par l'équipement central du réseau CPL, le CCo, pour gérer les Global Links, c'est-à-dire les différents liens entre stations CPL du réseau, et les allocations de temps de transmission dans le cadre de la technique d'accès au média TDMA.

Synchronisation et contrôle des trames

Le contrôle des trames s'effectue grâce au champ FCS, qui est inclus dans le bloc de données de la trame. Ce champ est utilisé par la station destination pour renvoyer le type de réponse approprié (ACK, NACK ou FAIL) à la station source.

La station source vérifie alors l'intégrité de cette réponse grâce au champ RFCS de la trame de réponse, comme l'illustre la figure 3.15.

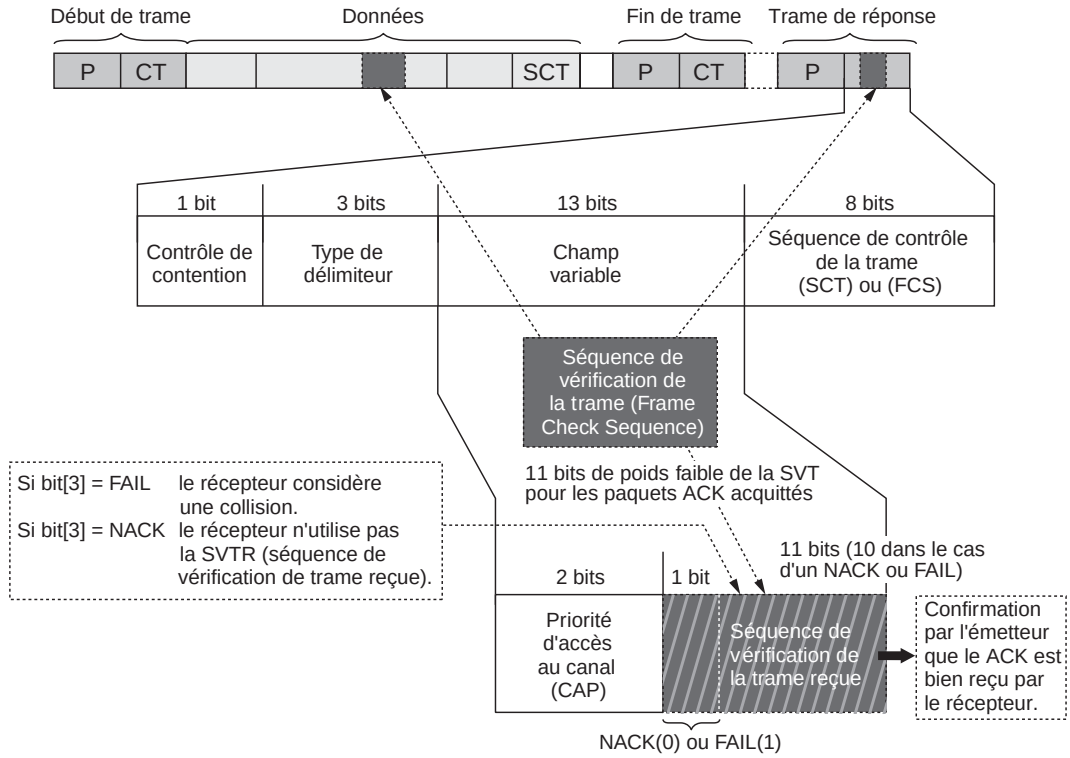


Figure 3.15

Séquence de vérification de la trame (FCS)

La trame de réponse est envoyée par la station destination après une période intertrame minimale de 26 µs et maximale de 1 695 µs *(voir figure 3.16)*. La trame de réponse étant d'une taille définie beaucoup plus courte que les trames de données, elle a beaucoup plus de chances d'être transmise et n'occupe que très peu de la bande passante totale.

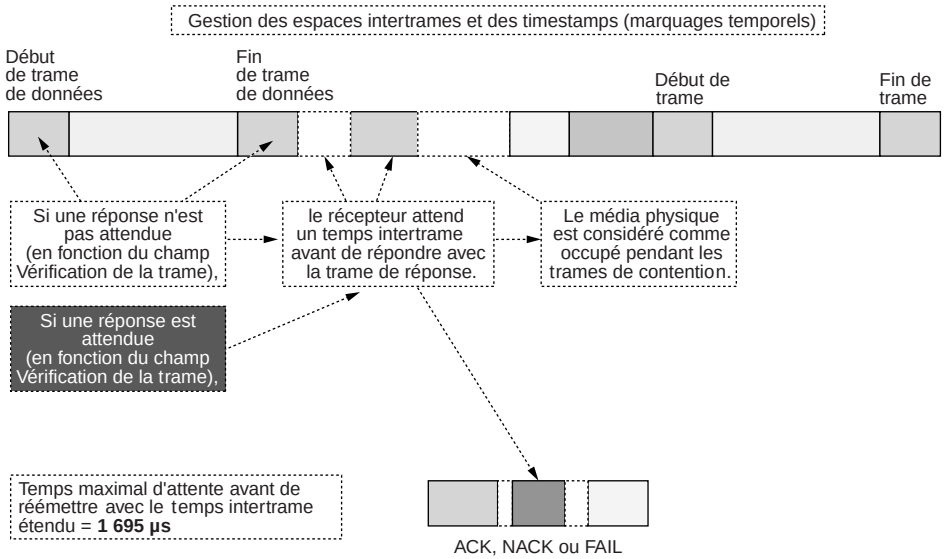


Figure 3.16

Gestion des espaces intertrame

Synchronisation des trames HomePlug AV

Les récents développements des CPL ont permis d'améliorer les performances des équipements, tout en conservant l'interopérabilité avec les équipements des versions antérieures. Au sein du consortium HomePlug, les derniers développements ont permis de publier les spécifications de la version HomePlug AV (pour Audio et Vidéo), qui est beaucoup plus performante pour la gestion de la qualité de service (QoS).

La figure 3.17 illustre l'organisation des trames balises *(beacon)*, dans HomePlug AV. Fondé sur une architecture maître-esclave, ce standard utilise les fonctionnalités d'accès au média de CSMA et de TDMA. CSMA est privilégié pour les trafics de données moyennement ou non prioritaires, et TDMA pour les trafics de données prioritaires, pour lesquels la QoS est importante (flux de données temps réel, comme dans la VoIP, ou flux de données importants, comme dans la VoD).

La gestion de la QoS est obtenue par le biais d'une technique très performante, propre aux technologies CPL, qui consiste à synchroniser des trames balises TDMA sur le signal 50 Hz du réseau électrique. Ce signal parfaitement déterministe est synchronisé sur l'ensemble du réseau EDF public et des réseaux électriques privés. Il est donc possible d'obtenir une synchronisation des équipements CPL sans horloge spécifique, en utilisant les passages par zéro du signal 50 Hz.

Cette technique permet d'atteindre les déterminismes performants nécessaires aux communications de données critiques. Le maître du réseau CPL gère les allocations d'accès aux slots TDMA entre les équipements esclaves du réseau en fonction de leur besoin.

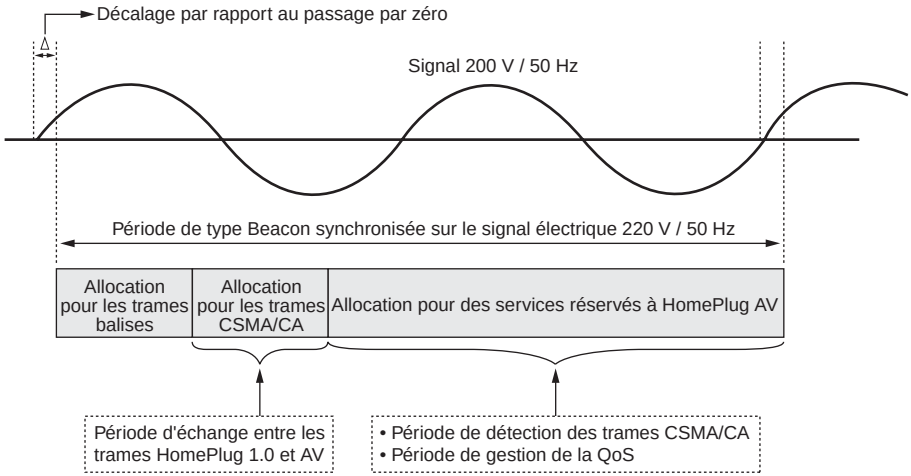


Figure 3.17

Synchronisation des trames balises HomePlug AV sur le signal 50 Hz

Gestion des priorités des trames

La gestion de la priorité des trames pour l'accès au média est assurée par le champ CAP (Channel Access Priority) et par la taille de la fenêtre de contention *(CW)*, comme l'illustre la figure 3.18.

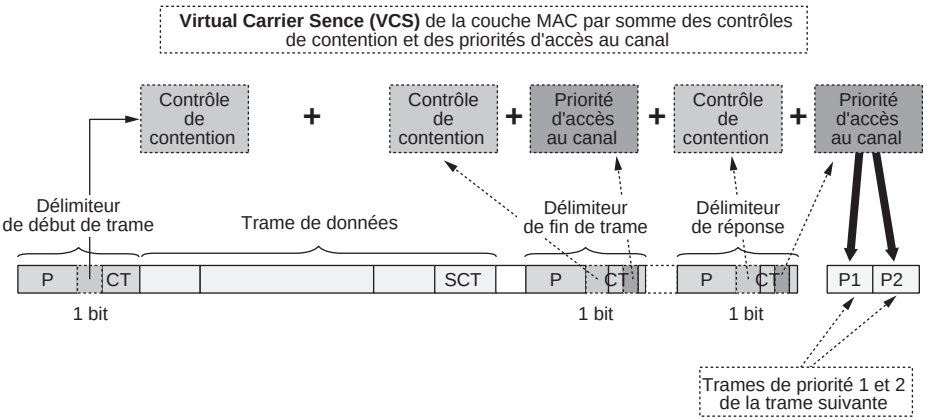


Figure 3.18

Gestion de la priorité des trames par la variable CAP (Channel Access Priority)

La variable CAP influence l'accès au média, comme nous l'avons vu à la figure 3.7, où les paramètres *CW* et DC sont fixés par la procédure de back-off et donnés par le tableau de correspondance en fonction des valeurs de CAP respectives des équipements CPL du réseau.

La variable CAP est utilisée par une station CPL pour informer les autres stations de sa priorité d'accès au média. Cette variable fixe les valeurs des données des trames de priorités PRP1 et PRP2, qui sont lues par les stations CPL du réseau pour connaître les différents niveaux de priorité. Les autres stations sont donc informées en avance de la priorité de chacun des équipements CPL.

L'ensemble de ce processus, appelé VCS (Virtual Carrier Sense), est utilisé en conjonction avec le PCS (Physical Carrier Sense) lors des tentatives d'accès au média.

Gestion des canaux de fréquences (Tone Map)

Comme nous l'avons vu précédemment, il existe plusieurs techniques de modulation des symboles OFDM en fonction de la qualité des liens CPL entre les équipements. À la différence de Wi-Fi, où chaque station peut configurer le canal de fréquences sur lequel elle désire transmettre des données, dans les CPL, toute la bande de fréquences est utilisée.

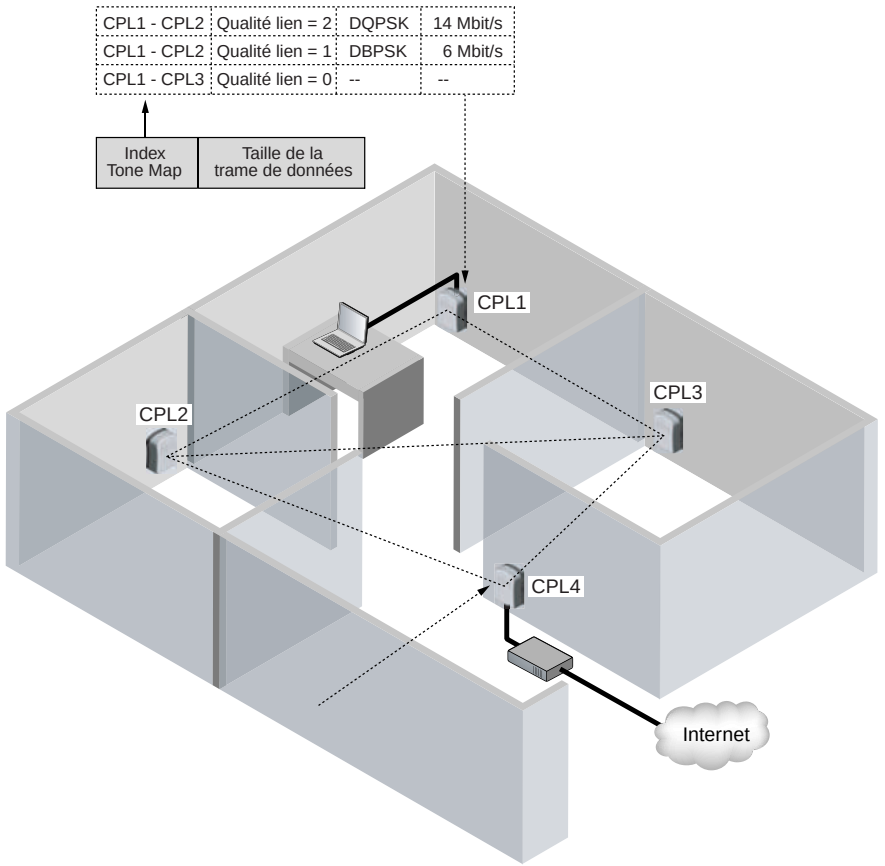


Figure 3.19
Gestion des Tone Maps entre équipements CPL

La figure 3.19 illustre un réseau simple, avec quatre stations CPL. Chacune d'elles évalue la qualité du lien CPL qui la relie aux autres stations. Elle stocke ensuite cette information dans la table de correspondance d'un registre de l'équipement CPL. Ce registre peut être accédé grâce à l'un des champs délimiteurs de début de trame, dit Tone Map. Chacune des stations remet à jour régulièrement la table Tone Map, le temps de remise à jour pouvant varier de 10 ms à plusieurs secondes, selon les paramétrages des stations CPL.

Il peut arriver que certaines stations se voient au niveau CPL, alors que d'autres ne se voient pas. Il est important que les stations qui servent de passerelle vers d'autres réseaux voient toutes les stations concernées par cet autre réseau. Par exemple, dans le cas de la figure 3.19, CPL1 ne peut accéder à Internet, car si les liens sont bons vers CPL2 et CPL3, le canal de transmission est inutilisable vers CPL4. Si le câble électrique est trop long ou que le réseau électrique soit trop perturbé, cela entraîne une atténuation et une dégradation du signal CPL rendant impossible les communications de données des couches supérieures.

La figure 3.20 illustre tous les champs du délimiteur de début de trame. Dans le champ variable, les cinq premiers bits sont utilisés par la table Tone Map. Cette Tone Map permet de stocker l'état des liens vers quinze autres stations CPL. Cela détermine la limite du nombre de stations CPL possibles dans un même réseau CPL (16 stations pour HomePlug 1.0 et 1.1, 250 stations dans HomePlug AV). Certaines valeurs sont réservées pour le mode ROBO ou pour des implémentations particulières du standard HomePlug 1.0.

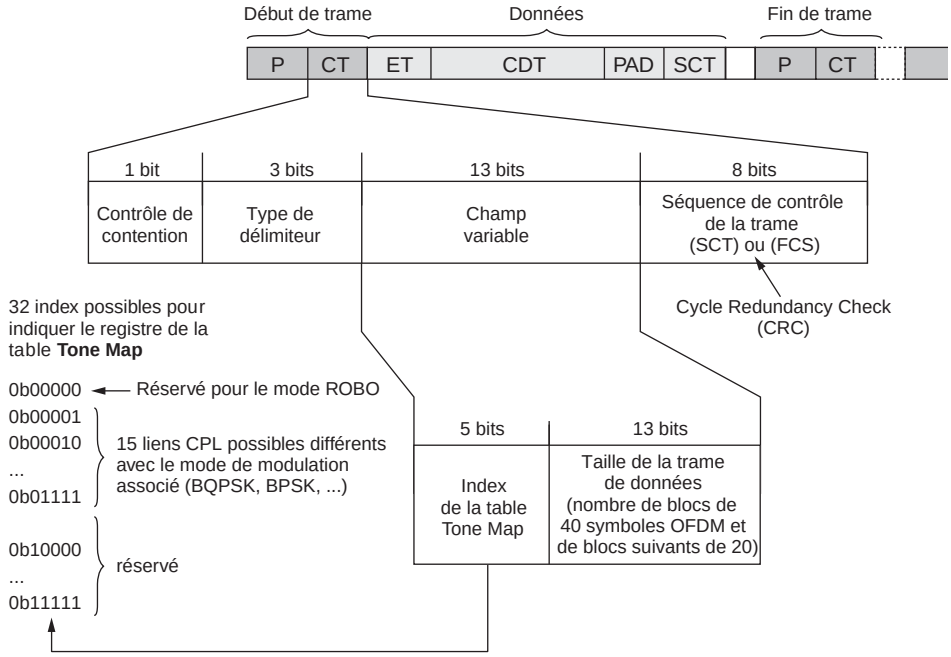


Figure 3.20

Détails du délimiteur de début de trame HomePlug 1.0 et Tone Map associée

Segment Bursting et Contention-Free Access

Deux modes particuliers, le Segment Bursting et le Contention-Free Access, permettent d'accéder à une plus grande priorité sur le réseau CPL afin d'envoyer les segments successifs d'un bloc de services sans attendre les fenêtres de contention obligatoires avant d'émettre les trames.

Dans le cas du Segment Bursting, des stations CPL de niveau de priorité CA3 peuvent mettre le paramètre CC (Contention Control) à la valeur 1. Il est alors possible pour la station source d'émettre deux segments consécutifs sans attendre de grande valeur de contention. Ce mode améliore les performances et peut se révéler utile pour des applications de type VoIP demandant une exception de priorité particulière.

La figure 3.21 illustre la fonctionnalité de Segment Bursting qui permet à un équipement CPL de transmettre avec la priorité maximale (CA3) une suite de blocs de services.

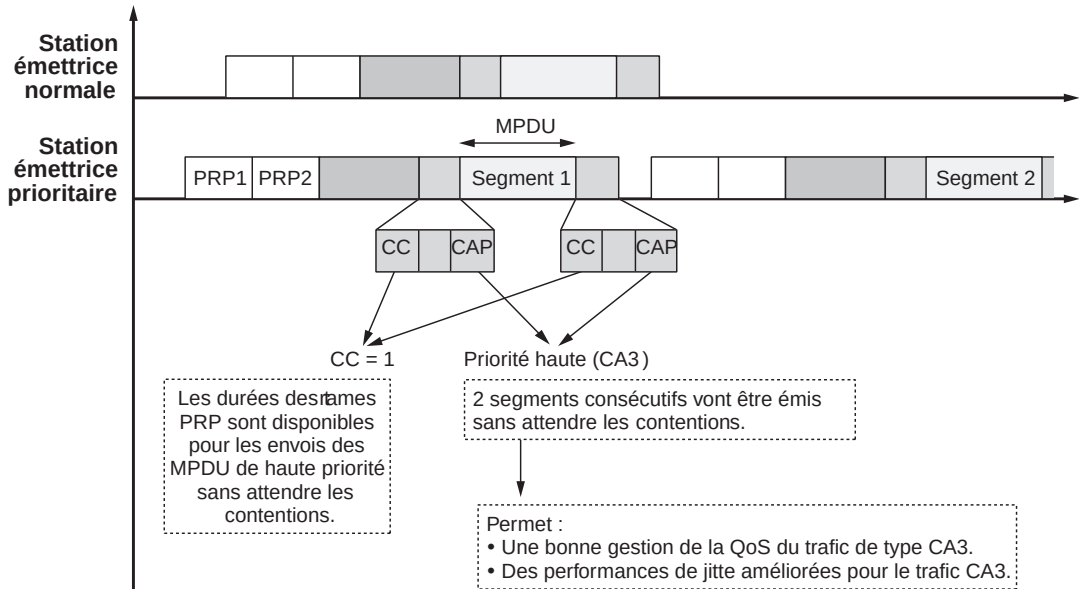


Figure 3.21

Gestion du mode Segment Bursting

Dans le cas du Contention Free Access (CFA), la station source est autorisée à émettre tous les segments de priorité CA3 et à transmettre sept MPDU consécutives en plaçant le champ CC à 1.

Fonctionnalités de niveau trame

Pour comprendre les fonctionnalités proprement réseau des technologies CPL, il est important de rappeler la structure des trames de données qui sont transportées sur le réseau électrique.

La modélisation des réseaux en sept couches selon le modèle OSI permet de comprendre comment les technologies CPL articulent les échanges de données au niveau de chaque couche protocolaire. Les technologies CPL interviennent uniquement au niveau de la couche PHY et de la couche MAC, ce qui leur permet d'être vues de leurs interfaces comme des réseaux Ethernet IEEE 802.3. Les ingénieurs réseau n'ont dès lors plus qu'à considérer les configurations IP, TCP et applicatives vues de l'utilisateur des technologies CPL.

La figure 3.22 illustre la position des technologies CPL au regard des couches du modèle OSI.

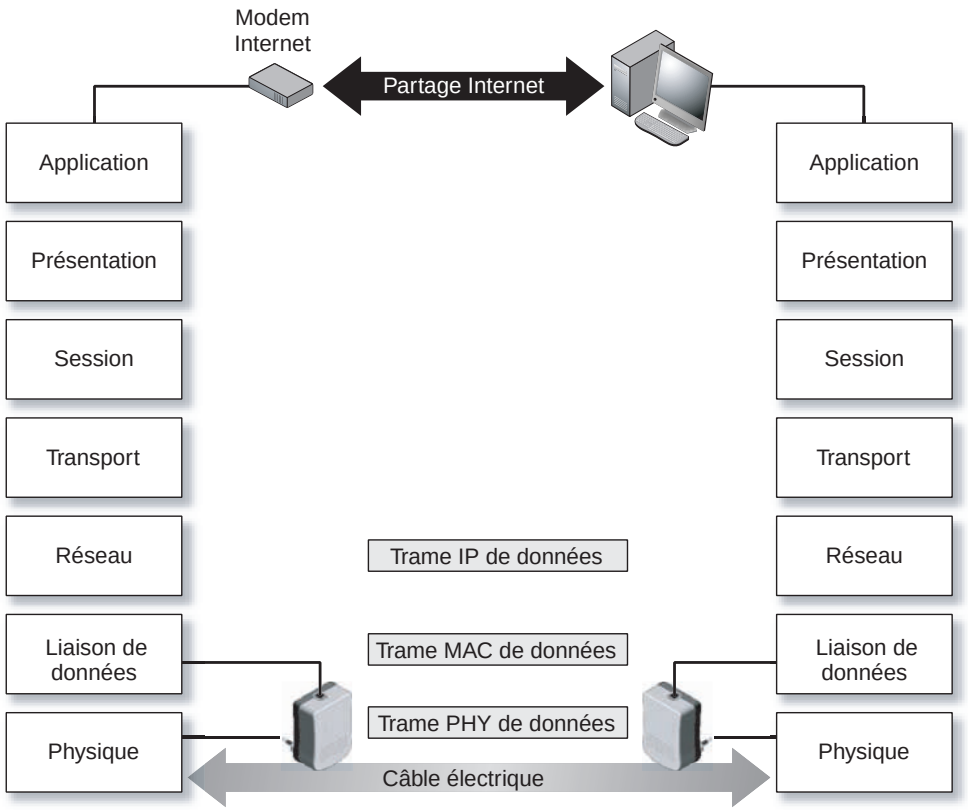


Figure 3.22
Technologies CPL et modèle OSI

Encapsulation MAC

Contrairement aux trames IEEE 802.11, qui constituent le socle des couches protocolaires des technologies Wi-Fi, les trames CPL peuvent être considérées comme des encapsulations MAC.

La figure 3.23 illustre l'encapsulation MAC des trames CPL HomePlug 1.0.

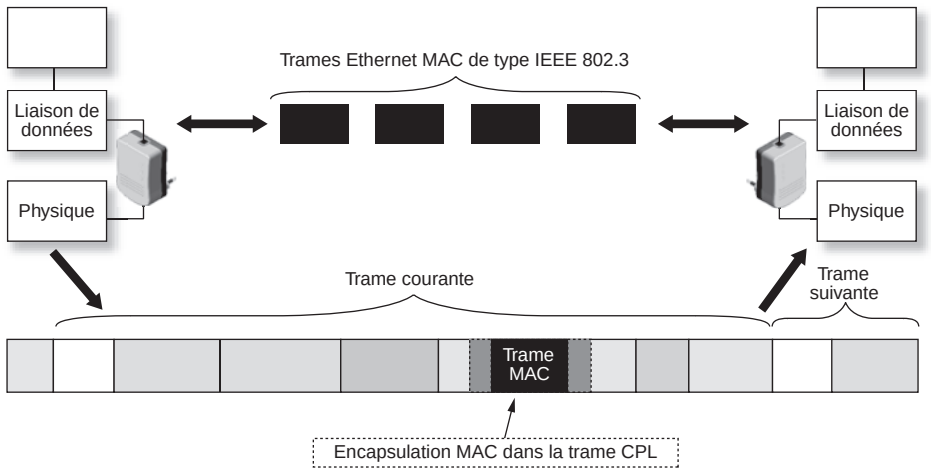


Figure 3.23

Encapsulation MAC dans HomePlug 1.0

Du point de vue de la couche liaison de données, les trames Ethernet MAC sont désencapsulées des trames physiques pour être présentées au niveau de l'interface Ethernet des équipements CPL.

Fragmentation-réassemblage

Dans une transmission CPL, qui utilise un média partagé et perturbé par d'autres usages, avec une liaison Ethernet filaire, utilisant un câble dédié à l'usage des communications de données, le taux d'erreur sur les câbles électriques est plus important (10^{-5} pour les câbles électriques contre 10^{-9} pour le câble Ethernet).

Le lien CPL peut être soumis à différentes contraintes, telles que l'affaiblissement du fait d'interférences, le multitrajet sur les câbles électriques, les effets de diaphonie entre câbles électriques. Ces contraintes ont pour effet d'atténuer la puissance du signal, ce qui ne permet plus au lien CPL de délivrer correctement l'information.

Un taux d'erreur élevé entraîne la retransmission de toutes les données erronées envoyées sur le réseau. Cette retransmission engendre un coût important en terme d'utilisation de la bande passante, surtout lorsque les données envoyées ont une taille importante.

Pour éviter un trop grand gaspillage de bande passante, on utilise un mécanisme de fragmentation, qui permet de réduire le nombre de retransmissions dans des environnements fortement bruités comme les CPL

La fragmentation

Les trames de données des couches réseau (IP, etc.) ou supérieures sont vues par la couche liaison de données comme des successions de MPDU (Mac Protocol Data Unit) formant des BS (blocs de services). Les BS sont ensuite découpés en morceaux de 1 500 octets au maximum, appelés segments.

Un segment peut donc faire 1 500 octets ou moins. Dans ce dernier cas, il est rempli de bits de bourrage pour obtenir une MPDU de taille fixe. La taille de 1 500 octets correspond à 160 symboles OFDM au niveau de la couche physique.

Chacun des segments formant le BS est numéroté, de façon à être reconnu, permettant de reconstituer le BS émis par la station source (Source Address au niveau MAC) vers la station destination (Destination Address).

La figure 3.24 illustre les différents segments envoyés par la station source et numérotés afin d'être repérés par la station destination. Comme nous le verrons avec les fonctionnalités ARQ de la couche MAC, si un des segments du BS n'arrive pas à la station destination ou arrive endommagé, des processus de NACK (Non Acknowledgment) ou FAIL (Failure) sont mis en place entre la station source et la station destination, préludant à la réémission des segments manquants ou endommagés.

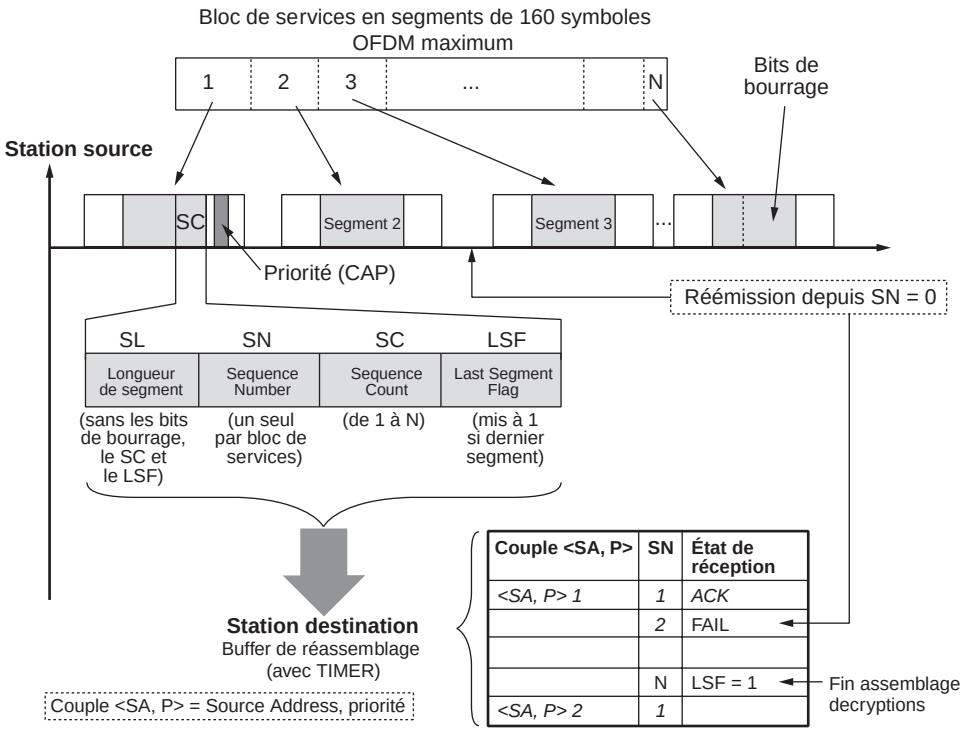


Figure 3.24

Fragmentation des trames de données

Le réassemblage

Lors de leur réception, les segments sont mis en tampon et indexés dans le buffer de réassemblage de la station destination avec l'adresse de la station et la priorité. Une fois tous les segments d'un BS arrivés, le bloc de données est désencapsulé et transmis aux couches supérieures du modèle OSI. Les BS forment ensuite des trames IP, avec des entêtes TCP ou UDP.

Le buffer de réassemblage peut dès lors être vidé pour permettre la réception des trames suivantes. La taille du buffer est destinée à favoriser la vitesse de transmission maximale sur le canal de transmission. Cependant, la nature de l'accès au média (CSMA) n'étant pas déterministe, le buffer ne peut anticiper la vitesse de transmission des segments et peut se trouver dans une situation de saturation, où il ne peut plus accepter de segments supplémentaires. Il demande alors à la station source de réémettre plus tard les segments non traités.

Autres fonctionnalités

Les CPL implémentent d'autres fonctionnalités réseau afin d'optimiser l'utilisation du canal de transmission, notamment en terme de vitesse de transmission des données.

Cette optimisation est atteinte en utilisant une adaptation dynamique du débit de données au niveau physique, en fonction de la qualité des liens CPL.

L'utilisation de la bande passante globale peut être également optimisée en n'envoyant les données que vers les équipements CPL concernés. Ces dernières fonctionnalités rejoignent celles que l'on retrouve dans d'autres technologies réseau, telles que Wi-Fi.

Variation dynamique du débit

Comme indiqué précédemment, la technologie CPL réajuste en permanence l'état des liens entre stations du réseau.

Les liens CPL dépendant de l'état du média et des interférences avec les autres équipements électriques connectés ou inducteurs sur le réseau, la vitesse de transmission doit être réajustée en permanence par le choix du mode de modulation des symboles OFDM formant les trames.

Pour l'utilisateur, le débit utile entre les terminaux connectés au réseau CPL varie dynamiquement en fonction des liens CPL.

Le tableau 3.5 recense les différentes vitesses de transmission, ou débit PHY, des équipements CPL du standard HomePlug 1.0 en fonction de la Tone Map établie pour chaque station vis-à-vis des autres stations du réseau.

Tableau 3.5 Débits dynamiques du standard HomePlug 1.0

Technique de modulation	Paramètre de l'encodeur	FEC (taux de codage du code convolutionnel)	Débit PHY (Mbit/s)	
DQPSK	23/39 à 238/254	$^3/_4$	14,1	139 débits PHY possibles, entre 0,9 et 14
DQPSK	23/39 à 238/254	$^1/_2$	9,1	
DBPSK	23/39 à 238/254	$^3/_4$	4,5	
ROBO (DBPSK)	31/39 à 43/51	$^1/_2$	0,9	

Unicast, broadcast et multicast

Dans la mesure où les CPL peuvent être vues comme des techniques d'encapsulation MAC, les divers modes d'envoi des trames MAC, qu'ils soient unicast, broadcast ou multicast, sont autorisés.

Dans le mode unicast, une station du réseau transmet des données vers une seule autre station à l'aide de son adresse MAC. En mode broadcast, au contraire, une station transmet ses données vers toutes les stations du réseau en utilisant une adresse MAC dédiée à ce mode et comprenant tous les bits à 1. En mode multicast, une station transmet à un groupe d'autres stations du réseau, en utilisant une seule adresse MAC pour l'ensemble du groupe de stations. Il faut pour cela avoir prédéfini le groupe de stations avec les adresses MAC associées. Les adresses MAC multicast utilisent un préfixe afin d'être reconnues sur le réseau. Ce préfixe utilise les vingt-quatre premiers bits (sur 48) de l'adresse MAC.

Comme nous le verrons au chapitre 5, les modes broadcast et multicast sont supportés grâce au flag multicast (sur un bit) du champ de contrôle de bloc de la trame de données MPDU.

Le mode unicast est également possible dans la mesure où les stations CPL étant identifiées par leur adresse MAC, si une station connaît l'adresse MAC d'une autre station, elle peut adresser les MPDU directement et uniquement à cette station.

Qualité de service

Devenue très importante dans les réseaux IP, la qualité de service permet de différencier les priorités des différents trafics sur le réseau. Comme nous le verrons au chapitre 6, les services IP demandent des contraintes différentes en terme de vitesse de transmission, de délai de parcours du réseau et de jitte entre les trames transmises sur le réseau.

Ces contraintes sont déterminantes pour les applicatifs comme pour les couches supérieures du modèle OSI que ce soit pour maintenir une connexion TCP pour des trafics HTTPS, une connexion FTP, etc.

Il est donc nécessaire d'implémenter des niveaux de priorités pour les trames de niveau physique et de niveau MAC en fonction des contraintes des applications des couches

supérieures. Cela doit s'effectuer dans les trames, dans la mesure où le média est partagé, à la manière d'un concentrateur réseau de niveau MAC.

La qualité de service est rendue possible dans les réseaux CPL grâce aux priorités des équipements du réseau. Ces dernières sont indiquées par le paramètre CAP, qui est interprété dans les périodes de résolution des priorités (PRP1 et PRP2), qui se situent juste avant les trames de contention.

La figure 3.25 illustre les niveaux de priorité (CA0, CA1, CA2 et CA3) présents dans les périodes de résolution de priorités PRP1 et PRP2. Le bit de contention compris dans le délimiteur de fin de trame et dans les trames de réponse permet de prioriser les trames par rapport à celles des stations de même priorité ou de priorité inférieure.

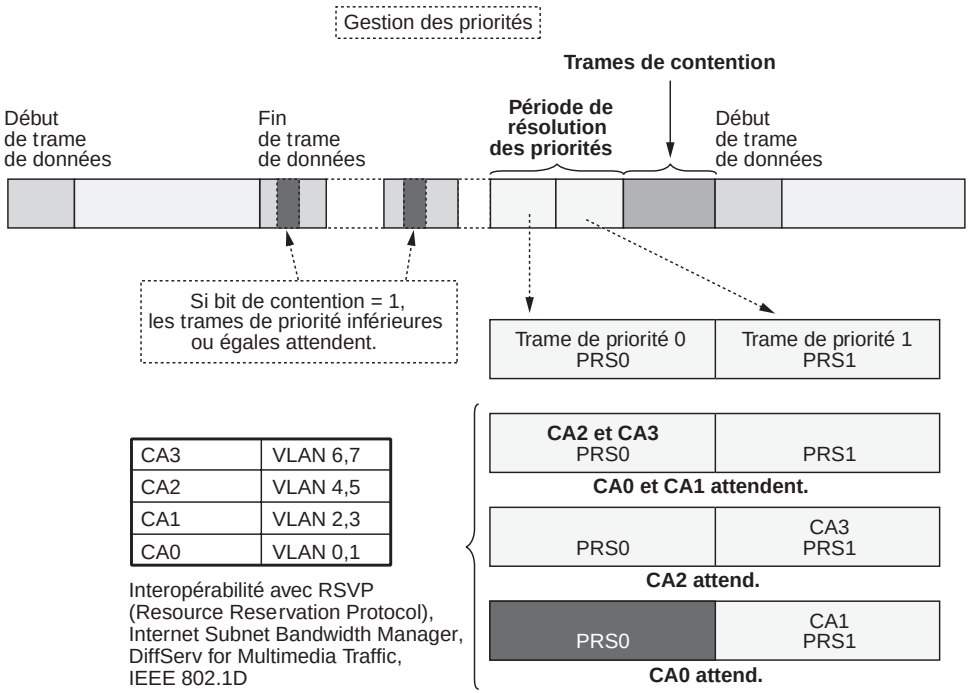


Figure 3.25
Gestion de la qualité de service

Utilisation des étiquettes VLAN

L'utilisation des étiquettes VLAN est compatible avec les technologies CPL, car la valeur de ces étiquettes est interprétée dans la valeur du paramètre CAP de la station CPL.

Un des avantages des technologies CPL est de permettre la création de réseaux virtuels à plusieurs niveaux des couches OSI (réseaux virtuels CPL, réseaux VLAN,

surcouches MAC, etc.), offrant une grande souplesse aux intégrateurs de réseaux CPL.

Les étiquettes VLAN permettent d'implémenter un certain nombre de services IP pour différents niveaux de trafic de données et d'applications, notamment les suivants :

- RSVP (ReSerVation Protocol)
- Internet Subnet Bandwidth Manager
- DiffServ for Multimedia Traffic
- IEEE 802.1D

4

Sécurité

La sécurité a été le principal point faible des réseaux Wi-Fi. Dans le cas des CPL, ce souci est beaucoup moins présent du fait de la difficulté d'accès au média physique. En effet, dans Wi-Fi, le support de transmission étant radio, quiconque se trouvant dans la zone de couverture du réseau peut en intercepter le trafic ou même reconfigurer le réseau à sa guise. Si le câble électrique des CPL est également un support partagé par les différents équipements du réseau, il est beaucoup plus difficile d'accès et présente des dangers importants du fait de la présence du signal 220 V/50 Hz.

Cependant, le réseau électrique étant étendu « universellement », les câbles propagent le signal CPL hors des limites du réseau électrique privé, que ce soit de manière conduite ou rayonnée, ce qui implique d'implémenter des niveaux de sécurité logicielle adéquats.

Il est possible de sécuriser les réseaux CPL actuels de la même manière que les réseaux fixes filaires haut débit. L'ajout de serveurs d'authentification ou de tunnels sécurisés, par exemple, permet d'éliminer toute menace.

La sécurité est un enjeu important pour le déploiement des réseaux locaux en entreprise, où l'application de téléphonie IP ne cesse de se développer. Dans un tel contexte, il est essentiel de disposer de mécanismes de sécurité fiables, sous peine de voir toutes les communications écoutées.

Problématique générale de la sécurité réseau

Comme tout autre réseau, les CPL peuvent être soumis à différents types d'attaques, soit pour en perturber le fonctionnement, soit pour intercepter les informations transmises. L'avantage des réseaux CPL vient toutefois du support qu'ils utilisent, le câble électrique, qui les rend particulièrement résistants aux attaques puisque difficilement accessibles.

Cependant, pour éviter toute divulgation d'information, le trafic réseau doit être chiffré, de manière que quiconque n'appartenant pas à un réseau logique CPL ne puisse le récupérer et le déchiffrer.

Outre l'écoute clandestine, les principales attaques auxquelles peut être soumis un réseau sont celles qui visent à l'empêcher de fonctionner, jusqu'à le voir s'effondrer, ou à y accéder et à le reconfigurer à sa guise.

Les seules parades à ces types d'attaques sont la cryptographie, qui empêche les intrus d'accéder aux données échangées dans le réseau, l'authentification, qui permet l'identification et l'autorisation de toute personne voulant émettre des données, et le contrôle de l'intégrité, qui permet de savoir si les données envoyées n'ont pas été modifiées pendant la transmission.

La cryptographie

Le fait de rendre un texte ou un message incompréhensible grâce à l'utilisation d'un algorithme n'est pas nouveau. Les Égyptiens comme les Romains utilisaient des méthodes permettant de coder un texte ou un message. Ces techniques, relativement simples à l'origine, ont évolué, et c'est depuis la Seconde Guerre mondiale que la cryptographie a conquis le statut de science.

Le principe de base de la cryptographie est illustré à la figure 4.1. Une clé de cryptage est utilisée pour coder un texte en clair. Le texte chiffré est alors envoyé au destinataire. Ce dernier utilise une clé de décryptage afin de reconstituer le texte en clair. À tout moment pendant la transmission, un individu peut récupérer le texte chiffré, appelé cryptogramme, et essayer de le déchiffrer par diverses méthodes.

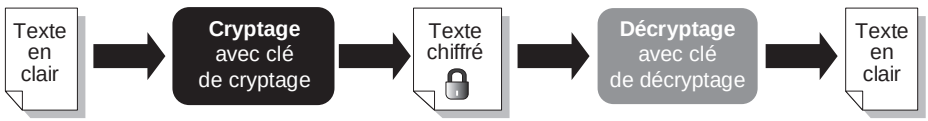


Figure 4.1
Chiffrement des données

> **Cryptologie**
>
> La cryptographie ne s'attelle qu'à la conception et aux méthodes de cryptage. L'action de chercher à déchiffrer un texte chiffré s'appelle la cryptanalyse. La cryptologie désigne pour sa part l'étude de la cryptographie et de la cryptanalyse.

En France, il existe une réglementation stricte sur la longueur des clés utilisées pour le chiffrement. Une clé d'une longueur maximale de 40 bits peut être utilisée pour tout usage public ou privé. Pour l'utilisation privée, la longueur de la clé ne peut excéder 128 bits. Pour une longueur de clé supérieure à 128 bits, la clé doit être transmise à la DCSSI (Direction centrale de la sécurité des systèmes d'information).

Il existe deux techniques de cryptographie, la cryptographie à clé symétrique et la cryptographie à clé asymétrique, plus connue sous le nom de cryptographie à clé publique.

La cryptographie à clé symétrique

La cryptographie à clé symétrique est fondée sur l'utilisation d'une clé unique, qui permet à la fois de chiffrer et de déchiffrer les données. Toutes les personnes voulant se transmettre des données de manière sécurisée doivent donc partager un même secret : la clé. Ce processus est illustré à la figure 4.2.

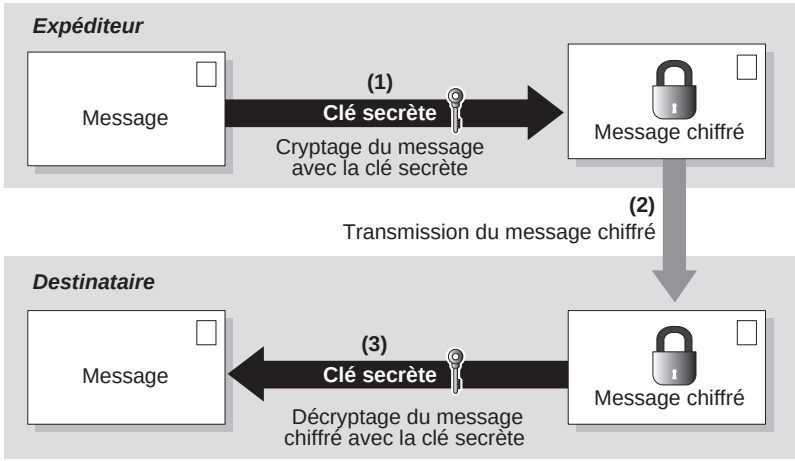


Figure 4.2
Cryptographie à clé symétrique

La faille de ce système réside évidemment dans la manière dont cette clé secrète partagée est transmise entre l'émetteur et le récepteur.

Différents algorithmes de cryptographie à clé symétrique ont été développés, notamment DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), la série RC2 à RC6 et AES (Advanced Encryption Standard).

DES (Data Encryption Standard)

L'algorithme DES a été développé dans les années 70 conjointement par IBM et la NSA (National Security Agency). Le DES est un algorithme de chiffrement dit par bloc. La longueur de la clé utilisée est fixe, 40 ou 56 bits. Le rôle du DES est d'effectuer un ensemble de permutations et de substitutions entre la clé et le texte à chiffrer de façon à coder l'information.

Le mécanisme de chiffrement suit plusieurs étapes :

1. Le texte à chiffrer est fractionné en blocs de 64 bits (8 bits sont utilisés pour le contrôle de parité).

2. Les différents blocs sont soumis à une permutation dite initiale.
3. Chaque bloc est divisé en deux parties de 32 bits : une partie droite et une partie gauche.
4. Seize rondes sont effectuées sur les demi-blocs. Une ronde correspond à un ensemble de permutations et de substitutions. À chaque ronde, les données et la clé sont combinées.
5. À la fin des seize rondes, les deux demi-blocs droit et gauche sont fusionnés, et une permutation initiale inverse est effectuée sur les blocs.

Une fois tous les blocs chiffrés, ils sont réassemblés afin de créer le texte chiffré qui sera envoyé sur le réseau. Le déchiffrement s'opère dans l'ordre inverse du chiffrement en utilisant toujours la même clé.

Le DES était jusqu'à récemment la référence en matière de cryptographie à clé symétrique. De nombreux systèmes l'utilisaient et l'utilisent encore actuellement. Le protocole d'échange d'information sécurisé par Internet SSL (Secure Sockets Layer) v1.0 l'utilise, par exemple, avec une clé de 40 bits.

Considéré cependant comme peu fiable, le DES n'est plus utilisé depuis 1998. Son algorithme de chiffrement a été repris et amélioré.

3-DES

3-DES, ou triple-DES, utilise trois DES à la suite. Les données sont donc chiffrées puis déchiffrées puis chiffrées avec deux ou trois clés différentes. La clé 3-DES peut avoir une taille de 118 bits, ce qui ne lui permet pas d'être utilisée en France. Le 3-DES est considéré comme raisonnablement sécurisé.

IDEA (International Data Encryption Algorithm)

IDEA (International Data Encryption Algorithm) est un algorithme d'une longueur de clé de 128 bits. Le texte à crypter est découpé en quatre sous-blocs. Sur chacun de ces sous-blocs, huit rondes sont effectuées. Chaque ronde est une combinaison de « ou » exclusif, d'addition modulo 2^{16} et de multiplication modulo 2^{16}. À chaque ronde, les données et la clé sont combinées. Cette technique rend l'IDEA particulièrement sécurisé.

L'algorithme IDEA est implémenté dans PGP (Pretty Good Privacy), le logiciel de cryptographie le plus utilisé au monde.

RC2

L'algorithme RC2 a été développé par Ron Rivest, d'où son nom de Ron's Code 2. Il s'appuie sur un algorithme par bloc de 64 bits et est deux voire trois fois plus rapide que le DES, avec une longueur de clé maximale de 2 048 bits.

L'algorithme est la propriété de RSA Security et est utilisé dans SSL v2.0.

RC4

Le RC4 (Ron's Code 4) n'utilise plus de bloc mais chiffre par flot. Sa spécificité réside dans l'utilisation de permutations pseudo-aléatoires pour chiffrer et déchiffrer les données.

Le RC4 définit deux mécanismes :

- **KSA (Key Scheduling Algorithm).** Génère, par des permutations simples, une table d'état en utilisant la clé de chiffrement.
- **PRGA (Pseudo-Random Generator Algorithm).** La table d'état générée par le KSA est placée dans un générateur de nombre pseudo-aléatoire, ou PRNG (PseudoRandom Number Generator), qui crée, par des permutations complexes, le flux de chiffrement, ou keystream.

Contrairement aux autres algorithmes, les données ne sont pas divisées en blocs afin d'être chiffrées ou déchiffrées. Dans le RC4, le chiffrement correspond à l'ajout des données au flux de chiffrement par un « ou » exclusif, tandis que le déchiffrement correspond à l'ajout des données chiffrées à ce même flux de chiffrement, toujours au moyen d'un « ou » exclusif.

Le RC4 est encore plus rapide que le RC2. Comme le RC2, il est la propriété de RSA Security. Le RC4 est utilisé dans SSL v2.0 et SSL v3.0 pour sécuriser les connexions ainsi que dans le protocole WEP de la série de standards 802.11 d'IEEE .

RC5 et RC6

Autre algorithme propriétaire de RSA Security, le RC5 est un algorithme de chiffrement par bloc, avec une taille de bloc variable, comprise entre 32 et 128 bits, un nombre de ronde variable, compris entre 0 et 255, et une longueur de clé dynamique, comprise entre 0 et 2 040 bits.

Le RC6 est une amélioration du RC5, dont il utilise les caractéristiques. La seule différence porte sur l'ajout de nouvelles opérations mathématiques au niveau des rondes.

Blowfish

Comme DES, Blowfish est un algorithme de chiffrement par bloc de 64 bits. Fondée sur le DES, sa clé a une taille variable, comprise entre 40 et 448 bits. Cet algorithme est particulièrement rapide et fiable.

Twofish

De la même manière que Blowfish, Twofish est un algorithme de chiffrement par bloc de 128 bits sur 16 rondes, avec une longueur de clé variable. Il est également à la fois fiable et rapide.

AES (Advanced Encryption Standard)

AES correspond à un appel d'offre lancé en 2000 par le NIST (National Institute of Standards and Technology) en vue de remplacer le DES, réputé peu fiable. Plusieurs algorithmes ont été proposés, comme le RC6 et Twofish, mais c'est Rijndael qui l'a emporté par sa simplicité et sa rapidité et qui porte désormais le nom d'AES.

AES est un algorithme par bloc de 128 bits, ou 16 octets, pour une clé de chiffrement, K, de 128, 192 ou 256 bits. Selon la taille de la clé, le nombre de rondes est respectivement de 10, 12 et 14.

Pour chaque ronde, AES définit quatre opérations simples :

- SubBytes, un mécanisme de substitution (S) non linéaire, qui est différent pour chaque bloc de données chiffré.
- ShiftRows, un mécanisme de permutation (P), qui décale les éléments du bloc.
- MixColumns, un mécanisme de transformation (M), qui effectue une multiplication entre les éléments du bloc de manière non pas classique mais dans un corps de Galois de type GF(2^8).
- AddRoundkey, un algorithme de dérivation de clé, qui définit à chaque ronde une nouvelle clé de chiffrement, Ki, où i correspond à la i-ème ronde, à partir de la clé de chiffrement K.

Avant d'être chiffrées, les données sont divisées en blocs de 128 bits. La première étape du chiffrement consiste à ajouter le bloc de données avec la clé de chiffrement par le biais d'un « ou » exclusif. Ensuite, chaque bloc subit dix rondes à la suite, constituées chacune d'une substitution (S), d'une permutation (P) et d'une transformation (M). À la fin de chaque ronde, une nouvelle clé de chiffrement est dérivée de la clé initiale, et le résultat de l'opération M est ajouté à cette clé, Ki, par un « ou » exclusif, le tout est envoyé à la ronde suivante. À l'issue de la dernière ronde, qui se passe du mécanisme de transformation M, le bloc de données est considéré comme chiffré.

Une fois que tous les blocs pour un message donné sont chiffrés, ils sont réassemblés afin de créer le message chiffré, qui peut alors être transmis sur le réseau. La procédure de chiffrement d'AES est illustrée à la figure 4.3.

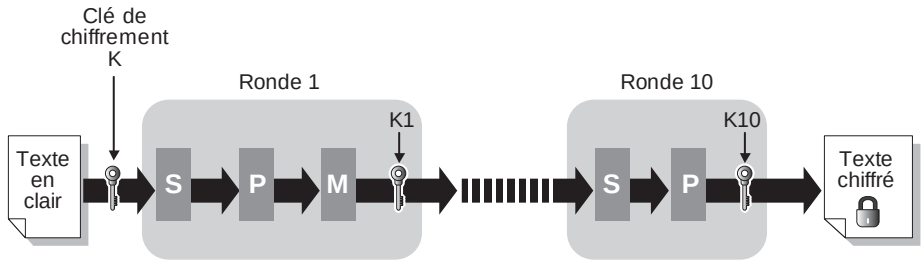


Figure 4.3
Chiffrement AES

Le déchiffrement est la fonction inverse du chiffrement, comme illustré à la figure 4.4.

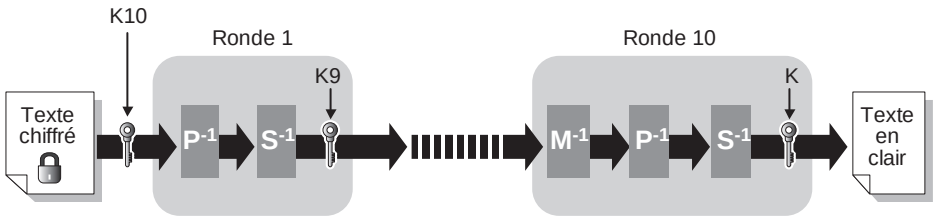


Figure 4.4
Déchiffrement AES

Utilisé par l'administration américaine en remplacement du DES, AES a aussi été choisi comme nouvel algorithme de chiffrement pour le standard IEEE 802.11i en remplacement du RC4.

La cryptographie à clé publique

La technique de cryptographie à clé publique résout le principal problème des clés symétriques, qui réside dans la transmission des clés.

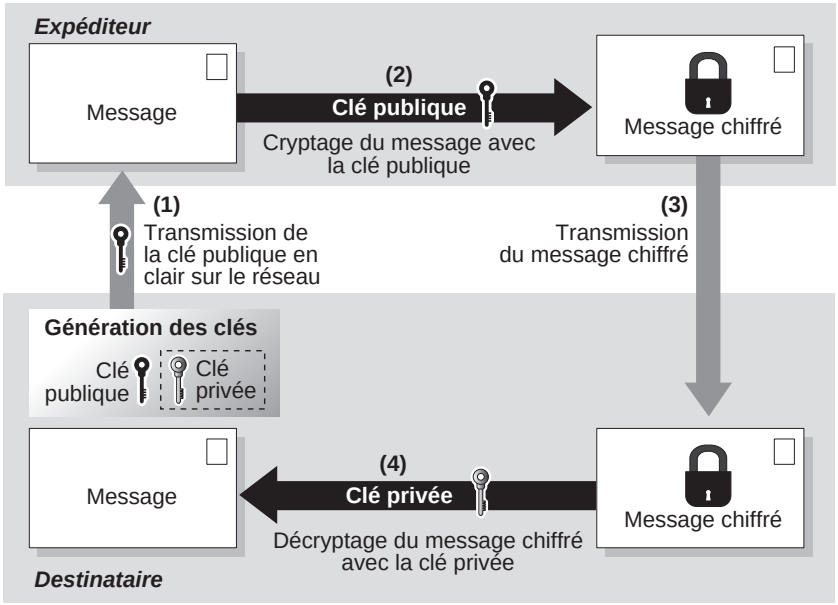


Figure 4.5
Cryptographie à clé publique

Dans la cryptographie à clé publique, deux types de clés sont utilisés :

- Une clé privée pour déchiffrer les données, qui doit rester confidentielle.
- Une clé publique, qui est laissée à la disposition de tous les utilisateurs. Cette clé permet de chiffrer les données.

Ces deux clés sont liées mathématiquement, de sorte qu'il est très difficile de trouver la valeur d'une des deux clés à partir de l'autre.

La clé publique est envoyée en clair sur le réseau pour être chiffrée. Dès que le destinataire reçoit les données chiffrées, il utilise sa clé privée pour les déchiffrer. Ce processus est illustré à la figure 4.5.

Comme dans la cryptographie à clé symétrique, différents algorithmes sont utilisés, notamment RSA (Rivest, Shamir, Adelman) et Diffie-Hellman.

Bien que cette technique permette de pallier la faiblesse de la cryptographie symétrique, à savoir la transmission de la clé, elle est beaucoup moins rapide que celle-ci.

RSA (Rivest, Shamir, Adelman)

Cet algorithme à clé publique porte le nom de ses trois inventeurs, Ron Rivest, Adi Shamir et Leonard Adelman. Créé en 1977, le RSA a été le premier algorithme à clé publique. Sa force réside dans une supposition portant sur la difficulté à factoriser de grands nombres.

RSA utilise des clés de longueur variable, de 512, 1 024 et 2 048 bits. Les clés de 512 bits sont considérées comme peu sûres. RSA est toujours utilisé aujourd'hui par SSL, IPsec et bien d'autres applications. Avec des longueurs de clé raisonnables, et jusqu'à de futures avancées mathématiques, le RSA est réputé fiable.

Diffie-Hellman

Cet autre algorithme à clé publique, inventé par Whitfield Diffie et Martin Hellman, a été le premier algorithme de chiffrement commercialisé. Étant vulnérable à certains types d'attaques, mieux vaut l'utiliser avec l'aide d'une autorité de certification.

Une de ses propriétés est de permettre de faire partager un secret à deux personnes sans nécessiter de transmission sûre. Il reste toujours utilisé aujourd'hui.

La cryptographie à clé mixte

La cryptographie à clé mixte, illustrée à la figure 4.6, fait appel aux deux techniques précédentes, à clé symétrique et à clé publique. Elle combine de la sorte les avantages des deux tout en évitant leurs inconvénients. Ces derniers sont bien connus, la cryptographie à clé symétrique ne permettant pas de transmission de clé sécurisée et

la cryptographie à clé publique utilisant des algorithmes trop lents pour le chiffrement des données.

Lors d'un envoi de données, l'expéditeur chiffre le message avec une clé secrète grâce à un algorithme à clé symétrique. Dans le même temps, il chiffre cette clé secrète avec la clé publique générée par le destinataire. La transmission de la clé secrète peut ainsi se faire de manière fiable et sécurisée.

Le chiffrement d'une clé secrète sur 128 bits avec un algorithme à clé publique est très rapide, compte tenu de la taille de cette clé. Le tout est ensuite transmis au destinataire. Ce dernier déchiffre la clé secrète de l'expéditeur à l'aide de sa clé privée. Le destinataire possède maintenant la clé secrète en clair et peut l'utiliser pour déchiffrer le message.

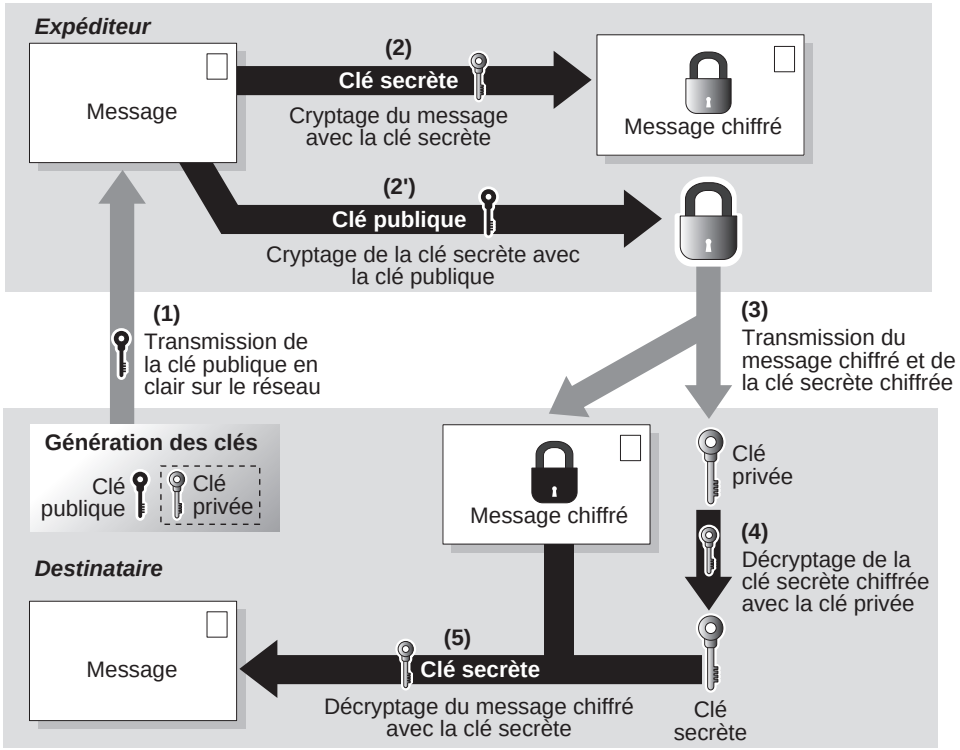


Figure 4.6
Cryptographie à clé mixte

Un autre avantage de cette technique est qu'il n'est plus nécessaire de chiffrer plusieurs fois un message lorsqu'il est destiné à plusieurs destinataires. Le message chiffré étant transmis avec sa clé secrète, il suffit de chiffrer cette clé avec les différentes clés publiques des destinataires.

La signature électronique

La signature électronique permet d'identifier et d'authentifier l'expéditeur des données. Elle permet en outre de vérifier que les données transmises sur le réseau n'ont pas subi de modification.

Différentes techniques permettent de signer un message à envoyer. L'une d'elles fait appel aux algorithmes à clé publique, mais les plus utilisées sont les fonctions de hachage.

Utilisation des clés publiques

Outre la confidentialité, l'avantage de la cryptographie à clé publique est qu'elle permet d'authentifier l'expéditeur d'un message. La signature électronique est la seconde utilisation des clés publiques.

Pour se faire authentifier, l'émetteur utilise sa clé privée pour signer un message. De son côté, le récepteur utilise la clé publique de l'émetteur pour vérifier si le message est signé. De cette façon, le récepteur peut vérifier tout à la fois que les données n'ont pas été modifiées et qu'elles ont bien été envoyées par l'émetteur.

La figure 4.7 illustre le fonctionnement de l'authentification par clé publique.

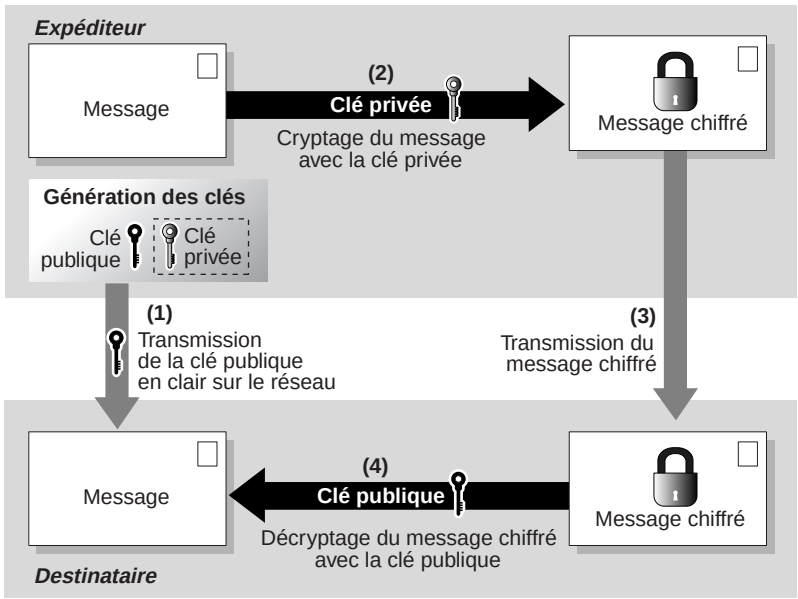


Figure 4.7
Authentification par clé publique

Si cette technique permet bien de signer les messages, elle n'en garantit pas pour autant la confidentialité, puisqu'il est possible d'intercepter le message chiffré et la clé publique et d'accéder au contenu des données.

La fonction de hachage

La fonction de hachage offre une solution de remplacement à l'utilisation de la signature grâce à des clés publique et privée.

Le rôle de la fonction de hachage est de créer une sorte d'empreinte numérique du message qui doit être envoyé. La taille de cette empreinte, appelée digest, est très petite comparée à celle du message. Une autre caractéristique de cette technique est qu'il est très difficile, voire impossible, de retrouver le message d'origine à partir de son empreinte. Cela garantit l'authenticité et l'intégrité du message envoyé.

La figure 4.8 illustre un expéditeur voulant envoyer un message tout en garantissant son authenticité. Il crée pour cela une empreinte du message par l'intermédiaire d'une fonction de hachage H. Le message et son empreinte sont envoyés au destinataire, qui applique la même fonction de hachage H au message reçu afin de comparer cette nouvelle empreinte et celle qu'il a reçue. Si les empreintes sont les mêmes, c'est que le message n'a pas été modifié.

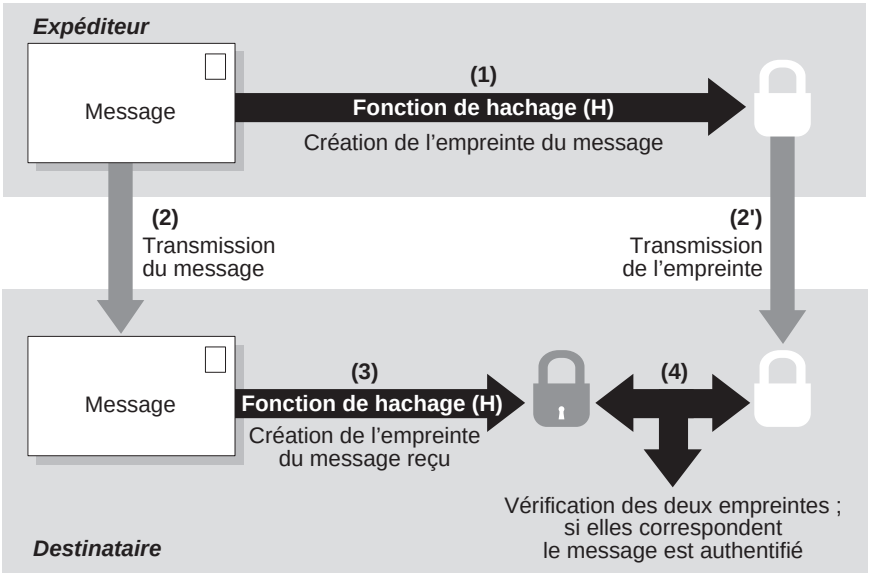


Figure 4.8
Hachage d'un message

MD5

On voit de plus en plus sur Internet des fichiers à télécharger accompagnés de leurs empreintes, généralement du MD5, destinées à vérifier l'intégrité des données reçues.

La fonction de hachage est souvent combinée avec la cryptographie à clé publique. Le processus est le suivant :

1. L'émetteur hache le message.
2. L'empreinte est chiffrée avec la clé privée de l'expéditeur.
3. Le message, la clé publique de l'expéditeur et l'empreinte chiffrée sont envoyés sur le réseau.
4. Le destinataire reçoit le message, qu'il hache à son tour pour en extraire une nouvelle empreinte.
5. Cette empreinte est comparée avec celle qu'il a reçue chiffrée, qu'il déchiffre grâce à la clé publique fournie par l'expéditeur.
6. Si les deux empreintes correspondent, le message est authentifié.

Ce processus est illustré à la figure 4.9.

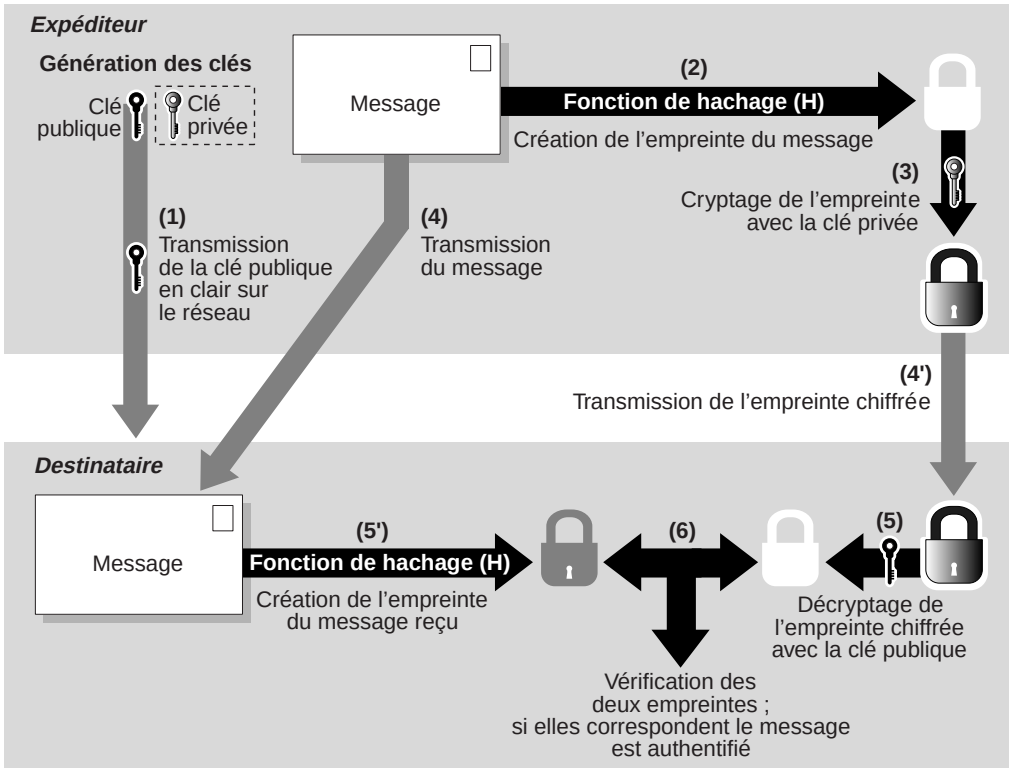


Figure 4.9
Hachage et clé publique

Différentes techniques de hachage sont utilisées, notamment les suivantes :

- **MD2, MD4 et MD5.** Message Digest 2, 4 et 5 ont été développés par Ron Rivest pour RSA Security. Ce sont des fonctions de hachage qui produisent toutes des empreintes d'une taille de 128 bits. Le MD2 est le plus fiable mais n'est optimisé que pour des machines 8 bits, alors que les deux autres le sont pour des machines 32 bits. MD4 a été abandonné car trop sensible à certaines attaques. MD5 est une évolution de MD4. Il est considéré comme fiable, même s'il est vulnérable à certaines attaques, et est utilisé dans de nombreuses applications. MD5 a été standardisé par l'IETF sous la RFC 1321.
- **SHA et SHA1.** Le SHA (Secure Hash Algorithm) et son évolution ont été développés par la NSA. Ces deux algorithmes produisent des empreintes de 160 bits pour un message pouvant atteindre une taille de deux millions de téraoctets. La taille de son empreinte le rend très difficile à percer, mais il est plus lent que MD5.

Les attaques réseau

De tout temps, les réseaux ont été soumis à différents types d'attaques. Les attaques peuvent être passives, comme dans le cas de l'écoute d'un réseau visant à récupérer des informations en « craquant » les différents mots de passe et clés de chiffrement. Dans d'autres cas, les attaques sont actives, l'attaquant tentant de prendre le contrôle de machines ou d'en détériorer certains équipements.

Les attaques les plus connues sont les suivantes :

- **Attaque par déni de service (DoS).** Parmi les plus redoutées, cette attaque consiste à inonder un réseau de messages afin que les équipements de ce dernier ne puissent plus les traiter, parfois jusqu'à s'effondrer.
- **Attaque par force brute.** Consiste à tester toutes les combinaisons possibles afin de récupérer un mot de passe ou une clé de chiffrement utilisés dans un réseau.
- **Attaque par dictionnaire.** Est utilisée pour récupérer un mot de passe ou une clé en recourant à une base de données contenant un grand nombre de mots.
- **Attaque par spoofing.** S'appuie sur l'usurpation d'une identité afin d'accéder au réseau. Est généralement associée aux attaques par force brute ou par dictionnaire, qui permettent d'accéder à certaines informations, comme les login et mot de passe d'un utilisateur.
- **Attaque sur l'exploitation des trous de sécurité.** De nombreux protocoles et systèmes d'exploitation sont vulnérables du fait de leur conception. Ces failles peuvent être utilisées soit pour permettre à l'attaquant de s'introduire dans la machine ou dans le réseau, soit pour prendre le contrôle de la machine ou récupérer des données.
- **Attaques par virus, vers et cheval de Troie.** Très connues, ces attaques permettent soit de détériorer des fichiers voire des composants de la machine, soit de prendre le contrôle d'une machine (virus et vers) et d'en exploiter les ressources (cheval de Troie).

La sécurité dans les CPL

Pour accroître la sécurité des réseaux CPL, HomePlug met en place un système de réseaux privés CPL fondé sur des clés de cryptage connues des équipements CPL autorisés dans ce réseau.

Ce mécanisme repose sur l'enregistrement des différents équipements CPL d'un même réseau logique de manière sécurisée, fiable et simple pour l'utilisateur ou l'administrateur réseau. Ces fonctionnalités facilitent le déploiement de réseaux CPL.

Les principales caractéristiques de l'enregistrement d'un équipement CPL sur un réseau CPL sont les suivantes :

- **Sécurité.** Un équipement ne peut s'enregistrer sur un réseau CPL que s'il dispose des clés de cryptage suffisantes et qu'il soit autorisé et enregistré par les équipements gestionnaires du réseau. Il doit être possible d'associer facilement de nouveaux équipements mais également de supprimer rapidement des équipements d'un réseau CPL.
- **Fiabilité.** Un même réseau CPL doit offrir une stabilité dans la configuration des clés de cryptage et supporter de manière stable les connexions/déconnexions électriques des équipements CPL du réseau. Il doit être également possible de récupérer une configuration originelle en cas de perte de clés ou de déconfiguration d'un équipement.
- **Simplicité.** Il doit être simple pour un administrateur réseau de gérer la configuration des clés de cryptage des différents réseaux logiques CPL. HomePlug 1.0 et Turbo définissent pour cela une seule clé permettant de crypter les échanges de données sur le réseau électrique. Plus élaboré, HomePlug AV définit plusieurs clés réseau, dont la gestion est assurée par l'équipement coordinateur du réseau assurant la centralisation des clés.

Un réseau logique CPL repose donc sur une clé de cryptage, appelée NEK (Network Encryption Key) dans la spécification HomePlug, qui chiffre les données échangées entre les différents équipements CPL *(voir figure 4.10).*

La configuration d'un réseau CPL avec une clé NEK peut s'effectuer de plusieurs manières :

- **Par l'interface Ethernet.** Une trame de configuration de la clé NEK est envoyée en broadcast aux équipements CPL d'un même réseau à l'aide d'un outil de configuration. Tous les équipements CPL connectés par le biais de leur interface Ethernet récupèrent cette configuration.
- **Par l'interface électrique.** Une trame de configuration de la clé NEK est envoyée par le biais du réseau électrique aux équipements CPL connectés. Cette opération n'est possible qu'à condition de connaître une seconde clé, appelée DEK (Default Encryption Key). Propre à chaque équipement CPL, cette clé est inscrite dans la mémoire de l'équipement par le constructeur en suivant les spécifications HomePlug.

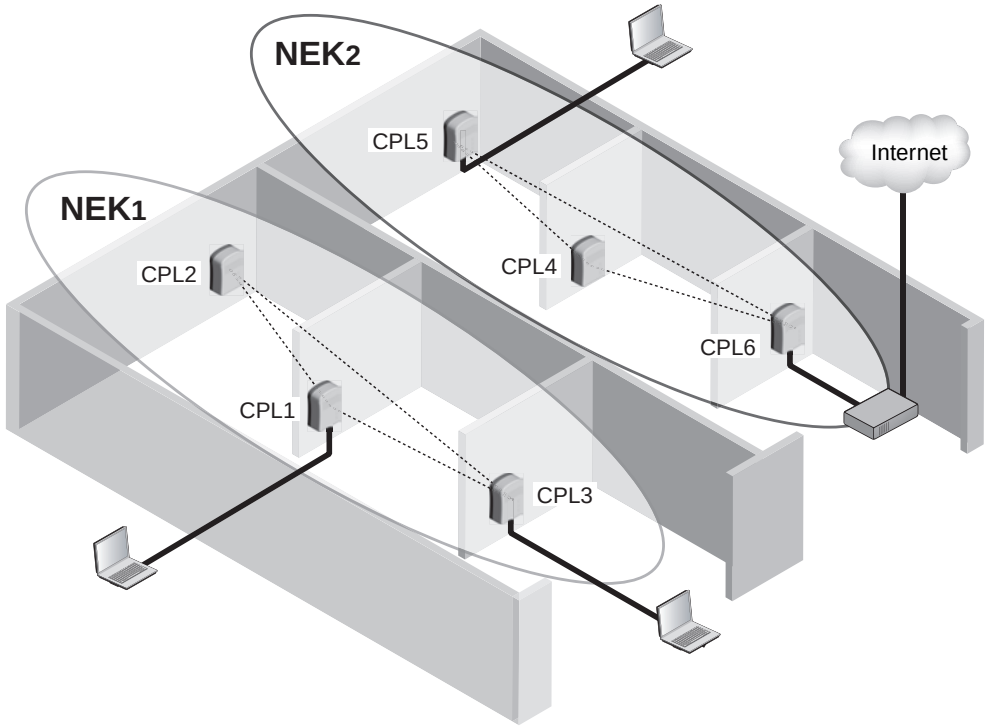


Figure 4.10
Réseaux logiques CPL avec des clés NEK différentes

La clé DEK est utilisée par les deux équipements CPL – celui du poste configurateur et celui qui doit recevoir la nouvelle NEK – pour échanger la NEK sur le réseau électrique de manière cryptée.

- **Par une interface Web.** Si les équipements CPL sont évolués, comme ceux de la marque Oxance, il est possible de gérer les configurations de clés par une interface Web unique.

Accès au média physique

Dans Wi-Fi, le support de transmission est partagé. Quiconque se trouvant dans la zone de couverture du réseau peut donc en intercepter le trafic ou même reconfigurer le réseau à sa guise. De plus, si une personne malveillante est assez bien équipée, cette dernière n'a pas besoin d'être située dans la zone de couverture du réseau. Il lui suffit d'utiliser une antenne avec ou même sans l'aide d'un amplificateur pour y accéder.

Dans le cas des CPL, le support de transmission est également partagé, mais l'accès au média physique est beaucoup plus difficile et, surtout, potentiellement dangereux.

Plusieurs techniques plus ou moins réalistes permettent cependant d'accéder aux données échangées sur un réseau CPL, notamment les suivantes :

- Disposer d'un équipement CPL ayant la bonne clé NEK du réseau visé.
- Récupérer les données physiques *via* les radiations électromagnétiques émises par le réseau CPL dans l'environnement proche des câbles électriques. Cela exige toutefois une chaîne d'acquisition complexe et coûteuse.
- Construire un équipement CPL spécifique, capable de récupérer les trames physiques cryptées afin de tenter de les décrypter.

La figure 4.11 illustre la conception interne d'un équipement CPL, avec ses deux interfaces : d'un côté l'interface Ethernet connectée à un réseau Ethernet où circulent les trames en clair, de l'autre l'interface CPL connectée au réseau électrique où circulent les trames cryptées.

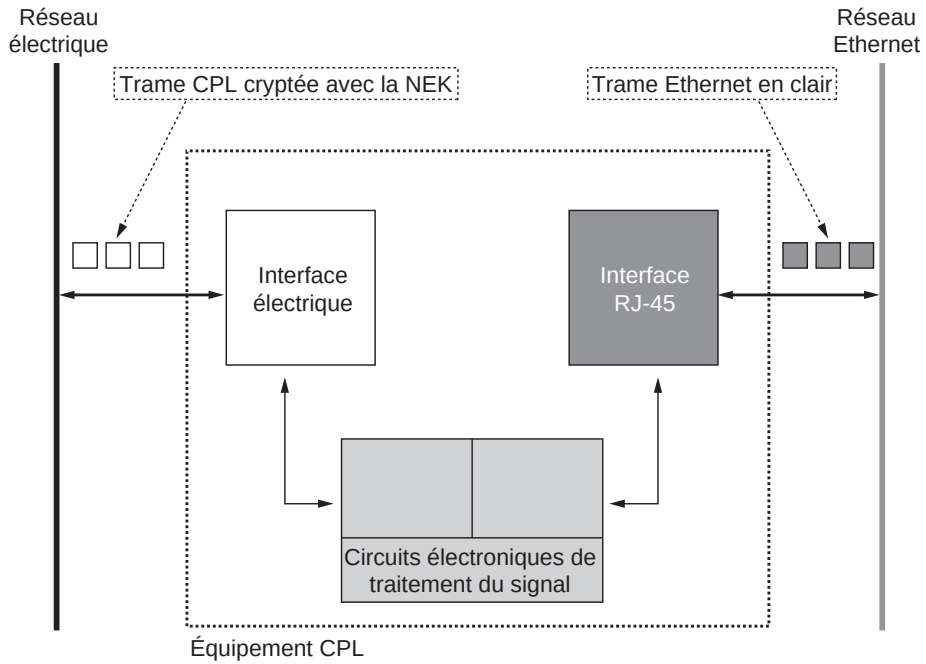


Figure 4.11

Conception interne d'un équipement CPL permettant de crypter les trames échangées

Un équipement CPL est constitué d'une interface électrique, qui émet et reçoit les trames sur le réseau électrique, et d'une interface Ethernet (prise RJ-45), qui émet et reçoit des trames sur le réseau Ethernet. Entre ces deux interfaces, les données ne circulent que si l'équipement détient la bonne clé NEK du réseau CPL.

Si un équipement CPL ne dispose pas de la clé NEK du réseau, les trames Ethernet ne sont pas disponibles sur l'interface Ethernet. Il est donc impossible d'accéder facilement aux trames CPL cryptées.

Accès aux trames physiques

Les données qui sont échangées sur un réseau CPL sont transportées dans des trames CPL dites « trames physiques ».

Les trames CPL circulent sur le réseau électrique entre toutes les prises électriques de manière cryptée. Comme expliqué précédemment, le média physique est d'un accès difficile, si bien que les trames sont relativement « protégées » des attaques visant à accumuler assez de trames pour pouvoir les tester avec un outil de « brute forcing » visant à essayer toutes les combinaisons ou utilisant différents algorithmes de décryptage.

De plus, les trames CPL sont transportées sur plusieurs bandes de fréquences, dont chacune peut utiliser différentes techniques de transport de l'information, autrement dit de modulation des données binaires sur le canal de transmission.

Comme nous l'avons vu aux chapitres 2 et 3, les différents équipements CPL du réseau adaptent en permanence leur technique de transmission numérique en fonction de la qualité des liens CPL, c'est-à-dire de la capacité du canal de transmission en terme de débit binaire. À cet effet, la Tone Map indexe les liens entre l'équipement CPL qui la stocke et tous les autres équipements CPL du réseau.

Pour accéder aux trames physiques, il est donc nécessaire de connaître en permanence cette Tone Map afin d'identifier la technique de transport de l'information entre équipements CPL du réseau.

L'authentification

L'authentification d'un équipement CPL consiste en la connaissance de la clé NEK qui identifie le réseau auquel il appartient. Si un équipement CPL n'a pas la bonne clé NEK, il ne peut échanger des données avec les équipements du réseau CPL auquel il veut se connecter.

La figure 4.12 illustre les principales étapes de l'accès d'un équipement CPL à un réseau identifié par la clé de cryptage NEK (Network Encryption Key) de HomePlug 1.0 et Turbo. Cette clé NEK, ici appelée NEK2, est l'identifiant du réseau CPL puisque seuls les équipements CPL ayant une configuration avec cette clé appartiennent à ce réseau.

Certains équipements CPL plus évolués, comme ceux de la marque Oxance, permettent de créer une authentification des équipements au niveau de l'adresse MAC en plus de la clé NEK. Cette authentification est gérée depuis l'interface d'administration du réseau par le biais d'une liste des adresses MAC autorisées à faire partie du réseau CPL.

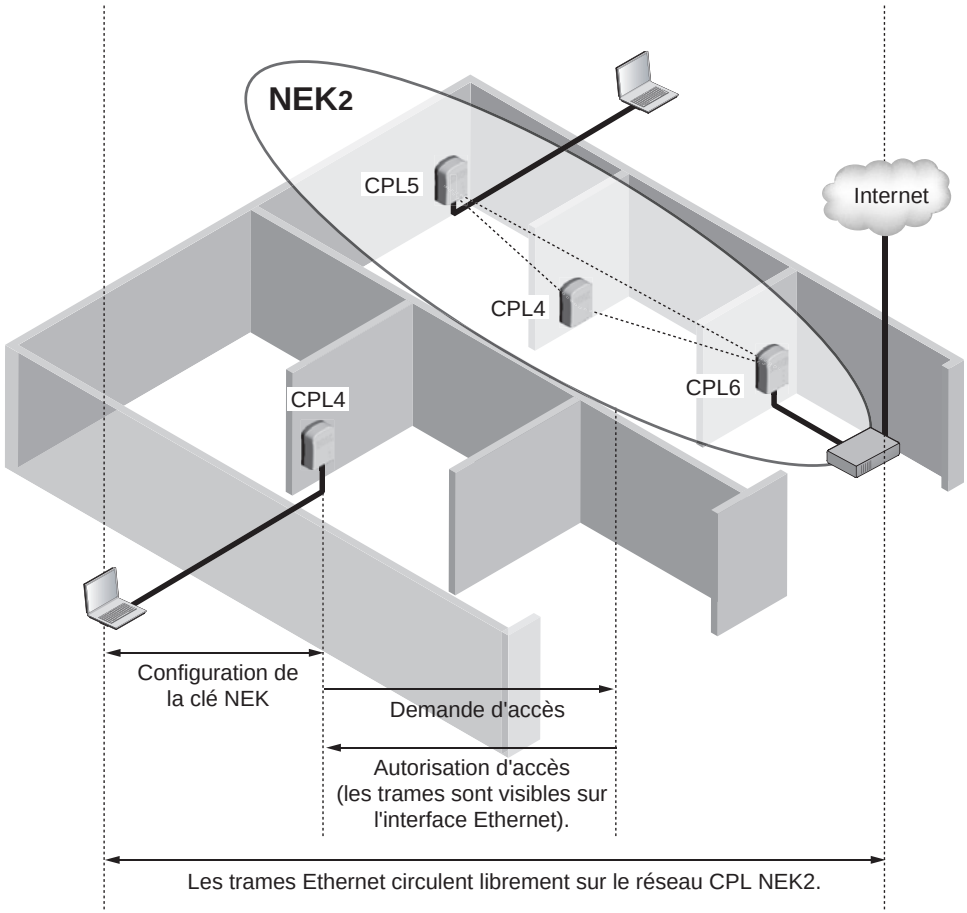


Figure 4.12
Accès d'un équipement à un réseau CPL identifié par sa clé NEK

Les clés réseau

Dans un réseau informatique, les clés réseau sont un moyen de protéger les données échangées en les cryptant avant leur émission sur le réseau. Dans un réseau CPL, les données circulent sur le réseau électrique, qui est un réseau partagé. Il est donc important de crypter les données afin d'éviter qu'elles soient récupérées. Les réseaux CPL utilisent pour cela des clés, qui permettent d'identifier un réseau et tous les équipements CPL qui en font partie.

Dans HomePlug 1.0, il existe deux clés de cryptage, NEK et DEK, stockées dans un registre propre à chaque équipement et accessible *via* le paramètre EKS (Encryption Key Select).

La clé NEK identifie le réseau CPL de la même manière que la clé WEP permet de protéger les données d'un réseau Wi-Fi. Elle effectue en outre les tâches suivantes :

- créer plusieurs réseaux CPL sur un même réseau électrique ;
- crypter les données circulant entre les équipements CPL ;
- authentifier les équipements appartenant au réseau CPL.

NEK par défaut des réseaux CPL HomePlug

Dans HomePlug, la NEK par défaut est égale, en ASCII, à la valeur 0x46D613E0F84A764C, qui équivaut au mot **HomePlug.** Tout équipement CPL HomePlug acheté dans le commerce est configuré avec cette clé de cryptage.

Si un utilisateur non averti tente de faire fonctionner son équipement ainsi, sans notion particulière de configuration réseau, le prix à payer est l'absence totale de sécurité, dans la mesure où tous les équipements de ce standard sont capables de récupérer les données échangées sur le réseau électrique irriguant un bâtiment ou une maison individuelle.

La clé DEK identifie un équipement CPL particulier. Elle permet de configurer des équipements CPL à distance, à travers le réseau électrique de l'installation domestique ou professionnelle.

Cette clé permet de créer une communication cryptée entre l'équipement CPL qui détient la clé NEK du réseau et l'équipement CPL qui cherche à appartenir au réseau CPL.

Comme nous le verrons au chapitre 9, dédié aux configurations pratiques du réseau CPL, cette clé peut se révéler très utile pour configurer des équipements à distance depuis un point central d'administration du réseau.

Calcul de la clé NEK

Le standard PKCS#5 spécifie deux méthodes pour mettre en place une cryptographie dérivée de mots de passe. HomePlug a choisi la méthode PBFDK1, qui exige comme paramètres d'entrée un mot de passe (entré par l'administrateur), un « grain de sel », paramètre constant spécifié par HomePlug et qui est une sorte de clé publique, un nombre d'itérations, c'est-à-dire le nombre de fois que l'opération spécifiée dans la formule PBFDK1 va être réitérée en boucle pour accroître l'efficacité du cryptage, et une longueur de sortie de la clé dérivée.

La méthode PBFDK1 utilise la fonction de hachage MD5, qui permet de définir l'empreinte du message crypté de manière synthétique et unique, en l'occurrence le cryptage et l'empreinte numérique du mot de passe du réseau CPL.

Elle est décrite par la fonction suivante :

$$DK = PBFDK1 (P, S, c , dkLen)$$

Dans laquelle :

- DK = clé dérivée (avec dkLen égale à 8, DK étant la NEK) ;
- P = mot de passe (entré par l'administrateur du réseau) ;
- S = grain de sel (égal en ASCII à 0x0885 6DAF 7CF5 8185) ;
- c = nombre d'itérations (1 000 fois) ;
- dkLen = longueur de la clé dérivée en octets (8 octets).

Selon le standard FIPS PUB 112, les règles d'usage pour les mots de passe consistent à définir une longueur comprise entre 4 et 8 octets, même si des mots de passe plus longs (jusqu'à 24 octets) sont possibles.

PBFDK1 spécifie que la fonction de hachage MD5 doit être appliquée 1 000 fois de manière itérative en utilisant les résultats de l'itération précédente, la première valeur étant la concaténation du mot de passe et du grain de sel.

Les itérations se déroulent de la manière suivante :

$T_1 = MD5 (P|S)$

$T_2 = MD5 (T1)$

…

$T_{1000} = MD5 (T_{999})$

$DK = T_{1000} <0…7>$

où (P|S) est une concaténation de P et de S.

L'algorithme MD5 (RFC 1321)

L'algorithme MD5 produit un message digest (MD) de 128 bits depuis un message d'entrée. Il est théoriquement impossible pour deux messages distincts d'obtenir le même MD.

Il est possible de résumer l'algorithme MD5 de la manière suivante :

$m_{ext} = m + m_{pad} + m_l$

où

- m_{ext} est le message étendu produit par l'algorithme MD5.
- m est le message d'entrée de longueur arbitraire converti en suite binaire.
- m_{pad} est constitué de bits de bourrage (1 suivi de zéros) concaténés au mot m de sorte que la longueur de m_{ext} soit égale à 448 modulo 512.
- m_l est la longueur en bits du message original m, exprimé sous forme de blocs binaires de 64 bits.

Le message étendu, m_{ext}, subit quatre phases de rotation de bits, chacune d'elles incluant 16 opérations. À chaque opération, une valeur fixe est ajoutée au résultat. Cette valeur fixe ajoutée à chacun des résultats des 64 opérations (valeur différente pour chacune des opérations) est calculée grâce une fonction SINE (sinusoïdale) et stockée dans un tableau de 64 lignes (une ligne pour chaque opération).

Chaque ligne stocke donc une valeur fixe calculée de la manière suivante :

$Ajout_i = int(2^{32} \times abs(sin(i)))$

où *i* est exprimé en radians.

Ces 64 nombres fixes ($Ajout_i$) ne seront jamais plus grands que 32 bits.

Sécurité dans HomePlug AV

Les principales fonctionnalités de sécurité implémentées dans HomePlug AV sont les suivantes :

- Cryptage fondé sur l'AES 128 bits en mode CPC (Cipher Block Chaining).
- Protection des données par une clé NEK (rotation de valeurs de NEK toutes les heures) encryptant les données physiques.
- Authentification pour rejoindre un réseau CPL au moyen d'une clé NMK (Network Membership Key) permettant de distribuer les clés NEK sur le réseau.
- Autorisation d'un nouvel équipement CPL par configuration :
  - à l'aide d'une trame transportant la clé NMK sur l'interface Ethernet ;
  - à l'aide d'une clé DAK (Direct Access Key) correspondant à la clé DEK de HomePlug 1.0 ;
  - à l'aide du bouton Easy Connect ;
  - à l'aide d'une clé MDAK (Méta DAK) ;
  - à l'aide d'un couple de clés PPK (Public Private Key encryption).
- Support des protocoles HLE (Higher Layer Entities) tels que IEEE 802.1x.

Le tableau 4.1 récapitule les caractéristiques de gestion de sécurité des différentes technologies CPL avec leur gestion de clés, leur niveau de cryptage et les avantages et inconvénients de chacune des méthodes.

Tableau 4.1 Gestion des clés de cryptage en fonction de la technologie CPL

Technologie	Gestion des clés	Cryptage	Avantage	inconvénient et faille
HomePlug 1.0	NEK	DES-56bits	Simplicité	– Faiblesse du DES – Une seule clé par équipement
HomePlug Turbo	DEK	*idem*	*idem*	*Idem*
HomePlug AV	– NEK – NMK – DAK	AES-128 bits (rotation de clés)	Haut niveau de cryptage	Faille possible avec le bouton Easy Connect
Ascom	Échange de clés	RC4 + Diffie-Hellman (128 bits)	Configuration facilitée par l'interface	Faiblesse du RC4
DS2	Échange de clés maître-esclave	3DES	Configuration centrale par console d'administration sur l'équipement maître	Interception des échanges de clés lors des authentifications
Oxance	– NEK – DEK	– DES-56 bits – AES-128 bits	Gestion par interface centralisée Web	Faiblesse possible de l'interface Web

Les attaques

Comme nous l'avons vu en début de chapitre, le but d'une attaque ne se limite pas à se connecter à un réseau afin d'y récupérer des données par le biais de failles. Il peut aussi viser à en perturber le fonctionnement, aussi bien au niveau réseau qu'au niveau physique.

Les attaques par décryptage

L'objectif de cette attaque est d'essayer de découvrir la clé NEK d'un réseau CPL afin de s'y connecter et de récupérer les données échangées.

Les deux techniques suivantes permettent de découvrir la clé NEK dans HomePlug 1.0 :

- Accéder aux trames physiques et en stocker suffisamment pour pouvoir les décrypter avec des algorithmes adéquats. Cette technique est toutefois très complexe et exige des solutions matérielles spécifiques coûteuses.
- Essayer toutes les combinaisons possibles de clés NEK pour accéder au réseau.

Le temps nécessaire pour tester toutes les combinaisons possibles de clés NEK peut être estimé de la façon suivante : la clé NEK est codée avec l'algorithme DES-56 bits dérivé d'un mot de passe entré par l'utilisateur du réseau CPL et pouvant varier de 4 à 24 caractères.

Le nombre d'essais possibles est donc au maximum de :

$$N = 2^{58} \approx 2{,}88 \times 10^{17}$$

Pour une trame Ethernet de 64 octets avec une carte réseau à 100 Mbit/s, le temps de transmission est de :

$$T_{trame} = \frac{64 \times 8 \text{ bits}}{100 \times 1\,024 \times 1\,024} \approx 4{,}88 \times 10^{-6} \text{ sec}$$

Le temps total nécessaire pour essayer toutes les combinaisons est alors :

$$T_{total} = \mathrm{N} \times T_{trame} = 2{,}88 \times 10^{17} \times 4{,}88 \times 10^{-6} \approx 1{,}4 \times 10^{12} \text{ sec} \approx 44\,591 \text{ années}$$

Nous constatons que cette technique exige beaucoup trop de temps pour pouvoir être utilisée efficacement.

Les attaques par déni de service

Le but d'une attaque n'est pas nécessairement de casser un algorithme de chiffrement pour récupérer la clé et écouter ou pénétrer le réseau. Certaines attaques ont pour unique fonction de saboter le réseau en empêchant son fonctionnement. Ce type d'attaque, appelé déni de service, ou DoS (Denial of Service), est largement répandu dans tous les types de réseaux.

Dans les réseaux CPL, le déni de service le plus simple correspond au brouillage. Ces réseaux fonctionnant sur une bande de fréquences de 1 à 30 MHz, l'utilisation d'un appareil radio utilisant la même bande avec des puissances supérieures à celle des CPL peut

provoquer des interférences et donc une chute de performance globale, voire empêcher complètement le réseau de fonctionner. Cette attaque est la plus simple à mettre en œuvre. Elle est aussi malheureusement imparable.

IEEE 802.1x et l'amélioration de la sécurité des CPL

IEEE 802.1x est une architecture d'authentification proposée par le comité 802 de l'IEEE. Il ne s'agit en aucun cas d'un protocole à part entière mais de lignes de conduite, ou guidelines, permettant de définir les différentes fonctionnalités nécessaires à la mise en œuvre d'un service d'authentification de clients sur n'importe quel type de réseau local, Ethernet comme CPL.

L'architecture de 802.1x, appelée Port-based Network Access Control, repose sur deux éléments clés, les protocoles EAP et RADIUS.

La notion de port est un élément important de cette architecture d'authentification. Le port définit tout type d'attachement à une infrastructure de réseau local. Dans les CPL comme dans Ethernet, c'est la connexion de deux machines qui est considérée comme un port.

L'architecture de 802.1x est illustrée à la figure 4.13. Elle est constituée des trois éléments distincts suivants :

- Un client, qui correspond à l'utilisateur qui voudrait se connecter au réseau *via* sa station.
- Un contrôleur, généralement un switch ou un routeur, qui relaye et contrôle les informations entre tout demandeur et le serveur d'authentification.
- Un serveur d'authentification, qui authentifie l'utilisateur.

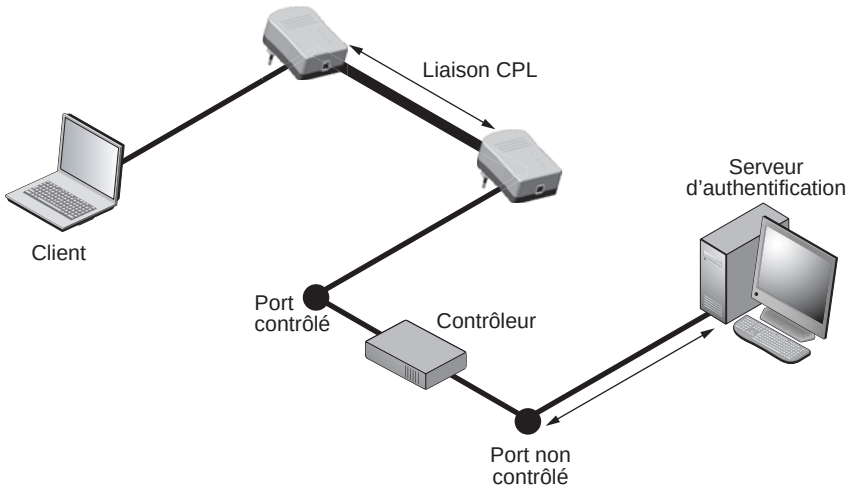


Figure 4.13

Architecture d'authentification d'IEEE 802.1x

Pour chaque port, le trafic du réseau peut être ou non contrôlé. Entre le client et le contrôleur, le port est contrôlé, de telle sorte que seuls des messages d'authentification EAP, de type requête-réponse, sont transmis. Tout autre type de trafic est rejeté. Entre le contrôleur et le serveur d'authentification, en revanche, tout type de trafic est accepté car le support est supposé sûr.

Dans 802.1x, l'authentification s'appuie sur le protocole EAP (Extensible Authentication Protocol) et l'utilisation d'un serveur RADIUS (Remote Authentication Dial-In User Service).

RADIUS et Diameter

802.1x ne définit pas de protocole d'authentification particulier côté serveur. Il est possible d'utiliser deux protocoles d'authentification client-serveur, RADIUS et Diameter. RADIUS, le plus simple, est devenu le serveur par défaut de toute architecture 802.1x. Diameter a pour principale contrainte de reposer sur la couche de transport SCTP (Stream Control Transmission Protocol), qui n'est pas autant implémentée que TCP.

EAP (Extensible Authentication Protocol)

EAP a été défini à l'origine pour le protocole PPP (Point-to-Point Protocol) comme extension aux protocoles d'authentification existants PAP (Password Authentication Protocol) et CHAP (Challenge Handshake Authentication Protocol). Par rapport à ces deux protocoles, EAP fournit, de manière relativement simple, de nombreuses méthodes d'authentification. Cette simplicité vient du fait qu'EAP n'est qu'une enveloppe de transport de ces méthodes d'authentification.

Dans le cadre d'une architecture 802.1x CPL, cinq méthodes d'authentification EAP sont utilisées :

- **EAP-MD5.** Cette solution repose sur la fonction de hachage MD5. Pour s'authentifier, l'utilisateur fournit un login-mot de passe, dont l'empreinte MD5 est transmise à fin d'authentification au serveur. Cette solution est réputée peu fiable, bien que seule l'empreinte soit transmise sur le réseau et non le login-mot de passe. Elle n'est plus supportée par Windows XP SP1.
- **EAP-TLS.** TLS (Transport Layer Security) est un mécanisme permettant la mise en place d'une connexion sécurisée. Ses fonctionnalités sont l'authentification mutuelle entre le client et le serveur, le chiffrement des données et la gestion dynamique des clés. TLS constitue la base de SSL 3.0, que l'on retrouve dans HTTPS, un protocole utilisé par de nombreux sites Web (banques, sites de réservation en ligne, etc.). Mis à part le chiffrement, EAP-TLS reprend les caractéristiques de TLS mais encapsulées dans des paquets EAP.
- **EAP-TTLS.** EAP-TTLS (Tunneled TLS) est une solution de Funk Software qui repose sur l'utilisation de deux tunnels, l'un pour l'authentification par EAP-TLS et le second pour sécuriser les transmissions avec une méthode d'authentification laissée au choix des constructeurs (EAP-MD5, PAP, CHAP, etc.).

- **PEAP.** Protected EAP est une solution proposée par Microsoft, RSA et Cisco Systems. Comme EAP-TTLS, PEAP repose sur l'instauration de deux tunnels, mais utilisant tous deux EAP-TLS comme méthode d'authentification.
- **LEAP.** Proposé par Cisco, Lightweight EAP correspond à une version allégée des solutions précédentes mais dotée des mêmes fonctionnalités : authentification mutuelle entre le client et le serveur et gestion dynamique des clés.

Bien que ces solutions reposent sur une authentification mutuelle entre le client et le serveur, parfois même agrémentée d'une autre méthode d'authentification pour sécuriser le transport des données, elles ne sont pas sans faille. L'attaque MIN (Man In the Middle) permet, par exemple, à un attaquant placé entre le client et le serveur, c'est-à-dire au milieu, de récupérer les messages et d'usurper l'identité d'un client pour se faire authentifier à sa place.

En conclusion, 802.1x est une solution qui permet d'améliorer la sécurité des réseaux CPL en s'ajoutant à la gestion des clés NEK sécurisant les trames physiques sur le réseau électrique.

RADIUS (Remote Authentication Dial-In User Server)

RADIUS est un protocole centralisé d'autorisation et d'authentification de l'utilisateur. Conçu à l'origine pour l'accès à distance, il est aujourd'hui utilisé dans de nombreux environnements, tels les VPN et les points d'accès Wi-Fi, et est devenu un standard IETF (RFC 2865).

Situé au-dessus du niveau 4 de l'architecture OSI, il utilise le protocole de transport UDP pour des raisons évidentes de rapidité et repose sur une architecture client-serveur.

Comme illustré à la figure 4.14, le client envoie des attributs de connexion auprès du serveur. L'authentification entre le serveur et le client se fait par l'intermédiaire d'un secret partagé, qui est généralement formé d'une clé et des attributs du client. Pour s'authentifier, le serveur envoie un challenge au client, que seul le secret partagé peut résoudre. Il vérifie les attributs envoyés par le client et la réponse au challenge et, s'ils sont corrects, accepte le client.

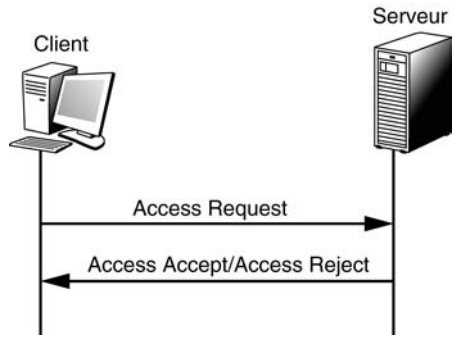


Figure 4.14
Négociation RADIUS

IEEE 802.1x dans les CPL

EAPoL (EAP over LAN) est la version d'EAP utilisée dans le cadre des réseaux locaux Ethernet, Wi-Fi comme CPL. Il se présente comme une encapsulation Ethernet vue de la liaison entre le terminal client et le serveur Radius.

L'échange de messages EAPoL pour l'authentification d'une station auprès d'un point d'accès est illustré à la figure 4.15.

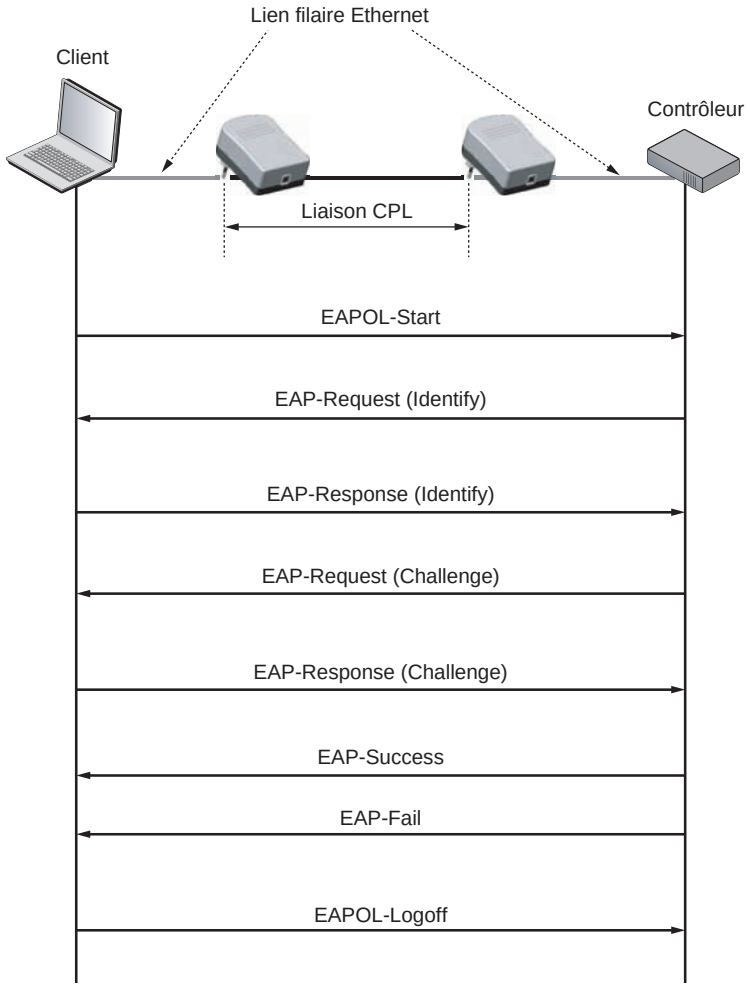


Figure 4.15

Échange de messages EAPoL entre un point d'accès et une station

L'authentification est toujours à l'initiative de la station qui envoie une requête EAPoL-Start. Le point d'accès lui transmet une ou plusieurs requêtes, auxquelles elle doit répondre.

La phase d'authentification se termine soit par un message EAP-Success, qui garantit que la station est authentifiée, soit par un message EAP-Failure, et, dans ce cas, la station n'est pas authentifiée. La station peut se désauthentifier à tout moment en envoyant une requête EAPoL-Logoff.

802.1x utilise un serveur d'authentification vers lequel le point d'accès relaye les informations, comme illustré à la figure 4.16. La phase d'authentification ne peut être initiée que par la station. Après avoir reçu la demande d'authentification, le point d'accès demande à la station de s'identifier par une EAP-Request (Identity). Dès que la station s'identifie auprès du point d'accès par une EAP-Response (Identity), cette requête est transmise au serveur d'authentification (Access Request).

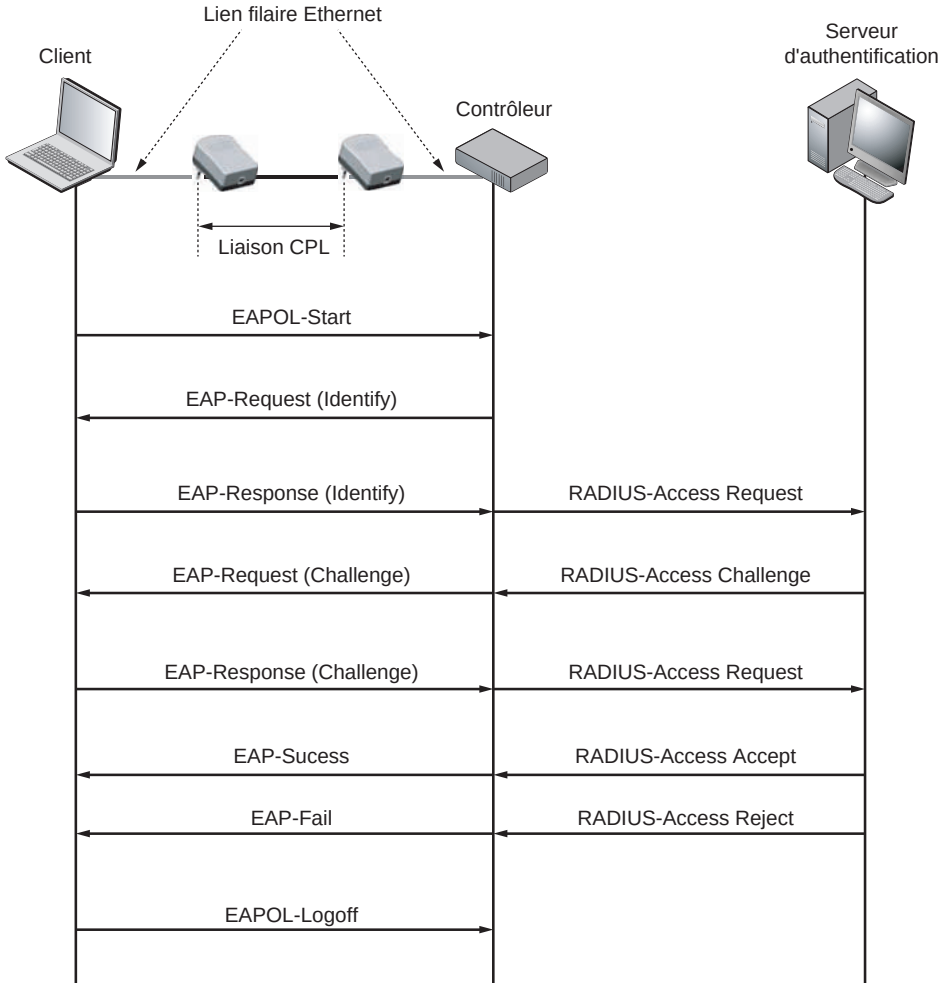


Figure 4.16

Phase d'authentification dans IEEE 802.1x

Généralement, la station et le serveur d'authentification se partagent un secret (clé, login-mot de passe, certificat), qui dépend de la méthode d'authentification utilisée. Dès que le serveur d'authentification reçoit une requête d'un client (une station) connecté au réseau CPL, il envoie à la station un message Access Challenge contenant un challenge. Ce challenge ne peut être résolu que par le secret partagé entre la station et le serveur d'authentification. Si le challenge n'est pas résolu, la station ne peut s'authentifier ; s'il l'est, le serveur d'authentification authentifie la station, qui peut dès lors se connecter au réseau par l'intermédiaire du port contrôlé situé entre elle et l'équipement CPL permettant l'accès au réseau local CPL.

Tout type de serveur supportant EAPoL peut être utilisé comme serveur d'authentification. Le plus répandu reste toutefois RADIUS.

Les réseaux privés virtuels

Le rôle des réseaux privés virtuels, ou VPN (Virtual Private Network), est de fournir un tunnel sécurisé de bout en bout entre un client et un serveur. Les VPN permettent, entre autre chose, d'identifier et d'autoriser l'accès ainsi que de chiffrer tout trafic circulant dans le réseau.

À ce jour, IPsec est le protocole le plus utilisé dans les VPN. Standard de référence, IPsec s'appuie sur différents protocoles et algorithmes en fonction du niveau de sécurité souhaité :

- authentification par signature électronique à clé publique (RSA) ;
- contrôle de l'intégrité par fonction de hachage (MD5) ;
- confidentialité par l'intermédiaire d'algorithmes symétriques, tels que DES, 3DES, AES, IDEA, Blowfish, etc.

L'utilisation d'un VPN est la manière la plus fiable de sécuriser un réseau sans fil. C'est aussi la méthode la plus utilisée.

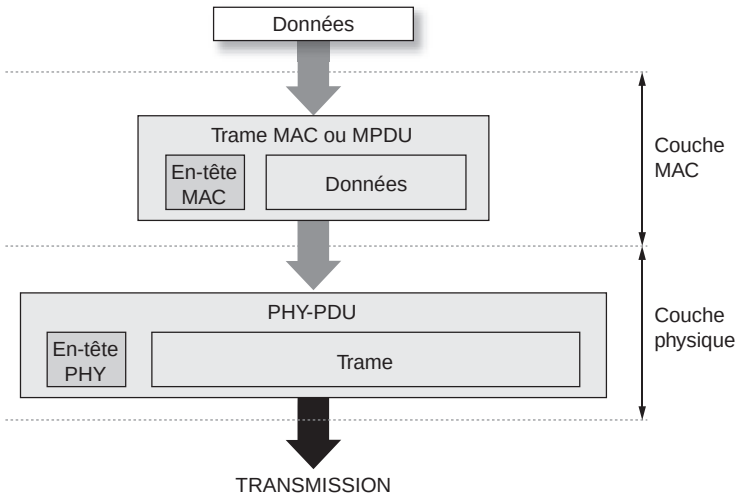
5

Trames

Pour envoyer de l'information, les stations CPL doivent préparer des trames de données, c'est-à-dire des blocs de données comportant un en-tête et une zone indiquant la fin de la trame. Le bloc contenant les données utilisateur est doté d'un format spécifique, qui dépend de la technique d'accès au support physique utilisée. Le support électrique étant partagé, il faut déterminer une technique permettant le passage de multiples trames provenant de machines différentes. À cette structure de trame émise sur le niveau physique, s'ajoute une seconde structure de trame, encapsulée dans la première.

La figure 5.1 illustre la transmission de données dans l'architecture d'un accès CPL au travers des couches MAC (liaison de données) et physique (PHY). Le premier niveau

Figure 5.1
Transmission des données dans l'architecture d'un accès CPL



correspond à la technique d'accès au support électrique. La trame correspondant à ce protocole porte le nom de trame MAC, ou MPDU (MAC Protocol Data Unit).

Toutes les données venant des couches supérieures à la couche MAC sont encapsulées dans la trame MAC. Cette trame MAC est encapsulée dans une seconde trame, de niveau physique, de façon à assurer le transport de la trame sur l'interface physique, ou interface électrique. Cette trame est appelée PDU (physical Protocol Data Unit).

Ce chapitre examine la structure des trames CPL utilisées dans HomePlug 1.0 et présente les grandes caractéristiques des trames dans HomePlug AV.

Les trames de niveau physique

Si l'on observe la structure complète de la trame HomePlug 1.0 au niveau physique échangée en permanence entre les équipements CPL *(voir figure 5.2)*, on constate qu'elle est constituée d'un certain nombre d'éléments encadrant la trame de données dite longue et qui comportent les données des couches protocolaires de plus haut niveau du point de vue du modèle OSI.

En terme de longueur temporelle, la trame HomePlug 1.0 peut être quantifiée par des valeurs minimales et maximales, avec une partie fixe (en-têtes), une partie variable de données et une partie utilisée pour les durées de contention au niveau du processus CSMA/CA, comme indiqué au tableau 5.1.

Tableau 5.1 Longueur temporelle de la trame HomePlug 1.0

	Fixe (en-têtes)		Variable (données)		Contention (CSMA/CA)		Longueur temporelle
MIN	205,52 µs	+	313,5 µs	+	$N \times 35{,}84$ µs	=	519,02 µs + ($N \times 35{,}84$ µs)
MAX	205,52 µs	+	1 489,5 µs	+	$N \times 35{,}84$ µs	=	1 692,02 µs + ($N \times 35{,}84$ µs)

La trame HomePlug 1.0 est donc constituée de trames de données dites longues, qui comportent les données des trames MAC, et de trames de données dites courtes, qui comportent les informations de réponse des autres équipements CPL.

Retenons que la durée moyenne d'une trame HomePlug 1.0 est de 1 600 µs.

Du point de vue des techniques de modulation du niveau physique, la trame de données HomePlug 1.0 est constituée de symboles OFDM (Orthogonal Frequency Division Multiplexing). Ces symboles forment des blocs, qui, à leur tour, constituent la trame complète.

La figure 5.3 illustre les durées respectives de ces différents blocs OFDM.

L'addition des différentes durées des blocs de symboles OFDM définit la durée complète de la trame. Il est ainsi possible de calculer la vitesse de transmission maximale possible et le débit binaire au niveau de la couche liaison de données.

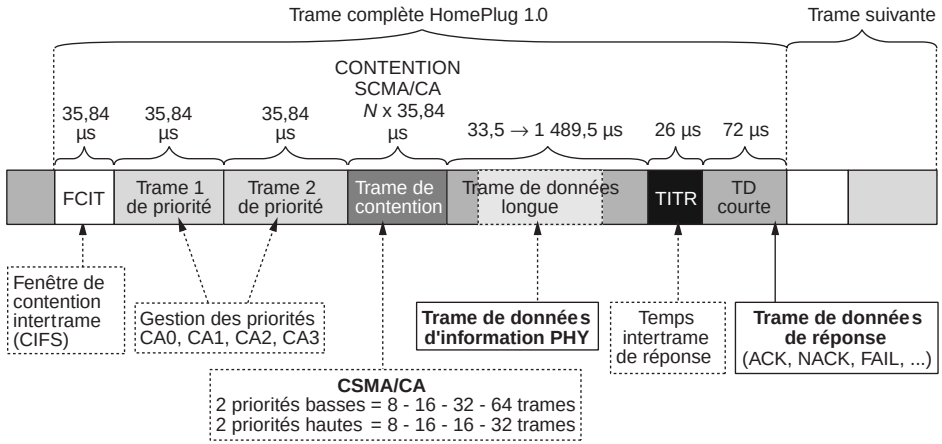


Figure 5.2

Structure de la trame HomePlug 1.0

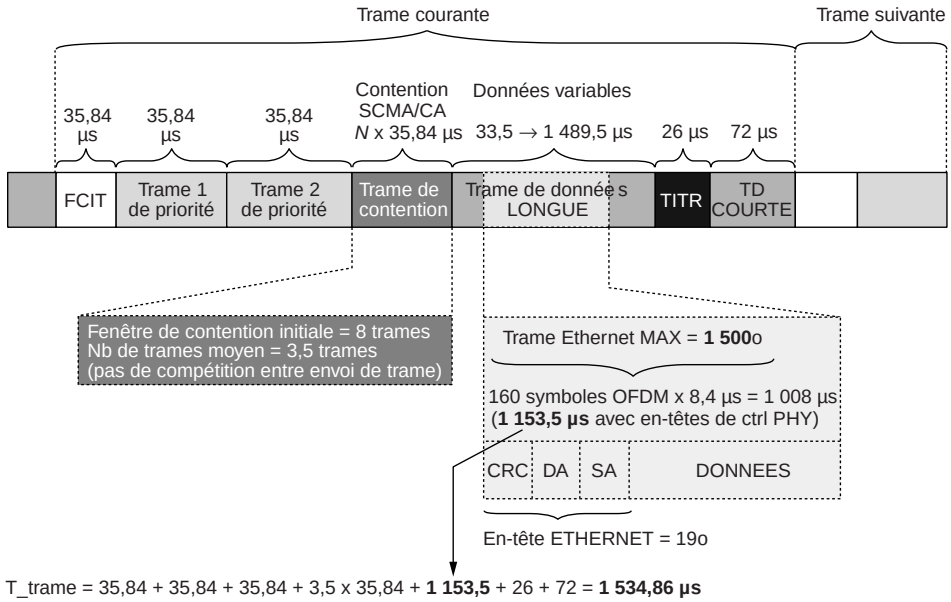


Figure 5.3

Durées des blocs de symboles OFDM de la trame complète HomePlug 1.0

Avec une trame de 2 705 octets, la vitesse de transmission maximale est obtenue de la façon suivante :

$$\text{Débit}_{\text{PHY\_MAX}} = 2\,705 \times 8 \text{ bits}/1\,534{,}86\ \mu\text{s} = 14{,}1 \text{ Mbit/s}$$

Avec une trame de données Ethernet d'une longueur maximale de 1 500 octets, le débit maximal est le suivant :

$$\text{Débit}_{\text{PHY\_MAX}} = 1\,500 \times 8 \text{ bits}/1\,534{,}86\ \mu\text{s} = 7{,}81 \text{ Mbit/s}$$

Le tableau 5.2 récapitule les vitesses de transmission maximales théoriques du standard HomePlug 1.0. Comme nous le verrons à la partie II de l'ouvrage, ces valeurs sont inférieures dans la réalité.

Tableau 5.2 Vitesse de transmission maximale selon la technique de modulation

Mode	Code de correction d'erreur (Forward Error Correction)	Vitesse de transmission théorique maximale (Mbit/s)
DQPSK $^3/_4$	$^3/_4$ code de convolution et code de Reed-Solomon	14,1
DQPSK $^1/_2$	$^1/_2$ code de convolution et code de Reed-Solomon	9,19
DBPSK	Code de convolution et code de Reed-Solomon	4,59
ROBO (DBPSK 1/2), répétition de chaque bit quatre fois	$^1/_2$ code de convolution et code de Reed-Solomon	1,02

L'évolution des technologies CPL promet des vitesses de transmission améliorées, comme indiqué au tableau 5.3

Tableau 5.3 Vitesse de transmission maximale annoncée des différentes technologies CPL

Technologie CPL	Vitesse de transmission annoncée
HomePlug Turbo	85 Mbit/s
HomePlug AV	200 Mbit/s
Spidcom SPC200-e	220 Mbit/s
DS2	200 Mbit/s

Architecture des couches physique et liaison de données de HomePlug AV

Les derniers développements techniques du consortium HomePlug ont permis d'améliorer les performances de HomePlug 1.0 dans la nouvelle version HomePlug AV (pour Audio et Vidéo).

L'architecture de la couche physique et de la couche liaison de données est modifiée tout en permettant l'interopérabilité avec les équipements HomePlug 1.0 afin d'autoriser le mode maître-esclave.

La figure 5.4 illustre l'architecture de ces deux couches.

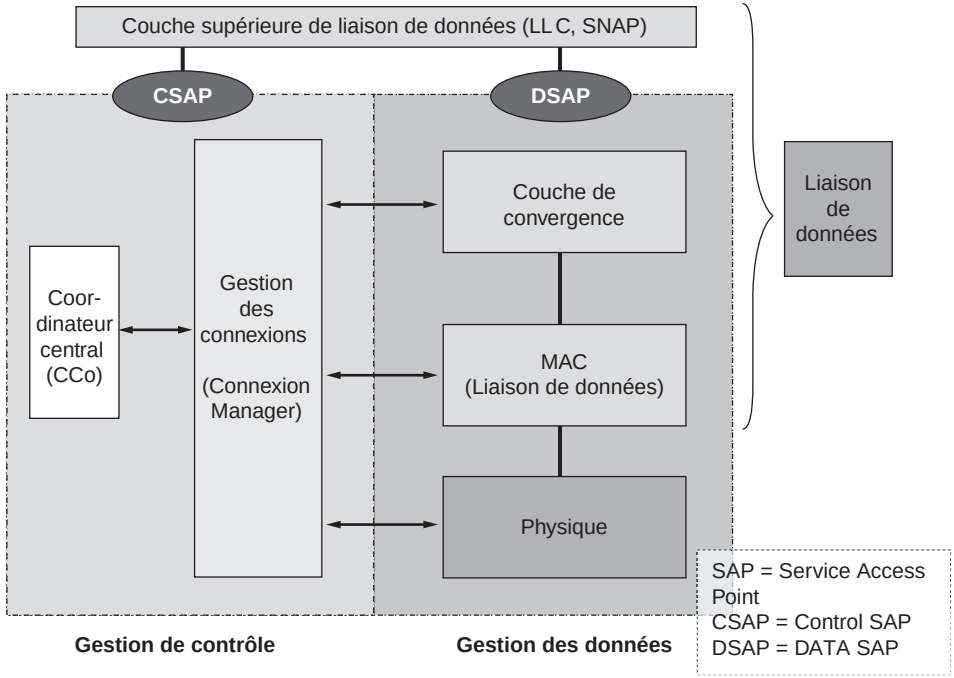


Figure 5.4
Architecture de HomePlug AV

Ces couches assurent la gestion de deux fonctions simultanées : la gestion des contrôles entre le maître et les esclaves du réseau, principalement pour assurer les différentes fonctionnalités de QoS, et la gestion des données, pour l'encapsulation MAC et la mise à disposition des données dans les couches supérieures.

La trame de l'interface OFDM

L'interface OFDM (Orthogonal Frequency Division Multiplexing) est la technique d'accès utilisée par les CPL. Cette technique d'accès est également utilisée par Wi-Fi dans les standards IEEE 802.11a et 802.11g, ainsi que par les technologies ADSL et de diffusion TV terrestre.

Cette technique présente une grande robustesse vis-à-vis des interférences que présente le média de communication. Le principe de la technique OFDM est de séparer la bande de fréquences en sous-bandes étroites, chacune transportant une partie de l'information binaire. Pour obtenir une bonne efficacité spectrale, les réponses fréquentielles de chacune des sous-bandes sont orthogonales et se recouvrent légèrement.

Les symboles OFDM

Comme expliqué précédemment, les trames HomePlug 1.0, Turbo et AV sont composées de symboles OFDM de données binaires assemblés en blocs.

La figure 5.5 donne une représentation temporelle et fréquentielle des bandes de fréquences OFDM utilisées par les technologies CPL. La bande de fréquences est divisée en 84 sous-bandes, dont 78 seulement sont utilisées, afin de respecter les réglementations fréquentielles vis-à-vis des réseaux de radioamateurs (respect des bandes amateur 40 m, 30 m, 20 m et 17 m).

Chaque sous-bande de fréquences transporte les trames OFDM, lesquelles sont constituées de deux grandes parties :

- **CP (Cyclic Prefix),** qui permet de délimiter temporellement la partie transportant les données.
- **Trame de données,** composée de symboles OFDM, eux-mêmes composés de 428 échantillons, ou *samples*, chacun.

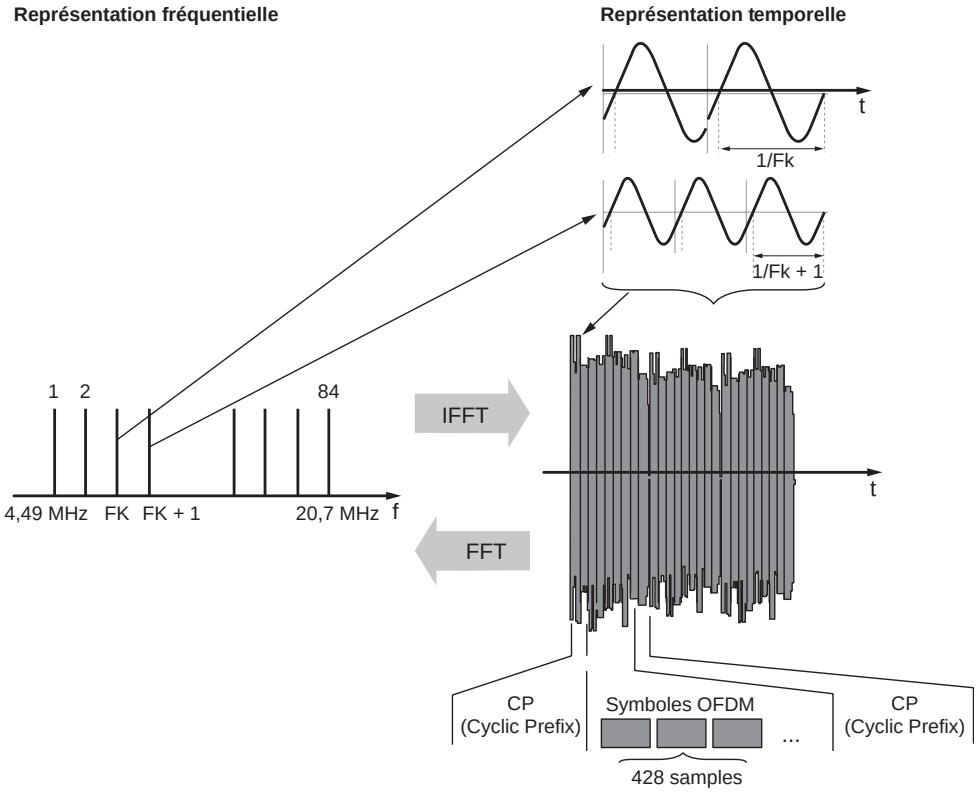


Figure 5.5

Représentation temporelle et fréquentielle des bandes de fréquences OFDM

Les blocs OFDM de la trame HomePlug sont composés de 20 ou 24 symboles. Ceux de la trame ROBO sont composés uniquement de 40 symboles.

La figure 5.6 donne le détail d'un symbole OFDM, ainsi que les durées respectives de ses différentes parties : 8,4 µs pour HomePlug 1.0 et 40,96 µs pour HomePlug AV.

La trame de données dite « longue » est elle-même constituée de 20 à 120 blocs OFDM formant les données de la couche liaison de données et les blocs de services.

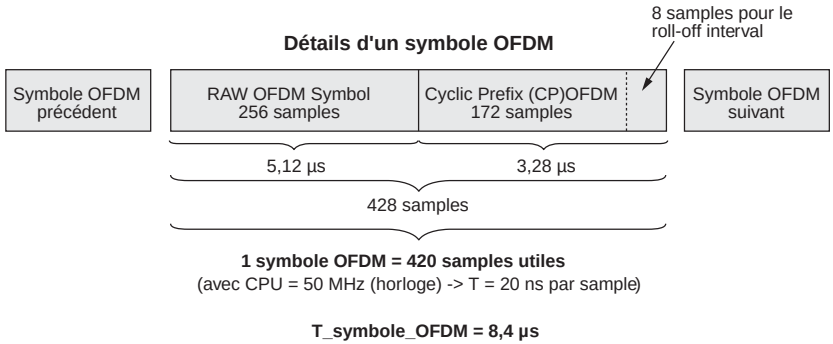


Figure 5.6
Détails d'un symbole OFDM

Les symboles OFDM sont modulés dans chaque sous-bande de fréquences en modulation de phase en fonction de la qualité du lien entre les équipements CPL.

Schémas des transmissions OFDM

Contrairement aux schémas de transmission monoporteuse, les schémas de transmission OFDM permettent de partager la complexité de l'égalisation de puissance du signal transmis entre l'émetteur et le récepteur. Cela garantit une implémentation simple et bon marché des récepteurs CPL.

Les autres avantages des schémas de transmission OFDM sont les suivants :

- Utilisation efficace de la bande de fréquences, contrairement aux techniques de multiplexage fréquentiel classique. Les différents canaux se chevauchent en terme spectral tout en gardant une parfaite orthogonalité.
- Égalisation numérique et décodage simple et optimal grâce à l'utilisation d'intervalles de garde, même si elle s'accompagne d'une baisse de débit des données. Ajoutée à l'utilisation de codes convolutifs, de codes de Viterbi et de codes en blocs (Reed-Solomon), cette technique se révèle d'une grande efficacité.
- Robustesse au bruit impulsif grâce à une technique multiporteuse. Chaque porteuse est affectée d'un bruit indépendant des autres porteuses. Dans la technique monoporteuse, le bruit peut affecter un certain nombre de symboles. Dans la technique OFDM, les pertes de symboles dans une porteuse n'affectent pas les autres porteuses.
- Grande flexibilité de l'allocation de débit binaire pour chaque utilisateur ou chaque porteuse. Chaque porteuse peut être codée indépendamment des autres en fonction des qualités des liens physiques et des techniques de modulation les mieux adaptées.
- Amélioration de l'estimation préalable du canal de transmission. Les techniques OFDM utilisent des trames dites d'apprentissage, qui permettent d'identifier dans le domaine fréquentiel les capacités du canal de transmission.

La figure 5.7 donne une vue d'ensemble des symboles OFDM dans chaque canal (sous-bande de fréquences).

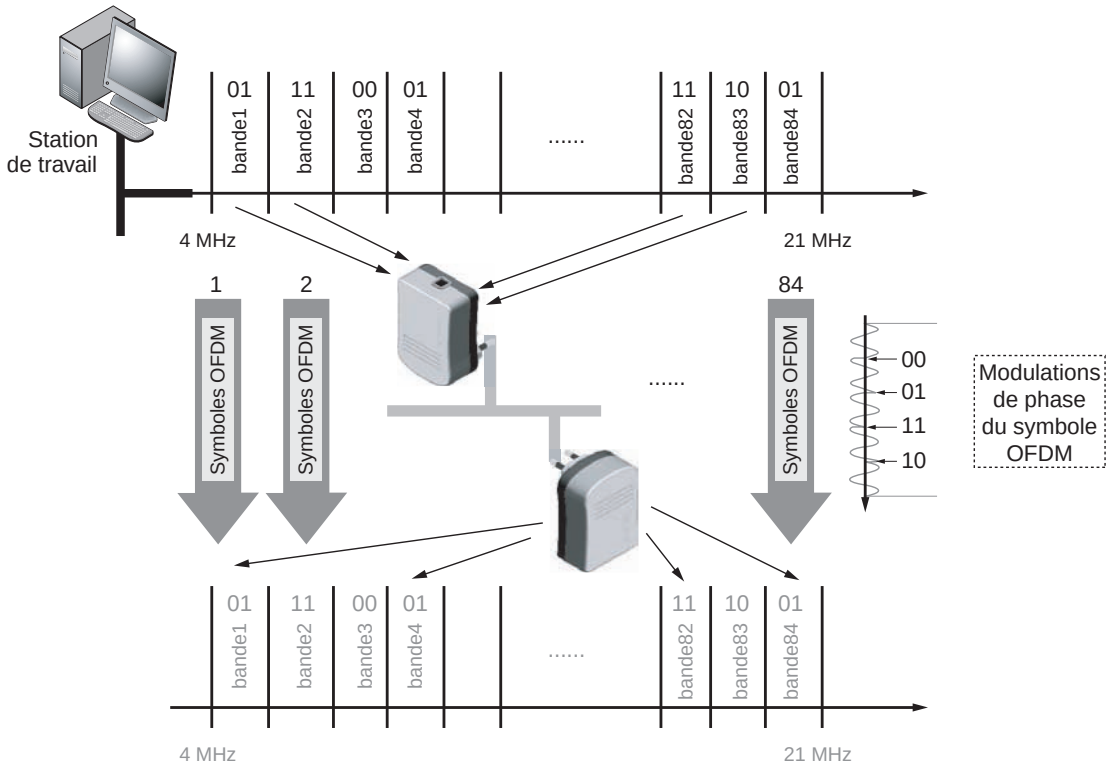


Figure 5.7

Répartition des symboles OFDM sur les bandes de fréquences

La trame HomePlug 1.0 utilise plusieurs techniques de modulation, de répartition fréquentielle et de correction d'erreur, qui forment un ensemble de traitement des données pour chaque équipement CPL entre l'interface analogique physique et l'interface Ethernet de type RJ-45.

Utilisation de la bande de fréquences pour les équipements HomePlug AV

Les évolutions techniques dans le domaine du traitement du signal dans des milieux comportant beaucoup d'interférences ont amené les développeurs de solutions CPL au sein du consortium industriel HomePlug à utiliser au maximum la bande de fréquences

autorisée des 1-30 MHz afin d'atteindre des vitesses de transmission situées autour de 200 Mbit/s.

HomePlug AV utilise 917 sous-bandes de fréquences au niveau physique. Chaque bande utilise ensuite des symboles OFDM afin de coder les données de manière orthogonale dans le domaine fréquentiel. Les bandes sont donc indépendantes du point de vue fréquentiel et n'interfèrent pas les unes avec les autres.

Dans chaque bande de fréquences, les données et leurs symboles OFDM sont codés par un code de convolution de type turbocode. C'est ensuite qu'intervient la modulation, potentiellement différente pour chaque bande de fréquences *(voir figure 5.8).*

Cette modulation peut aller du type BPSK, codant 1 bit par symbole et par bande de fréquences, jusqu'au type 1024-QAM, codant 10 bits par symbole et par bande de fréquences.

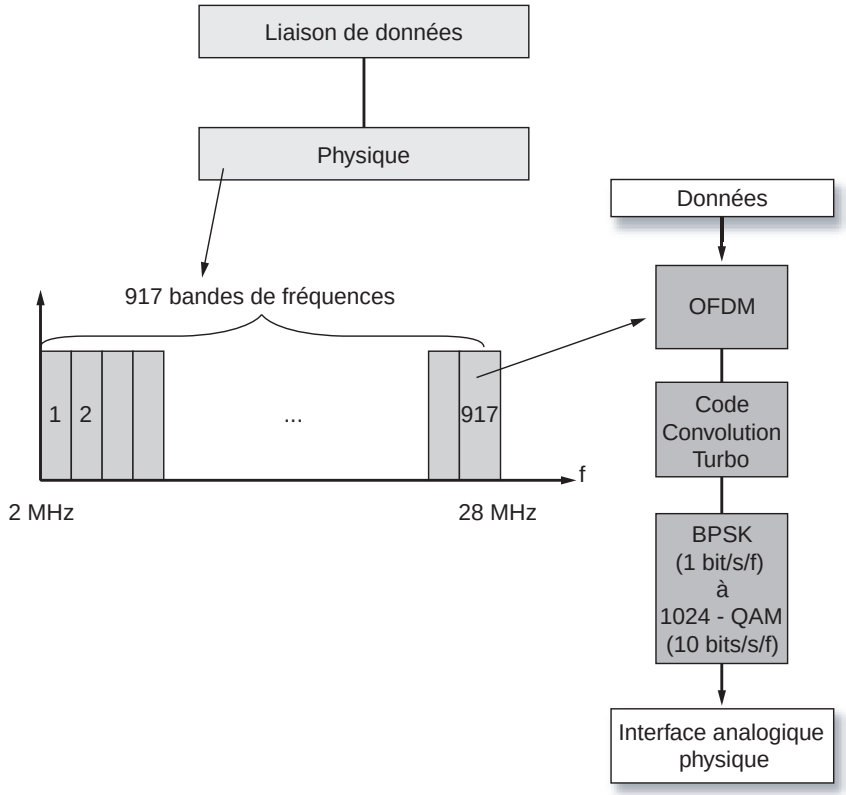


Figure 5.8
Détails de l'utilisation de la bande de fréquences dans HomePlug AV

Les blocs fonctionnels

Un équipement CPL est donc constitué de différents éléments électroniques de traitement du signal. Chaque élément électronique est doté d'une fonction précise dans la chaîne de traitement du signal qui transporte les données depuis l'interface connectée à un réseau Ethernet ou depuis l'interface connectée à un réseau électrique.

La figure 5.9 illustre les blocs fonctionnels qui permettent l'envoi et la réception des trames HomePlug 1.0 entre les différents équipements CPL du réseau, avec les adaptations relatives à la qualité du canal de transmission électrique.

Ces adaptations doivent se faire le plus efficacement possible afin d'atteindre des performances optimisées pour les couches protocolaires supérieures et les différents terminaux connectés sur les interfaces Ethernet de chaque équipement CPL.

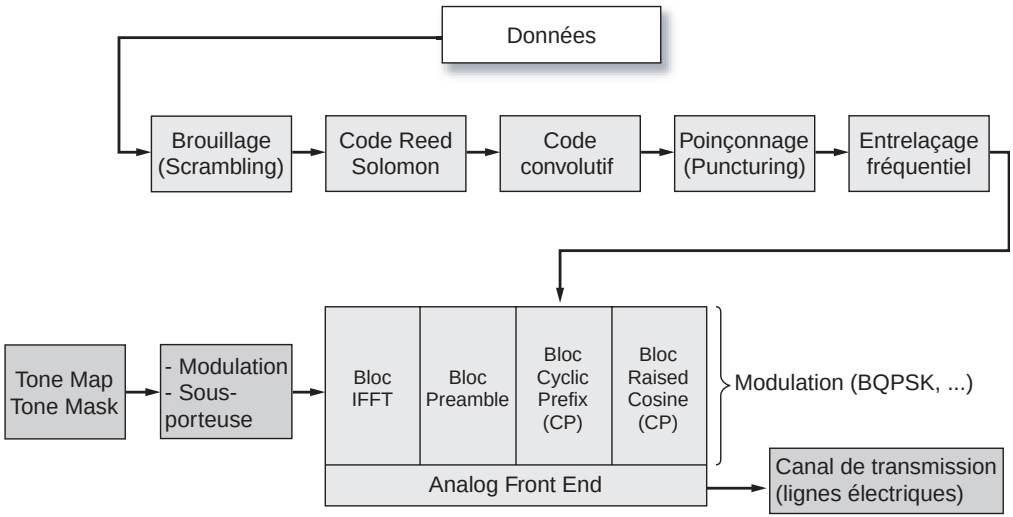


Figure 5.9

Blocs fonctionnels de traitement du signal de données dans HomePlug 1.0

Différences entre les trames HomePlug et les trames 802.11b

Fonctionnellement, les différentes parties des trames HomePlug 1.0 présentent quelques différences avec les trames IEEE 802.11b.

La différence principale concerne l'encapsulation MAC des technologies CPL. Les données de type MAC y sont définies dans des trames complètes, alors que les trames IEEE 802.doivent implémenter la couche LLC et un processus plus complexe de reconstitution de la trame MAC.

La figure 5.10 illustre, dans les cadres fléchés, les champs qui diffèrent entre les deux standards puisque 802.11 utilise une technique de contention légèrement différente et des espaces intertrames supplémentaires.

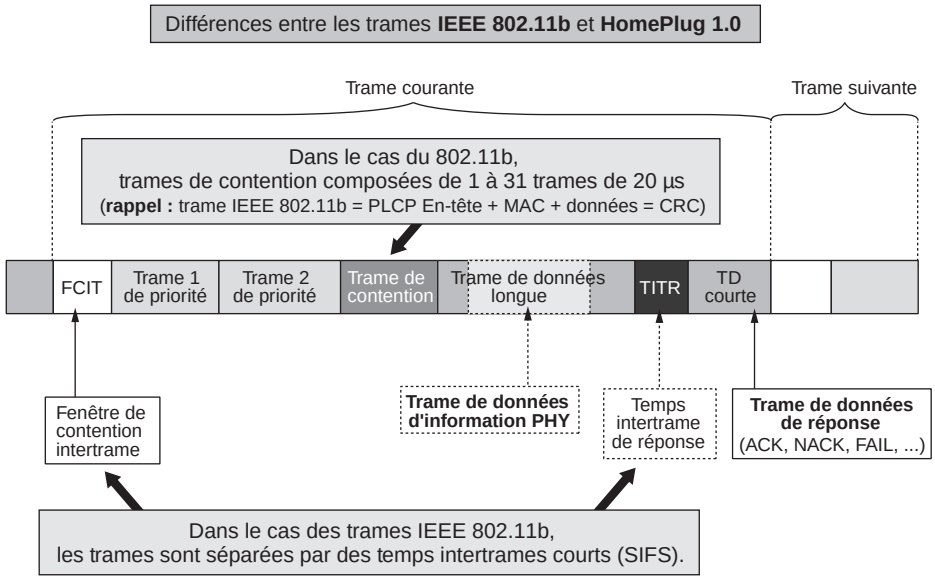


Figure 5.10

Différences entre les trames HomePlug 1.0 et les trames IEEE 802.11b

La trame physique CPL

Dans HomePlug 1.0, les trames de niveau physique, ou PHY PDU (PHYsical Protocol Data Unit), sont fortement liées avec les trames de niveau MAC, car certaines informations de la couche MAC sont disponibles au niveau de la couche PHY.

Au niveau de la couche physique, il existe deux types de PPDU, une longue et une courte, ainsi qu'un certain nombre d'éléments délimitant ces PPDU ou permettant leur espacement suffisant afin que les stations aient le temps de transmettre ou de recevoir les trames.

Les différents éléments des trames physiques HomePlug 1.0 sont les suivants :

- Trois délimiteurs :
  - **SOF (Start Of Frame),** qui est utilisé pour délimiter le début de la trame.
  - **EOF (End Of Frame),** qui est utilisé pour délimiter la fin de la trame.
  - **Short PPDU,** qui est la trame de réponse renvoyée par la station destination pour indiquer l'acquittement des données transmises.

- Deux intervalles de temps entre deux transmissions de trames :
  - **CIFS (Contention distributed Inter-Frame Spacing),** qui est l'intervalle de fin de trame avant le délimiteur de fin de trame.
  - **RIFS (Response Inter-Frame Spacing),** qui est l'intervalle de temps pendant lequel une station attend une réponse de la part de la station destination.
- **Long PPDU,** qui contient les trames de données.

La figure 5.11 illustre l'ensemble des parties constituant une trame physique CPL dans HomePlug 1.0 et Turbo avec la trame longue contenant les données des couches supérieures, l'intervalle intertrame permettant de délimiter les trames sur le média physique et la trame courte utilisée pour gérer les réponses des équipements CPL et optimiser les temps de communication sur le média.

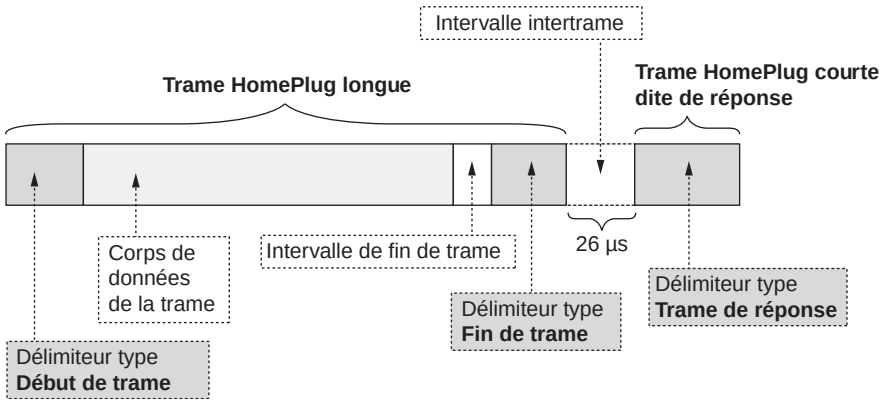


Figure 5.11
Éléments des trames physiques HomePlug 1.0

Les trames longues de niveau physique, aussi nommées PLCP-PDU (Physical Level Common Protocol-PDU), ne sont autres que les blocs d'éléments binaires qui sont émis sur la couche physique.

Ces trames longues, dites aussi Long PPDU, sont constituées de six parties, le préambule, le Frame Check, l'en-tête, le corps de trame, les bits de bourrage et le FCS :

- Le préambule inclus dans le SOF indique les timestamps des trames de type MAC.
- Le FC (Frame Check) permet le contrôle de la trame. Cette dernière est composée de quatre symboles OFDM très résistants au bruit sur le canal de transmission et utilisant un code de convolution de type turbocode. Ce code est largement utilisé en traitement du signal dans HomePlug AV. Ces quatre symboles doivent être impérativement transmis sur le canal de transmission afin de permettre à la station destination de connaître l'état de la liaison et le nombre d'erreurs dans les données transmises.

- L'en-tête contient diverses informations, concernant notamment le débit de la connexion, lequel peut varier en fonction de la qualité du signal.
- Le corps de trame contient les informations provenant de la couche MAC, juste au-dessus. Ces informations sont encore appelées MPDU (MAC Protocol Data Unit).
- Les bits de bourrage sont utilisés pour remplir la trame dans le cas où les données utiles ne permettent pas d'atteindre la taille minimale d'une trame.
- Le FCS (Frame Check Sequence) permet de vérifier l'intégrité des données contenues dans le corps de trame.

L'ensemble des durées de la trame HomePlug 1.0, sans les en-têtes de priorité et de contention, est estimé à 1,5 ms, incluant le corps de trame, qui comporte 160 symboles OFDM pour une durée de 1,328 ms.

La figure 5.12 illustre les éléments constitutifs de la trame longue dans HomePlug 1.0 et Turbo. Cette trame longue est globalement constituée de trois parties : le début de trame permettant d'identifier sur le réseau une trame longue, les données (dans lesquelles on retrouve le corps de la trame avec les données des couches supérieures) et la fin de trame permettant d'identifier une fin de trame et donc d'indiquer aux équipements CPL qu'ils peuvent envoyer les trames suivantes.

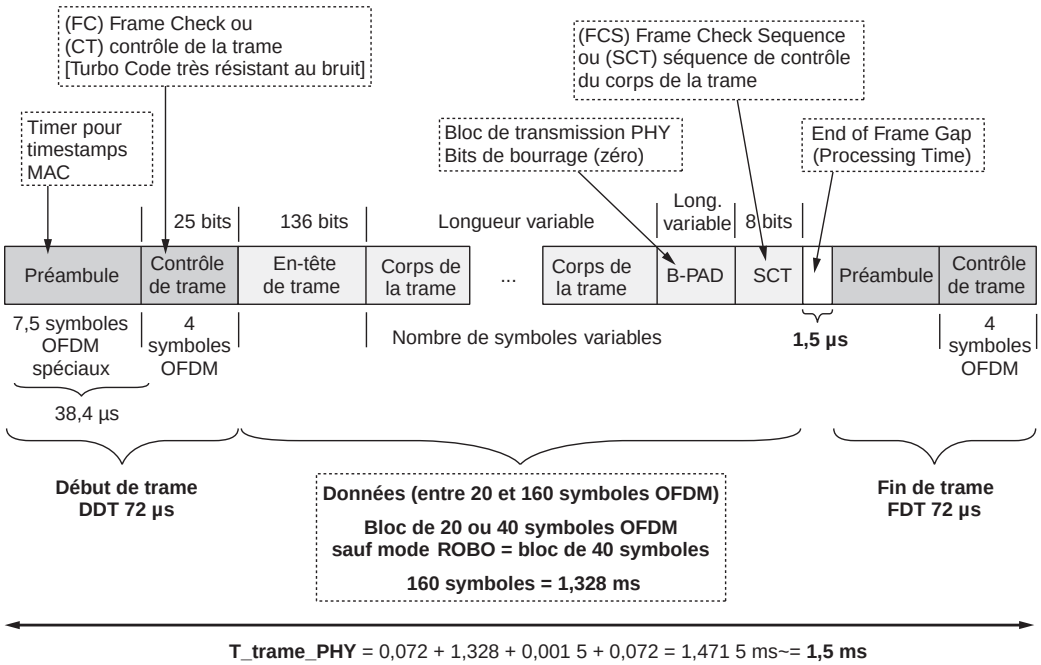


Figure 5.12
Structure de la trame longue HomePlug 1.0

Le délimiteur de début de trame physique

Le délimiteur de début de trame contient deux parties, le préambule et le FC :

- Le préambule contient l'horodateur d'envoi de la trame.
- Le FC (Frame Check), ou contrôle de trame, contient plusieurs champs : un champ de contrôle de contention, qui permet de vérifier le niveau de contention des trames transmises, un champ indiquant le type du délimiteur, un champ variable, comportant lui-même deux champs particulièrement importants pour les communications CPL (la Tone Map qui stocke les états des liaisons entre les stations CPL et la taille de la trame de données qui suit), et une séquence de contrôle de la trame. Ce dernier champ utilise un CRC (Cycle Redundancy Check) pour vérifier la séquence de contrôle de l'intégrité de la trame *(voir figure 5.13).*

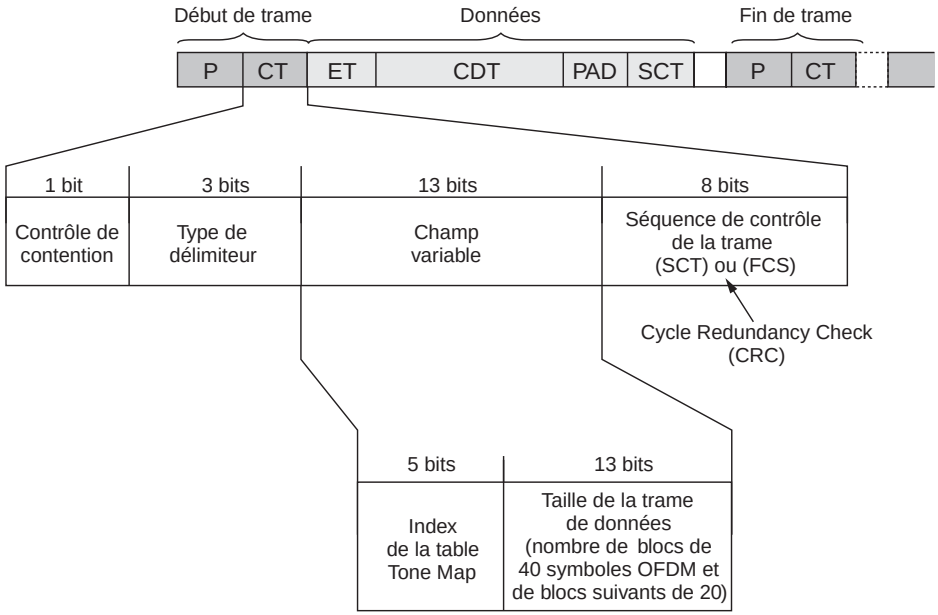


Figure 5.13

En-tête de début de trame de la trame physique

Le corps de données de la trame physique

Le corps de données de la trame physique est illustré à la figure 5.14. Il comporte une MDPU encapsulée dans la PPDU. La MPDU comporte les champs EB (En-tête de bloc), PAD (bits de bourrage), au cas où les données ne remplissent pas complètement la partie données, et le SCB (séquence de contrôle de bit).

Le champ SCB utilise un ICV (Integrity Check Value) pour vérifier l'intégrité des données formant le corps de données.

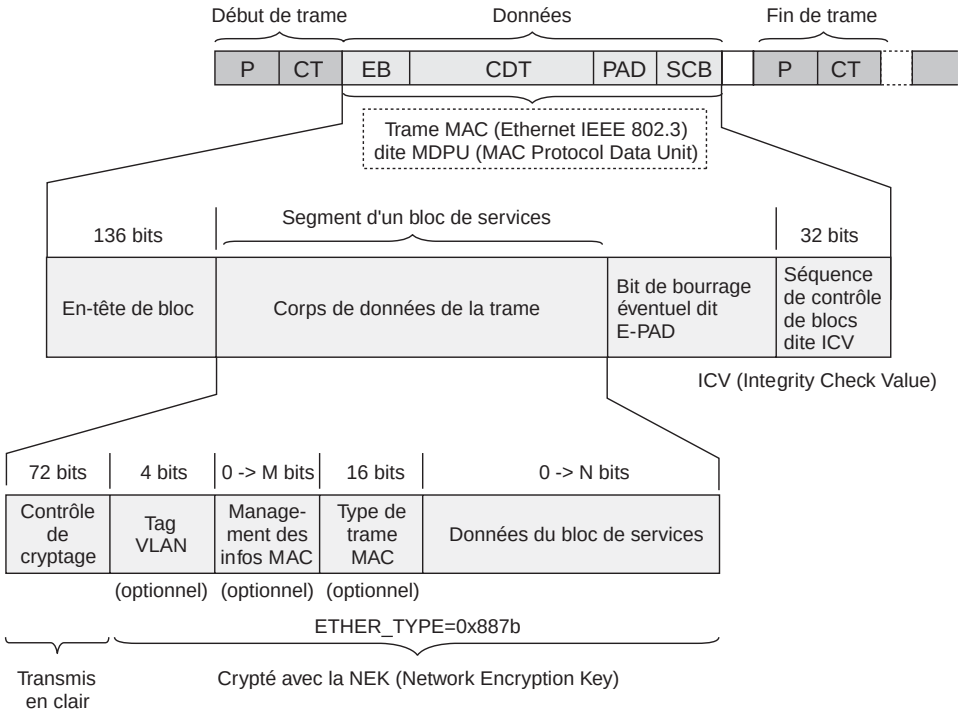


Figure 5.14

Corps de données de la trame physique

Le délimiteur de fin de trame physique

La trame physique se termine par un délimiteur de fin de trame, qui est composé d'un préambule et d'un champ de contrôle de la trame.

Le champ de contrôle de la trame est composé des quatre champs suivants *(voir figure 5.15) :*

- Contrôle de contention, qui permet de vérifier l'état des périodes de contention entre trames.
- Type de délimiteur, spécifiant si le délimiteur est en début ou en fin de trame.
- Champ variable, spécifique de ce délimiteur, qui contient le niveau de priorité de la station CPL (indiqué par le paramètre CAP).

- FCS, qui utilise un CRC sur 16 bits pour le contrôle de l'intégrité des trames. Le FCS est calculé aussi bien sur l'en-tête que sur le corps de trame. Les techniques utilisées dans le FCS sont définies classiquement dans les principaux standards de transport de trames sur une liaison.

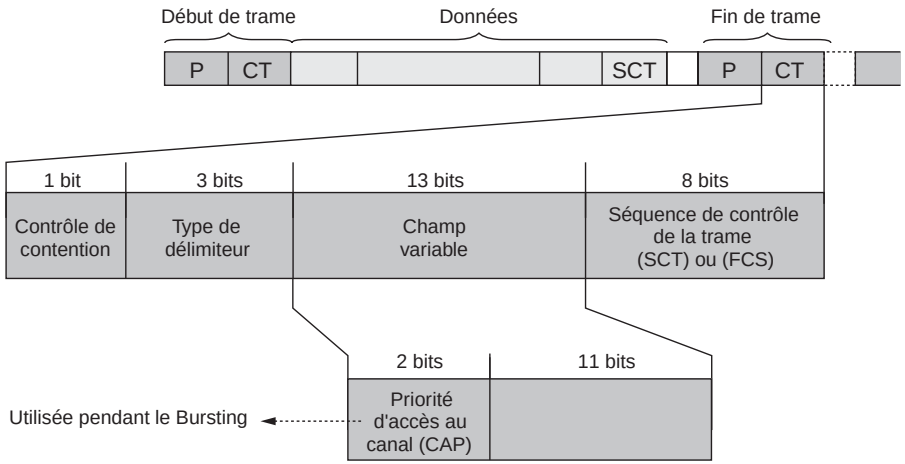


Figure 5.15
Champs de fin de trame de la trame physique

Les trames MAC

Situées juste au-dessus de la couche physique, les trames MAC (Médium Access Control) permettent une liaison avec les couches des niveaux supérieurs.

Comme indiqué précédemment, la technologie CPL peut être vue comme une encapsulation MAC, les trames MPDU étant encapsulées dans des PPDU longs. De même, toutes les données venant des couches supérieures à la couche MAC sont encapsulées dans la trame MAC.

La trame MAC HomePlug 1.0

Dans le cas de HomePlug 1.0, l'encapsulation de la trame IEEE 802.3, ou MPDU (Mac Protocol Data Unit), est incluse dans le corps de trame de la trame CPL entre les délimiteurs de début et de fin de trame.

Les trames Ethernet HomePlug 1.0 sont facilement identifiables sur un réseau Ethernet, car elles ont toutes le champ de type de trame MAC ETHERTYPE marqué à la valeur hexadécimale 0x887b. Ce paramètre permet de créer des applications au niveau de la couche liaison de données dédiées aux technologies CPL HomePlug. Dans le cas de HomePlug AV, la valeur du champ ETHERTYPE est égale à 0x88e1.

En plus du contrôle de cryptage sur 72 bits, le corps de données est crypté par la clé de cryptage NEK (Network Encryption Key), échangée entre les différentes stations CPL du réseau.

Les MPDU constituent ce qu'on appelle un bloc de services (BS). Si le BS dépasse la taille limite des trames MAC, de 1 500 octets, le BS subit une fragmentation en segments, qui sont envoyés en séquence par les stations source. Les MPDU subissent alors une séquence de fragmentation-réassemblage au cours de la transmission et de la réception par les différentes stations CPL du réseau.

Chaque segment d'une MPDU est numéroté et séquencé afin d'être réassemblé par la station destination.

Format de l'en-tête MAC

La trame MAC commence par un en-tête assez complexe, contenant trois champs d'une longueur totale de 17 octets, comme illustré à la figure 5.16.

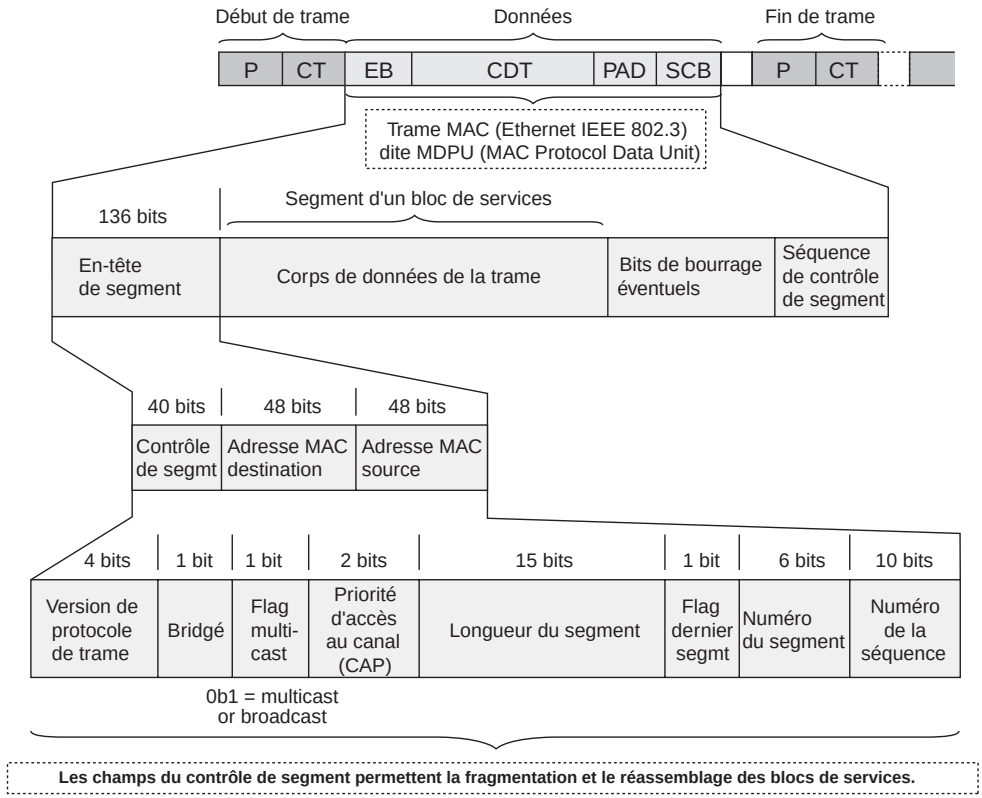


Figure 5.16

En-tête de la trame MAC de HomePlug 1.0

Le champ contrôle de bloc

Le premier champ de l'en-tête porte sur 40 bits, subdivisés en huit sous-champs. Le rôle de ce champ est de transporter les informations de contrôle nécessaires à la couche MAC.

La figure 5.16 illustre le champ contrôle de trame et son découpage en sous-champs. Les rôles des différents sous-champs sont les suivants :

- **Version de protocole :** définit la valeur du protocole utilisé. Cette valeur est réservée et ne sera utilisée que lors d'une évolution du standard.
- **Bridgé :** indique si la station CPL qui transmet les données est en mode pont et peut potentiellement relayer les trames vers d'autres stations du réseau.
- **MCF (Multicast Flag) :** indique si les trames sont envoyées en mode multicast ou broadcast en plaçant cette valeur à 0b1.
- **CAP (Channel Access Priority) :** reprend le niveau de priorité de la station source par rapport aux autres stations du réseau CPL.
- **Longueur du segment :** permet de connaître la longueur des données du segment transmis.
- **LSF (Last Flag Segment), ou flag dernier segment :** permet de savoir, si la valeur est placée à 0b1, que ce segment est le dernier du BS.
- **Numéro du segment :** indique l'ordre de fragmentation et de réassemblage des différents segments du BS.
- **Numéro de séquence du segment :** à chaque trame est assigné ce numéro initié à 0 et incrémenté par pas de 1 pour toutes les autres trames transmises. Si une trame est fragmentée, tous les segments de cette trame portent le même numéro de séquence.

Les champs adresse

Dans HomePlug, les champs d'adresse ont tous une longueur de 6 octets et le même format que les adresses définies dans le standard IEEE 802.3.

L'adresse sur 48 bits est composée des quatre parties suivantes :

- **Individual/Group (I/G) :** le premier bit indique si l'adresse est individuelle (1) ou de groupe (0).
- **Universal/Local (U/L) :** le deuxième bit indique si l'adresse est locale (1) ou universelle (0). Si l'adresse est locale, les 46 bits suivants sont définis localement.
- **Organizationally Unique Identifier :** numéro assigné par l'IEEE, correspondant aux 22 bits suivant les bits I/G et U/L.
- **Numéro de série :** les trois deniers octets, soit 24 bits, correspondent au numéro de série généralement défini par le constructeur.

Format hexadécimal

L'écriture hexadécimale, ou système de numérotation en base 16, de l'adresse MAC est généralement préférée à l'écriture binaire.

Les adresses MAC sont constituées de deux familles d'adresses distinctes, les adresses dites individuelles, qui adressent une seule station sur le réseau, et les adresses de groupe, qui adressent plusieurs stations sur le réseau. L'adresse MAC dans ce dernier cas représente tout un groupe de stations.

Il existe deux types d'adresses de groupe :

- **Adresse broadcast.** Cette adresse est associée à un groupe de stations, lequel est composé de l'ensemble des stations constituant le réseau. L'utilisation d'une adresse broadcast permet d'envoyer des informations à toutes les stations du réseau. Le format d'une adresse broadcast est toujours de 48 bits, tous mis à 1.
- **Adresse multicast.** Comme pour l'adresse broadcast, cette adresse est associée à un groupe de stations, mais en nombre fini. Ce type d'adresse commence toujours par les premiers 24 bits de l'adresse MAC sur 48 bits égale à 01 :00 :5^{E} (en hexadécimal).

Une trame MAC 802.3 comme celle utilisée dans HomePlug contient les deux champs d'adresse différents suivants :

- **DA (Destination Address) :** adresse à laquelle est transmise la trame ou le segment. L'adresse DA peut être individuelle ou de groupe.
- **SA (Source Address) :** adresse ayant transmis la trame ou le segment. L'adresse SA est toujours une adresse individuelle.

Format d'une trame MAC chiffrée

Grâce au standard IEEE 802.3, il est possible de chiffrer une trame pour sa traversée du support électrique, de telle sorte qu'aucun utilisateur ne puisse déchiffrer l'information.

En réalité, comme l'illustre la figure 5.17, une trame chiffrée ne l'est que partiellement. Le cryptage de la trame s'effectue grâce aux deux champs suivants :

- **IV (Initialization Vector) :** vecteur d'initialisation ayant un bloc de bits concaténé au bloc de données principales pour le chiffrement de la trame. L'IV est réinitialisé après chaque utilisation. Le mélange entre cet IV et les données crée une clé de chiffrement unique.
- **EKS (Encryption Key Select) :** index permettant de récupérer la clé NEK permettant de déchiffrer la trame.

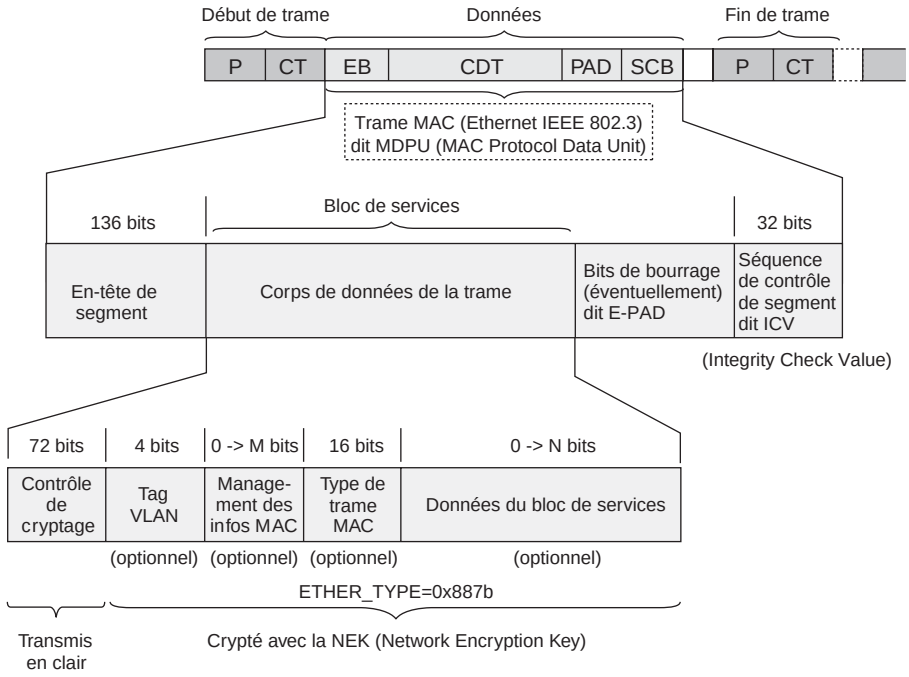


Figure 5.17

Détails de la trame MAC HomePlug 1.0 chiffrée

Format des trames de contrôle et de gestion

Les trames de contrôle et de gestion ont pour fonction d'envoyer les commandes et informations de supervision aux éléments du réseau qui en ont besoin pour fonctionner.

Comme l'illustre la figure 5.18, ce sont les informations de longueur de trame et de réponse attendue par la station source qui permettent la gestion et le contrôle des trames *(voir le chapitre 3).*

Certains fabricants de produits CPL implémentent des couches MAC spécifiques pour faciliter la gestion et le contrôle du réseau. La marque Oxance a ainsi développé une couche spécifique pour HomePlug.

Dans les équipements Oxance *(www.oxance.com),* l'architecture des trames de communication entre équipements CPL comporte des couches PHY et MAC de type HomePlug 1.0 classique et une couche de niveau MAC et IP constituant le PLRP (Power Line Routing Protocol). C'est cette dernière qui permet une gestion simplifiée de l'ensemble des équipements CPL du réseau.

La figure 5.19 illustre un réseau constitué d'équipements CPL Oxance vus par IP comme une seule adresse réseau, simplifiant d'autant la gestion du réseau. Nous reviendrons sur la configuration de ces équipements aux chapitres 9, 10 et 11.

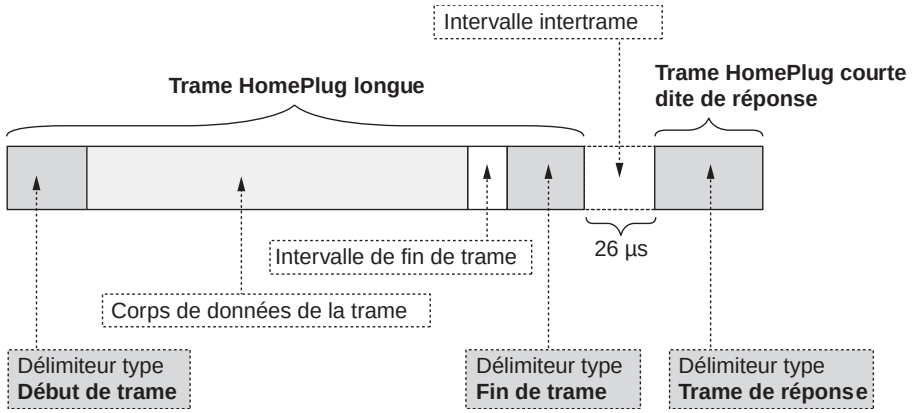


Figure 5.18

Champs de contrôle et de gestion des trames CPL

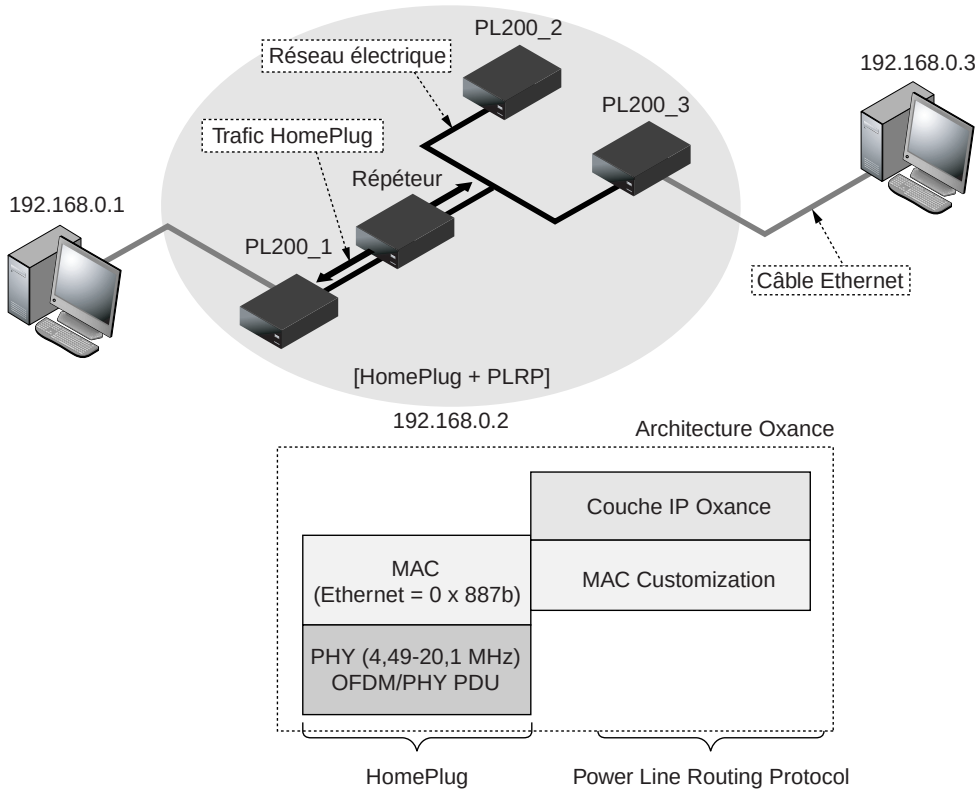


Figure 5.19

Architecture de la technologie PLRP dans les équipements Oxance

PARTIE II

Pratique des CPL

La première partie de l'ouvrage a présenté l'architecture des réseaux CPL et expliqué leur fonctionnement du point de vue théorique. Cette deuxième partie, résolument pratique, détaille les règles à respecter pour installer de tels réseaux en mettant l'accent sur les nouvelles possibilités applicatives apportées par les concepts de diffusion de données sur un réseau électrique, ainsi que sur les contraintes électriques et le choix, l'installation et la configuration des équipements.

Le caractère à la fois simple et pratique des réseaux CPL leur assure un développement rapide, qui ne va pas manquer de se poursuivre avec l'arrivée des nouvelles versions des technologies CPL, engendrant en retour de nouvelles applications.

Du point de vue applicatif, les réseaux CPL n'apportent pas de rupture particulière, et l'on y retrouve les applications classiques, notamment de voix et de vidéo. L'utilisation d'un réseau électrique pour transporter les données en haut débit a toutefois engendré des applications inattendues, comme le transport des données dans une voiture ou l'utilisation du CPL comme dorsale d'un réseau Wi-Fi.

Nous n'en sommes encore qu'aux prémices de ces nouveaux usages, et les applications vont évoluer avec le temps pour intégrer davantage de convivialité, de simplicité et surtout de fonctionnalités, ce qui est sans doute le plus important aux yeux des utilisateurs.

Si la philosophie du CPL paraît simple de prime abord, il n'en va pas de même quand on se plonge dans ses spécificités techniques. Au niveau électrique, par exemple, les notions de topologie de réseau électrique et d'interférences sont des caractéristiques essentielles à considérer lors de l'installation d'un réseau CPL. Il est en outre important de différencier les notions de débit utile et de débit théorique. Ce dernier correspond à la vitesse de transmission du réseau. Le débit utilisable est moindre du fait des mécanismes mis en œuvre par les protocoles réseau des différentes couches (physique, liaison de données, réseau, transport, etc.). Ces mécanismes ont été amplement commentés aux chapitres 3 et 5 précédents.

L'équipement de base d'un réseau CPL a fortement évolué au cours de ces dernières années. Au départ, on ne trouvait que des terminaux sous forme de boîtiers volumineux, de type *desktop*, relativement inadaptés aux besoins des utilisateurs. Actuellement, les équipements proposent toutes sortes de configuration, avec plusieurs interfaces et de

nombreuses fonctionnalités réseau intégrées (routeur, modem, point d'accès Wi-Fi, switch, etc.), qui permettent de constituer des configurations adaptées aux besoins.

La configuration d'un réseau Wi-Fi commence par celle du terminal, et donc de l'adaptateur CPL. Nous la détaillons dans cette partie pour les systèmes d'exploitation Windows XP, Linux et FreeBSD. Une fois le terminal configuré vient la phase d'installation. Cette dernière doit respecter un certain nombre de contraintes, telles que la topologie du réseau électrique, la sécurité et les performances.

En suivant les conseils et étapes de configuration expliqués pas à pas tout au long des chapitres de cette partie, le lecteur sera à même d'installer et de configurer lui-même un réseau CPL dans les meilleures conditions possibles.

Nous conclurons cette partie et l'ouvrage en présentant les futurs standards des réseaux CPL, qui, dans un avenir proche, constitueront les briques de base de l'Internet domestique et professionnel, facilitant le développement de la domotique, fondée, rappelons-le, sur les échanges de données au sein d'une maison ou d'un bâtiment.

6

Applications

De nombreuses études prospectives montrent que, d'ici à quelques années, 90 % des terminaux connectés en réseau ne seront pas des ordinateurs. Cette perspective démontre que de nombreux appareils électriques et électroniques de tout type dans de nombreux domaines (industrie, hôpitaux, domotique, électronique, arts numériques, etc.) seront dotés d'une interface réseau de type RJ-45 permettant de se connecter à un réseau local de type Ethernet.

Ces dernières années ont été les témoins de la prédominance des deux standards majeurs des réseaux que sont Ethernet et IP. Partant de ce constat, il est logique de penser que les réseaux de communication entre appareils vont principalement se développer sur les supports de communication les plus pratiques et les plus fiables. Dans cette optique, les CPL constitueront sans doute des acteurs de premier ordre, du fait de l'étendue du réseau électrique (réseau de prises électriques, réseau de lumière, etc.), pour doter les différents appareils des plus récentes fonctionnalités de la communication en réseau.

Les réseaux CPL apportent de nouveaux usages au monde des réseaux, dont la plus importante est sûrement la facilité, puisque l'utilisateur n'a qu'à utiliser les prises électriques du bâtiment pour constituer un réseau informatique.

Ce réseau, une fois installé, offre des débits suffisants pour des applications temps réel et multimédias. Il peut en outre faire office de dorsale d'un réseau Wi-Fi. Le réseau CPL devient alors le complément idéal de Wi-Fi, permettant d'étendre sa couverture et d'obtenir le meilleur de cette technologie.

Voix, vidéo et multimédia

La voix et la vidéo sont des applications temps réel complexes à mettre en œuvre dans les réseaux asynchrones tels que les CPL. Elles représentent pourtant probablement une partie de l'avenir de ces réseaux, en tant que prolongement de l'application téléphonique.

En 2005, la téléphonie classique autour de PABX et sa distribution vers les postes téléphoniques ont commencé à être remplacées par de la téléphonie sur IP dans un environnement CPL. Début 2007, les réseaux CPL devraient diffuser des canaux de télévision et prendre en charge des applications de vidéoconférence entre utilisateurs. Quant au multimédia, il devrait rapidement devenir un critère majeur du choix de la technologie CPL, notamment dans les entreprises.

Téléphonie sur CPL

Le débit n'est pas un problème en soi pour le transport de la parole téléphonique, puisqu'il peut descendre jusqu'à 5,6 Kbit/s et qu'une telle valeur est largement supportée par les réseaux CPL.

En revanche, l'application de téléphonie étant interactive, il ne doit pas s'écouler plus de 300 ms entre le moment où l'information part d'un utilisateur et celui où elle arrive au destinataire. Si le réseau est symétrique, le temps maximal aller-retour ne doit donc pas dépasser 300 ms. Cette valeur est le maximum autorisé pour une application avec interaction humaine.

La deuxième contrainte pour le transport de la parole téléphonique est la synchronisation. Les informations doivent être disponibles à des instants précis au récepteur. Il faut notamment que les octets provenant de la numérisation soient remis à des instants de synchronisation parfaitement déterminés. Par exemple, si la compression génère un flux à 8 Kbit/s, cela implique une synchronisation chaque microseconde. Un octet doit donc être délivré au récepteur chaque microseconde. Si la parole n'est pas compressée, la synchronisation d'une voie à 64 Kbit/s s'effectue toutes les 125 µs.

La troisième grande caractéristique de la téléphonie CPL est l'utilisation de la technique VoIP (Voice over IP). Les octets de parole sont acheminés dans des paquets IP et utilisent les mêmes ressources réseau que les paquets acheminant les autres applications. La téléphonie sur CPL est donc intégrée dans le cadre classique de la parole sur IP.

La figure 6.1 illustre la contrainte de synchronisation au niveau du téléphone distant. Bien que partant régulièrement de l'émetteur, les paquets arrivent de façon irrégulière au récepteur, rendant assez difficile la remise des octets de parole au récepteur à des instants précis. Cette irrégularité à l'arrivée est due à la traversée du réseau CPL, qui rend aléatoire l'arrivée des paquets de parole.

La méthode d'accès utilisée pour obtenir le droit de transmettre vers le point d'accès, le CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), rend aléatoire le temps de traversée du réseau CPL. De plus, pour atteindre le destinataire, les paquets doivent

souvent traverser des réseaux plus vastes et passer par des nœuds de transfert intermédiaires dont le temps de traversée est également aléatoire.

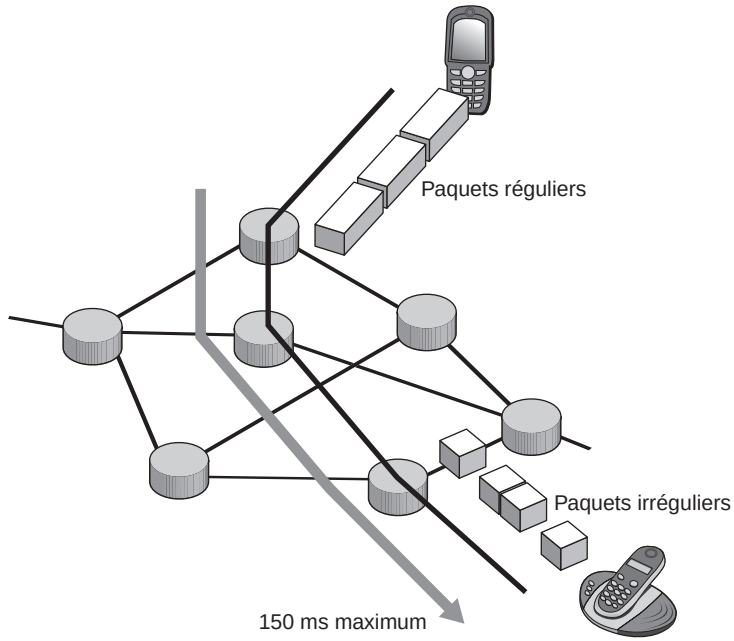


Figure 6.1
Contraintes de la communication téléphonique

Paquétisation-dépaquétisation de la parole

Nous allons supposer que la parole est compressée à 8 Kbit/s, ce qui est le standard le plus classique dans les environnements de téléphonie sur IP.

Les octets de téléphonie doivent être paquétisés dans un paquet IP, lui-même encapsulé dans une trame Ethernet, ou plus exactement dans une trame CPL, pour être transmis sur le réseau électrique.

À la vitesse de 8 Kbit/s, la synchronisation s'effectue chaque microseconde. Si n est le nombre d'octets utilisables dans une trame CPL, le temps de remplissage est de $n \times 1$ ms. La longueur minimale de la trame CPL étant de 64 octets, il faut 64 ms pour la paquétisation.

La dépaquétisation ne demande pas vraiment de temps supplémentaire, car elle se fait en parallèle de la paquétisation. Le temps de paquétisation-dépaquétisation est donc égal au minimum à 64 ms. En réalité, on a tendance à ajouter le temps de paquétisation et de dépaquétisation pour tenir compte des temps de latence que l'on trouve dans la plupart des paquétiseurs-dépaquétiseurs.

Ce temps de 64 ms est acceptable pour rester en dessous des 150 ms de trajet aller. Cependant, cette valeur de 64 ms peut s'avérer trop importante si le paquet doit traverser d'autres réseaux que le réseau CPL ou si les paquétiseurs-dépaquétiseurs sont beaucoup plus lents. C'est la raison pour laquelle les paquets de parole ne sont remplis que de 16 octets de parole et que le reste est complété par des octets de bourrage pour atteindre la taille minimale de la trame. Ces 16 octets permettent de rester à un temps de paquétisation-dépaquétisation de l'ordre de 16 ms.

Débit réel

Le débit réel sur le réseau est en réalité bien supérieur à 8 Kbit/s, car le paquet contient quantité d'informations supplémentaires, comme les en-têtes et les octets de bourrage. On considère que le débit réel sur un réseau CPL ou tout autre réseau à transfert de paquets est de l'ordre de 60 à 70 Kbit/s en utilisant le standard IPv4 et après encapsulation dans une trame Ethernet.

Si le standard IPv6 est utilisé, les champs de supervision sont encore plus importants, et l'on considère qu'une voie de parole dépasse les 100 Kbit/s.

Le temps demandé par le codeur-décodeur, ou codec, pour numériser le signal à partir d'un signal analogique ou *vice versa* peut être estimé à 5 ms. Nous obtenons donc 26 ms pour le codage, le décodage et la paquétisation-dépaquétisation. Le temps total admissible de transport devient donc de 124 ms (150 ms de transport au maximum, comme indiqué au début de cette section, moins 26 ms pour les différents délais). Ce temps de transport inclut la technique d'accès MAC au réseau CPL.

Temps de transit

Dans le CPL, le temps d'attente pour accéder au support électrique peut être relativement long. Si, par exemple, cinq clients sont connectés au même réseau électrique en utilisant des trames de 1 500 octets et en intégrant les temps d'accès liés au CSMA/CA, nous obtenons une attente de l'ordre de 10 ms, voire davantage. Si l'on suppose que la parole téléphonique est destinée à un autre employé d'une même entreprise, lui-même connecté à un réseau CPL, il faut ajouter à nouveau une dizaine de millisecondes d'accès au réseau.

Au total, le temps de transit reste, en supposant un trafic relativement important mais sans collision, de l'ordre de 100 ms. Ce temps permet le transport d'une parole téléphonique dans de bonnes conditions sur un réseau CPL.

Du fait que la génération CPL actuelle ne gère pas les priorités, les paquets des autres utilisateurs passent avec la même priorité, même s'ils transportent des données sans intérêt immédiat. Par exemple, un client travaillant sous une application peer-to-peer (P2P) et récupérant un fichier vidéo de plusieurs gigaoctets voit ses paquets passer aléatoirement devant les paquets d'un utilisateur en train de téléphoner. C'est la raison pour laquelle une limitation drastique du nombre d'utilisateurs ou du trafic global est indispensable dans la présente génération CPL. La prochaine génération CPL HomePlug AV sera capable de gérer les priorités des paquets téléphonie et vidéo, permettant d'assurer la qualité de service sur le réseau de données.

Si le nombre d'utilisateurs dépasse la dizaine ou que le débit utile est supérieur à 5 Mbit/s, un réseau CPL HomePlug 1.0 ne permet pas d'assurer avec certitude, c'est-à-dire avec la qualité de service nécessaire, le transport de la parole téléphonique. Dans ce cas, il faut faire appel à une autre technique pour attribuer des priorités aux paquets transportant la parole téléphonique.

Différenciation des paquets IP

Deux solutions peuvent être déployées à court terme pour mettre en œuvre cette différenciation entre les paquets qui transitent par les CPL :

- Une technique de contrôle des paquets IP au niveau même du protocole IP. Dans ce cas, le gestionnaire du réseau CPL ralentit l'arrivée des acquittements des paquets non prioritaires délivrés par les stations réceptrices, de telle sorte que ces flots soient maintenus dans un état de *slow-start,* dans lequel les stations émettrices ne peuvent envoyer que quelques paquets et doivent se mettre en attente des acquittements.
- Utiliser le standard HomePlug AV, dont la sortie est prévue pour fin 2006, qui détermine des priorités au niveau de la couche MAC. Dans ce cas, il suffit d'attribuer aux terminaux téléphoniques la priorité de plus haut niveau.

De ces deux solutions, la meilleure est évidemment la seconde, puisqu'elle intervient au niveau le plus bas de l'architecture et privilégie clairement les flots de parole téléphonique. L'autre solution est plus artificielle, puisqu'elle consiste à restreindre les flots non prioritaires sans mesurer le besoin réel de bande passante des clients prioritaires, de type parole téléphonique.

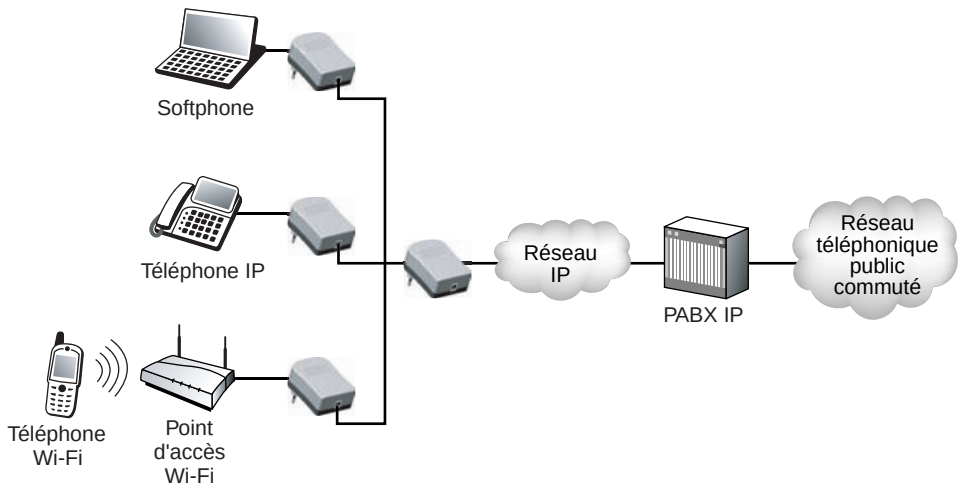


Figure 6.2

Équipements traversés par un flot de parole numérique CPL

La figure 6.2 illustre les différents organes traversés lors du transport de la parole téléphonique dans un cadre plus vaste qu'une simple conversation d'un terminal à un autre

d'un même réseau CPL. Après la traversée du réseau CPL de départ, le flot de paquets téléphoniques chemine dans un réseau IP fixe, qui peut être celui d'un opérateur, puis passe par une passerelle spécialisée, le PABX IP, avant de franchir l'infrastructure téléphonique classique. Le PABX IP transforme les adresses IP en adresses téléphoniques et effectue les transcodages nécessaires d'un flot compressé vers un flot téléphonique d'opérateur à 64 Kbit/s.

Le logiciel Asterisk permet typiquement de constituer un IPBX (PABX), qui gère au niveau du serveur les appels IP locaux et les appels sortants vers le RTC (réseau téléphonique commuté).

Téléphonie de qualité hi-fi

Les CPL permettent de transporter des paroles de qualité bien supérieure à celle de la voix téléphonique classique. En effet, n'ayant pas vraiment de contraintes de débit, ils peuvent absorber une bande passante importante, susceptible de transporter une qualité hi-fi ou presque.

Supposons une parole à 512 Kbit/s compressée à 64 Kbit/s. Pour remplir les 64 octets de données téléphoniques il ne faut que 8 ms. Globalement, le débit du flot de paquets IP est le même que précédemment, mais, faute d'être rempli avec des octets de bourrage, il ne contient que des octets utiles. Avec le même débit réel, on peut donc transporter une parole de qualité bien supérieure.

Cette technique n'est pas encore très répandue parce que les équipements téléphoniques ne sont pas toujours compatibles avec une telle qualité. La compatibilité pourrait être trouvée en utilisant un micro-ordinateur avec une carte son. Malheureusement, cette solution ne s'avère pas meilleure, car les cartes son du commerce sont très lentes et demandent un temps de traitement d'une cinquantaine de millisecondes, ce qui, lorsqu'il faut en traverser deux, celles de l'émetteur et du récepteur, rend le temps de transit inacceptable.

Cet exemple montre en tout cas qu'une extension intéressante de la téléphonie sur CPL pourrait être une téléphonie de haute qualité.

Vidéo

La vidéo est une autre application qui devrait se développer à l'avenir dans les réseaux CPL. Cette application a surtout besoin d'un débit élevé, lequel devient accessible dans les environnements CPL.

Suivant le type d'application vidéo considéré, la contrainte temporelle est plus ou moins forte. Nous examinons ci-après les deux principaux cas de figure, le streaming vidéo et les visioconférence et vidéoconférence.

Streaming

Avec le streaming sans voie de retour, comme la vidéo à la demande, ou VoD (Video on Demand), et la télévision, entre l'instant d'émission du flux vidéo depuis la source et l'instant où cette vidéo est jouée à l'écran, il peut s'écouler un temps assez long, de l'ordre de plusieurs secondes jusqu'à une quinzaine de secondes. Le spectateur n'a pas forcément la sensation que la source vidéo émet bien avant qu'il voie les images.

La seule contrainte à respecter pour ces applications est le temps d'attente au début de la vidéo. Il est assez agaçant d'avoir à patienter pendant que l'application s'initialise à chaque changement de chaîne du fait de la resynchronisation au niveau du récepteur. L'objectif du streaming est de laisser un peu d'avance au flot de paquets pour atteindre le récepteur et d'avoir suffisamment de paquets en mémoire dans le récepteur pour qu'il n'y ait pas d'interruption dans la délivrance des paquets au client. Cette contrainte est illustrée à la figure 6.3.

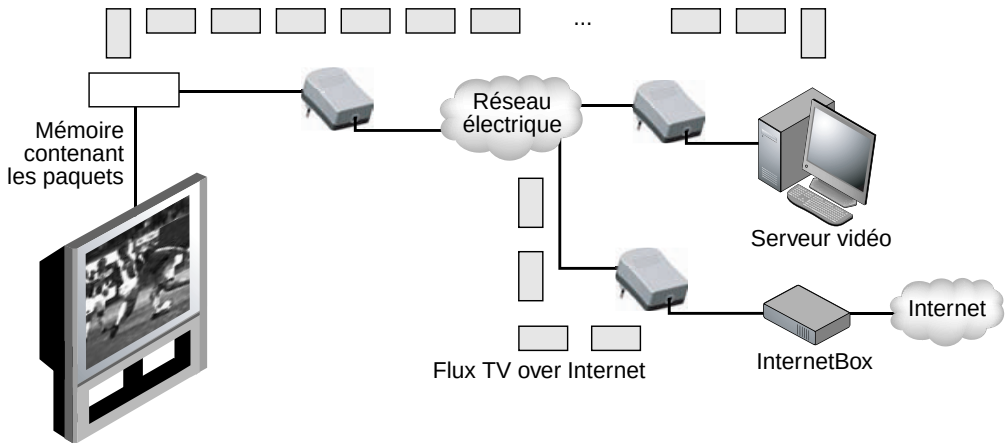


Figure 6.3

Application de streaming vidéo sur un réseau CPL

La vidéo peut provenir soit d'un signal analogique numérisé puis compressé, soit d'un signal numérique déjà compressé. Elle peut être fortement compressée ou demander un débit élevé, selon les possibilités du réseau et la puissance de calcul des émetteurs et des récepteurs.

Plus le débit est important et la compression faible, plus la qualité de l'image est bonne. Ce besoin de débit est une caractéristique importante de la transmission d'une image vidéo. Cette caractéristique ne pose pas de problème particulier aux réseaux CPL tant que le réseau n'est pas saturé. Analysons dans un premier temps les débits nécessaires pour acheminer une voie de vidéo.

Débits nécessaires à l'acheminement de la vidéo

Les équipements vidéo utilisent principalement les normes MPEG les plus récentes. Le DVB (Digital Video Broadcasting) est également largement utilisé.

MPEG recourt à des algorithmes de compression inter- et intratrame. Le débit peut descendre jusqu'à une valeur de 1,5 Mbit/s pour une qualité télévision, avec très peu de perte par rapport à l'image de départ. De nouveaux développements ont amélioré la qualité des images, avec des débits pour MPEG-2 de l'ordre de 4 Mbit/s. La norme MPEG-4 permet d'envisager une compression encore plus forte en incluant, le cas échéant, les éléments nécessaires à la reconstruction de l'image à l'autre extrémité.

La télévision diffusée présente la difficulté d'un débit très variable dans le temps, qui doit s'adapter au réseau de transport. Les algorithmes compressent plus ou moins l'information en fonction du temps et des ressources disponibles sur le support. Si le réseau est presque entièrement disponible, la qualité de l'image peut être fortement améliorée. Si, au contraire, il est encombré par des informations diverses provenant de différentes sources, une dégradation de la transmission vidéo doit être envisagée, si la qualité de service demandée par l'utilisateur le permet. Pour optimiser globalement le transfert de l'application, un mécanisme de contrôle est indispensable.

La télévision numérique haute définition, ou HDTV (High Definition Television), demande un débit de l'ordre de 5 à 10 Mbit/s, selon la qualité demandée par l'utilisateur. Un tel débit de 5 Mbit/s est tout juste supporté par les réseaux HomePlug 1.0 et Turbo. Avec HomePlug AV (40 Mbit/s), il suffit que seulement deux utilisateurs accèdent au service.

Il faudra donc attendre fin 2006 pour voir arriver la diffusion HDTV sur les réseaux CPL, mais pour un nombre d'utilisateurs restreint à une dizaine au maximum.

Problèmes de capacité

Un réseau CPL doit pouvoir offrir des connexions permettant à une application de vidéo d'utiliser à chaque instant le débit optimal lui permettant de conserver une qualité de service acceptable.

Examinons en premier lieu les difficultés posées par la capacité. Pour la parole téléphonique, il n'y a aucun problème puisque, une fois compressé, le flot est de 8 Kbit/s, voire de 5,6 Kbit/s. Pour la vidéo, en revanche, la capacité nécessaire à une image de qualité télévision MPEG-2 varie entre 2 et 8 Mbit/s. Avec la génération MPEG-4, elle descend à 1 Mbit/s. En tout état de cause, elle se situe à l'heure actuelle au niveau de 2 Mbit/s. Ces valeurs peuvent tomber à quelques centaines de kilobits par seconde en diminuant la qualité de la vidéo.

Dans le cas où le débit d'un réseau HomePlug 1.0 s'avère insuffisant pour diffuser une vidéo de bonne qualité, celui d'un réseau HomePlug Turbo ou HomePlug AV devrait suffire. Le débit utile étant respectivement de l'ordre de 10 Mbit/s et 40 Mbit/s pour ces deux technologies, il suffit d'avoir une estimation de son propre flot et du flot des autres applications sur le réseau pour ne pas dépasser ces valeurs.

Il est possible de rendre les flux de streaming encore plus prioritaires en utilisant les mêmes techniques de priorité que dans le transfert de la parole téléphonique. Dans ce cas, en utilisant les réseaux HomePlug Turbo et AV, il n'y a plus de problème de débit.

Si la capacité est suffisante, c'est-à-dire si le nombre d'utilisateurs est suffisamment petit par rapport à la capacité demandée ou si des priorités sont mises en œuvre, le second problème à résoudre est celui du respect de la latence pour effectuer la resynchronisation des octets. C'est la raison pour laquelle le temps de latence est généralement de l'ordre de plusieurs secondes, voire de plusieurs dizaines de secondes si nécessaire. Dans ce cas, une fois l'application de streaming lancée, la première image n'apparaît qu'au bout de ce temps de latence.

Visioconférence et vidéoconférence

La visioconférence et la vidéoconférence sont des applications à interactivité humaine, ce qui leur impose un temps de latence de 150 ms. Comme expliqué précédemment, il faut respecter le processus de resynchronisation des données pour reformer l'application isochrone au récepteur. Pour cela, une qualité de service doit être associée au transport de ces applications.

La différence entre les deux catégories d'applications provient de la qualité de l'image diffusée.

Dans la visioconférence, l'image peut être en noir et blanc et saccadée, du fait d'un nombre d'image par seconde inférieur à la normale. Cette application peut utiliser un écran à faible résolution afin de diminuer le débit. Ces caractéristiques ne nécessitent qu'une capacité de transport inférieure à la centaine de kilobits par seconde.

La vidéoconférence exige un débit bien supérieur, de plusieurs mégabits par seconde, pour obtenir une qualité d'image comparable à celle de la télévision. Pour aller vers la qualité cinéma, il faut atteindre la cinquantaine de mégabits par seconde, ce qui n'est pas envisageable dans le cadre des réseaux HomePlug actuels mais pourrait le devenir avec la prochaine génération HomePlug AV.

La difficulté principale pour ces deux applications est de maîtriser les synchronisations pour rejouer les images en temps voulu. Pour réaliser cette synchronisation, on peut mettre en œuvre les deux mêmes techniques utilisées pour la parole téléphonique : la gestion de priorités au niveau IP ou au niveau trame de HomePlug AV. Cette dernière solution permet de donner une priorité sur l'accès aléatoire de la couche MAC et d'octroyer des temporisateurs plus courts aux stations prioritaires. En d'autres termes, les stations prioritaires passent devant les autres tant qu'elles ont des trames à transmettre. La seule condition à respecter est que la somme des débits des stations prioritaires reste inférieure à la valeur du débit utile disponible.

Dans les réseaux CPL HomePlug 1.0, il est difficilement envisageable de faire passer de la vidéoconférence de bonne qualité. Avec les extensions HomePlug AV à 200 Mbit/s (débit théorique), pour peu que le nombre de clients soit réduit, il sera possible de faire transiter une ou deux voies de vidéoconférence de bonne qualité, bien que la probabilité d'une désynchronisation augmente rapidement avec le trafic.

Multimédia

Les applications multimédias utilisent généralement au moins un flot de parole ou de vidéo superposé à d'autres flots de données. Ces applications ne posent pas davantage de problème aux réseaux CPL que la voix téléphonique ou la vidéo. La seule contrainte supplémentaire qu'elles apportent provient de la synchronisation des applications simultanées qui réalisent le processus multimédia.

Pour transporter les applications multimédias, les réseaux doivent réaliser un compromis entre complexité et temps de transit. Pour retrouver la qualité du signal original pour des documents numériques, on considère que la compression doit être limitée à un facteur 3. C'est le cas des applications d'imagerie, dans lesquelles la qualité est primordiale, telles les radiographies aux rayons X, par exemple. On obtient des facteurs variant de 10 à 50 pour les images fixes et de 50 à 200 pour la vidéo. La moyenne des compressions se situe à 20 pour les images fixes et à 100 pour la vidéo.

Ces compressions déforment très légèrement l'image mais exploitent les capacités de récupération de l'œil humain. L'œil est en effet beaucoup plus sensible à la luminance, c'est-à-dire à la brillance des images, qu'à la chrominance, ou couleur. On retrouve cette caractéristique dans le codage de la télévision haute définition, où la résolution de la luminance repose sur une définition de l'image de 720 sur 480 points, alors que le signal de chrominance n'exploite qu'une définition de 360 sur 240 points. La luminance demande plus de bits de codage par point que la chrominance.

Nous avons vu que les réseaux CPL étaient capables de prendre en charge les débits nécessaires pour faire transiter les flots des applications multimédias. Pour cela, il suffit de limiter le nombre de clients pouvant accéder à un réseau électrique (*voir le chapitre 8*).

Le problème réside donc moins dans la capacité du réseau que dans la gestion des contraintes temporelles. Les deux contraintes de temps réel et de synchronisation sont très difficiles à obtenir avec des réseaux asynchrones tels que les CPL, dans lesquels il n'y a pas de gestion du temps et où le transport des données ne s'effectue pas de manière déterministe *(voir le chapitre 3).*

HomePlug AV sera en cela indispensable au transport des applications multimédias, puisqu'il est le seul à pouvoir classifier les paquets suivant des priorités de façon à obtenir la qualité de service nécessaire aux applications transportées par chaque flot.

Qualité de service

Comme nous l'avons vu au chapitre 3, HomePlug 1.0 et Turbo ne proposent pas de qualité de service dans leur technologie, puisque les temps de transfert des données ne sont pas déterministes. La qualité de service doit être implémentée par les couches applicatives au-dessus de la couche MAC pour pallier ce non-déterminisme.

HomePlug AV propose quant à lui une implémentation de la qualité de service, avec une garantie pour les différents services demandant un débit et un temps de transfert des

données stable. Cette qualité de service est assurée par l'allocation de slots de temps TDMA pour chaque type de service de données.

Le tableau 6.1 donne des exemples de réseaux CPL domestiques en fonction de scénarios d'utilisation pour un couple seul, un couple avec trois jeunes enfants et un couple avec un jeune enfant et deux adolescents.

Tableau 6.1 Scénarios d'utilisation d'un réseau CPL domestique

Application	Débit nécessaire	Scénario d'utilisation					
		Couple seul		Couple avec trois jeunes enfants		Couple avec un jeune enfant et deux adolescents	
		Qté	Débit	Qté	Débit	Qté	Débit
HDTV de type Home Cinema	22-28 Mbit/s	1	22-28	1	22-28	1	22-28
IPTV	3-7 Mbit/s	1	3-7	3	9-21	2	6-14
Système audio numérique de type Home Theater	5,4 Mbit/s	1	5,4	1	5,4	1	5,4
CD audio numérique	2 × 0,8 Mbit/s					3	4,8
Téléphonie sur IP	(0,064 + 0,016) = 80 Kbit/s (codec G.711)	2	0,16	2	0,16	3	0,24
Données IP	2 Mbit/s	2	4	2	4	5	10
TOTAL		6	34,5-44,4	9	40,6-58,4	15	48,4-62,2

Réseau local CPL

L'utilisation des CPL pour constituer un réseau local informatique est la plus évidente et la plus répandue parmi le grand public et les professionnels. Les familles s'équipent volontiers de plusieurs ordinateurs personnels pour partager un certain nombre d'applications et l'accès à Internet, tandis que les environnements professionnels s'échangent des applications métier et Internet.

Partage de connexion Internet

L'une des applications les plus fréquentes des CPL est le partage de la connexion Internet entre plusieurs terminaux ou ordinateurs d'un même réseau.

La technologie CPL permet de mettre facilement en réseau les différents ordinateurs de l'habitation ou du bureau et de les connecter au modem de connexion Internet par le biais du réseau électrique. L'architecture d'un tel réseau se présente alors comme illustré à la

figure 6.4. Les PC connectés à ce réseau par des équipements CPL récupèrent le signal *via* le réseau électrique. L'un des gros avantages des CPL est que toute prise électrique de l'habitat est susceptible de récupérer le signal Internet.

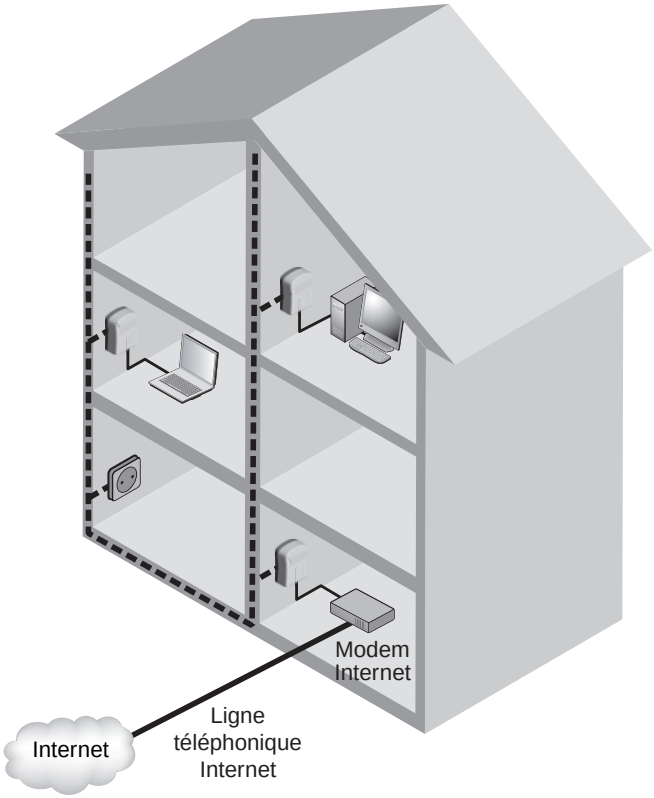


Figure 6.4
Partage de connexion Internet

Le débit est évidemment partagé entre les différents utilisateurs du réseau, qui voient la bande passante de la connexion Internet divisée par le nombre d'utilisateurs.

Partage de fichiers et d'imprimante

Un réseau local CPL permet de mettre en place toutes les applications que l'on trouve dans les réseaux informatiques câblés ou sans fil domestiques ou professionnels.

Le partage de fichiers et le partage d'imprimante sont deux des applications les plus fréquemment utilisées :

- **Partage de fichiers.** Un serveur connecté au réseau électrique par le biais d'un équipement CPL héberge les fichiers à partager entre les utilisateurs du réseau.

Ces utilisateurs se connectent à ce serveur *via* le réseau électrique et des équipements CPL correctement configurés.

- **Partage d'imprimante.** De la même manière, il est possible de placer l'imprimante à un emplacement favorable de l'habitation ou des locaux professionnels et de la connecter au réseau CPL à l'aide de son interface Ethernet (connecteur RJ-45). Les autres utilisateurs peuvent dès lors l'utiliser comme imprimante réseau grâce à son adresse IP.

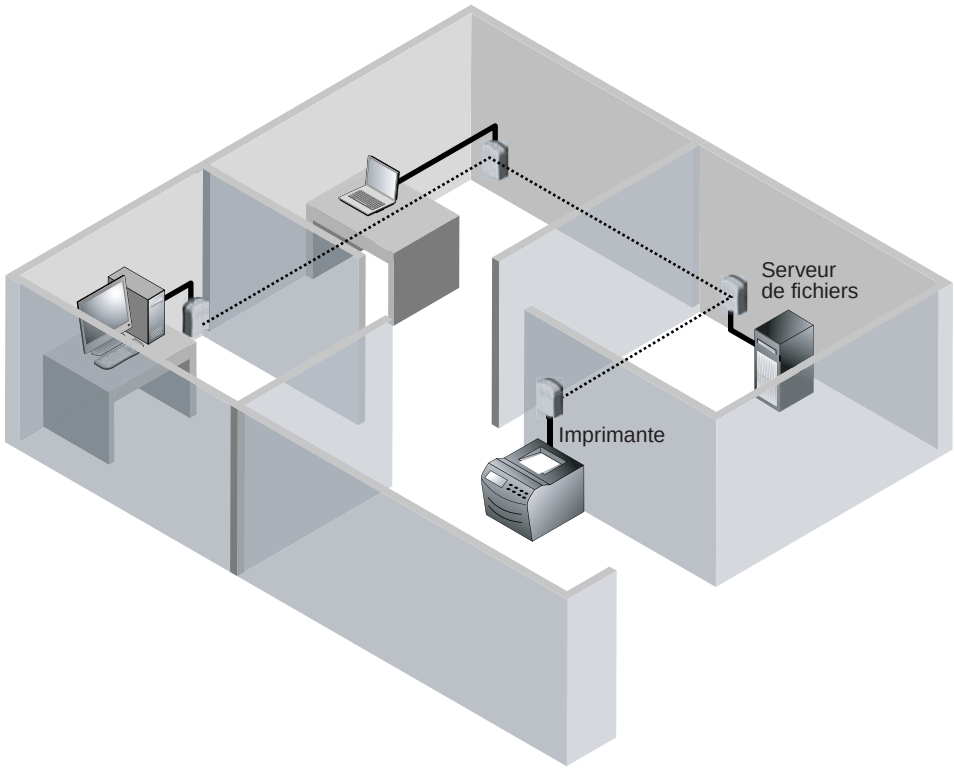


Figure 6.5
Partage de fichiers et d'imprimante dans un réseau local CPL

Diffusion audio

Un réseau local CPL permet de diffuser des données sur le réseau électrique, incluant les données audio (*voir figure 6.6*) provenant de différentes sources, notamment les suivantes :

- **Serveurs de fichiers audio.** Les fichiers sont de type MP3 ou WAV numériques et sont envoyés sur le réseau électrique pour être récupérés par des équipements CPL connectés aux équipements hi-fi de l'installation.

- **Système hi-fi.** Il est possible de partager le signal audio d'un système hi-fi vers un autre système hi-fi ou vers des enceintes audio. Dans ce dernier cas, le réseau électrique remplace les câbles audio stéréo qui permettent la connexion entre le système hi-fi et les enceintes d'écoute.

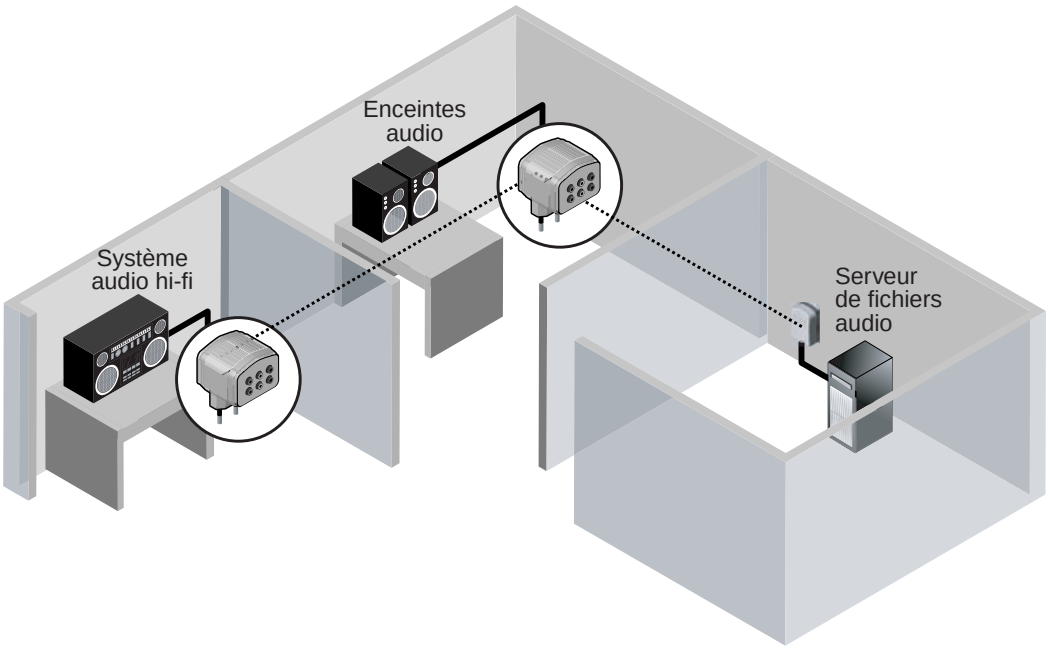


Figure 6.6
Diffusion audio dans un réseau CPL

Applications ludiques

Les applications ludiques (jeux vidéo) utilisent de plus en plus les réseaux informatiques pour connecter les différents joueurs entre eux. Les terminaux de jeu équipés d'interface réseau peuvent utiliser le réseau électrique pour se connecter les uns aux autres, exactement comme dans le cas d'un partage de fichiers sur un réseau local CPL.

Vidéosurveillance

La généralisation des caméras IP équipées d'interfaces réseau Ethernet (connectique RJ-45) permet de les connecter à un réseau local CPL *via* les prises de courant. Cela offre une grande flexibilité dans le placement des caméras, lesquelles doivent de toute façon être alimentées en énergie par une prise de courant à proximité. La figure 6.7 illustre cette application.

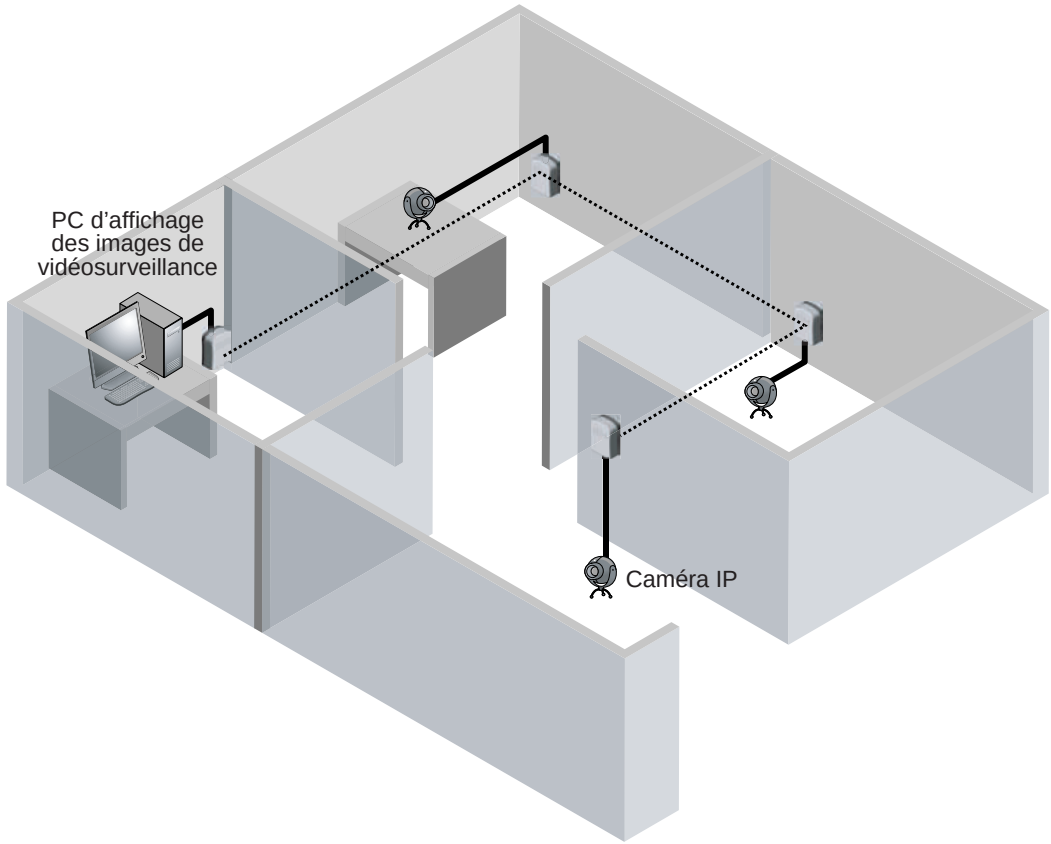


Figure 6.7
Vidéosurveillance sur réseau local CPL

Dorsale d'un réseau Wi-Fi

Comme nous le verrons au chapitre 13, dédié aux réseaux hybrides, chacune des technologies constitutives d'un réseau informatique présente des avantages et des inconvénients.

Wi-Fi permet de constituer un réseau informatique radio offrant mobilité et flexibilité aux utilisateurs au sein du bâtiment où est installé le réseau. Cependant, les contraintes matérielles de cette technologie l'obligent à s'appuyer sur une dorsale Ethernet câblée pour disposer d'une couverture entière du bâtiment. Ce rôle de dorsale Ethernet peut être dévolu à un réseau local CPL en connectant les points d'accès Wi-Fi au réseau électrique.

La figure 6.8 illustre l'architecture de ce type de réseau, dans lequel chaque point d'accès Wi-Fi constituant une cellule radio est relié au réseau par un équipement CPL.

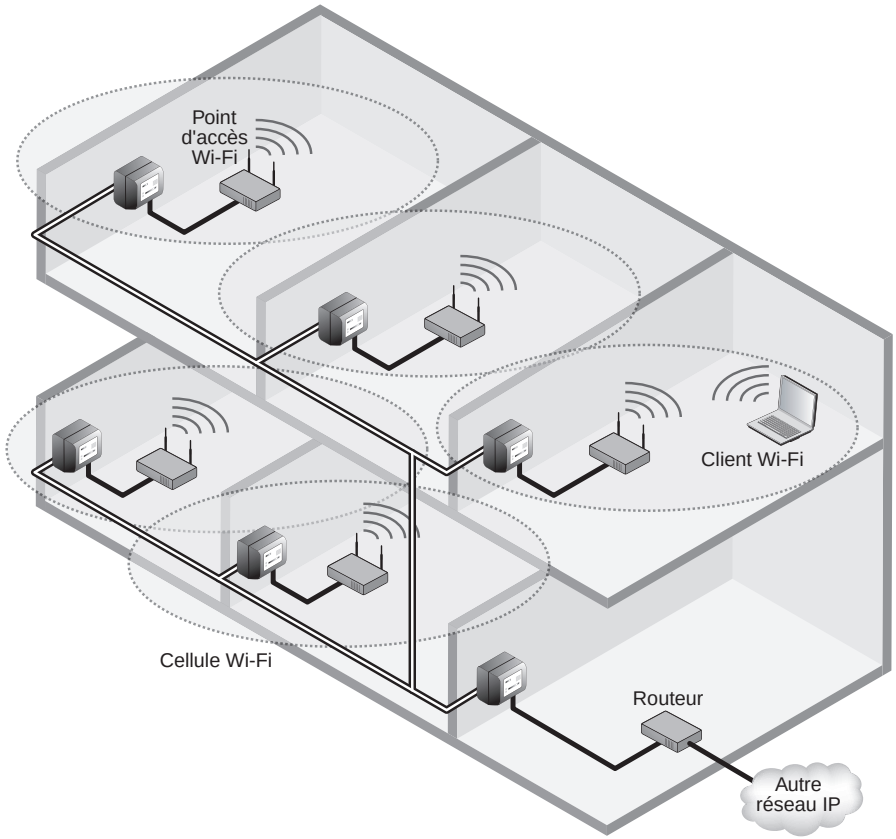


Figure 6.8

Réseau local CPL faisant office de dorsale d'un réseau Wi-Fi

InternetBox et CPL

De nombreux FAI, comme Wanadoo, Free, Neuf-Cegetel, Alice, Club-Internet, AOL, etc., proposent désormais, par le biais d'InternetBox, des solutions d'accès à des services Internet dits « multi-play », notamment les suivants :

- **Données.** L'InternetBox est avant tout un modem d'accès à Internet qui permet aux utilisateurs d'accéder aux services données tels que le Web, la messagerie, FTP, IRC, P2P, etc.
- **Voix.** Services de téléphonie sur IP, l'InternetBox se comportant comme un récepteur téléphonique auquel se branchent les téléphones analogiques utilisés sur le réseau téléphonique commuté (RTC).

- **Vidéo.** IPTV, pour la diffusion des chaînes TV sur les réseaux IP, vidéo à la demande, ou VoD (Video on Demand).
- **Futurs services IP.** Téléphonie mobile domestique, domotique pour l'habitat (gestion de l'énergie, serveur familial, etc.), etc. Ces services feront de l'InternetBox une véritable passerelle intelligente dans un futur proche.

Chacun de ces services devra être acheminé jusqu'à l'utilisateur final (poste de télévision, téléphone, ordinateur, électroménager IP, etc.) *via* un réseau Ethernet. Le réseau local CPL constitue une excellente solution pour cela puisqu'il utilise un réseau disponible dans tout bâtiment.

Comme l'illustre la figure 6.9, ces services demandent une liaison Ethernet entre l'InternetBox et le décodeur vidéo ou les téléphones, liaison qui peut être assurée par des équipements CPL.

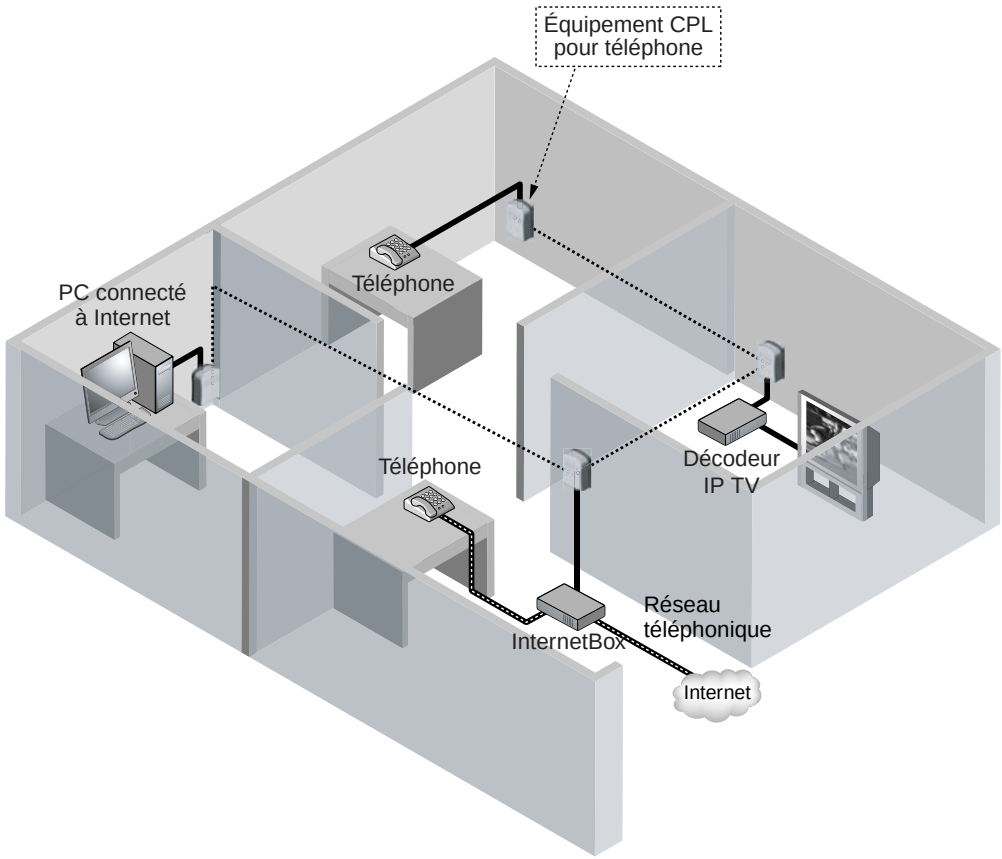


Figure 6.9
InternetBox et CPL

D'ores et déjà, Wanadoo propose dans son pack MaLigneTV les équipements suivants :

- Livebox (InternetBox de France Télécom) ;
- décodeur TV ;
- Pack de deux équipements CPL de type Devolo dLAN HomePlug Turbo à 85 Mbit/s.

Nouvelles applications des CPL

La maturité des technologies CPL a convaincu certains industriels d'utiliser les CPL comme support de transmission pour des applications qui n'étaient jusqu'alors soit pas du tout en réseau, soit disponibles uniquement sur des réseaux propriétaires et coûteux.

Le fait qu'un nombre de plus en plus important d'équipements industriels dispose d'une interface réseau permet la constitution de réseaux de nouveaux types auxquels il est possible de se connecter, notamment dans les bateaux, les espaces publics et les automobiles.

CPL dans un bateau

Un bateau de taille conséquente est typiquement un bâtiment qui dispose de nombreux réseaux électriques pour alimenter, éclairer, diffuser des signaux sonores, relier des automates, etc.

Ces réseaux électriques sont les supports idéaux pour constituer des réseaux locaux CPL permettant la diffusion des applications suivantes :

- Internet dans le navire ;
- signaux sonores ;
- remontée d'informations des machines et des capteurs vers la cabine de navigation.

L'usage des CPL est particulièrement indiqué dans un bateau puisqu'il s'agit d'un espace où les travaux de câblage sont souvent impossibles et où les systèmes radio tels que Wi-Fi ont du mal à traverser les parois métalliques.

CPL dans l'industrie

Dans le monde industriel, les contraintes des applications sont plus sévères que dans les réseaux locaux grand public ou professionnels. Ces contraintes ont jusqu'à présent ralenti le développement des CPL, mais la maturité de HomePlug et les premiers retours sur les déploiements de réseaux CPL ont conduit à considérer les CPL comme des solutions viables pour les connexions entre machines.

Les applications de l'industrie qui utilisent actuellement des réseaux CPL sont les suivantes :

- réseaux de capteurs ;

- connexion d'automates ;
- PC situés dans des espaces confinés où le câblage est difficile (en haut d'une grue, dans des espaces de tuyauteries métalliques rendant impossible l'usage de Wi-Fi, etc.).

CPL dans les espaces publics

De la même manière que le monde industriel, les espaces publics disposent de plus en plus d'équipements communicants ou équipés d'interfaces Ethernet prêtes à être connectées à un réseau local.

Parmi les diverses applications qui utilisent déjà les CPL pour relier ces équipements, citons notamment les suivantes :

- diffusion de contenu vers des bornes multimédias ;
- remontées d'informations des distributeurs de boissons ;
- trafic d'authentification pour badgeuses ;
- informations des machines à sous.

CPL sur câble coaxial

Comme nous le verrons au chapitre 7, dédié aux équipements, les CPL peuvent utiliser non seulement le câble électrique 220 V/50 Hz, mais également d'autres types de câbles pour transporter le signal dans la bande des 1 à 30 MHz. Un des câbles les plus utilisés par les équipements CPL est le câble coaxial, classiquement utilisé par les câblo-opérateurs pour diffuser le signal TV provenant des chaînes dites câblées.

Ce câble présente des caractéristiques de propagation et d'immunité aux interférences (du fait que le câble est protégé, voire blindé) très intéressantes pour le transport du signal CPL. Le câble coaxial peut donc avantageusement compléter un réseau électrique dans la constitution d'un réseau CPL afin de pallier certains problèmes de topologie liés à la seule utilisation du réseau électrique (réseau trop vétuste, réseau électrique trop complexe par rapport aux besoins des applications, etc.).

CPL sans courant électrique

La propagation du signal CPL sur les câbles électriques n'a pas besoin du signal d'énergie 220 V/50 Hz. Il est possible d'imaginer un réseau CPL sans que l'électricité fonctionne dans le bâtiment du moment que les équipements CPL peuvent être alimentés d'une manière ou d'une autre sur batterie. Ils pourront dès lors utiliser le réseau électrique pour communiquer entre eux, mais sans y puiser leur énergie. Cette application inédite des CPL peut se révéler utile dans les cas où l'électricité est coupée et où certains équipements informatiques sur batterie désirent maintenir leur communication pendant le temps de la coupure.

CPL dans le véhicule automobile

- Les automobiles ont de plus en plus besoin de transporter des données internes entre les différents organes de contrôle, de commande et le tableau de bord. Ces échanges d'information nécessitent des câblages qui peuvent représenter jusqu'à 3 km et 50 kg.
- L'équipementier Valeo et le fabricant de produits CPL Spidcom ont travaillé de concert pour mettre en place une solution utilisant les CPL pour communiquer au tableau de bord les informations des capteurs du véhicule.
- Ce type de réseau CPL peut également être utilisé pour diffuser des vidéos de caméra externe ou de lecteur DVD embarqué.

Perspectives économiques

Comme nous l'avons vu dans ce chapitre, la plupart des applications transportées par les réseaux électriques doivent faire face aux multiples contraintes inhérentes aux CPL, à savoir le débit, la topologie mais aussi le nombre d'utilisateurs présents sur le réseau.

Le nombre de ces applications ne cesse de croître, mais la plupart d'entre elles sont déjà présentes dans les réseaux classiques, comme la voix ou la vidéo.

Le nombre de terminaux CPL est lui aussi en constante augmentation, et l'on trouve maintenant des produits CPL chez la plupart des revendeurs de matériels informatiques et réseau.

Le CPL doit donc être considéré non plus seulement comme une technologie réseau mais comme un moyen simple de connecter des équipements entre eux en permettant le partage d'information. L'apparition du CPL dans le monde de la hi-fi en est un exemple frappant. Un serveur central connecté à Internet peut délivrer n'importe quel type de flux (vidéo ou audio) à tout équipement (écran LCD ou minichaîne) situé dans la maison par le biais de liaisons CPL.

Les perspectives économiques des réseaux CPL sont donc importantes, notamment pour les raisons suivantes :

- Arrivée de produits HomePlug AV fin 2006.
- Engagement des FAI à élargir la diffusion des services des InternetBox à tout l'habitat. Cette stratégie généralisera à terme l'utilisation du CPL parmi le grand public.
- Compréhension grandissante dans le grand public d'une technologie désormais mature, particulièrement simple d'utilisation (pas de nouveau câblage, utilisation des prises de courant, configuration simplifiée, sécurité, etc.).
- Compréhension par les professionnels de la complémentarité des CPL par rapport au câble et à Wi-Fi, notamment grâce à la mise au point de produits CPL dédiés aux besoins d'administration et de gestion des réseaux professionnels.

La figure 6.10 illustre la croissance attendue des CPL d'ici à 2010. Sa facilité de déploiement, conjuguée à la baisse des coûts des équipements et au développement de produits alliant plusieurs technologies (passerelle, routeur, modem, pare-feu, serveur, etc.), promet sans nul doute cette technologie à un grand avenir.

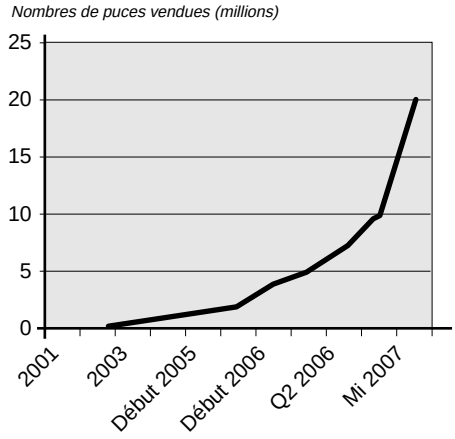


Figure 6.10

Nombre de puces HomePlug vendues dans le monde

7

Équipements

Depuis l'arrivée, en 2003, de la spécification HomePlug 1.0, le marché des équipements réseau CPL n'a cessé de croître. Au départ axé sur les petits réseaux, avec peu de débit et peu d'ordinateurs, il s'est ensuite tourné, avec l'appui des FAI, vers les particuliers, très demandeurs d'une technologie permettant le partage de connexion Internet tout en éliminant la contrainte du câblage et en restant relativement facile d'utilisation.

Ce chapitre présente l'ensemble des produits CPL disponibles actuellement sur le marché, afin de connecter des terminaux au réseau local ou de constituer ou d'optimiser le réseau CPL (filtres, répéteurs, injecteurs, etc.).

Les technologies CPL

Depuis l'apparition des premiers équipements CPL haut débit, plusieurs technologies ont été développées, mais aucun standard international n'est pour l'instant apparu.

Dans les technologies proposées au public, plusieurs approches ont été mises en œuvre, notamment les suivantes :

- choix du mode réseau ;
- techniques de modulation ;
- nombre de sous-bandes ;
- implémentation de la couche MAC.

Avec plus de 90 % du marché des équipements CPL, la technologie HomePlug est tellement répandue qu'elle en vient à représenter un standard de fait.

Les différentes technologies CPL sont récapitulées au tableau 7.1 en fonction des choix du mode réseau.

Tableau 7.1 Technologies CPL en fonction du mode réseau

Technologie		Mode
Ascom APA 450 (4,5 Mbit/s)		Maître-esclave
Itran (Main.net) PLTNet & ITM1 (2 Mbit/s)		Maître-esclave
HomePlug	1.0	Pair-à-pair
	1.0 Turbo	Pair-à-pair
	AV	Centralisé
DS2	DSS4200 (45 Mbit/s)	Pair-à-pair
	200 Mbit/s	Maître-esclave
Spidcom	45 Mbit/s	Pair-à-pair
	SPC200 (200 Mbit/s)	Maître-esclave

Les différents modes réseau (maître-esclave, pair-à-pair et centralisé) sont utilisés par les technologies CPL en fonction des contraintes de chaque application. Ascom et Itran ont compté parmi les premiers à développer des équipements CPL à base d'interface Ethernet. Ils ont d'abord privilégié le mode maître-esclave pour ses capacités d'administration centralisée.

Mode maître-esclave

Le mode maître-esclave permet d'utiliser la logique du réseau électrique – composé d'un compteur électrique en tête de réseau, considéré comme un maître du réseau électrique, et de ses disjoncteurs et départs, considérés comme des esclaves de ces disjoncteurs –, sur lequel s'appuie le réseau CPL pour son support physique, et de placer l'équipement dit maître sur la partie en tête de réseau et les équipements esclaves sur les différents départs du réseau CPL.

La figure 7.1 illustre l'architecture d'un réseau CPL BT (basse tension) de distribution électrique en mode maître-esclave. On retrouve l'équipement maître au niveau du transformateur MT/BT (moyenne tension vers basse tension). Cet équipement contrôle le bon fonctionnement du réseau CPL, et plus particulièrement les liens réseau qui existent avec les équipements esclaves situés derrière les compteurs électriques des habitations.

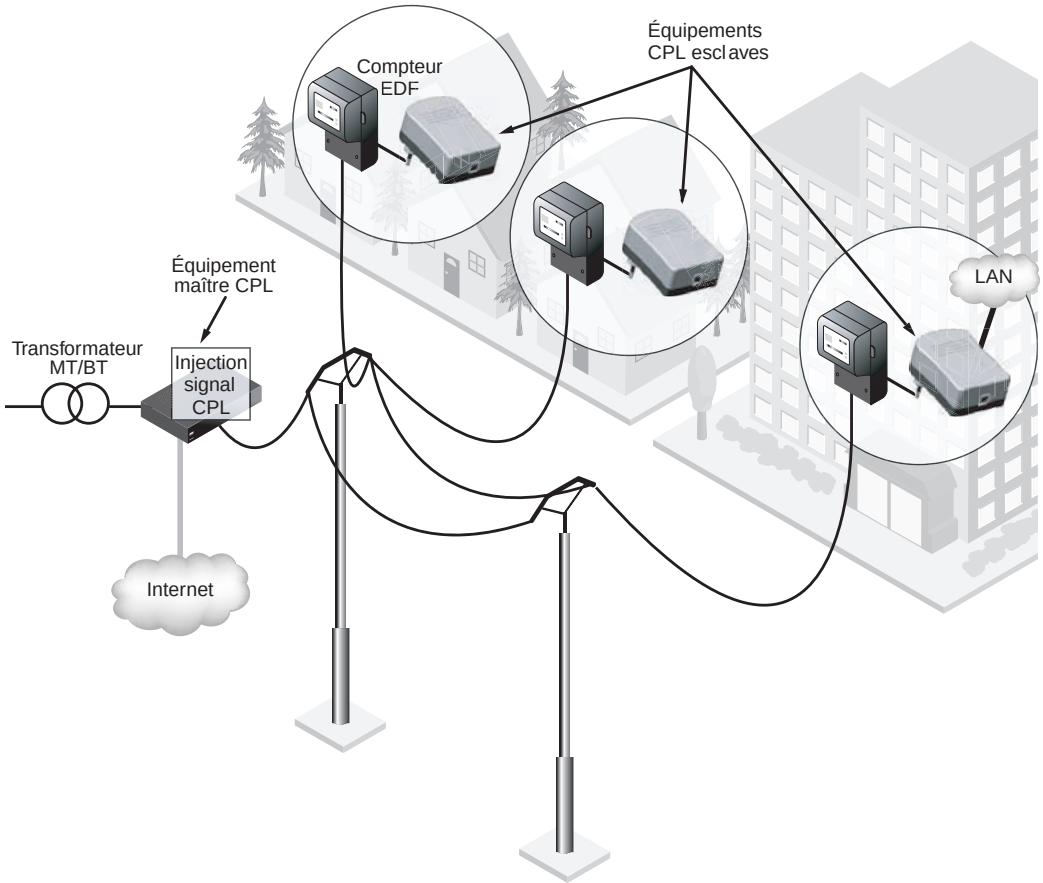


Figure 7.1

Architecture simplifiée du mode maître-esclave pour le réseau public

La figure 7.2 illustre une autre architecture en mode maître-esclave sur un réseau électrique domestique. Nous y retrouvons les équipements classiques du réseau électrique privé, dont nous avons eu un aperçu au chapitre 2.

Partent du tableau électrique, des câbles électriques alimentent prises, ampoules et équipements électriques. Ces câbles raccordés au tableau électrique sont communément appelés départs électriques, puisqu'ils partent d'un point central (le tableau électrique) et parcourent l'ensemble du bâtiment en fonction des besoins d'alimentation électrique.

Dans cette topologie, l'équipement CPL maître se situe idéalement à ce point central qu'est le tableau électrique. Les équipements esclaves sont constitués par les prises électriques disséminées tout le long du réseau électrique.

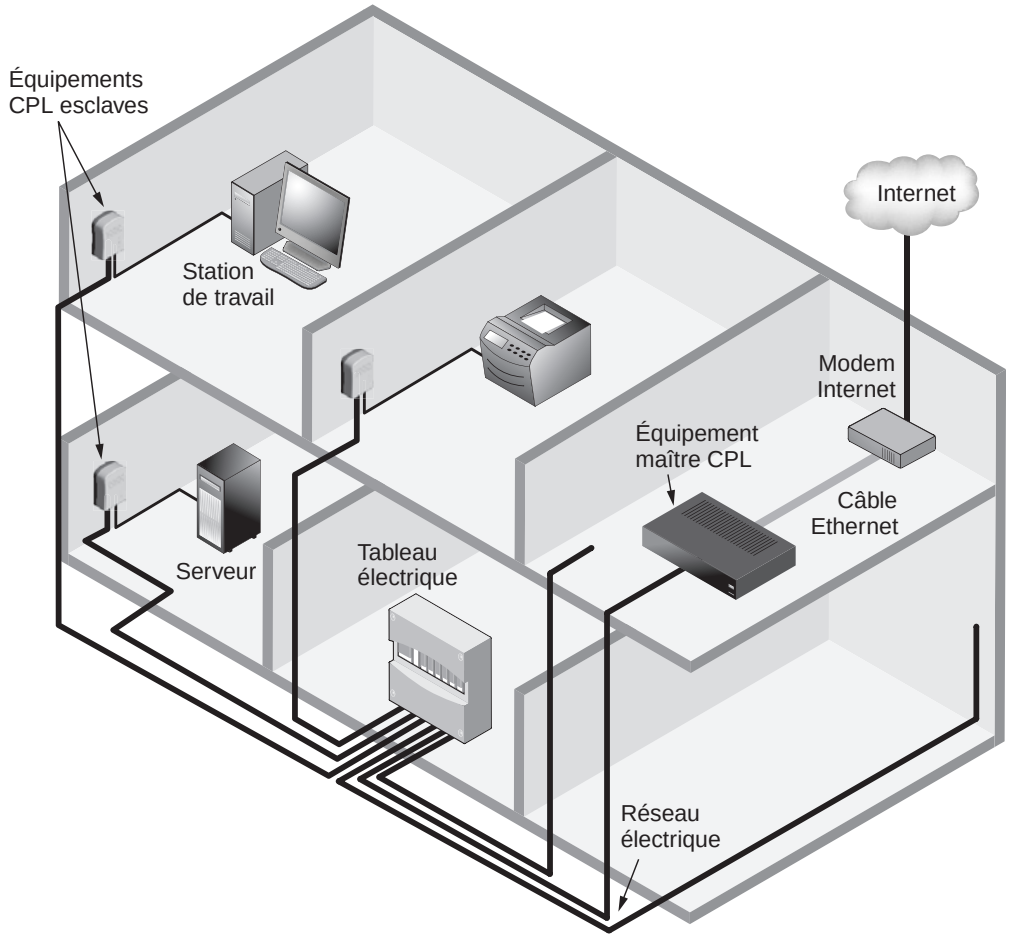


Figure 7.2

Place des équipements dans un réseau CPL BT domestique en mode maître-esclave

L'équipement maître fait fonction de passerelle entre le réseau filaire (connecté, par exemple, à un modem d'accès à Internet) et le réseau local CPL, qui utilise le réseau électrique. Cet équipement a également en charge la gestion du réseau et des différents équipements esclaves.

Le tableau 7.2 récapitule les principaux avantages et inconvénients du nombre de départs électriques.

Tableau 7.2 Avantages et inconvénients du nombre de départs électriques

Nombre de départs	Avantage	Inconvénient
Un seul départ	– Conception plus facile – Répétition potentielle avec les équipements maîtres – Supervision plus facile	– Bande passante divisée – Multitrajets possibles pour les trames en circulation – Possibilité de boucles
Plusieurs départs	– Plus large couverture réseau – Séparation des réseaux utiles	– Supervision plus compliquée

Parmi les nombreux constructeurs d'équipements CPL ayant opté pour le mode maître-esclave, citons notamment les suivants :

- **Main.net.** Développe des produits pour les réseaux électriques BT publics qui privilégient ce mode afin de correspondre à la topologie des réseaux électriques. Il s'agit classiquement d'une topologie en étoile. Le transformateur MT/BT, utilisé comme point d'injection du signal CPL, est situé au centre de l'étoile, et les équipements CPL des utilisateurs finals viennent se placer aux extrémités des différents départs électriques depuis le transformateur.
- **Ascom.** Développe des produits pour les réseaux électriques BT publics et domestiques utilisant ce mode depuis 1998. Cette génération de produits offrait un débit de 250 Kbit/s. Un des équipements faisait office de maître, tandis que les autres étaient esclaves. La configuration s'opérait en mode Telnet ou à l'aide de fichiers de configuration et d'un système client-serveur TFTP.
- **DS2 et Spidcom.** Après avoir utilisé le mode pair-à-pair pour sa facilité de déploiement, développent dorénavant des produits en mode maître-esclave afin de bénéficier d'une administration centralisée et d'une meilleure gestion de la QoS dans l'allocation des trames TDMA pour les applications temps réel comme la vidéo.
- **Oxance.** Développe des produits HomePlug en mode hybride. La technologie Oxance utilise les couches physiques de HomePlug 1.0, qui fonctionnent en mode pair-à-pair, auxquelles elle ajoute une couche logique IP, qui se comporte comme si l'un des équipements du réseau CPL était le maître du réseau IP. Cet équipement fait office de passerelle CPL vers les autres réseaux IP ainsi que de serveur SNMP pour remonter les différents paramètres du réseau CPL. Nous reviendrons sur les configurations et les aspects techniques de ces produits aux chapitres 9 et 10.

Cas des équipements Ascom APA

Les équipements Ascom APA, au débit de 4,5 Mbit/s, incarnent une des toutes premières générations de matériels CPL haut débit. L'équipement maître était accessible par le biais d'une interface Telnet pour la configuration des équipements puis supervisable depuis une console d'administration SNMP v2/v3. Le maître était capable de gérer 63 esclaves au maximum.

☞

Cas des équipements Ascom APA *(suite)*

Les figures 7.3 à 7.6 illustrent des équipements maîtres et esclaves Ascom APM 45.

Figure 7.3
Équipement maître gestionnaire du réseau CPL Powerline APM-45o ASCOM

Figure 7.4
Équipement esclave Powerline APA-45i ASCOM permettant la connexion des terminaux clients au réseau local CPL

Figure 7.5
Interfaces de l'équipement esclave

Figure 7.6
Détails des interfaces Ethernet LAN RJ-45, USB et RJ-11 de l'équipement esclave

Certains équipements CPL permettent d'effectuer des déports d'interfaces téléphoniques sur le réseau CPL. La société Phonex, par exemple, développe des équipements à interface RJ-11 pour transporter les communications analogiques voix sur le réseau électrique.

Mode pair-à-pair

Dans le mode maître-esclave, un équipement maître se situe à un niveau hiérarchique supérieur (il gère et contrôle le réseau), et les équipements esclaves se situent à un niveau hiérarchique inférieur (leur fonction se limite à communiquer avec l'équipement maître). Dans le mode pair-à-pair, tous les équipements ont le même niveau hiérarchique et échangent des données avec tous les autres équipements CPL du réseau. Le réseau est donc constitué de liens *N* vers *N*.

Comme illustré à la figure 7.7, le mode pair-à-pair est idéal pour les réseaux locaux puisque l'architecture des LAN doit permettre à tout terminal (typiquement des PC) d'échanger des données avec tout autre terminal du réseau LAN. HomePlug 1.0 et Turbo utilisent ce mode.

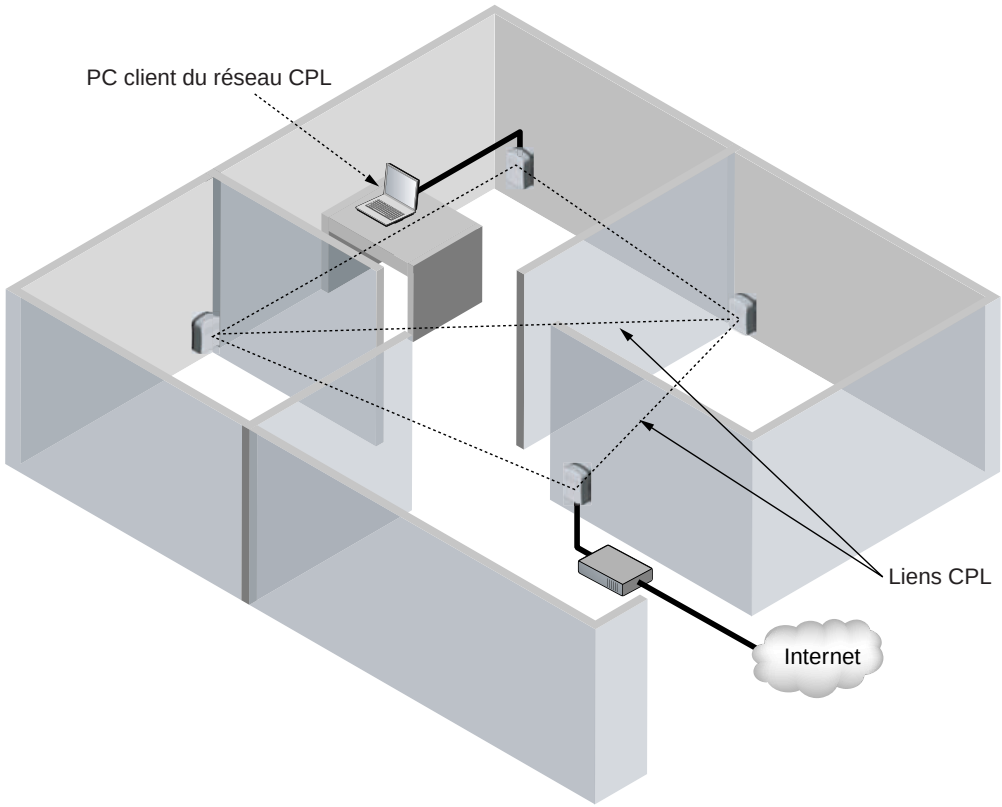


Figure 7.7
Architecture d'un réseau CPL en mode pair-à-pair

Mode centralisé

Comme nous l'avons vu au chapitre 3, HomePlug AV utilise le mode centralisé, qui est un mélange entre les modes maître-esclave et pair-à-pair.

Dans les réseaux CPL HomePlug AV, un des équipements tient le rôle d'équipement central et gère les communications entre les stations CPL du réseau. Les échanges entre stations CPL se font directement, sans passer par l'équipement central. Les stations doivent toutefois s'identifier auprès de l'équipement central et respecter les allocations temporelles données par ce dernier.

Les modems CPL

L'essence de la technologie CPL consistant à utiliser le réseau électrique, les équipements CPL quels qu'ils soient se branchent sur les prises électriques ou injectent directement le signal sur les câbles électriques. L'injection de signal, qui permet de connecter un équipement CPL directement sur le câble électrique, est décrite un peu plus loin dans ce chapitre.

Bien que la technologie CPL ne recoure pas au processus de modulation-démodulation mis en œuvre dans les modems, on parle de modem CPL pour désigner l'équipement sur lequel se branchent les terminaux qui désirent participer au réseau CPL.

Contrairement aux interfaces Wi-Fi, qui sont intégrées dans les terminaux sous forme de cartes, les interfaces CPL ne sont pas intégrées dans les terminaux. Le terminal, généralement un ordinateur, se connecte donc à l'équipement, lequel comporte deux interfaces, une pour le branchement au réseau électrique, l'autre (RJ-45 ou USB) pour la connexion au terminal.

Équipement le plus répandu dans les réseaux CPL, le modem CPL est également le plus simple à utiliser, puisqu'il se présente comme un appareil électrique standard, doté d'une prise mâle à brancher sur une prise électrique et d'une interface USB ou Ethernet à connecter au terminal.

Dissipation de chaleur dans les modems CPL

Les premiers équipements CPL HomePlug 1.0 en boîtier plastique connaissaient des problèmes de dissipation de chaleur du fait de l'alimentation permanente en 200 V/50 Hz. Cela entraînait des pannes dans les composants électroniques, qui ne supportaient pas une présence trop longue de chaleur dans les boîtiers.

Les équipements CPL se sont améliorés, avec l'apparition de composants plus robustes, d'ailettes de refroidissement et de trous d'aération *(voir figure 7.8, droite)* leur permettant de fonctionner correctement, même dans des situations dans lesquelles les équipements étaient empilés ou placés dans des environnements peu aérés et à des températures pouvant atteindre 70 °C. Les boîtiers sont désormais plutôt en plastique pour les équipements grand public et en métal pour les équipements professionnels.

Vu de l'extérieur, un modem CPL présente donc les deux interfaces suivantes :

- prise électrique mâle ;
- interface réseau USB ou Ethernet RJ-45.

Le modem présente généralement trois voyants, ou LED, qui indiquent à l'utilisateur la présence du signal 220 V/50 Hz, ainsi que celle du signal CPL sur l'interface électrique et celle du réseau Ethernet sur l'interface RJ-45 *(voir figure 7.8, gauche).*

Certains équipements comportent jusqu'à cinq voyants afin d'aider l'utilisateur à diagnostiquer le bon fonctionnement de l'équipement.

À l'intérieur du boîtier, toute l'architecture matérielle s'articule autour du composant principal qu'est la puce CPL HomePlug *(voir figure 7.8, milieu).* Le constructeur Intellon est le principal fournisseur de puces HomePlug.

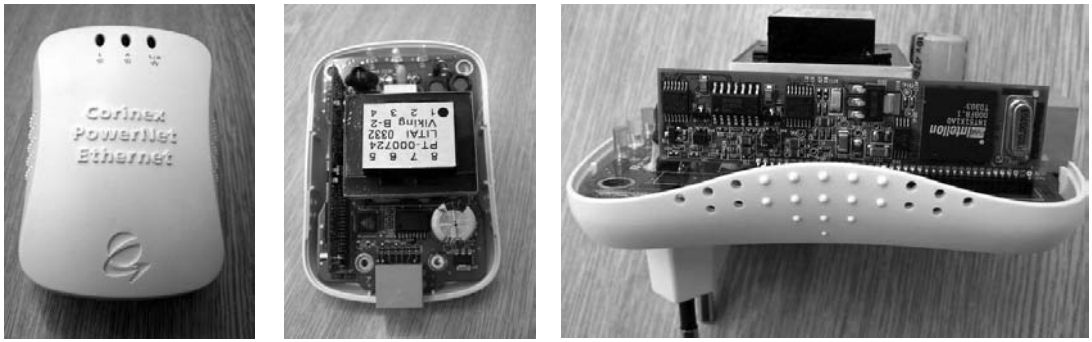


Figure 7.8
Extérieur et intérieur d'un modem CPL HomePlug Corinex PowerNet

Le tableau 7.3 récapitule les différentes versions de puces apparues au fil des versions de la technologie HomePlug.

Tableau 7.3 Modèles de puces Intellon

HomePlug	Puce
1.0 (appelé également 1.0.1)	INT5130, INT51MX
Turbo (appelé également 1.1)	INT5500
AV	INT6000

Autour de cette puce CPL, qui implémente toutes les fonctionnalités des réseaux CPL présentées au chapitre 3, un certain nombre de composants et de circuits électroniques permettent d'optimiser le fonctionnement du modem CPL :

- Couplage au réseau électrique, autrement dit branchement du modem CPL au réseau électrique.
- Contrôle du gain du signal CPL afin d'optimiser l'émission/réception des données, y compris dans des conditions difficiles, du fait notamment des bruits sur le réseau électrique.
- Stockage d'informations sur l'état du réseau CPL. Cette fonction est assurée par une EPROM (mémoire persistante au redémarrage du modem) et une SRAM (mémoire volatile effacée au redémarrage du modem), qui conservent les informations d'état des liens CPL, de clés de cryptage du réseau ou d'autorisation d'accès.

La figure 7.9 illustre l'architecture matérielle d'un modem CPL HomePlug 1.0.

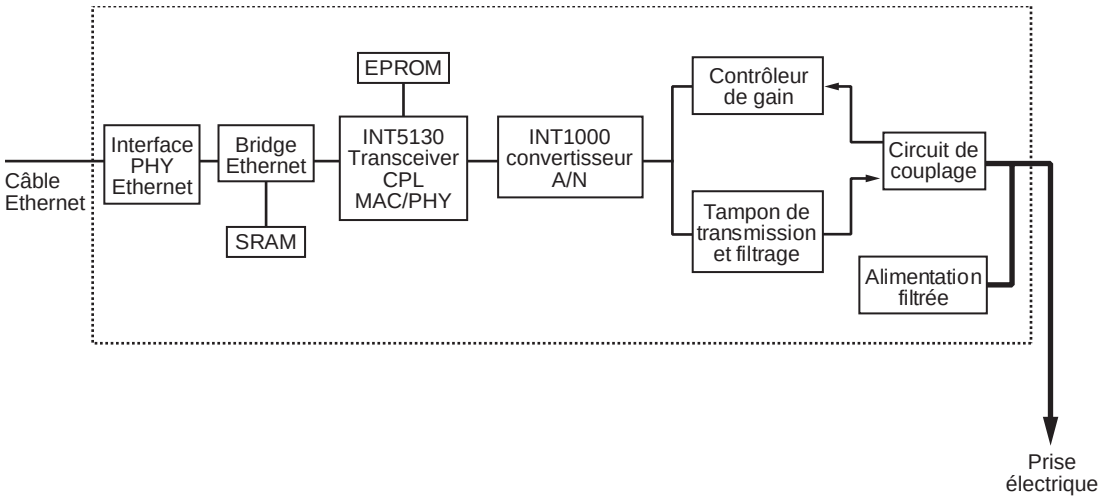


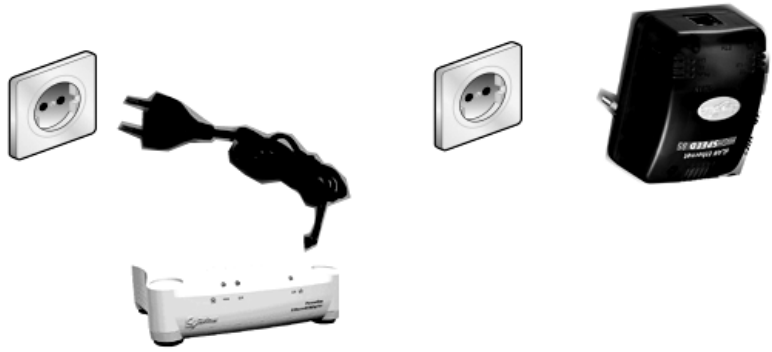
Figure 7.9

Architecture matérielle d'un modem CPL

Les constructeurs ont élaboré deux types de modems CPL, les modems dits « desktop », qui se présentent comme des boîtiers à poser sur une table ou sur un support, avec un cordon électrique pour se brancher sur les prises électriques, et les modems dits « wallmount », qui se présentent comme des boîtiers intégrés se branchant directement sur les prises électriques. La majorité des modems CPL sont des wallmount, du fait de leur facilité d'utilisation.

La figure 7.10 illustre des exemples de modems wallmount (à gauche) et desktop (à droite).

Figure 7.10
Modems CPL wallmount et desktop



Les modems CPL USB

Les modems CPL USB proposent une interface USB permettant de les connecter aux ports USB des ordinateurs ou terminaux réseau. Le port USB fait office de carte réseau virtuelle pour se connecter au réseau CPL.

L'intérêt de ces modems réside dans le fait que tous les ordinateurs ne disposent pas de carte réseau, alors qu'ils sont tous équipés de ports USB. Leur configuration est toutefois moins simple que celle d'un modem CPL Ethernet.

La figure 7.11 illustre un modem CPL USB Sagem de type F@st Plug.

Figure 7.11
Modem CPL USB Sagem de type F@st Plug

Les modems CPL Ethernet

La généralisation des cartes réseau dans les ordinateurs, terminaux réseau et équipements électroniques et même dans les appareils d'électroménager simplifie la constitution de réseaux par le biais des connecteurs RJ-45 de la carte Ethernet.

Ce type de modem est devenu l'équipement CPL le plus répandu. Simple à utiliser et à configurer, il voit de surcroît ses prix baisser continuellement.

La figure 7.12 illustre un modem CPL Ethernet Devolo de type dLAN Ethernet HighSpeed 85.

Figure 7.12
Modem CPL Ethernet Devolo de type dLAN Ethernet HighSpeed 85

La carte réseau Ethernet des modems CPL a d'abord été de type 10baseT (10 Mbit/s) pour les modems HomePlug 1.0, offrant un débit utile maximal au niveau de la couche MAC de 8,2 Mbit/s, puis 100baseT (100 Mbit/s) pour les modems HomePlug Turbo et AV.

L'augmentation des performances des équipements CPL HomePlug amènera probablement les fabricants à utiliser des cartes 1000baseT (1 000 Mbit/s) afin de ne pas limiter les débits sur l'interface Ethernet. Il ne serait pas étonnant non plus de voir apparaître des équipements CPL fibre optique.

La société Devolo propose des équipements comportant les deux interfaces, USB et Ethernet.

La figure 7.13 illustre un modem CPL Devolo de type dLAN duo avec interfaces USB et Ethernet.

Figure 7.13
Modem CPL Devolo de type dLAN duo, avec interfaces USB et Ethernet

La figure 7.14 illustre des modems CPL de marque Devolo au standard HomePlug AV, avec, à gauche, un modèle de type wallmount grand public, au milieu, un modèle de type desktop professionnel, et, à droite, un modèle de type wallmount professionnel avec interfaces Ethernet et USB**.**

Figure 7.14
Équipements CPL HomePlug AV de marque Devolo

Les modems CPL câble TV

Certains fabricants de modems CPL proposent des équipements CPL permettant de se connecter à un réseau de télévision câblé. Ces équipements présentent une importante immunité aux perturbations électromagnétiques.

Le câble TV utilise les deux bandes de fréquences suivantes :

- données dans la bande 1-24 MHz ;
- signal TV dans la bande 47-862 MHz.

Les réseaux des câblo-opérateurs sont beaucoup moins répandus que le réseau électrique et comportent généralement peu de prises TV. De tels réseaux peuvent toutefois se révéler complémentaires du réseau électrique du fait de leur débit relativement constant, plus stable en tout cas que celui du réseau électrique.

Un réseau câble TV étant un réseau partagé, son débit est divisé par le nombre d'utilisateurs présents sur le support.

Les équipements CPL câble TV utilisent plusieurs types de connecteurs, notamment les connecteurs F-Type pour se connecter sur le câble TV. Sur un réseau câblé, la distance de propagation est généralement de 500-700 m, tout en gardant un débit utile important.

La figure 7.15 illustre, de gauche à droite, un modem CPL câble TV CableLAN de marque Corinex, des câbles coaxiaux, un connecteur F-Type et un splitter Channel Vision.

Figure 7.15
Modems CPL câble TV CableLAN de marque Corinex, câbles TV, connecteur F-type et splitter

Les modems CPL câble TV ont évolué en même temps que les évolutions des technologies HomePlug et de leur débit. Il est possible d'utiliser ces modems pour les deux applications suivantes :

- Circulation des données sur le réseau câblé TV pour en faire la dorsale du réseau CPL.
- Utilisation de l'interface coaxiale à l'aide d'un adaptateur, appelé injecteur *(voir plus loin dans ce chapitre)*, qui permet d'émettre le signal CPL directement sur les câbles électriques, sans recourir aux prises de courant.

Bien que ces modems CPL utilisent un support qui n'est pas le câble électrique, ils sont compatibles HomePlug par le biais de technologies de HomeNetworking telles que HomePNA (Home Phoneline Network Alliance) ou UPA (Universal Powerline Association).

Le tableau 7.4 fournit les débits des principaux modems CPL câble TV en fonction de la technologie utilisée.

Tableau 7.4 Débits des principaux modems CPL câbles TV

Modem CPL câble TV	Technologie	Débit (Mbit/s)
Corinex CableLAN	HomePNA 1.0	10
Corinex CableLAN AV	HomePNA 3.0	128
Corinex CableLAN 200	Pre-UPA	200

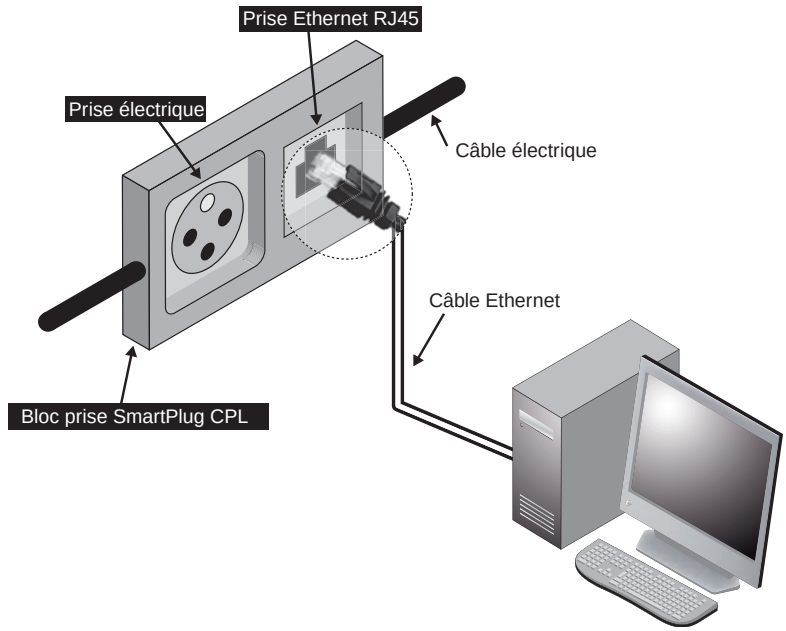
Le standard HomePNA permet également d'utiliser les câbles téléphoniques domestiques pour transporter des données. La société Corinex commercialise notamment le produit CableLAN Combo Adapter, qui utilise le standard HomePNA 3.0 et dispose de deux interfaces, l'une coaxiale (connecteur F-Type) et l'autre téléphonique (connecteur RJ-11).

Les modems CPL intégrés dans la prise électrique

Certains constructeurs proposent des modems CPL directement intégrés dans la prise électrique.

Les sociétés Lea et Legrand ont développé une prise CPL, appelée SmartPlug, qui intègre un modem CPL HomePlug dans le bloc prise et une connectique Ethernet RJ-45. Le schéma de principe de la SmartPlug est illustré à la figure 7.16.

Figure 7.16
Schéma de principe de la prise électrique CPL SmartPlug de LEA-Legrand



Les modems CPL/Wi-Fi

Comme nous le verrons au chapitre 13, dédié aux réseaux hybrides, les technologies CPL et Wi-Fi sont parfaitement complémentaires et permettent aux utilisateurs de construire un réseau complet, avec une couverture radio optimale. Le réseau CPL joue le rôle de dorsale du réseau Wi-Fi afin d'offrir à ce dernier une meilleure couverture radio.

Les dernières évolutions de la technologie HomePlug permettent de comparer les performances des deux technologies. HomePlug Turbo offre un débit utile maximal au niveau physique de 85 Mbit/s, et le standard IEEE 802.11g 55 Mbit/s. Les équipements CPL/Wi-Fi permettent de bénéficier à la fois de la facilité d'utilisation du CPL et de la mobilité de Wi-Fi.

Certains de ces équipements intègrent les composants CPL et Wi-Fi, tandis que d'autres proposent des emplacements PCMCIA dans un modem CPL permettant à l'utilisateur d'utiliser la meilleure carte Wi-Fi pour son réseau radio.

La figure 7.17 illustre des modems CPL/Wi-Fi Thesys *(à gauche)* et Devolo MicroLink dLAN Wireless *(à droite)*.

Figure 7.17
Modems CPL/Wi-Fi Thesys et Devolo

Certains constructeurs travaillent actuellement à l'optimisation de la couche MAC entre CPL et Wi-Fi afin d'augmenter la fiabilité de ces réseaux hybrides et leurs performances au niveau de la couche MAC. Ces projets devraient déboucher sur des produits commercialisés en 2007.

Une des applications optimales du CPL en complément de Wi-Fi consiste à utiliser le réseau d'éclairage d'un bâtiment pour constituer une dorsale CPL et de placer les équipements CPL/Wi-Fi à proximité des ampoules.

La société taïwanaise Lite-On propose ainsi le produit ORB, qui se présente sous la forme d'une ampoule CPL/Wi-Fi, qui, outre son rôle d'ampoule d'éclairage permet de diffuser efficacement le signal radio Wi-Fi dans la pièce. Cette ampoule est connectée en CPL à la fois au réseau d'éclairage et aux autres équipements CPL ou CPL/Wi-Fi du réseau d'éclairage et du réseau électrique d'alimentation.

Les modems CPL multifonctions

Certains produits CPL incluent différentes fonctions réseau permettant de répondre aux besoins des ingénieurs réseau comme des utilisateurs, notamment les suivants :

- Modem CPL/hub Ethernet permettant de connecter plusieurs PC à un même modem Ethernet CPL.
- Modem CPL ADSL/routeur permettant de diffuser le signal provenant de la connexion Internet sur le réseau électrique. Certains équipements y ajoutent même une carte Wi-Fi.

La figure 7.18 illustre des modems CPL hub NetGear *(à gauche)* et Thesys NetPlug *(à droite).*

Figure 7.18
Modems CPL hub Netgear et Thesys NetPlug

La figure 7.19 illustre un équipement CPL Devolo MicroLink dLAN ADSL Modem Router.

Figure 7.19
Modem CPL ADSL/routeur Devolo

Les modems CPL audio et téléphonique

Le CPL permettant de faire circuler des données sur le réseau électrique, certains constructeurs ont depuis longtemps développé des produits CPL audio et téléphonique.

Un modem CPL audio se branche d'un côté sur le réseau électrique et de l'autre sur un équipement hi-fi tel qu'une enceinte d'écoute audio, une chaîne hi-fi, un serveur de fichiers audio, etc.

La figure 7.20 illustre un modem CPL audio Devolo MicroLink dLAN Audio, avec les connecteurs Cinch (deux pour les voies Out et deux pour les voies In) et SPDIF (un pour la voie In et un pour la voie Out) et Audio Jack (un pour la voie In et un pour la voie Out), permettant de diffuser quatre canaux audio de 192 Kbit/s sur le réseau électrique.

Il est nécessaire d'effectuer une configuration des modems CPL audio afin de paramétrer les éléments du réseau local CPL et de charger les plug-in nécessaires aux serveurs de fichiers audio.

Il est également possible d'utiliser le CPL pour diffuser le signal analogique téléphonique au sein d'un bâtiment, où il est fréquent de ne trouver qu'une ou deux prises téléphoniques d'accès au RTC public. Il est alors pratique d'utiliser le réseau électrique présent dans toutes les pièces pour disposer de prises téléphoniques déportées des prises existantes.

Figure 7.20
Modem CPL audio Devolo MicroLink dLAN Audio

On utilise en ce cas deux modems CPL téléphoniques, l'un connecté à l'arrivée téléphonique France Télécom et l'autre à une prise électrique. C'est sur ce dernier qu'est raccordé le téléphone analogique au moyen d'un connecteur RJ-11.

La figure 7.21 illustre un modem CPL téléphonique Wingoline permettant de constituer un réseau de 24 modems au maximum sur un même réseau électrique. La bande de fréquences utilisée va de 3,3 à 8,2 MHz, et la distance de propagation sur les câbles est de 150 m, légèrement plus faible que celle des modems CPL Ethernet.

Figure 7.21
Modem CPL téléphonique Wingoline roda avec deux interfaces téléphoniques RJ-11

Les méthodes d'accès au média

Dans les réseaux CPL, la méthode d'accès au média consiste à « brancher » les équipements CPL sur le réseau électrique, de manière à obtenir les meilleures performances au niveau physique et donc les meilleurs débits utiles au niveau des couches supérieures.

Pour brancher un équipement CPL sur le réseau électrique il existe deux méthodes différentes, appelées couplages : le couplage capacitif et le couplage inductif.

Le couplage capacitif est celui utilisé majoritairement par les modems CPL. Le terme capacitif signifie que le modem CPL branché sur la prise électrique est vu comme une capacité, c'est-à-dire un condensateur. La figure 7.22 illustre le principe de fonctionnement du couplage capacitif.

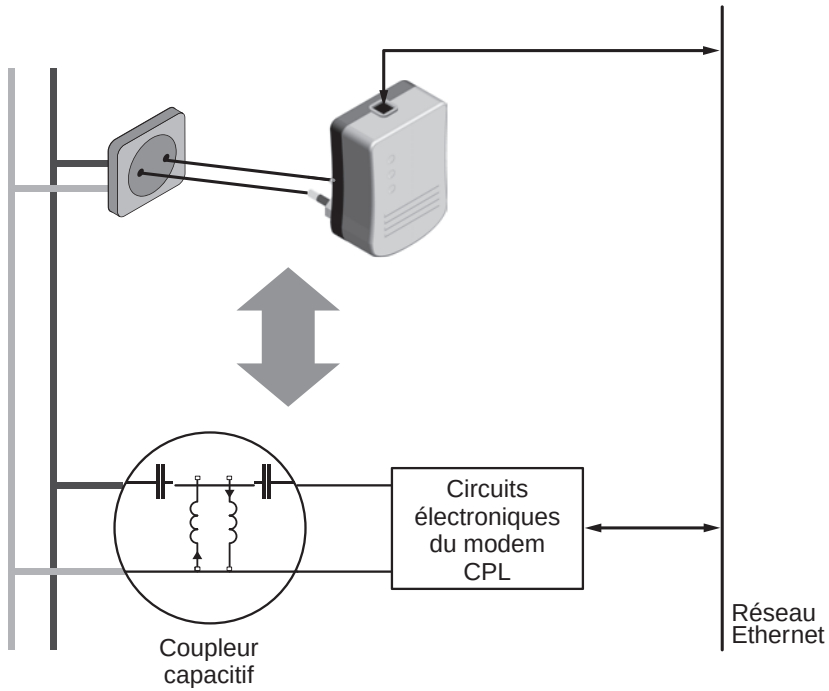


Figure 7.22
Principe du couplage capacitif

Couplage

Dans le domaine électrique, le couplage peut se définir comme la manière dont deux circuits électriques se connectent ensemble afin de générer une circulation d'électrons entre ces deux circuits. Cette circulation d'électrons est transportée par un champ électrique et magnétique créé entre les deux circuits électriques du fait de leurs caractères inductif et capacitif.

Le couplage inductif est beaucoup plus efficace que le couplage capacitif. Il utilise la méthode d'induction électromagnétique entre deux câbles électriques ou entre un câble électrique et une bobine enroulée autour de ce câble. Un coupleur inductif réduit l'atténuation de 10 à 15 dB pour certaines fréquences par rapport à un coupleur capacitif. L'atténuation entre la prise de courant et le coffret électrique varie de 10 à 30 dB. Elle est maximale entre 15 et 20 MHz.

Dans le domaine des réseaux CPL, les injecteurs sont les équipements qui permettent de brancher un équipement CPL sur le réseau électrique par l'intermédiaire d'un couplage inductif directement autour des câbles électriques, par exemple au niveau du tableau électrique d'un bâtiment.

La figure 7.23 illustre le principe d'un injecteur de signal CPL composé des deux éléments suivants :

- Une bobine magnétique enroulée autour du câble neutre du réseau électrique. Comme nous le verrons aux chapitres 11 et 12, le câble neutre est le câble le plus intéressant pour l'injection du signal CPL sur un réseau électrique, car il est distribué sur toute l'installation électrique.
- Un modem câble TV connecté par un câble (coaxial, par exemple) à la bobine magnétique.

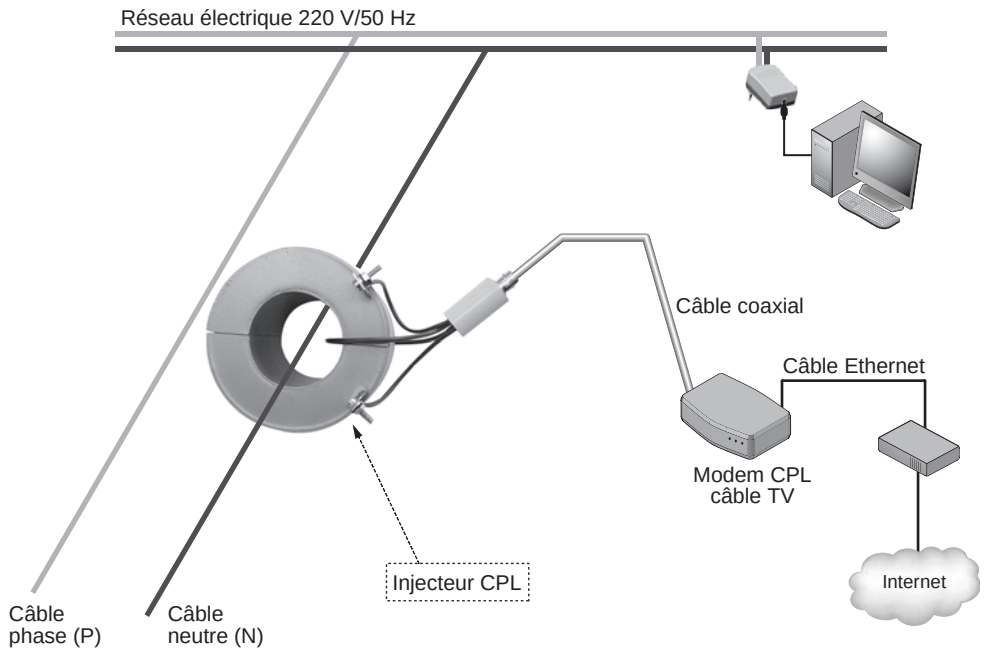


Figure 7.23

Injection du signal CPL par couplage inductif avec une bobine sur un réseau monophasé

La figure 7.24 illustre le même principe, mais deux ferrites sur un réseau triphasé.

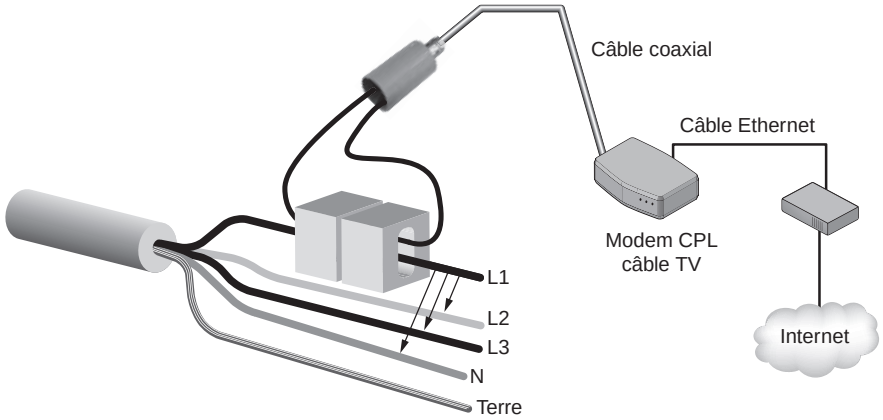


Figure 7.24
Injection du signal CPL par couplage inductif avec deux ferrites sur un réseau triphasé

Choix du câble d'injection

Il est préférable de faire l'injection sur le câble neutre pour un réseau monophasé et sur une des phases pour un réseau triphasé. Les performances sont meilleures en injectant sur un seul câble que sur plusieurs en même temps.

Cette méthode de branchement des équipements CPL nécessite d'accéder aux câbles électriques du réseau 220 V/50 Hz, contrairement au couplage capacitif, qui se limite au branchement d'un appareil sur une prise électrique. Il est donc important de demander à un électricien habilité d'effectuer l'opération de couplage, qui nécessite une connaissance des risques électriques à proximité des câbles et organes du réseau électrique.

La figure 7.25 illustre un injecteur CPL Eichhoff, avec la bobine magnétique ouverte *(à gauche)* et fermée (au milieu), comme elle l'est autour du câble électrique, et le connecteur coaxial *(à droite)* de type F-Type, qui permet de connecter l'injecteur au modem câble TV.

Figure 7.25
Injecteur CPL Eichhoff avec bobine et ferrites

Les méthodes de piquage

Les méthodes dites de piquage permettent de connecter des équipements CPL directement aux câbles électriques du réseau en perçant l'isolant du câble et le câble électrique lui-même.

De telles méthodes exigent de recourir à un électricien habilité à intervenir sur les réseaux électriques BT (basse tension) ou MT (moyenne tension) du fait du risque électrique.

La figure 7.26 illustre le principe de fonctionnement du couplage par piquage.

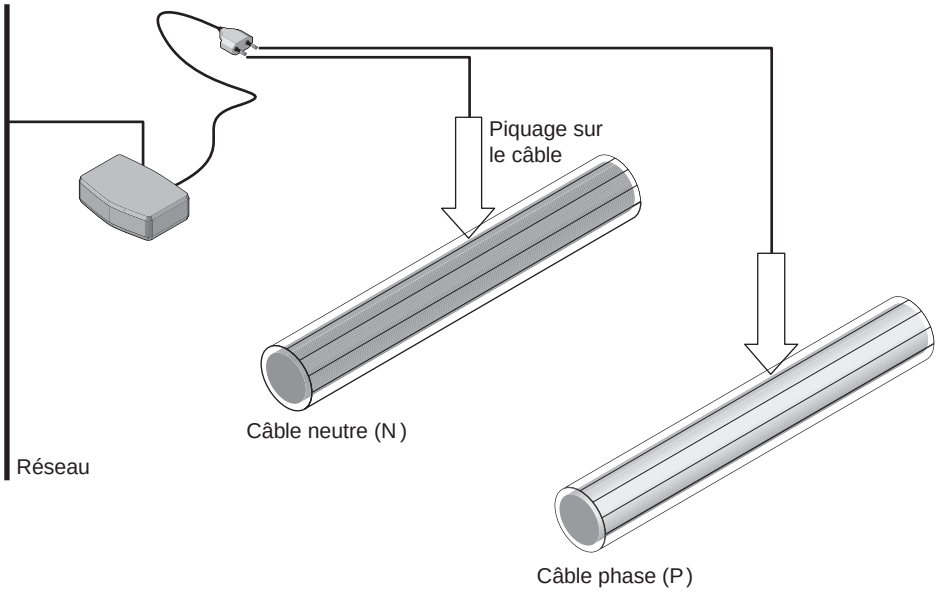


Figure 7.26
Couplage CPL par piquage

Transformateurs et compteurs

Pour concevoir la topologie d'un réseau CPL, il est nécessaire de connaître la portée du signal CPL sur le réseau électrique et d'identifier les points du réseau susceptibles de recevoir ce signal. Cette information permet en outre de sécuriser le réseau CPL.

Certains équipements présents sur le réseau électrique où les équipements CPL sont installés influent sur le réseau CPL dans la mesure où ils peuvent altérer le signal, voire le couper complètement. Il est alors nécessaire d'injecter le signal à des emplacements du réseau électrique où le signal CPL ne risque pas d'être coupé. Parmi les équipements d'un réseau électrique susceptibles de couper le signal CPL, citons notamment les suivants :

- Les transformateurs, composés de deux bobines permettant de changer la tension d'une valeur à une autre. Ces bobines font office d'isolateur entre deux parties d'un réseau électrique ; on parle d'isolation galvanique.

- Certains types de compteurs intégrant une isolation galvanique, se comportent également comme des coupeurs de signal CPL. Ces modèles sont toutefois relativement rares, et la plupart des compteurs laissent passer le signal CPL.

Dans ces deux cas, il peut être utile de surpasser ces équipements pour permettre au signal CPL de se prolonger sur l'ensemble du réseau électrique.

Les transformateurs

Les transformateurs étant par nature des équipements électriques établissant une isolation physique entre deux circuits électriques de tension différente, ils ne permettent pas de véhiculer le signal CPL entre les deux parties du réseau. Il est en ce cas nécessaire d'adjoindre au transformateur un équipement CPL permettant de récupérer le signal CPL d'un côté du transformateur et de le réinjecter de l'autre côté en le réamplifiant afin que le signal parcoure tout le réseau électrique BT jusqu'au modem CPL de l'utilisateur final.

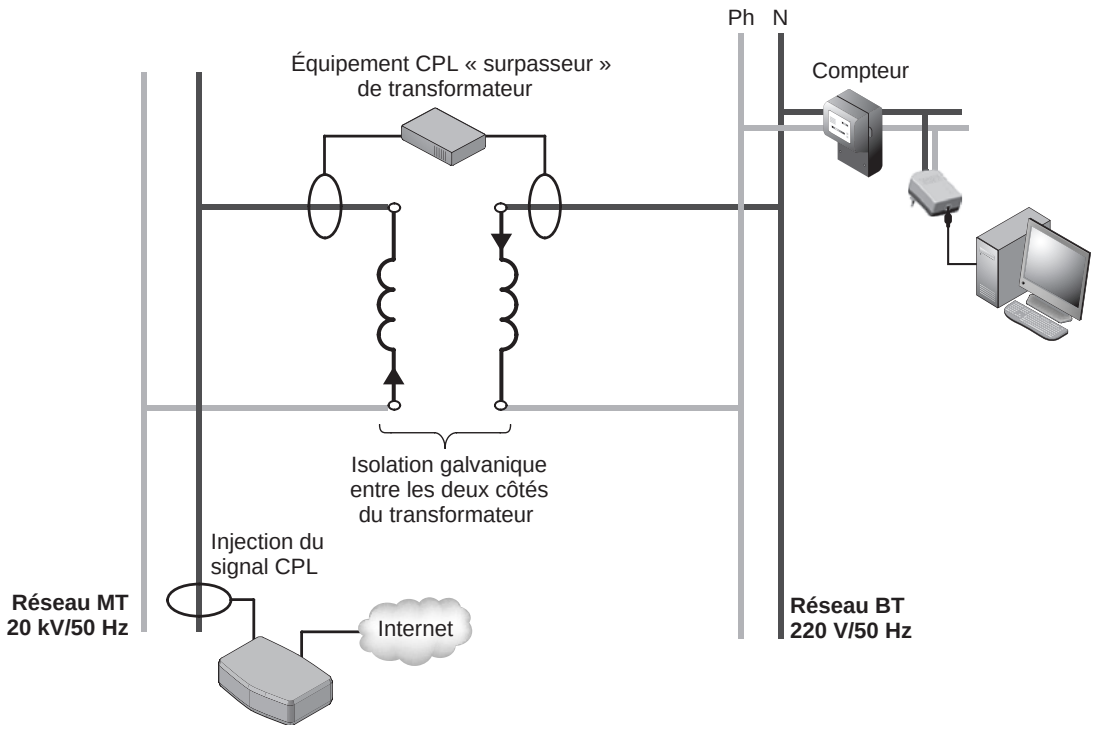


Figure 7.27
Surpassement d'un transformateur

La figure 7.27 illustre le principe de surpassement d'un transformateur avec les différents points d'injection du signal CPL et le modem CPL de l'utilisateur final situé derrière le compteur.

Cette opération d'installation d'un équipement CPL de surpassement d'un transformateur ne peut être effectuée que par des équipes habilitées par l'opérateur du réseau électrique. Il est en effet nécessaire d'accéder au local du transformateur MT/BT (moyenne tension vers basse tension).

Les compteurs

Les compteurs permettent de mesurer la consommation électrique d'une habitation et de facturer les usagers du réseau électrique EDF ou d'une autre régie électrique. Ce sont des éléments importants d'un réseau électrique pour le signal CPL puisqu'ils séparent le réseau électrique public et le réseau électrique d'un bâtiment, d'un logement ou d'une entreprise.

La grande majorité des compteurs laissent passer le signal CPL de chaque côté du réseau électrique. Il est donc important de configurer correctement le cryptage de son réseau local CPL si l'on veut éviter qu'une personne malveillante intercepte les données qui circulent sur le réseau électrique.

Les compteurs électromécaniques sont les plus anciens. Datant des années 1970, ils se rencontrent très fréquemment dans les installations électriques d'EDF. Ils laissent passer le signal CPL de part et d'autre du circuit électrique. Leur atténuation du signal CPL est évaluée à 20 dB.

Parmi les compteurs, trois des modèles de compteurs électromécaniques les plus courants dans le réseau EDF sont les suivants :

- compteur monophasé 10-30 A Schlumberger ;
- compteur monophasé 15-60 A Landis & Gyr ;
- compteur triphasé Landis & Gyr.

Pour contrecarrer le piratage des compteurs électromécaniques, ces derniers ont été peu à peu remplacés au cours des années 1990 par des compteurs électroniques. Très difficiles à pirater, ces derniers permettent une télérelève *via* le réseau EDF grâce à la technologie CPL basse fréquence très bas débit. Ils laissent également passer le signal CPL. On évalue leur atténuation du signal CPL à 15 dB.

Parmi les compteurs électroniques, trois des modèles les plus courants dans le réseau EDF sont les suivants :

- compteur monophasé 15-90 Siemens (1997) ;
- compteur triphasé 15-90 A Sagem (1993) ;
- compteur triphasé 10-60 A Schlumberger (1990).

Les répéteurs

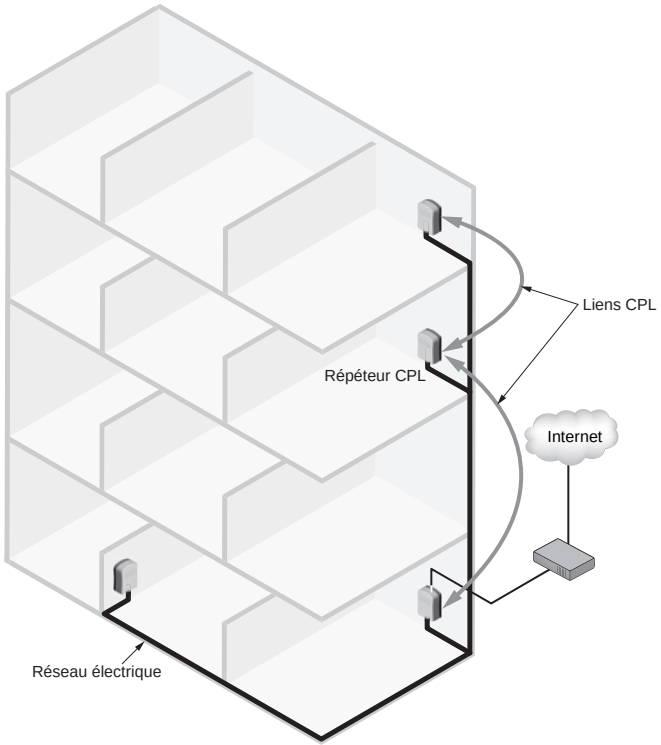
Les répéteurs sont des équipements fréquemment utilisés en télécommunications pour régénérer le signal de transmission de données lorsque les distances sont trop grandes pour que le signal reçu soit utilisable par les équipements de transmission de données.

Dans le cas des réseaux CPL, le réseau électrique provoque des atténuations du signal CPL (passage d'éléments du réseau électrique, bruits des appareils connectés, qualité des câbles électriques, etc.), qui rendent parfois impossible d'obtenir une liaison CPL entre deux points éloignés du réseau sans répétition du signal.

Il existe deux types de répéteurs, les passifs et les actifs. Les répéteurs passifs régénèrent le signal CPL en utilisant deux puces CPL relayant le signal de l'une vers l'autre. La répétition se fait à la fois au niveau de la couche physique et de la couche MAC. Les répéteurs actifs amplifient le signal CPL présent sur le câble électrique sans recourir à une nouvelle puce CPL pour relayer le signal. La répétition ne se fait qu'au niveau de la couche physique.

La figure 7.28 donne un exemple d'utilisation d'un répéteur.

Figure 7.28
Exemple d'utilisation d'un répéteur CPL



On ne trouve que peu de répéteurs dans le commerce puisque les équipements CPL permettent généralement de diffuser le signal CPL de manière satisfaisante. Il peut

cependant être intéressant de répéter le signal CPL pour obtenir des débits convenables sur tout le réseau électrique.

Les répéteurs CPL disponibles dans le commerce sont les suivants :

- Schneider IR LR 1100 ;
- Asoka PL8230-2RP (actif) ;
- Oxance PLT300, PLT320 (actif) ;
- CMM RPT1-0.

Répéteur CPL maison

Il est possible de fabriquer soi-même un répéteur CPL en utilisant des modems CPL Ethernet du commerce.

Il suffit de prendre deux modems CPL Ethernet et de les relier par un câble Ethernet (croisé ou droit, selon que les cartes réseau sont auto-sense ou non, c'est-à-dire qu'elles savent s'adapter ou non au croisement du câble réseau). Il faut ensuite configurer deux clés réseau CPL différentes sur chaque modem CPL, chaque clé permettant au modem de se connecter sur une partie du réseau CPL disposant de la même clé *(voir le chapitre 10)*.

La figure 7.29 illustre ce principe de fonctionnement.

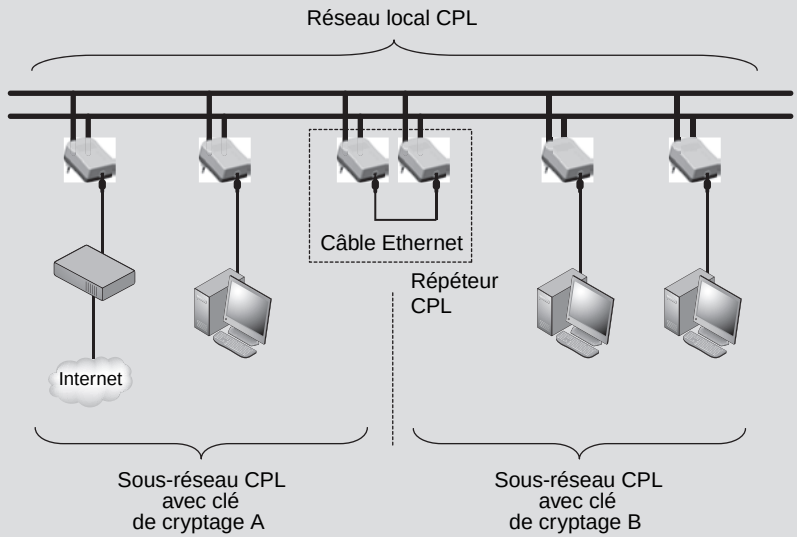


Figure 7.29

Répéteur CPL maison

Les deux sous-réseaux CPL communiquent entre eux par le biais du répéteur composé des deux modems Ethernet aux clés de cryptage différentes. Cette configuration présente toutefois l'inconvénient de diminuer le débit utile de l'ensemble du réseau local CPL puisque le répéteur utilise la bande de fréquences pour régénérer le signal CPL sur le réseau électrique.

Les filtres

Comme indiqué précédemment, le réseau électrique est un support de communication susceptible d'être altéré par des perturbations provenant des équipements électriques qui y sont branchés. Ces équipements électriques renvoient notamment des bruits électromagnétiques dans la bande de fréquences des équipements CPL. Il est dès lors intéressant d'installer des filtres au plus près des équipements perturbateurs afin de bloquer les fréquences générant les perturbations.

Un filtre CPL peut aussi être utilisé pour bloquer le signal CPL sortant afin qu'il ne se propage pas hors du réseau électrique délimité par le compteur.

La figure 7.30 illustre un réseau électrique comportant des équipements CPL, des équipements perturbateurs (variateur d'éclairage, sèche-cheveux, multiprise, disjoncteur) et l'emplacement des filtres CPL.

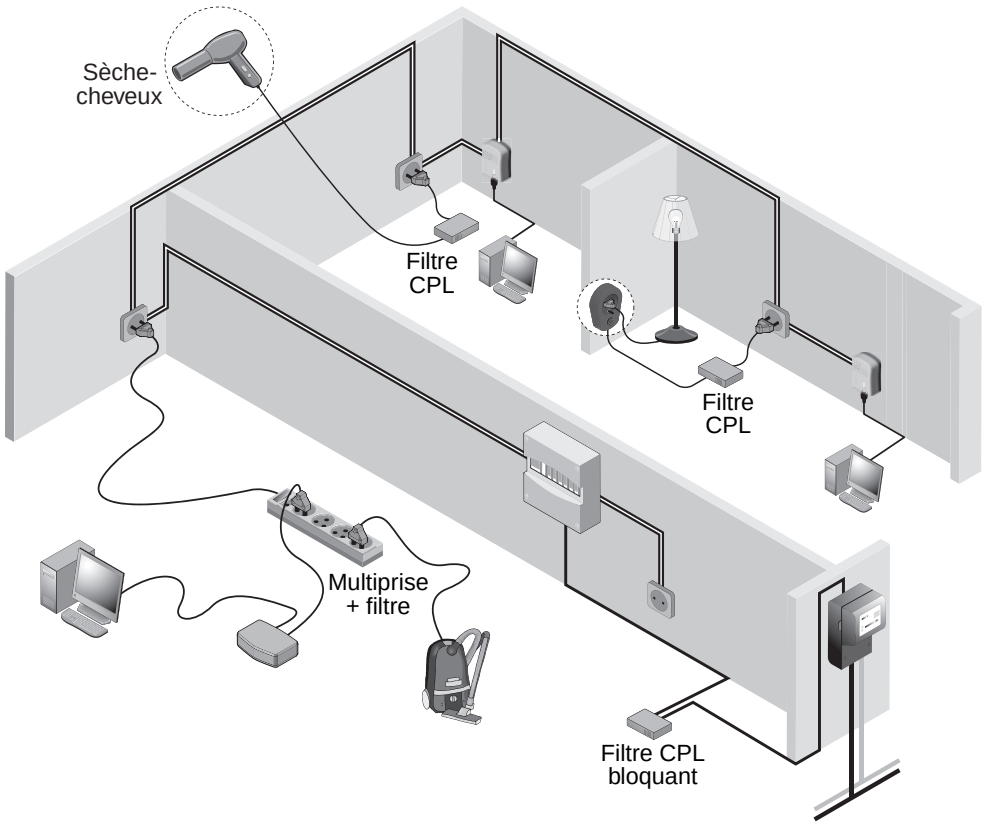


Figure 7.30
Placement de filtres CPL sur un réseau électrique domestique

Un filtre se branche entre l'équipement perturbateur et le réseau électrique. Il fait office de « sur-prise » électrique au-dessus de la prise électrique, l'équipement électrique perturbateur venant se brancher sur le filtre.

Le tableau 7.5 récapitule les principaux équipements électriques susceptibles de perturber un réseau local.

Tableau 7.5 Équipements électriques perturbant un réseau CPL

Équipement électrique	Cause des perturbations
Sèche-cheveux	Moteur
Écran cathodique	Tube cathodique
Perceuse	Moteur
Variateur de lumière	Gradateur et diodes Zener
Halogène	Gradateur et diodes Zener
Multiprise	Mauvaises connexions électriques et accumulation d'équipements sur une même prise
Équipement avec mauvais marquage CE	Hors des gabarits de perturbation

La figure 7.31 illustre un filtre CPL bloquant Eichhoff. Cet équipement se place entre le tableau électrique et le réseau électrique domestique, professionnel ou industriel afin d'éviter que le signal CPL dépasse le compteur et soit récupéré depuis un autre réseau électrique.

Figure 7.31
Filtre CPL bloquant de marque Eichhoff

La société CMM (courant multimédia) vend des filtres antibruit de type « sur-prise », qui se placent entre les équipements potentiellement perturbateurs du réseau CPL et la prise

électrique sur laquelle est branchée l'alimentation de l'équipement en question. Cet équipement est illustré dans la figure 7.32.

Figure 7.32
Filtre CPL antibruit de marque CMM

Les coûts du CPL

En corollaire de l'évolution des spécifications HomePlug et de l'augmentation de la demande, les prix des produits CPL n'ont cessé de baisser au cours des années 2005 et 2006. Entre 2003 (date de la sortie des premiers produits HomePlug 1.0) et 2005, cette baisse a été de l'ordre de 30 %.

L'arrivée, début 2006, des produits HomePlug Turbo a accentué cette baisse. On peut considérer que les prix des produits HomePlug 1.0 vont continuer de baisser de 20 à 50 %.

Dès l'apparition des premiers produits HomePlug AV, fin 2006, les produits HomePlug Turbo devraient subir à leur tour une baisse de 10 à 20 %.

Pour les particuliers, les CPL sont une solution idéale pour partager une même connexion Internet entre deux PC. C'est d'ailleurs l'application la plus commune des équipements CPL. Ces derniers, notamment les modems CPL multifonction, intègrent désormais toutes sortes de fonctionnalités et jouent les rôles de modem Internet, routeur, pare-feu, serveur DHCP, commutateur et point d'accès Wi-Fi, soit six équipements en un. Si l'on prend en compte le coût de toutes ces fonctionnalités, le prix de ces équipements CPL est finalement assez attractif. D'autant qu'il n'est plus nécessaire de poser des câbles ni de percer des trous.

Dans une entreprise, pour câbler un bâtiment en Ethernet, il faut tirer des câbles dans toutes les pièces et installer des armoires de brassage, ce qui n'est pas le cas avec le CPL. Un autre avantage du CPL sur Ethernet est le changement dynamique de topologie qu'il permet. Dans Ethernet, en effet, le changement de topologie demande généralement la pose de nouveaux câbles et se traduit par des coûts supplémentaires.

Le tableau 7.6 récapitule les coûts des équipements CPL à la fin du 1er semestre 2006.

Tableau 7.6 Coûts des équipements CPL

Équipement	Coût (en euro)
Modem USB : – HP 1.0 – Turbo	 50 à 100 80 à 100
Modem Ethernet : – HP 1.0 – Turbo – AV	 50 à 100 80 à 100 100 à 300
Modem câble TV	100 à 300
Prise intégrée	100 à 300
Équipement CPL/Wi-Fi	100 à 200
Équipement CPL multifonction	100 à 300
Équipement CPL audio et téléphonique	100 à 150
Injecteur inductif	120
Répéteur	200 à 400
Filtre	200 à 400

8

Installation

Les perturbations reçues et engendrées par les réseaux CPL doivent être prises en compte lors de l'installation du réseau. La topologie électrique du ou des bâtiments où seront installés les équipements est également un élément très important à prendre en compte pour constituer l'architecture du réseau CPL.

La définition de la topologie du réseau électrique est donc une étape essentielle. C'est elle qui détermine les performances de la transmission de données du réseau CPL. En effet, les équipements CPL, qu'ils soient mobiles ou fixes sur le réseau électrique, offrent aux liaisons de données différentes qualités selon leur position, l'existence d'équipements électriques perturbateurs situés à proximité et les filtres mis en place pour protéger le réseau électrique des injections de fréquences « parasites ».

Une autre contrainte concerne les débits réels, ceux annoncés ne correspondant jamais à ce dont dispose l'utilisateur. Certains mécanismes proposés par les CPL sont généralement à l'origine d'une baisse inattendue du débit. Cette baisse peut toutefois être minimisée par le choix de mécanismes appropriés et des paramètres associés lors de la configuration des équipements CPL et plus particulièrement de la passerelle CPL ou de l'équipement central.

Concernant la sécurité, nous verrons qu'il est important de mettre en place des techniques adéquates pour le cryptage des données et la séparation des réseaux logiques sur le réseau électrique, lequel peut être vu comme un bus de données partagé. La propagation du signal CPL dépassant les compteurs électriques d'une installation domestique, professionnelle ou industrielle, il est important de mettre en place des mots de passe pour le réseau local CPL protégeant les échanges de données.

Un réseau électrique est difficile à modéliser, et les performances peuvent varier rapidement en fonction de l'utilisation des équipements CPL. Ce chapitre rassemble les informations utiles pour comprendre ces variations et améliorer les performances.

Les bandes de fréquences

Les CPL grand public et professionnels utilisent deux bandes de fréquences, la bande 3-148 kHz pour les technologies bas débit et la bande 1-30 MHz pour les technologies haut débit.

Les technologies CPL pour réseaux électriques MT (moyenne tension), dits aussi BPL (Broadband PowerLine), sont autorisées à utiliser la bande de fréquences 30-50 MHz. Ces technologies sont installées et opérées sous la responsabilité des opérateurs des réseaux électriques MT.

Les bandes 3-148 kHz et 1-30 MHz sont dites sans licence, signifiant qu'il n'y a pas d'autorisation à demander ni d'abonnement à payer pour les utiliser. Elles sont toutefois réglementées en France par l'ARCEP (Autorité de régulation des communications électroniques et des postes), qui impose certaines limitations à leur utilisation en terme de puissance d'émission.

Ces bandes sont divisées en sous-bandes, sur lesquelles ont lieu les transmissions. Dans la mesure où toutes les technologies utilisent ces bandes de fréquences, des travaux de standardisation sont en cours pour permettre la coexistence des différents systèmes CPL sur un même réseau électrique. Nous revenons au chapitre 14 sur la coexistence et l'interopérabilité des technologies CPL.

Réglementation des fréquences radio

L'enjeu du déploiement de réseaux de télécommunications est d'obtenir les meilleures performances possibles en matière de débit, latence, jitte, CEM (compatibilité électromagnétique) et cohabitation des technologies, tout en respectant les limites imposées par les réglementations en vigueur.

Ces dernières fixent des limites quant à la puissance d'émission et aux bandes de fréquences autorisées. Des règles sont également édictées pour le niveau acceptable des perturbations engendrées en fonction des différentes technologies radio (radioamateur, radio ondes courtes analogique et numérique, etc.).

De par leur technologie et leur support, les équipements CPL sont émetteurs d'ondes radio induites dans les câbles électriques qui transportent les signaux.

Contrairement aux réseaux radio sans fil de type Wi-Fi, les équipements CPL vendus dans le commerce en Europe s'appliquent à rester dans les limites édictées par le Cenélec (Comité européen de normalisation électrotechnique) et l'ETSI (European

Telecommunications Standards Institute). Ces équipements sont conçus *de facto* pour respecter ces limites, et aucune modification matérielle ou logicielle n'est autorisée pour les outrepasser.

La brique logicielle des équipements HomePlug ne donne accès à aucun paramètre matériel (fréquence porteuse, sous-bandes de fréquences ou puissance d'émission). Cela signifie que les trames Ethernet qui sont envoyées par les outils de configuration des équipements CPL *(voir le chapitre 10)* ne permettent pas de modifier les fréquences et puissances utilisées par les équipements. Pour l'utilisateur du réseau CPL, la configuration ne donne donc pas accès aux paramètres de la couche physique, à la différence de Wi-Fi, avec ses 11 canaux et son paramétrage des puissances d'émission des interfaces.

La figure 8.1 illustre l'envoi d'une trame par l'outil de configuration vers l'équipement CPL à configurer. Cette trame est une trame Ethernet classique, reconnaissable sur un réseau par son champ ETHERTYPE, qui contient dans ses données les paramètres à configurer pour que le réseau CPL fonctionne au mieux.

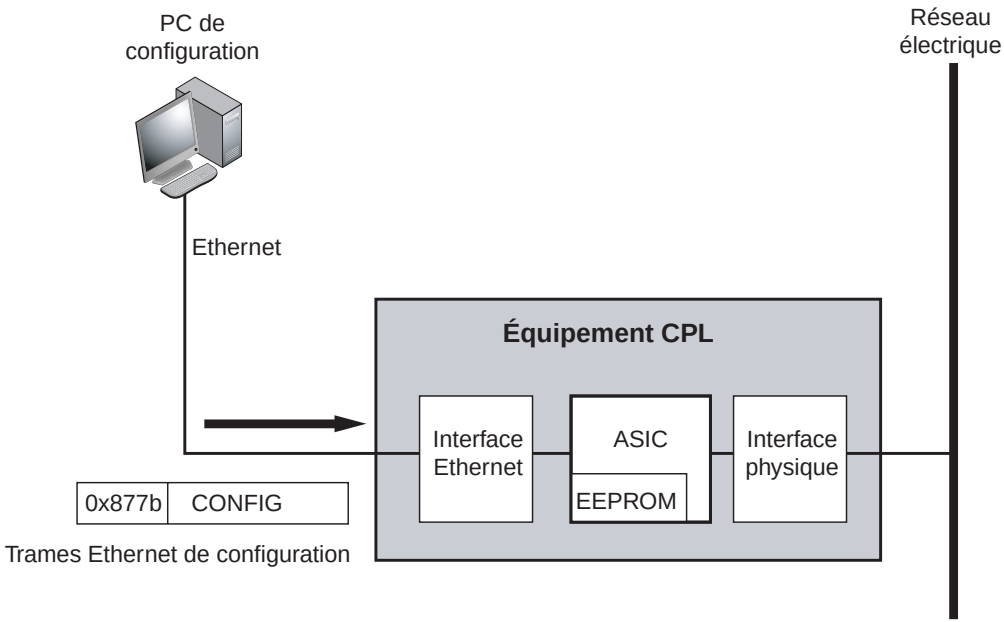


Figure 8.1
Trame Ethernet de configuration d'un réseau HomePlug

Le spectre d'utilisation des fréquences défini par l'ETSI se décompose globalement comme illustré à la figure 8.2. Faisant référence au TNRBF (tableau national de répartition des bandes de fréquences) édicté par l'ARCEP, il donne une idée de la répartition

des fréquences radio grand public situées à proximité de celles utilisées par les différentes technologies CPL.

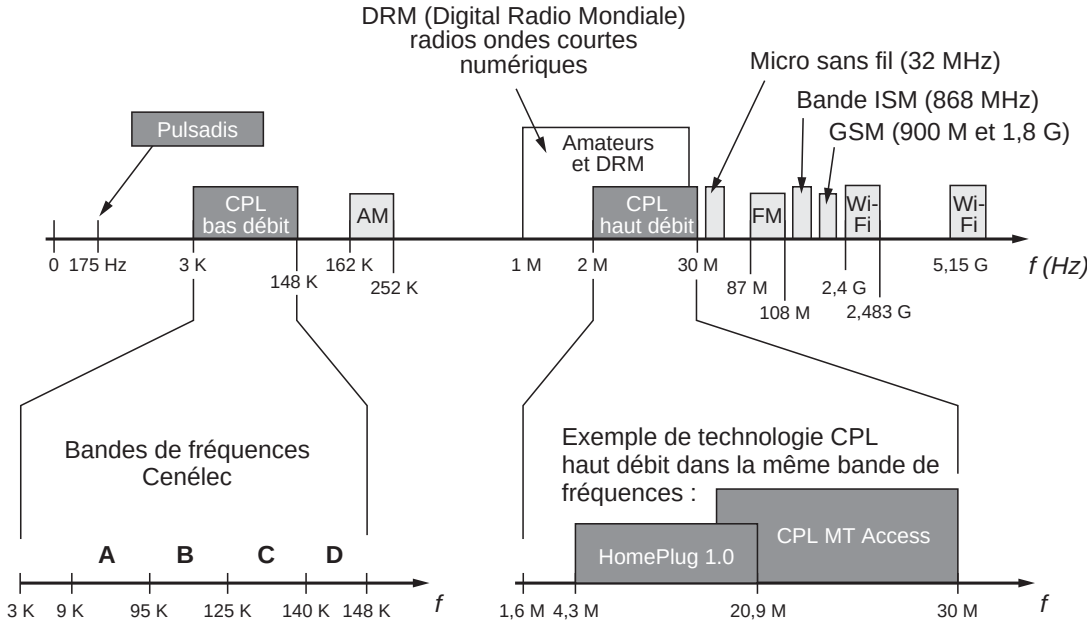


Figure 8.2
Bandes de fréquences des CPL

Comme expliqué précédemment, les réseaux CPL ne sont pas des réseaux radio, mais leur implémentation sur les câbles électriques produit des ondes rayonnées qui se propagent grâce aux câbles faisant fonction d'antennes radio. Les réseaux CPL sont donc vus par les organismes de régulation des télécommunications comme des réseaux radio, qui, à ce titre, doivent respecter des contraintes de puissance d'émission et de bandes de fréquences.

Comme indiqué précédemment, les fréquences utilisées par les CPL haut débit se situent dans la bande des 1-30 MHz. Cette bande est également utilisée par les radioamateurs et par la future radio ondes courtes numérique, dite DRM (Digital Radio Mondiale), qui permettra de diffuser des programmes radio en qualité numérique sur des liaisons très grande distance, mais également de réaliser des transferts de données à des débits de quelques dizaines de kilobits/s.

Les perturbations engendrées par les réseaux CPL sur les radioamateurs et la DRM ont fait l'objet de nombreuses discussions afin de rendre possible la cohabitation des différentes technologies. Ces discussions ont amené les développeurs de technologies CPL à inclure des techniques dites *d'extinction* des fréquences déjà occupées par d'autres

technologies radio. Baptisées *notching*, ces techniques consistent à écouter les canaux radio pour réajuster ou éteindre certaines fréquences.

Le « notching », ou extinction dynamique de bandes de fréquences

Comme illustré à la figure 8.3, lorsque le réseau CPL s'aperçoit que les fréquences f1 et f2 sont utilisées, il « éteint » les bandes de fréquences contenant f1 et f2 dans son spectre autorisé. Ces bandes de fréquences restent « éteintes » pendant toute la durée d'utilisation de f1 et f2 puis sont rallumées dès que ces fréquences ne sont plus utilisées.

Cette technique dynamique s'appuie sur l'écoute du niveau de signal sur bruit mesuré en dB pour chaque bande de fréquences.

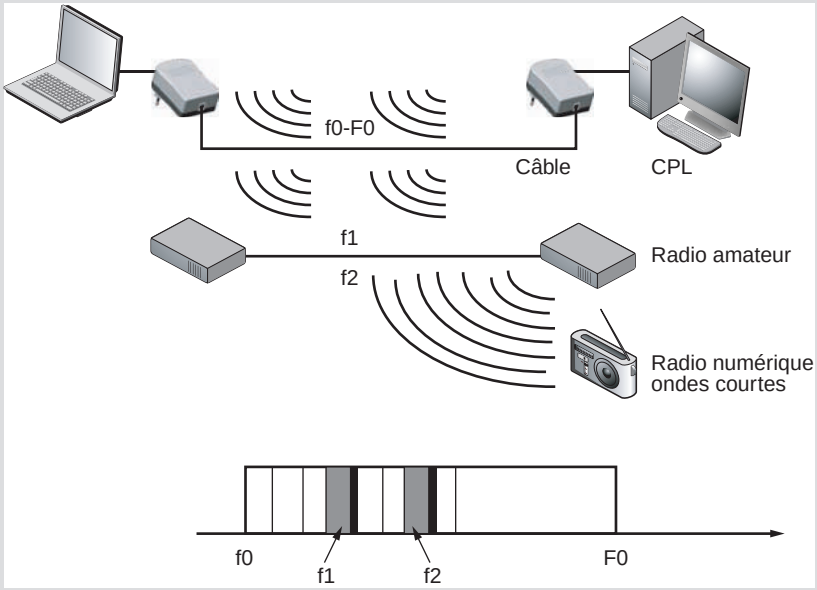


Figure 8.3

Notching des fréquences encombrées

Les CPL bas débit

Principalement utilisés dans la domotique et l'automotique (bus industriel des véhicules automobiles), les fréquences autorisées pour les CPL bas débit sont décrites par le Cenélec dans la norme EN-50065-1. Cette dernière définit les caractéristiques d'utilisation de toutes les bandes de fréquences comprises entre 3 et 148 kHz. La puissance d'émission du signal CPL est limitée par la tension maximale autorisée, qui est de 3,5 V pour ces bandes de fréquences.

Le tableau 8.1 récapitule les caractéristiques des bandes de fréquences des CPL bas débit.

Tableau 8.1 Bandes de fréquences Cenélec des CPL bas débit

Bande Cenélec	Bande de fréquences	Utilisation
	3-9 kHz	Limitée aux opérateurs de réseaux électriques (EDF, régies) pour leurs besoins propres, comme la télérelève
A	9-95 kHz	Limitée aux opérateurs de réseaux électriques
B	95-125 kHz	Usage domotique (babyphones, etc.)
C	125-140 kHz	Usage domotique (X10, etc.)
D	140-148 kHz	Usage domotique

Pour rappel, la bande radio AM couvre le spectre 162-252 kHz.

Les CPL haut débit

La bande de fréquences 1-30 MHz des CPL haut débit est plus ou moins utilisée. Elle est généralement vue comme constituée de deux sous-bandes, une bande inférieure, de 1-20 MHz, qui est surtout utilisée dans les CPL intérieurs à usage domestique, et une bande supérieure, de 2-30 MHz, surtout réservée aux CPL extérieurs à usage public du réseau électrique moyenne tension.

Concernant les CPL intérieurs à usage domestique, les différentes technologies employées, toutes fondées sur OFDM, partagent la bande de fréquences de manière différente pour atteindre les meilleures performances possibles en terme de débit et de latence. Ces performances sont obtenues par une amélioration constante des techniques de modulation de la couche physique (PHY) et des couches de liaison de données et MAC, incluant leurs méthodes d'accès au média physique.

Les techniques de modulation font l'objet d'un document standardisé RNRT (Recherche nationale en réseaux et télécommunications), intitulé IDILE (Internet haut débit sur ligne d'énergie) et coédicté par l'ENST (École nationale supérieure des télécommunications), Supélec, Spidcom, Schneider et EDF. Ce standard permet de tester les dernières techniques de modulation sur des cartes à interface CPL pour être testées sur le réseau EDF public ou sur des réseaux privés.

HomePlug 1.0 utilise la bande 4,49-20,7 MHz et 84 sous-porteuses, la bande de fréquences 0-25 MHz étant divisée en 128 bandes de 195,312 5 kHz d'utilisation. De cette manière, si chacune des bandes est numérotée de 1 à 128, HomePlug 1.0 utilise les bandes 23 à 106.

Cas particulier du signal Pulsadis d'EDF pour les compteurs à tarification jour/nuit

Le signal Pulsadis est plus connu sous le nom de signal jour-nuit, car il est utilisé par les compteurs EDF pour faire basculer un certain nombre d'équipements sous tension la nuit afin de profiter des tarifs EJP ou Tempo d'EDF. Ce signal est envoyé sur le réseau de distribution électrique d'EDF à la fréquence de 175 Hz.

La figure 8.4 illustre l'architecture électrique d'un réseau électrique BT avec l'implémentation du signal Pulsadis depuis les postes de contrôle d'EDF jusqu'au compteur de l'abonné.

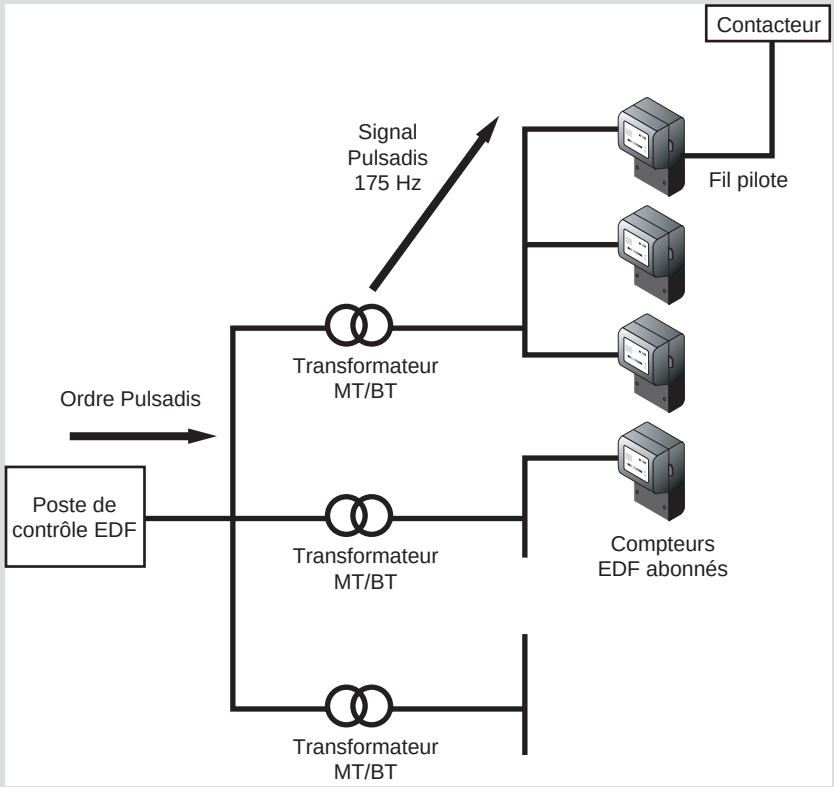


Figure 8.4

Architecture d'implémentation du signal Pulsadis sur le réseau électrique EDF BT

Une fois reçu par les compteurs EDF à tarification jour/nuit, ce signal déclenche les contacteurs des équipements électriques dûment équipés au niveau du tableau électrique domestique. Cela permet, par exemple, d'allumer les chauffe-eau pendant la nuit avant de rebasculer en heures pleines à 7 heures le matin.

Ce signal est basse fréquence, permettant ainsi sa bonne propagation sur le réseau électrique. Sa fréquence de 175 Hz est différente du 50 Hz et de ses harmoniques (100 Hz, 300 Hz, 600 Hz, etc.). Le signal est composé d'impulsions binaires d'une seconde espacées d'une seconde et demie. La trame ainsi constituée fait 102,25 secondes.

Aux États-Unis, certaines bandes de 23 à 106 sont utilisées par les radioamateurs (17 m, 20 m, 30 m, 40 m). Huit bandes correspondant aux fréquences des radioamateurs ne sont donc pas utilisées. Le total des bandes HomePlug 1.0 est donc de 84 – 8 = 76.

Le tableau 8.2 récapitule les bandes de fréquences haut débit utilisables selon chaque type de technologie CPL.

Tableau 8.2 Bandes de fréquences des technologies CPL haut débit

Technologie CPL	Bande de fréquences	Nombre de porteuses OFDM
HomePlug 1.0	4,49-20,7 MHz	76
HomePlug 1.1	Idem	Idem
HomePlug AV	2-28 MHz	917
DS2 – 45 Mbit/s – 200 Mbit/s	 – 1,6-30 MHz – 2,46-11,725 MHz + 13,8-22,8 MHz	 – 100 – 1 280 + 1 280
Spidcom	– 2-30 MHz – 30-60 MHz (extérieur)	– 900 – *Idem*
Main.net	4,3-13 MHz	NC

La bande de fréquences 1-30 MHz étant divisée en sous-bandes, chaque sous-bande transporte les porteuses de la modulation OFDM au niveau du canal de transmission. Il n'y a donc pas, à la différence de Wi-Fi, de canaux à proprement parler, que l'on pourrait configurer pour construire l'architecture du réseau. Dans les CPL, c'est toute la bande de fréquences qui fait office de canal de transmission, toutes les sous-bandes étant utilisées pour améliorer la robustesse des transmissions.

Contrairement à Wi-Fi, également, la configuration du réseau n'exige pas de faire des choix en fonction des autres canaux attribués. L'ensemble des canaux, ici appelés sous-bandes, de la bande autorisée sont utilisés. Le réseau peut donc être encombré par les différentes technologies qui coexistent sur un même réseau électrique. Dans ce cas, la technologie CPL utilise les sous-bandes libres ou peu occupées. Nous reviendrons au chapitre 13 sur la cohabitation entre technologies CPL et les travaux en cours sur une norme d'interopérabilité.

La figure 8.5 illustre le domaine fréquentiel des différentes sous-bandes OFDM de la modulation CPL, ainsi que les données binaires associées dans le cas d'un réseau CPL HomePlug 1.0.

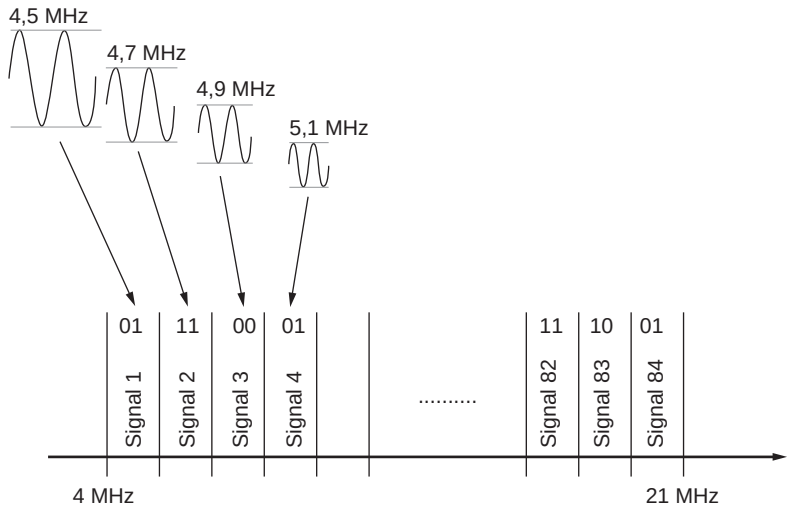


Figure 8.5

Sous-bandes OFDM de la modulation CPL HomePlug 1.0

Compatibilité électromagnétique et canaux de fréquences

Les différents appareils électriques et électroniques que nous utilisons dans un contexte domestique, professionnel ou industriel produisent des émissions d'ondes radio électromagnétiques dans l'environnement proche de leur lieu de fonctionnement.

Ces ondes radio électromagnétiques sont à des fréquences pouvant perturber le fonctionnement des équipements CPL du réseau et empêcher les communications de données dans les sous-bandes de fréquences. Certains équipements produisent plus de perturbations que d'autres sur les réseaux CPL. Le marquage CE en vigueur dans la Communauté européenne stipule les limites d'émissions radio électromagnétiques des équipements électriques et électroniques vendus dans le commerce.

Nous avons au chapitre 7 *(voir le tableau 7.7)* une liste des appareils perturbateurs des réseaux CPL. Nous y reviendrons un peu plus loin dans ce chapitre à propos des interférences.

Réciproquement, les équipements CPL émettent, autour des câbles électriques, des ondes électromagnétiques susceptibles de perturber le fonctionnement des équipements de télécommunications environnants. Le CISPR (Comité international spécial des perturbations radioélectrotechniques) de la CEI (Commission électrotechnique internationale) indique les limites d'émission d'ondes des équipements CPL.

Les technologies CPL actuelles, telles que HomePlug AV, mettent en œuvre une technique de *notching* afin de respecter ces contraintes d'émission.

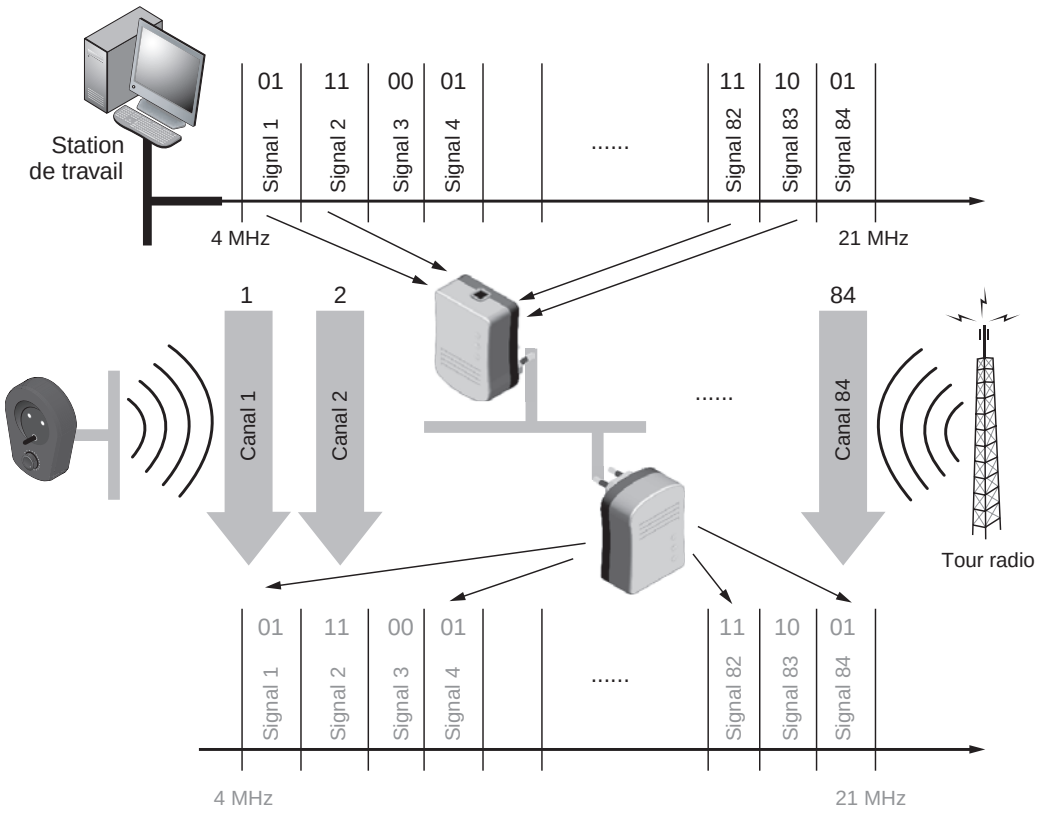


Figure 8.6
Modulation OFDM multicanal de la technologie CPL

La figure 8.6 montre que le canal de transmission peut être vu comme *N* sous-bandes avec leurs sous-porteuses, toutes fonctionnant en même temps et transportant chacune une partie des données de la couche physique.

Puissance d'émission des équipements CPL

La puissance mesurée du signal émis par les équipements CPL du marché est classiquement de 20 dBm (mesuré dans la bande des 1-30 MHz).

La puissance peut être exprimée par les grandeurs *P* ou *G* :

$$P = 10^{G/10} \text{ et } G = 10 \log P$$

où *G* correspond au gain (en dBm ou dBi) et *P* à la puissance (en mW).

Le tableau 8.3 donne la correspondance entre la puissance et le gain.

Tableau 8.3 Correspondance gain/puissance

Gain (en dBm)	Puissance (en mW)
3	2
5	3,1
7	5
9	8
15	31,6
19	79,4
24	251,1

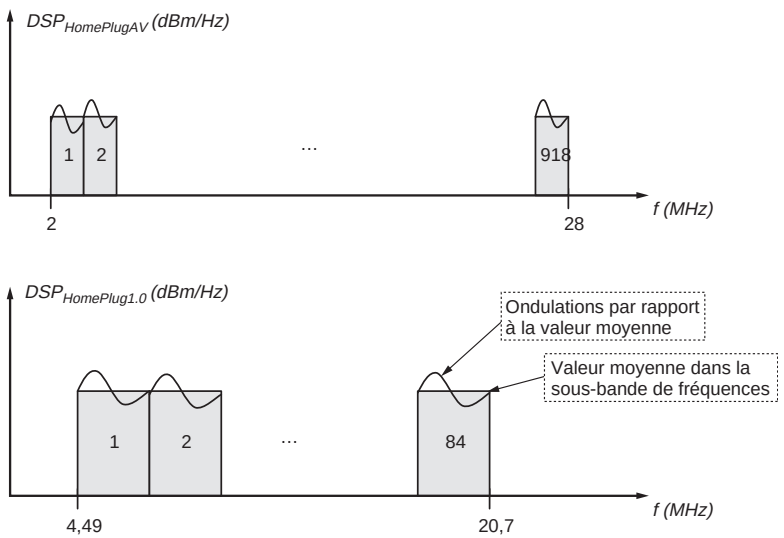
La limite de puissance étant fixée à 100 mW (équivalent à 20 dBm mesurés dans la bande 1-30 MHz) pour les équipements CPL des réseaux électriques, les performances des canaux de transmission sont fonction de la portée du signal.

Pour correspondre aux régulations en terme de CEM (compatibilité électromagnétique) imposées par le comité CISPR, les équipements CPL doivent limiter la valeur de leur puissance d'émission. Cette puissance d'émission est mesurée en valeur quasi-crête, et non pas moyenne. Cela correspond dans le domaine fréquentiel à une DSP (densité spectrale de puissance), c'est-à-dire à une répartition uniforme de la puissance totale d'émission sur toutes les sous-bandes de fréquences de la bande 1-30 MHz.

La technologie HomePlug 1.0 comporte 84 sous-bandes de 195,31 kHz, alors que HomePlug AV en comporte 918 plus étroites, de 24,414 kHz. L'ondulation de la DSP est donc moins importante dans HomePlug AV, ce qui permet d'augmenter la puissance d'émission de 2,2 dB pour les données de la PPDU.

La figure 8.7 illustre l'écart de DSP entre HomePlug 1.0 et AV. La DSP est exprimée en dBm/Hz.

Figure 8.7
Différences de DSP entre HomePlug 1.0 (en haut) et HomePlug AV (en bas)



Le tableau 8.4 récapitule la valeur moyenne de la puissance d'émission des différents éléments de la trame physique HomePlug dans ces deux versions.

Tableau 8.4 Puissance d'émission dans chaque sous-bande

Élément de la trame physique	Puissance moyenne d'émission	
	HomePlug 1.0.1	HomePlug AV
Préambule	3 dB	3 dB
FC (Frame Control)	0 dB	3 dB
Données de la PPDU	0 dB	2,2 dB
PRS (Priority Resolution Symbol)	3 dB	3 dB

Les spécifications HomePlug 1.0 et AV stipulent que, pour respecter les limites d'émission EM (électromagnétiques), les équipements CPL doivent avoir une DSP égale ou inférieure à – 50 dBm/Hz.

La figure 8.8 illustre la courbe de la DSP de HomePlug AV dans la bande 1-30 MHz. On observe clairement que certaines fréquences sont moins émissives que d'autres (– 80 dB par rapport à – 50 Hz). On peut considérer qu'une fréquence dont la DSP est de l'ordre de – 80 dB n'est pas perceptible pour le réseau électrique et les équipements à proximité des câbles électriques.

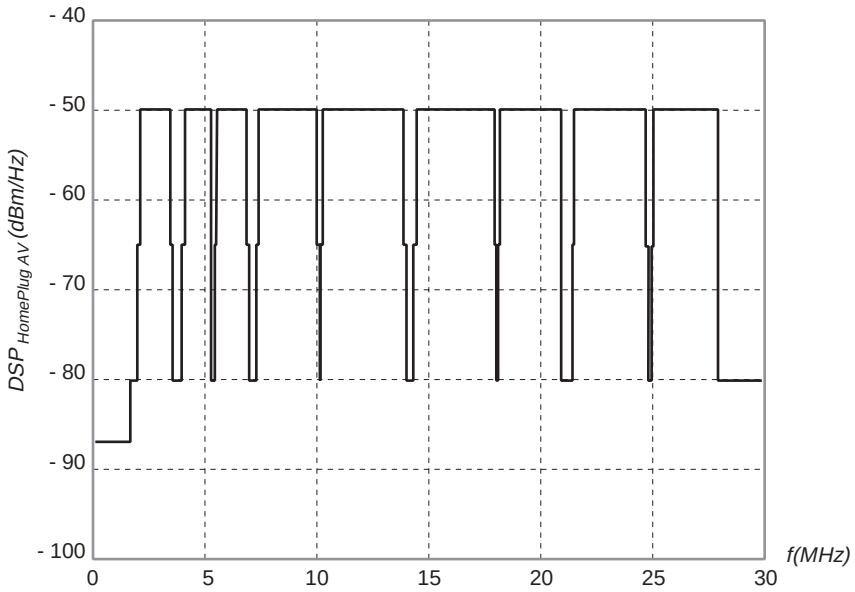


Figure 8.8

Masque DSP limite pour HomePlug AV dans la bande de fréquences 1-30 MHz

Le tableau 8.5 récapitule les différentes sous-bandes de HomePlug AV, de 1,71 à 28 MHz, avec leur DSP max. (exprimée en dBm/Hz) et le fait que la sous-bande soit active ou non (si une autre technologie utilise déjà cette sous-bande), avec les numéros des sous-bandes de 0 à 1 535. La dernière colonne donne les technologies radio présentes dans cette sous-bande.

Tableau 8.5 DSP et régulations dans chaque sous-bande HomePlug AV

Fréquence centrale de la sous-bande (MHz)	DSP max. (dBm/Hz)	Porteuse on/off	Commentaire
F = 1,71	– 87	Porteuses 0-70 off	Bande de diffusion AM et en dessous
1,71 < F < 1,8	– 80	Porteuses 71-73 off	Entre la bande AM et la bande amateur 160 m
1,8 = F = 2	– 80	Porteuses 74-85 off	Bande amateur160 m
2 < F < 3,5	– 50	Porteuses 86-139 on	Porteuses HomePlug
3,5 = F = 4	– 80	Porteuses 140-167 off	Bande amateur 80 m
4 < F < 5,33	– 50	Porteuses 168-214 on	Porteuses HomePlug
5,33 = F = 5,407	– 80	Porteuses 215-225 off	Bande amateur 5 MHz
5,407 < F < 7	– 50	Porteuses 226-282 on	Porteuses HomePlug
7 = F = 7,3	– 80	Porteuses 283-302 off	Bande amateur 40 m
7,3 < F < 10,10	– 50	Porteuses 303-409 on	Porteuses HomePlug
10,10 = F = 10,15	– 80	Porteuses 410-419 off	Bande amateur 30 m
10,15 < F < 14	– 50	Porteuses 420-569 on	Porteuses HomePlug
14 = F = 14,35	– 80	Porteuses 570-591 off	Bande amateur 20 m
14,35 < F < 18,068	– 50	Porteuses 592-736 on	Porteuses HomePlug
18,068 = F = 18,168	– 80	Porteuses 737-748 off	Bande amateur 17 m
18,168 < F < 21	– 50	Porteuses 749-856 on	Porteuses HomePlug
21 = F = 21,45	– 80	Porteuses 857-882 off	Bande amateur 15 m
21,45 < F < 24,89	– 50	Porteuses 883-1015 on	Porteuses HomePlug
24,89 = F = 24,99	– 80	Porteuses 1016-1027 off	Bande amateur 12 m
24,99 < F < 28	– 50	Porteuses 1028-1143 on	Porteuses HomePlug
F = 28	– 80	Porteuses 1144-1535 off	Bande amateur 10 m

Topologie des réseaux électriques

Il existe deux types de câblage pour les réseaux électriques de tout bâtiment, qu'il soit domestique, professionnel ou industriel :

- Monophasé, constitué de deux câbles (neutre et phase). La différence de potentiel électrique entre ces deux câbles est de 220 V, qui circulent depuis le tableau électrique jusqu'aux prises et lumières du bâtiment.
- Triphasé, constitué de quatre câbles (un neutre et trois phases). La différence de potentiel électrique entre le câble neutre et un câble phase est de 220 V et celle entre deux câbles phase de 380 V. Certains bâtiments utilisent un réseau électrique triphasé plutôt que monophasé parce qu'il permet de véhiculer davantage de puissance électrique et donc d'alimenter plus d'équipements électriques dans le bâtiment. Les réseaux triphasés permettent également d'alimenter les moteurs électriques, qui ont besoin de tension triphasée pour fonctionner.

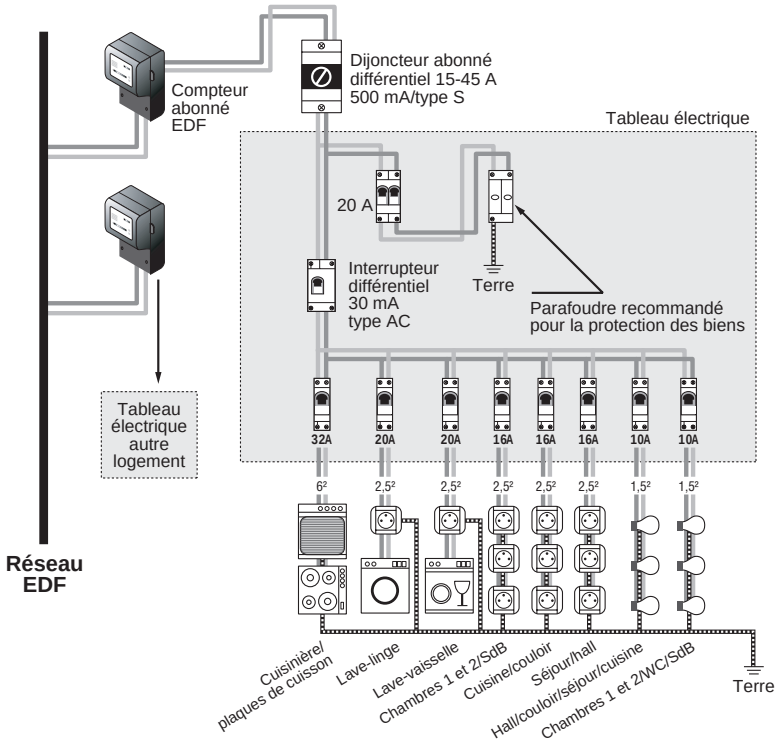
Ces deux topologies sont plus précisément décrites dans les sections qui suivent.

Câblage monophasé

La majorité des habitations (appartement, maison, petit immeuble) sont câblés en monophasé, car leurs besoins en alimentation électrique sont inférieurs à un courant de 60 A.

Figure 8.9

Topologie d'un réseau électrique monophasé domestique



Comme l'illustre la figure 8.9, une installation électrique monophasée comporte plusieurs câbles (départs), qui partent du tableau électrique pour alimenter les équipements électriques et lumières de l'habitation. La norme NFC 15-100 détaille les types de disjoncteurs à placer.

La figure 8.10 illustre la topologie du réseau électrique monophasé d'un appartement, avec les différents câbles partant du tableau électrique. Les modems et équipements CPL se branchent sur les prises électriques des pièces de l'habitation. Le signal CPL se propage sur les câbles puis repasse par le tableau électrique pour repartir vers les différents câbles. La longueur du câblage peut dépasser les 300 m considérés comme la limite acceptable pour un débit utile suffisant.

Les équipements électriques branchés sur le réseau sont des sources potentielles de perturbations électromagnétiques pour le signal CPL. Il faut retenir que la longueur moyenne du câblage électrique entre le tableau et la prise la plus éloignée ne devrait pas dépasser 200 m.

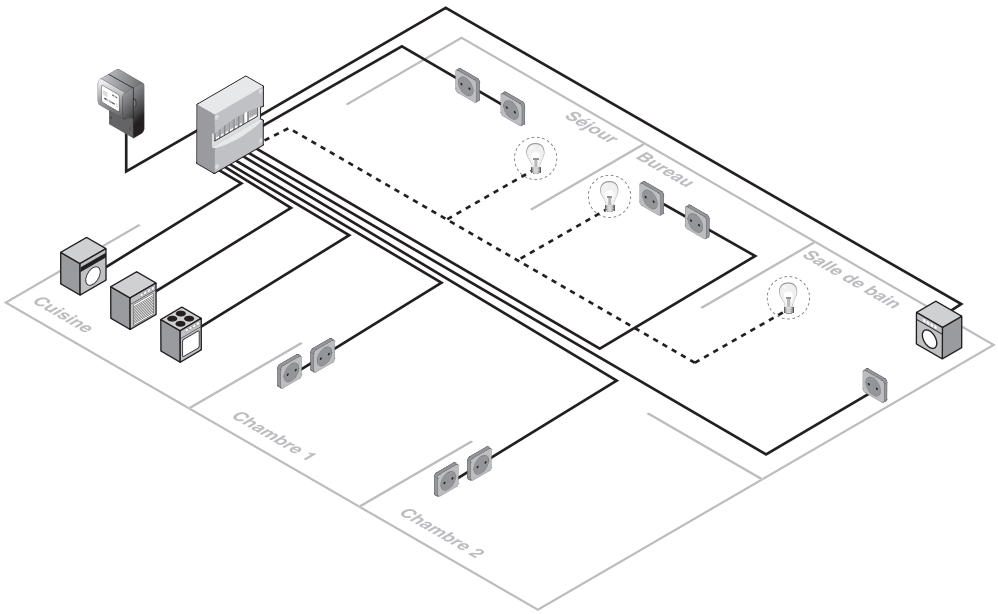


Figure 8.10
Topologie d'un réseau électrique monophasé d'appartement

Câblage triphasé

Dans les immeubles, grandes maisons, locaux professionnels ou usines, les besoins de puissance électrique sont supérieurs à ceux d'une habitation domestique, si bien que le réseau électrique y est souvent triphasé.

Quatre câbles (neutre, phases 1, 2 et 3) partent du tableau électrique et alimentent les prises électriques du bâtiment. La figure 8.11 illustre un exemple de câblage triphasé dans un bâtiment de plusieurs étages, avec les différentes phases électriques alimentant les étages du bâtiment. Chaque étage est parcouru par deux câbles partant du tableau : un câble de phase et le câble neutre.

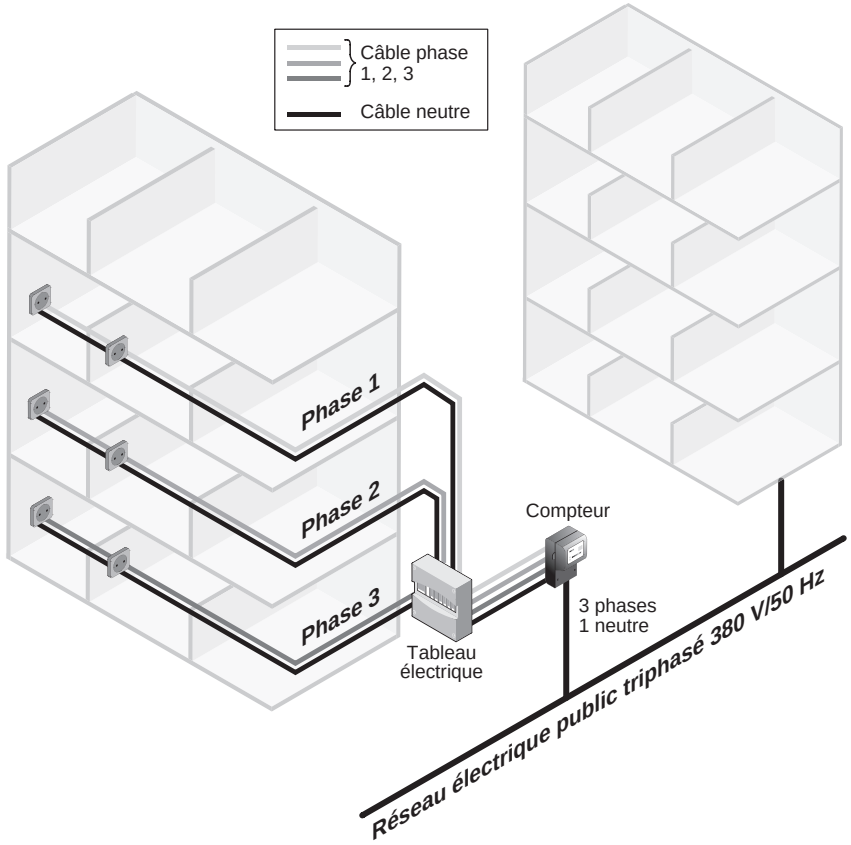


Figure 8.11

Topologie d'un réseau électrique triphasé de grand bâtiment

Le seul câble commun à tout le bâtiment est le câble neutre. Les autres câbles sont dissociés électriquement. Il est important de retenir que le signal CPL circulant dans un des câbles (neutre ou phase) peut être transmis dans les autres câbles par phénomène d'induction. Cela permet de constituer la topologie du réseau local CPL en utilisant au mieux les propriétés des câbles électriques.

De la même manière que dans les réseaux monophasés, la distance moyenne entre le tableau électrique et la dernière prise branchée sur le câble électrique ne doit pas dépasser 200 m. Si le signal CPL circule sur les câbles, traverse le tableau électrique et se

propage à nouveau sur d'autres câbles, la distance est alors supérieure à 200 m, et le débit utile peut chuter.

Le signal CPL traverse également le compteur et peut atteindre le réseau électrique de l'immeuble adjacent, ce qui peut se révéler utile si l'on désire constituer un réseau local CPL entre immeubles. Cela nécessite toutefois une bonne sécurité du signal CPL pour éviter l'écoute du réseau CPL.

Câbles d'un réseau électrique

La section des câbles peut avoir une influence sur la propagation du signal. Pour simplifier, on peut dire que plus la section du câble est importante, plus son atténuation est grande.

Le tableau 8.6 récapitule les différentes sections de câbles entre le compteur EDF (ou régie d'électrification) et le tableau électrique.

Tableau 8.6 Section des câbles de branchement EDF en fonction des puissances fournies

Courant assigné du disjoncteur de branchement	Section minimale des conducteurs en cuivre
45 A	10 mm^2
60 A	16 mm^2
90 A	25 mm^2

Le tableau 8.7 recense les sections de conducteurs électriques préconisées selon la fonction de l'appareil branché sur ce câble (norme NFC 15-100). Les sections de câble principalement utilisées sont donc de 1,5 mm^2 ou 2,5 mm^2.

Tableau 8.7 Section des câbles conducteurs en fonction des appareils électriques

Fonction	Nombre maximal de points d'utilisation par circuit		SECTION (MM^2) des conducteurs (Ph, N, T) en cuivre
	Norme NFC 15-100	Label Promotelec	
Éclairage et prise de courant commandée	8	5	1,5
Prise de courant	8	8	2,5
Machine à laver	1	1	2,5
Cuisinière (four + plaque) ou plaque de cuisson	1	1	6
Four seul	1	1	2,5
Plaque deux feux studio	1	1	2,5
Chauffe-eau à accumulation	1	1	2,5
Chauffage : convecteur, panneau radiant	5	5	1,5 mm^2 au minimum

Le tableau électrique

Le tableau électrique est le centre fédérateur du réseau électrique, depuis lequel partent tous les câbles électriques. Ce tableau est également l'élément protecteur des personnes vis-à-vis des risques électriques. Les équipements protecteurs sont appelés des disjoncteurs (ou fusibles pour les vieux réseaux). Ils peuvent être de plusieurs types. Chaque disjoncteur présente des caractéristiques spécifiques d'atténuation du signal CPL transporté sur ce câble.

La figure 8.12 illustre un exemple de tableau électrique fermé *(à gauche)*, ouvert *(au milieu)* et en vue de face *(à droite)*. Cette dernière identifie les équipements branchés au tableau.

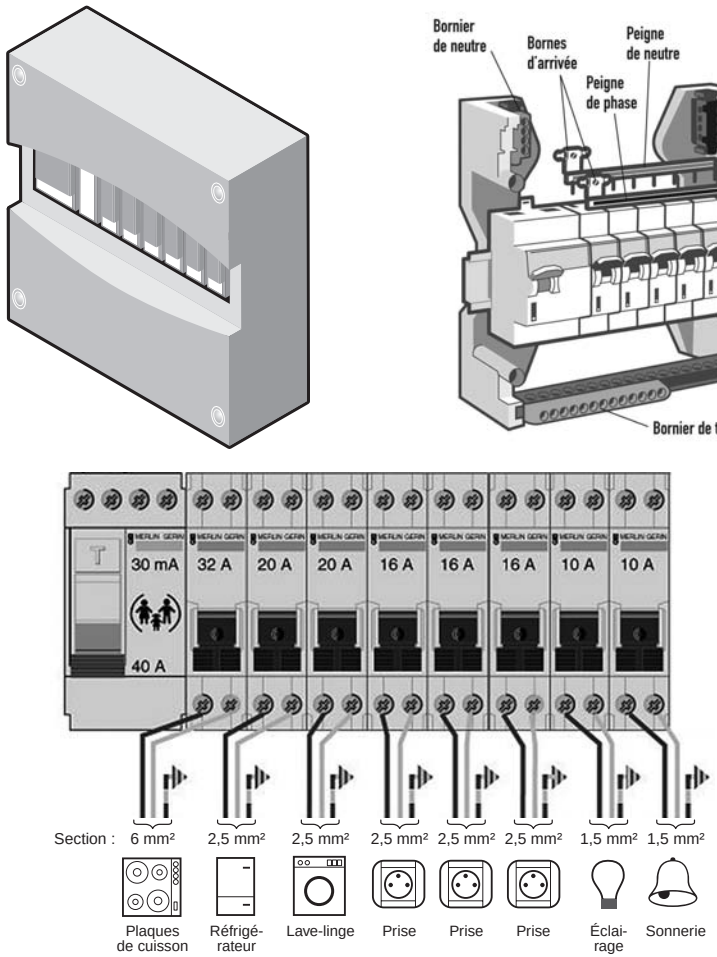


Figure 8.12

Tableau électrique d'une installation domestique

Atténuations sur le réseau électrique

Nous avons vu qu'au-delà de 300 m linéaires (dans un câble électrique enroulé, le phénomène d'auto-induction ne donne pas les mêmes résultats), le débit utile chutait rapidement du fait de l'atténuation du signal, au point de devenir trop faible pour proposer des qualités de services suffisantes pour les applications des couches supérieures.

Chaque câble comporte une section et des caractéristiques d'impédance différentes, qui induisent des atténuations différentes sur le signal CPL. Le câble HNS33S33, qui est utilisé dans les réseaux publics EDF BT présente à 100 m une atténuation de 14 dB pour un signal CPL à la fréquence de 30 MHz.

Longueur conseillée des câbles dans une installation domestique moyenne

Si l'on prend le cas d'une habitation française moyenne, c'est-à-dire une maison F4 de plain-pied de 100 m^2 pour ou un appartement T3-T4 de 65m^2, la longueur du câble entre le tableau électrique et les prises électriques est généralement de 15 m. La longueur de câble maximale entre le tableau électrique et le point le plus éloigné (point lumineux ou prise) est généralement de 50 m.

Il est important de limiter la chute de tension dans les câbles électriques à 2 % afin de conserver une tension acceptable pour les équipements électriques branchés sur le réseau de l'installation.

La formule permettant de déterminer la longueur de câble correspondante en monophasé est la suivante :

$$L = \Delta_u \times \frac{U_0}{100} \times \frac{1}{2\rho} \times \frac{S}{I}$$ (longueur exprimée en mètres)

où

Δ_u est la chute de tension en pourcentage.

U_0 est la tension du réseau électrique (230 V).

ρ est la résistivité du câble électrique (0,023 pour le cuivre et 0,037 pour l'aluminium).

S est la section des câbles en mm^2.

I est l'intensité du courant électrique parcourant le câble, exprimée en A.

Pour un câble monophasé en cuivre avec une chute de tension de 2 %, cette formule devient :

$$L = 100 \times \frac{S}{I}$$

Pour un câble alimentant des points lumineux de 1,5 mm^2 de section et d'un courant maximal autorisé de 16 A, il est conseillé d'avoir une longueur de câble de 9,3 m. Pour un câble alimentant des prises électriques de 2,5 mm^2 de section et de courant maximal autorisé de 20 A, il est conseillé d'avoir une longueur de câble de 12,5 m.

Les câbles électriques d'une installation BT (basse tension) dans un bâtiment sont de plusieurs types et plusieurs constitutions :

- Les câbles, appelés conducteurs, phase, neutre et terre sont placés dans les murs ou dans des gaines individuelles mais ne sont pas regroupés dans une gaine. Ce type de câblage induit une plus grande émission électromagnétique dans l'environnement proche. Du fait de ces pertes d'émissions électromagnétiques, la propagation du signal CPL dans les câbles subit une atténuation assez importante. Ces câbles se retrouvent typiquement dans les installations sous les références H07 V-U ou H07 V-R

(conducteurs rigides), H07 V-K (conducteurs souples) pour les montages sous conduits, moulures ou plinthes.

- Les câbles P, N, T sont placés ensemble de manière torsadée, avec le câble de terre au centre de la torsade, à l'intérieur d'une gaine. Ce type de câble permet une bien meilleure propagation du signal CPL puisque les câbles induisent des couplages électromagnétiques entre eux. De plus, comme pour le câble téléphonique, la disposition en torsade permet de mieux guider le signal CPL et d'éviter les atténuations par dispersion électromagnétique dans l'environnement proche. Le signal reste relativement confiné dans la gaine et atteint de meilleures performances, à la fois en distance et en débit. Ces câbles se retrouvent typiquement dans les installations sous les références FR-N 05 VV-U ou R (câbles rigides), A05 VV-F ou H 07 RNF (câbles souples) pour montages en apparent, dans les vides de construction, moulures, plinthes ou conduits.
- Les câbles P, N et T sont torsadés ensemble par l'installateur électrique avant d'être mis dans des goulottes ou dans les murs du bâtiment. Ce type de câblage offre une bonne propagation du signal CPL et peu de pertes par émissions électromagnétiques.

Éléments de choix de la topologie du réseau CPL

Le réseau local CPL doit s'adapter au réseau électrique du bâtiment. Chaque bâtiment peut avoir différents types de câbles, différents tableaux électriques, différents coupe-circuits (fusibles, disjoncteurs), mais aussi des éléments de circuit en série (prises connectées en série sur le câble électrique) ou en parallèle (prises connectées directement sur des câbles venant du tableau électrique).

De la même manière qu'un réseau Wi-Fi doit s'adapter à la structure des murs d'un bâtiment, qui se comportent comme autant d'obstacles à la propagation des ondes radio, un réseau CPL doit s'adapter au réseau électrique et aux chemins de câbles, qui se comportent comme des obstacles à la propagation du signal CPL.

La topologie du réseau local CPL doit s'adapter à celle du réseau électrique de l'une ou l'autre des façons suivantes :

- Établir dans la mesure du possible la topologie du réseau électrique, par exemple en récupérant le schéma du réseau ou en effectuant des tests CPL sur les différentes prises électriques du bâtiment.
- Trouver les meilleurs points de branchement des équipements CPL sur le réseau électrique afin d'obtenir la meilleure couverture CPL possible. Le tableau électrique est un point central pour le réseau électrique puisque tous les câbles électriques en partent.
- Identifier les zones du réseau électrique où le signal CPL n'est pas reçu ainsi que les parties du bâtiment connectées à d'autres réseaux électriques ou à travers différentes prises électriques révélant des longueurs de câbles excessives ou subissant trop de perturbations.

Nous reviendrons sur ces éléments de choix des topologies aux chapitres 11 et 12.

Propagation du signal CPL

Un des problèmes récurrents de la technologie CPL est la propagation du signal sur les câbles électriques. Ces derniers ayant une résistivité propre, la propagation du signal subit une atténuation proportionnelle à la longueur du câble.

Les tests effectués par les constructeurs de matériels CPL et les laboratoires de tests en télécommunications et les retours des déploiements de réseaux CPL permettent de fixer quelques chiffres sur la propagation du signal CPL.

Les câbles dits intérieurs sont les câbles utilisés dans les réseaux électriques privés, c'est-à-dire dans les bâtiments domestiques, professionnels et industriels. Les différentes mesures effectuées sur des câbles électriques en cuivre de 1,5 et 2,5 mm^2 de diamètre permettent d'évaluer l'atténuation du signal en fonction de la longueur de câble.

La figure 8.13 illustre les résultats de ces tests à trois fréquences significatives : 10, 20 et 30 MHz. On observe que l'atténuation est plus forte pour les fréquences plus élevées de la bande 1-30 MHz. La longueur des câbles d'une installation domestique étant en moyenne de 200 m, l'atténuation du signal CPL permet de conserver les échanges de données, car les équipements utilisent des interfaces suffisamment sensibles pour recevoir le signal.

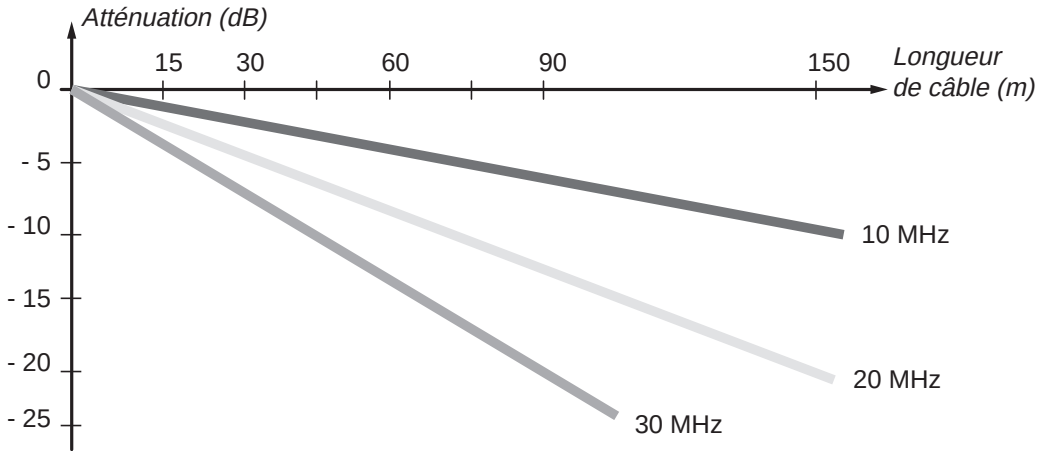


Figure 8.13

Atténuation du signal CPL en fonction de la longueur de câble intérieur

Les câbles dits extérieurs sont les câbles du réseau électrique public EDF ou d'une régie électrique. Ces câbles sont de type BT ou MT triphasé et sont soit enterrés, et donc relativement peu sensibles aux perturbations électromagnétiques, soit aériens, et plus sensibles en ce cas aux perturbations électromagnétiques mais beaucoup moins que les

câbles intérieurs qui subissent des perturbations à proximité des différents appareils domestiques.

Le tableau 8.8 récapitule les résultats obtenus pour différentes technologies CPL.

Tableau 8.8 Distance de propagation du signal CPL sur les câbles extérieurs

Technologie CPL	Type de câble	Distance	Débit TCP (Mbit/s)
Oxance HomePlug Turbo (1.1)	Enterré	1 300 m	3
Spidcom	Enterré	3 000 m	3

Interférences

La notion d'interférences est essentielle dans les réseaux CPL. Le signal CPL qui se propage sur les câbles électriques engendre des émissions électromagnétiques dans la bande de fréquences 1-30 MHz dans l'environnement proche des câbles, et il est lui-même perturbé par les équipements électriques branchés sur le réseau électrique.

De plus, un lien entre deux stations CPL n'a pas nécessairement les mêmes caractéristiques dans les deux sens de communication. Les caractéristiques physiques du média de communication (impédance, charge, capacité) peuvent donc changer selon le sens de propagation du signal.

Les différents organismes de normalisation et de standardisation nationaux, européens et internationaux ont établi des réglementations visant à déterminer les limites d'émissions électromagnétiques des équipements CPL opérant sur un réseau électrique. Comme nous l'avons vu au chapitre 1, les émissions électromagnétiques de ces équipements doivent rester inférieures à une valeur quasi-crête maximale imposée. Cette valeur limite de la DSP (densité spectrale de puissance) a été définie par l'amendement CISPR 22 de la CEI à – 50 dBm/Hz.

Interférences subies sur le réseau électrique

Le réseau CPL subit des interférences et des perturbations électromagnétiques en provenance des appareils électriques branchés sur les prises du réseau.

La figure 8.14 illustre les sources de perturbations que peut recevoir un réseau local CPL.

L'utilisation des appareils électriques et leur actionnement créent différents bruits (large bande, impulsionnel, gaussien, etc.), qui peuvent être évalués à un bruit moyen d'amplitude 30 dBìV/m sur l'ensemble de la bande de fréquences 1-30 MHz.

Il est difficile de dresser une liste exhaustive des appareils qui génèrent ces bruits, mais nombreux sont ceux qui ont été identifiés comme des sources potentielles : écran plasma, halogène, aspirateur, variateur de lumières, four à micro-ondes, téléviseur, écran d'ordinateur, air conditionné, appareil de chauffage, etc.

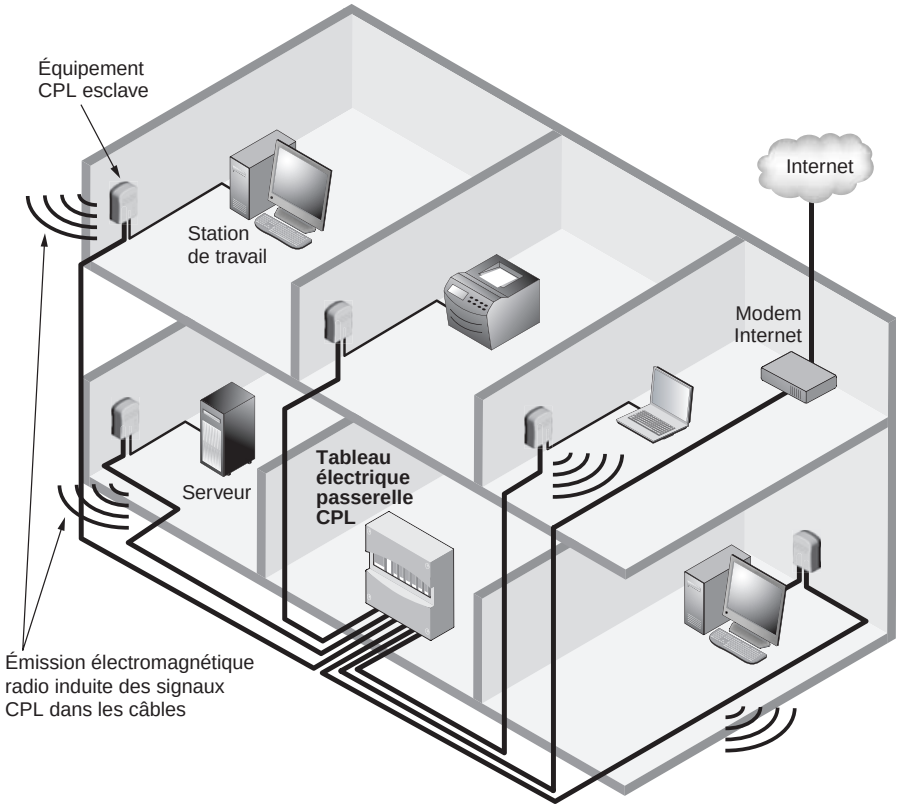


Figure 8.14

Perturbations électromagnétiques engendrées par les équipements CPL branchés sur le réseau électrique

La figure 8.15 illustre les différentes perturbations des équipements électriques en valeur moyenne des différentes mesures effectuées sur de nombreuses installations domestiques en fonction des heures de la journée. La fin de journée est évidemment chargée en perturbations puisque de nombreux équipements sont en marche en même temps sur le réseau électrique. On observe sur la figure que l'amplitude des perturbations varie en fonction de la fréquence, avec deux pics d'amplitude supérieure autour de 10 et 20 MHz.

Les technologies se sont grandement améliorées pour garantir la robustesse des communications de données sur les câbles électriques, mais il peut être nécessaire de prendre des précautions par rapport à certains appareils électriques comme les halogènes ou les aspirateurs branchés sur la même prise qu'un équipement CPL.

La figure 8.16 illustre la manière dont il faut utiliser une multiprise avec un équipement CPL. Une multiprise est en effet en elle-même une source de bruit pour les équipements CPL, à laquelle il faut ajouter le bruit des appareils perturbateurs branchés sur elle. Il est toujours préférable de brancher directement l'équipement CPL sur la prise murale quand c'est possible ou de le brancher sur une biplite (multiprise murale à deux prises).

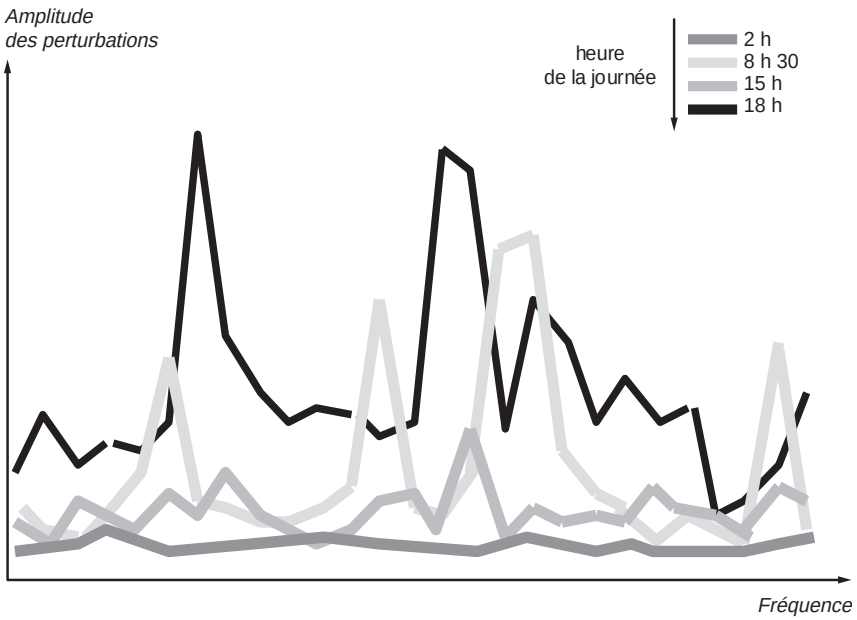
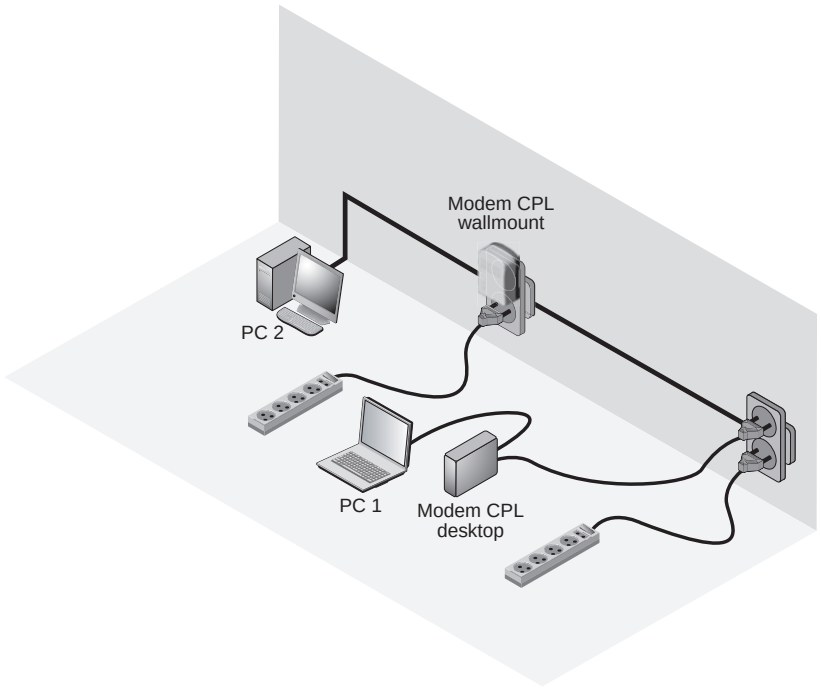


Figure 8.15
Amplitude des perturbations sur un réseau électrique domestique selon les heures de la journée

Figure 8.16
Utilisation optimale des multiprises et doubles prises



Les débits réseau

En plus des perturbations électromagnétiques, un réseau CPL est soumis à des contraintes liées à la technologie elle-même. Ces dernières concernent le débit, qui ne correspond jamais à celui espéré, et la sécurité.

Le débit théorique des réseaux HomePlug 1.0 est compris entre 1 et 14 Mbit/s. Le débit de 14 Mbit/s n'est qu'une valeur théorique, correspondant approximativement à 5 Mbit/s de débit utile, soit 0,625 Mo/s. HomePlug Turbo et AV offrent un débit théorique respectif de 5 à 85 Mbit/s et de 10 à 200 Mbit/s pour un débit utile respectif de 1 à 20 Mbit/s et de 5 à 60 Mbit/s.

Cette différence s'explique essentiellement par la taille des en-têtes des trames utilisées dans HomePlug, ainsi que par l'utilisation d'un certain nombre de mécanismes permettant de fiabiliser la transmission dans un environnement électrique. Une partie des données transmises sert au contrôle et à la gestion de la transmission afin de la fiabiliser. Seule une fraction du débit émis par l'équipement correspond au transport des données elles-mêmes.

Calcul du débit utile

Le débit utile correspond au débit des données transmises à un niveau *n* de la couche OSI. Les débits utiles de niveaux 1, 2, 3, etc., correspondent aux débits des données de ces niveaux, calculés en fonction de l'overhead utilisé pour la gestion et l'envoi de la transmission.

Comme nous l'avons vu au chapitre 5, les données envoyées sur cette interface électrique correspondent à une trame physique, ou PLCP-PDU. Cette trame est constituée d'un entête PLCP, composé de deux champs, et de données issues de la couche MAC. Comme illustré à la figure 8.17, chaque partie de la PLCP-PDU est envoyée à des vitesses différentes.

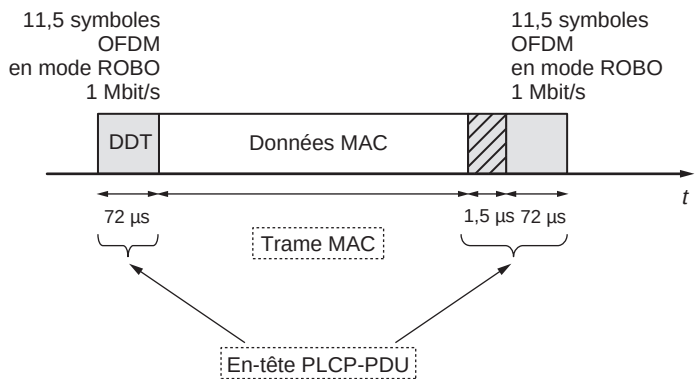


Figure 8.17
Structure d'une PLCP-PDU

L'en-tête PCLP-PDU comporte des délimiteurs de début et de fin de trame. Ces en-têtes sont transmis à 1 Mbit/s dans le cas du préambule long.

Le deuxième champ de la PLCP-PDU correspond à la trame MAC elle-même. Cette dernière est envoyée à des débits pouvant aller de 1 à 4,5, 9 ou 14 Mbit/s pour ce qui concerne HomePlug 1.0. Le mécanisme de variation de débit du CPL lui permet en effet de transmettre à des débits différents en fonction des caractéristiques de l'environnement électrique.

Pour calculer le débit utile de niveau 2, il faut connaître le temps de transfert, qui est égal au temps de propagation augmenté du temps de transmission. Comme l'interface électrique est utilisée comme support de transmission, nous pouvons considérer que le temps de propagation est nul, étant donné que la vitesse de déplacement des électrons sur un câble électrique est équivalente à la vitesse de la lumière. Le temps de transmission (*Tt*) correspond donc au temps nécessaire pour envoyer les données.

Par définition, le débit utile (*Du*) de niveau 2 correspond au volume des données utiles transmises divisé par le temps de transmission global, soit :

$$Du = \frac{\text{Données}}{Tt}$$

Considérons un réseau HomePlug 1.0 dont les trames utilisent un préambule court et dans lequel la vitesse de transmission est de 14 Mbit/s pour toutes les stations. Nous allons calculer le débit utile (Du_1) d'une PLCP-PDU lors de l'envoi de données d'une taille de 1 500 octets. La taille des données utiles étant connue, reste à calculer le temps de transmission, qui équivaut à la somme du temps de transmission de l'en-tête PLCP-PDU et de celui des données MAC.

Les données de la trame MAC comportent un en-tête sur 34 octets. Leur taille est donc de 1 534 octets. Leur temps de transmission (Tt_{MAC}) est fourni par la formule :

$$Tt_{MAC} = \frac{1\,534 \text{ octets} \times 8 \text{ bit/octet}}{14 \text{ Mbit/s}} \approx 0{,}000876 \text{ s}$$

L'en-tête PLCP-PDU, dont la taille est de 120 bits, est envoyé à 1 Mbit/s. Son temps de transmission ($Tt_{PLCP\text{-}PDU}$) est donc de :

$$Tt_{PLCP\text{-}PDU} = 72\ \mu s + 1{,}5\ \mu s + 72\ \mu s \approx 145{,}5\ \mu s$$

Le temps de transmission total (Tt_1) équivaut donc à :

$$Tt_1 = Tt_{MAC} + Tt_{PLCP\text{-}PDU} \approx 0{,}001\,021\,5 \text{ s}$$

Le débit utile équivaut au volume des informations transmises, soit 1 500 octets (12 000 bits), divisé par le temps de transmission, soit 1,021 ms, ce qui correspond à 11,74 Mbit/s :

$$Du_1 = \frac{1\,500 \text{ octets} \times 8 \text{ bit/octet}}{Tt_1} \approx 11{,}74 \text{ Mbit/s}$$

Cependant, ce débit ne correspond pas à la réalité. Dans le CPL, l'envoi de données doit respecter certaines règles liées à la méthode d'accès CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Cette dernière s'appuie sur un certain nombre de mécanismes, décrits en détail au chapitre 3, qui engendrent un overhead assez important.

Dans le cas idéal où une seule station transmet sur le support, lorsque la station transmet des données, elle écoute le support. Si celui-ci est libre, elle retarde sa transmission en attendant un temps CIFS. À l'expiration du CIFS, et si le support est toujours libre, elle transmet ses données. Une fois la transmission des données terminée, la station attend un temps RIFS pour savoir si ses données ont été acquittées. Comme illustré à la figure 8.18, l'overhead minimal engendré par les transmissions des temporisateurs CIFS et RIFS, de l'ACK et des en-têtes est loin d'être négligeable.

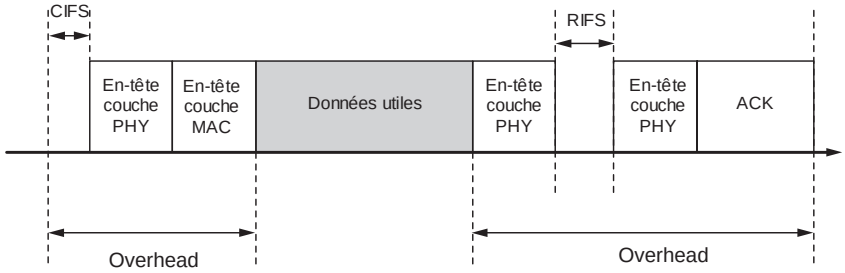


Figure 8.18
Overhead minimal lors d'une transmission de données

Nous allons calculer le débit utile associé à ce cas idéal (Du_2). Comme dans l'exemple précédent, nous prenons en compte l'utilisation de préambules courts pour des données de 1 500 octets transmises à une vitesse de 14 Mbit/s.

D'après nos calculs précédents, le temps de transmission des données correspond à Tt_1, soit :

$$Tt_{\text{Données}} = \frac{1\,534 \text{ octets} \times 8 \text{ bit/octet}}{14 \text{ Mbit/s}} + 145{,}5\ \mu\text{s} \approx 0{,}001\,670 \text{ s}$$

La trame ACK ayant une durée de 72 µs, son temps de transmission est de :

$$Tt_{\text{ACK}} = 72\ \mu\text{s} + 145{,}5\ \mu\text{s} = 0{,}000\,217\,5\ \mu\text{s}$$

Le CIFS et le RIFS sont des temporisateurs à valeur fixe. Cette valeur varie toutefois d'une technologie à une autre. Pour HomePlug 1.0, le CIFS est de 35,84 µs et le RIFS de 26 µs.

Le temps de transmission global est donc de :

$$Tt_2 = \text{CIFS} + Tt_{\text{Données}} + \text{RIFS} + Tt_{\text{ACK}} \approx 0{,}001\,949 \text{ s}$$

Le débit utile de notre cas idéal est donc le suivant :

$$Du_2 = \frac{1\,500 \text{ octets} \times 8 \text{ bit/octet}}{Tt_2} \approx 6{,}157 \text{ Mbit/s}$$

On voit que plus l'overhead est important, plus le débit utile diminue. Étant donné qu'une seule station transmet sur le support, ce débit correspond au débit maximal utile.

Tout se complique lorsque le réseau est composé de plus de deux stations qui essaient simultanément de transmettre sur le support. Lorsqu'une station entend que le support est occupé après avoir essayé d'accéder au support ou après avoir attendu un CIFS, elle retarde sa transmission. Elle arme pour cela un temporisateur, calculé au moyen de l'algorithme de back-off.

Le temps d'attente supplémentaire et le temporisateur de back-off aléatoire augmentent évidemment l'overhead, comme l'illustre la figure 8.19.

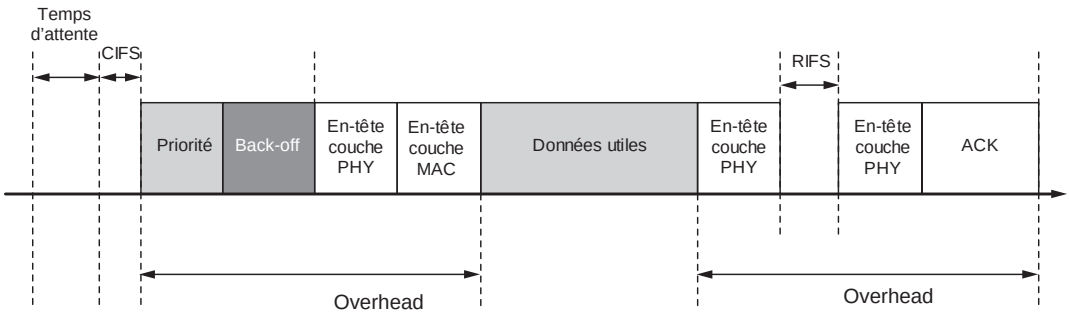


Figure 8.19

Overhead maximal lors d'une transmission de données

Le temps de transmission (Tt_3) devient :

$$Tt_3 = T_{\text{Attente}} + \text{CIFS} + T_{\text{Backoff}} + Tt_{\text{Données}} + \text{RIFS} + Tt_{\text{ACK}}$$

Le temps d'attente et le temporisateur de back-off n'étant pas fixes, il est difficile d'en déterminer les valeurs. On peut toutefois considérer que la somme du temps d'attente et du temps de back-off équivaut généralement au temps de transmission du cas idéal. Le temporisateur de back-off peut être considéré comme nul par rapport au temps d'attente. Quant à ce dernier, il correspond au temps de transmission d'une autre station.

Le débit utile équivaut donc à :

$$Du_3 = \frac{\text{Données}}{Tt_3} = \frac{\text{Données}}{T_{\text{Attente}} + T_{\text{Backoff}} + Tt_1}$$

et s'écrit :

$$Du_3 \approx \frac{\text{Données}}{2Tt_1} \approx \frac{Du_2}{2}$$

Lorsque le réseau est composé de deux stations, le débit utile de chaque station est à peu près égal au débit maximal utile divisé par le nombre de stations composant le réseau. On peut généraliser cette formule pour un réseau CPL composé de *n* stations émettant à la même vitesse.

Le débit utile pour chaque station équivaut à :

$$Du_3 \approx \frac{Du_2}{n}$$

De surcroît, nos calculs précédents n'ont pris en compte que le débit utile de niveau 2. Or les données de la trame MAC correspondent à une trame LLC, avec un en-tête sur 4 octets, qui contient un paquet IP, avec un en-tête sur 20 octets. Le paquet IP comporte lui-même un segment TCP, avec un en-tête sur 24 octets, contenant les données de l'utilisateur. On a donc au total 48 octets d'overhead supplémentaires. Nous n'avons pas non plus pris en compte le traitement des données dans les couches supérieures, 3 et 4, qui engendre également de l'overhead.

En conclusion, on peut dire qu'un réseau CPL n'atteint jamais la capacité annoncée sur le support physique. Si l'information est émise à la vitesse de 14 Mbit/s, le nombre de bits utiles pour l'utilisateur ne représente qu'approximativement la moitié de la capacité brute de l'interface électrique, soit en moyenne 5 Mbit/s (625 Ko/s) dans notre exemple.

Le tableau 8.9 récapitule les débits utiles des différents types de réseaux locaux.

Tableau 8.9 Débits utiles des réseaux locaux

Réseau	Débit théorique (Mbit/s)	Débit utile (Mbit/s)
Ethernet 10	10	8,08
Ethernet 100	100	90,06
HomePlug 1.0	14	5,1
HomePlug Turbo	85	40
HomePlug AV	200	150

Comparé à la vitesse de transmission sur le support, le débit utile est beaucoup plus important dans Ethernet que dans le CPL.

Débit réel maximal du CPL

Après avoir calculé à la section précédente les débits utiles de niveau 2 du CPL, nous allons monter à un niveau supérieur. Nous utiliserons pour cela le générateur de trafic Iperf, disponible à l'adresse *http://dast.nlanr.net/Projects/Iperf/*.

Iperf permet de générer tout type de trafic entre un client et un serveur. Pour notre test, illustré à la figure 8.20, nous utilisons les éléments suivants :

- un ordinateur IBM R50e fonctionnant sous Windows XP SP2 ;
- un ordinateur DELL Latitude D600 sous FreeBSD 5.4 ;
- deux modems CPL de même technologie (HomePlug 1.0, Turbo, AV et Spidcom 200) pour chaque ordinateur ;
- deux câbles Ethernet FTP de catégorie 5 blindés ;
- une multiprise standard quatre prises.

Le client (192.168.1.100), le serveur (192.168.1.110) et le point d'accès (192.168.1.120) doivent être configurés de manière à avoir la même adresse réseau, faute de quoi aucune communication n'est possible.

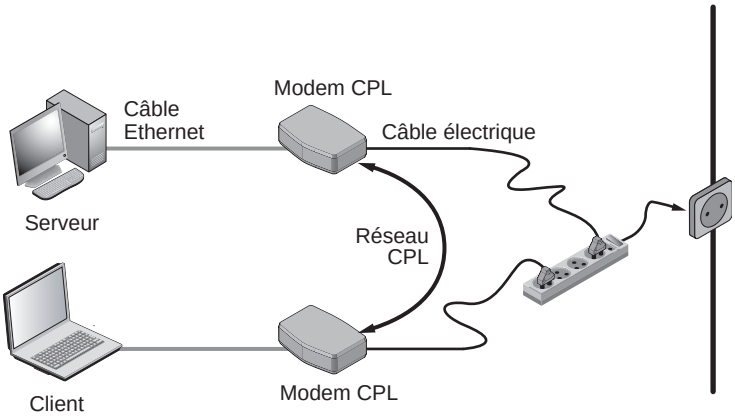


Figure 8.20
Configuration de test

Le test consiste à générer un trafic TCP de 100 Mo et à vérifier le débit utile associé en fonction du réseau traversé ou des mécanismes utilisés. Chaque valeur correspond à la moyenne de trois tests afin d'en garantir la fiabilité en excluant toute oscillation trop importante.

Au niveau du serveur, il suffit de saisir dans une fenêtre MS-DOS **iperf –s** pour initier le serveur. Côté client, la saisie de **iperf –c 192.168.1.110 –n 100000000** dans une fenêtre MS-DOS initie la transmission TCP de 100 Mo.

Le tableau 8.10 présente les résultats obtenus pour différentes technologies avec ce banc de test.

Tableau 8.10 Débits réels maximaux des technologies CPL

Standard ou technologie	Débit utile (Mbit/s)	Débit réel max. (Mbit/s)
HomePlug 1.0 (14 Mbit/s)	5,1	4,35 Mbit/s
HomePlug Turbo (85 Mbit/s)	40	11,5 Mbit/s
HomePlug AV (200 Mbit/s)	150	60,5 Mbit/s
DS2 (200 Mbit/s)	150	61,2 Mbit/s

Le tableau 8.11 récapitule les débits nécessaires pour certaines des applications classiques d'Internet, que ce soit en données, voix ou vidéo.

Tableau 8.11 Débits nécessaires pour les applications typiques d'Internet

application	Débit nécessaire
Surf Internet et e-mail : – descendant – montant	 50 Kbit/s 5 Kbit/s
Voix sur IP	80 Kbit/s
Streaming audio : – descendant – montant	 80 Kbit/s 14 Kbit/s
Canal vidéo SDTV	1,5 Mbit/s
Canal vidéo HDTV	8 Mbit/s

Variation du débit

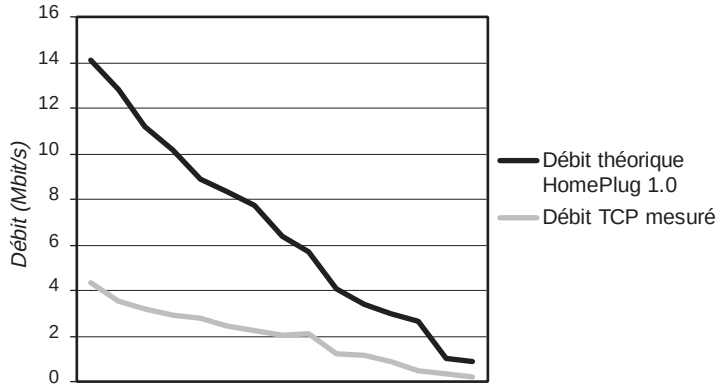
Dans un réseau CPL, les contraintes liées à l'interface électrique peuvent entraîner une variation du débit offert par le réseau. Comme expliqué précédemment, des interférences provenant des appareils électriques et la multiplication des équipements CPL sur le réseau électrique sont autant d'exemples qui peuvent entraîner des variations de débit.

La variation du débit des CPL s'effectue automatiquement dès que surviennent des interférences dans l'environnement. Ce mécanisme est transparent aux yeux des utilisateurs. Le débit de HomePlug 1.0 passe ainsi de 14,1 Mbit/s à 12,83, 10,16, 8,36, 6,35, 4,04, 2,67, voire 0,9 Mbit/s lorsque l'environnement est fortement dégradé.

La variation automatique du débit permet de donner à n'importe quelle station du réseau un débit différent.

La figure 8.21 illustre la variation du débit théorique et du débit utile suite aux mesures effectuées lors des tests avec l'outil Iperf.

Figure 8.21
Variation du débit théorique et utile avec la technologie HomePlug 1.0



Lorsque le réseau est composé de plusieurs stations, nous avons vu que le débit de chaque station correspondait au débit maximal utile divisé par le nombre de station. Or nous avons considéré que le temps d'attente était égal au temps de transmission d'une station donnée en considérant que la vitesse des transmissions était égale pour toutes les stations.

Dans les cas où les vitesses ne sont pas égales pour toutes les stations, le temps d'attente est prolongé. De ce fait, le débit global du réseau baisse fortement. Si une station du réseau émet à une vitesse de 1 Mbit/s, son temps de transmission est 14 fois supérieur à celui d'une station émettant à 14 Mbit/s. Cette station doit donc attendre 14 fois plus longtemps avant de transmettre ses données. Son débit utile moyen tend vers 1 Mbit/s.

La figure 8.22 illustre la probabilité de collision des données sur le réseau électrique en fonction du nombre d'équipements CPL actifs branchés.

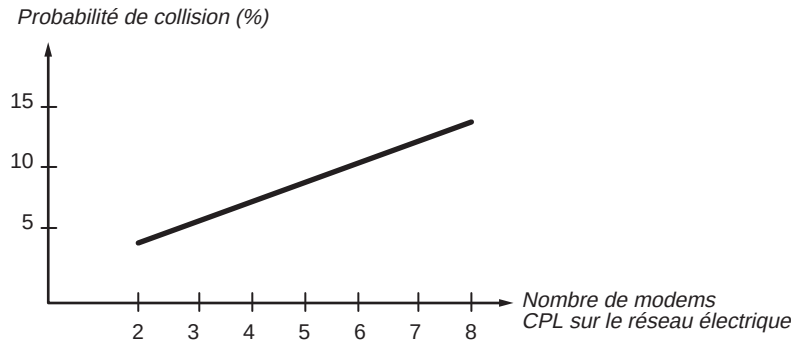


Figure 8.22
Probabilité de collisions en fonction du nombre de modems CPL sur le réseau électrique

La sécurité

Contrairement aux réseaux Wi-Fi, les réseaux CPL offrent une excellente sécurité dans la mesure où le support est inaccessible (câbles électriques enfouis dans les murs ou dans des boîtiers) et dangereux.

La sécurité est donc atteinte dès lors que l'utilisateur met en place une configuration correcte de mots de passe sur son réseau CPL. Nous détaillons cette configuration au cours des chapitres suivants, dédiés à la mise en œuvre d'un réseau local CPL.

9

Configuration

L'installation d'un réseau CPL est assez simple. Il suffit de brancher les équipements CPL à un réseau Ethernet ou à un modem (ADSL, câble, RTC, etc.) en prenant en compte les contraintes évoquées au chapitre précédent.

Après l'installation du réseau, vient la configuration des équipements CPL du réseau et des interfaces des terminaux (généralement cartes réseau des PC) raccordés aux équipements CPL. Nous détaillons dans ce chapitre la configuration des équipements CPL et des cartes Ethernet des terminaux raccordés. Nous détaillons en outre les différentes fonctionnalités proposées par ces équipements en fonction de l'utilisation visée, domestique, professionnelle ou industrielle.

La configuration du terminal (le PC) concerne l'installation et la configuration logicielle de la carte réseau, que cette dernière soit externe, Ethernet ou USB. L'installation de la carte diffère selon le système d'exploitation utilisé. Sa configuration, en revanche, est à peu près similaire d'un système à un autre, car elle s'appuie sur les paramètres de la technologie CPL utilisée (HomePlug, DS2, etc.).

Les sections qui suivent décrivent les paramètres à configurer selon les principales technologies CPL existantes, même si la spécification HomePlug fait désormais office de standard CPL de fait, vu la place écrasante qu'elle occupe sur le marché des équipements CPL.

Une fois la carte réseau configurée, le terminal n'est pas encore tout à fait prêt à communiquer avec le réseau. Pour établir la communication, il est encore nécessaire de lui affecter des paramètres réseau corrects, tels que adresse IP, masque, etc.

Configuration d'un réseau HomePlug 1.0 et Turbo

La configuration d'un réseau CPL avec des équipements HomePlug version 1.0 ou Turbo est relativement simple, dans la mesure où tous les équipements du réseau ont la même fonction hiérarchique, le réseau étant en mode pair-à-pair.

Les équipements du marché fondés sur la spécification HomePlug se configurent de la même manière et sont compatibles les uns avec les autres. Différents outils permettent de les configurer selon les systèmes d'exploitation visés. Nous les décrivons pour Windows XP et pour les systèmes Linux et FreeBSD.

Configuration d'un réseau CPL sous Windows XP

Les outils de configuration des équipements CPL HomePlug présentent quasiment tous les mêmes fonctionnalités de configuration des paramètres des puces HomePlug. Comme nous l'avons vu au chapitre 7, les puces HomePlug sont principalement issues du constructeur Intellon. Elles permettent de lire un certain nombre de valeurs stockées sur la qualité des échanges entre équipements CPL. Ce sont ces valeurs qui permettent de configurer et d'optimiser le réseau CPL.

Parmi les paramètres HomePlug que nous pouvons configurer, citons notamment les suivants :

- La clé NEK (Network Encryption Key), qui permet de sécuriser les échanges de données dans un même réseau local CPL.
- La clé DEK (Default Encryption Key), qui permet de configurer la clé NEK sur l'ensemble des équipements CPL distants, disséminés sur le réseau électrique.
- La priorité de transmission de l'équipement CPL parmi quatre possibles (CA0, CA1, CA2, CA3), qui permet de configurer certains équipements CPL comme des passerelles vers d'autres réseaux, notamment Ethernet.

Le tableau 9.1 récapitule les principaux paramètres que les outils de configuration HomePlug permettent de lire et de présenter à l'utilisateur du réseau CPL.

Tableau 9.1 Paramètres HomePlug 1.0 et Turbo visibles par les outils de configuration

paramètre HomePlug 1.0 et Turbo	Indications
BYTES PER 40 symbols	Nombre d'octets par bloc de 40 symboles OFDM (permet de calculer le débit PHY estimé pour HomePlug 1.0).
BYTES PER 336us Block (pour HomePlug Turbo)	Nombre d'octets par bloc de 336 ìs (permet de calculer le débit PHY estimé pour HomePlug 1.1 Turbo, parfois appelé Viper).
DATA_TX_COUNT	Compteur du nombre de données transmises
FAILS Received	Nombre de trames de type FAIL reçues
Frame Drops	Nombre de trames perdues

Tableau 9.1 Paramètres HomePlug 1.0 et Turbo visibles par les outils de configuration *(suite)*

paramètre HomePlug 1.0 et Turbo	Indications
ACK Counter	Nombre de trames de type ACK envoyées
NACK Counter	Nombre de trames de type NACK envoyées
FAIL Counter	Nombre de trames de type FAIL envoyées
Contention Loss Counter	Nombre de trames de contention perdues
CA0 Latency Counter	Nombre total de milliseconde entre la réception d'une demande d'envoi de trame CA0 et l'accès réussi au canal de transmission
CA1 Latency Counter	Nombre total de milliseconde entre la réception d'une demande d'envoi de trame CA1 et l'accès réussi au canal de transmission
CA2 Latency Counter	Nombre total de milliseconde entre la réception d'une demande d'envoi de trame CA2 et l'accès réussi au canal de transmission
CA3 Latency Counter	Nombre total de milliseconde entre la réception d'une demande d'envoi de trame CA3 et l'accès réussi au canal de transmission
Cumul Bytes per 40 Symbols Packet Counter	Cumul des trames reçues en nombre de 40 symboles OFDM
MAC Address	Adresses MAC des autres équipements CPL du même réseau

Estimation du débit PHY des communications entre équipements CPL

Les différents équipements CPL stockent dans la puce HomePlug la valeur instantanée des paramètres « BYTES in 40 Symbols » échangés par les équipements. Cette valeur permet d'estimer le débit PHY (au niveau de la couche physique) entre équipements CPL, comme nous l'avons vu au chapitre 3.

Le débit PHY maximal correspond au nombre de données (ou bits) permettant la meilleure modulation possible codée avec des blocs OFDM de 40 symboles d'une durée de 8,4 µs.

Cela donne, pour HomePlug 1.0 et Turbo :

HomePlug 1.0 :

$$Débit_{PHY\ MAX} = \frac{519 \times 8}{40 \times 8{,}4} = 12{,}357\ 142\ 86\ \text{Mbit/s}$$

HomePlug Turbo :

$$Débit_{PHY\ MAX} = \frac{2\ 812 \times 8}{40 \times 8{,}4} = 66{,}952\ 380\ 95\ \text{Mbit/s}$$

Toujours en utilisant les données évoquées au chapitre 3, il est possible de calculer le débit PHY en fonction des valeurs données par la puce HomePlug :

HomePlug 1.0 :

$$Débit_{PHY} = \frac{588 - 38}{481} \times \frac{BYTES_{in\,40\,symbols}}{42} + \left(14 - \frac{588 - 38}{481} \times \frac{519}{42}\right)$$

HomePlug Turbo :

$$\frac{BYTES_{per\,336\mu s\,bloc} \times 8}{40 \times 8{,}4}\ \text{Mbit/s}$$

où $Bytes_{per336\mu sbloc}$ représente le nombre d'octets dans un bloc de données au niveau de la couche physique d'une durée 336 µs.

Comme nous l'avons vu au chapitre 8, il existe une différence entre le débit physique et le début utile pour l'utilisateur. Le tableau 9.2 donne une estimation des correspondances entre ces deux débits, puisque les outils de configuration CPL HomePlug n'indiquent que le débit physique pour l'utilisateur.

Tableau 9.2 Correspondance entre débit physique affiché et débit utile

	Débit PHY (Mbit/s)	Débit utile (Mbit/s)
HomePlug 1.0	14	4,5-5
	12,83	3,5
	11	3,2
	10,16	2,9
	8,36	2,4
	6,35	2
	4,04	1,22
	3	0,89
	1	0,33
	0,9 (Mode ROBO)	0,2
HomePlug Turbo	85	12,5
	75	11,8
	55	9,42
	45	8,79
	35	8,23
	25	7
	14	4,5
	12,83	3,5

Parmi les différents outils de configuration CPL HomePlug 1.0 et Turbo, citons les trois suivants, qui diffèrent par leur interface et leur facilité d'utilisation :

- Power Packet Utility, d'Oxance *(http://www.oxance.com/download/Install-Config/Install_Config_CPL.exe).* La figure 9.1 illustre l'interface de configuration de cet outil.
- MicroLink dLAN et MicroLink Informer, de Devolo. Le premier sert à configurer le réseau CPL, et le second à vérifier l'état du réseau. La figure 9.2 illustre l'interface d'ajout d'adaptateurs dLAN de MicroLink dLAN, et la figure 9.3 l'interface de MicroLink Informer avec la liste des équipements CPL détectés et configurés sur le réseau électrique.

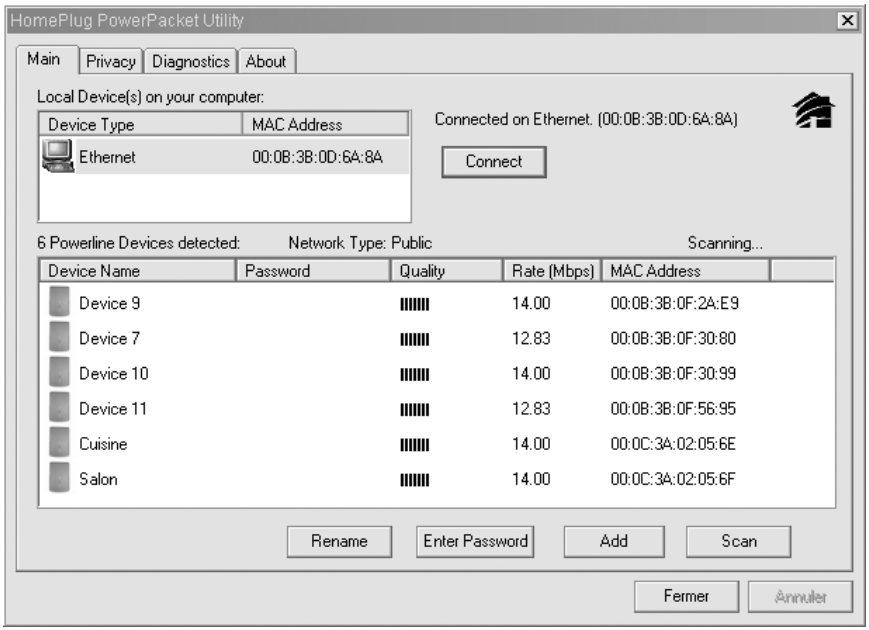


Figure 9.1
Interface de configuration de Power Packet Utility (Oxance)

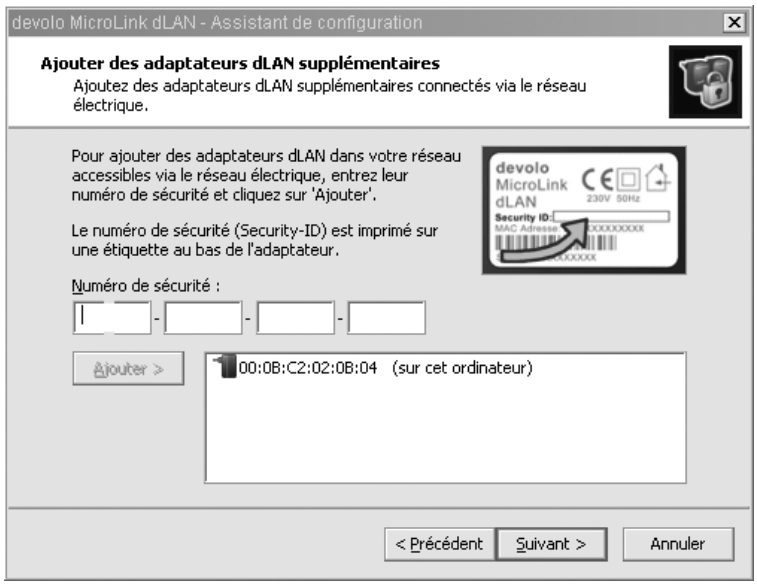
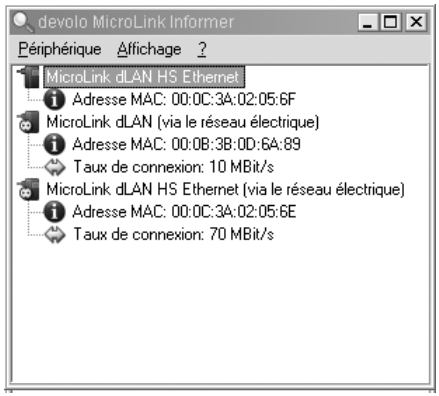


Figure 9.2
Interface d'ajout d'adaptateurs dLAN de MicroLink dLAN (Devolo)

Figure 9.3
Interface d'information du réseau CPL de MicroLink Informer (Devolo)



- SoftPlug, de LEA-Thesys *(http://209.236.239.167/Images/Upload/support_telechargement/Setup-SoftPlug.msi)*. Cet outil offre les mêmes fonctionnalités que les précédents, mais avec une interface peut-être plus facile à utiliser La figure 9.4 illustre cette interface.

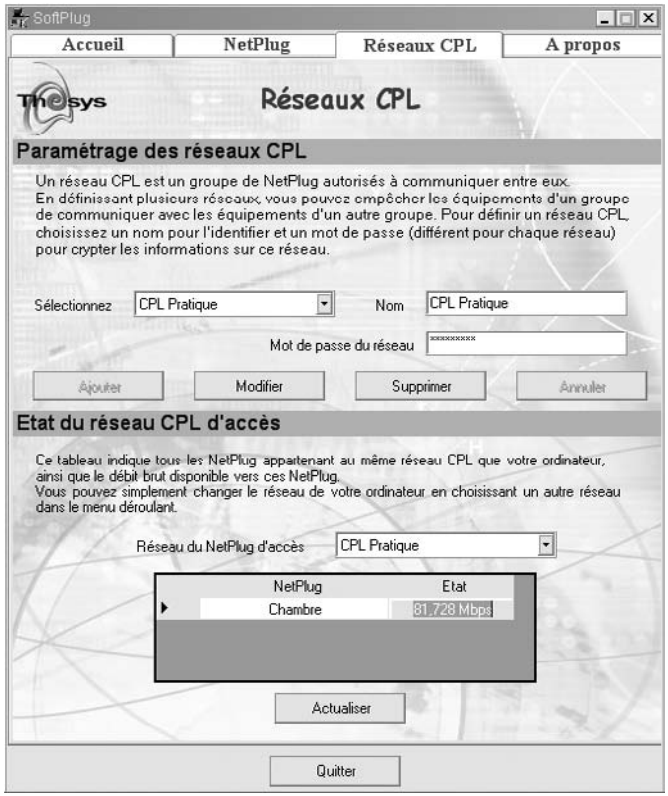


Figure 9.4
Interface de configuration de SoftPlug (LEA-Thesys)

Les modems CPL comportent pour la plupart des interfaces Ethernet. Certains proposent toutefois des interfaces USB permettant d'émuler une interface Ethernet « virtuelle », qui sera vue comme une nouvelle interface réseau par le terminal qui se connecte.

Le comportement des interfaces réseau virtuelles sur l'interface USB se révélant instable, il est recommandé de privilégier les équipements CPL avec interface Ethernet et connecteur RJ-45.

Installation du périphérique réseau dans le cas d'un équipement CPL USB

Une fois l'équipement CPL branché sur une prise électrique et relié à l'ordinateur de configuration grâce au câble USB, cet équipement est automatiquement détecté sous Windows 98, Me, NT, 2000 et XP. Il faut cependant impérativement installer le pilote USB de l'équipement CPL.

Nous avons retenu dans cette section le modem CPL HomePlug 1.0 dLAN duo de Devolo illustré à la figure 9.5.

Figure 9.5
Modem CPL USB/Ethernet dLAN duo (Devolo)

Il peut arriver que le matériel ne soit pas détecté automatiquement. Pour forcer la détection, il suffit d'ouvrir le Panneau de configuration (*via* le menu Démarrer) et de choisir Ajout de nouveau matériel. L'Assistant Ajout de nouveau matériel détecté s'ouvre alors, comme illustré à la figure 9.6.

Figure 9.6
L'Assistant Ajout de nouveau matériel détecté de Windows

Il suffit d'insérer le CD fourni par Devolo avec l'équipement CPL, de rechercher le programme **ml-dlan-usb-drv-r2.exe** et de le lancer. La fenêtre illustrée à la figure 9.7 s'affiche.

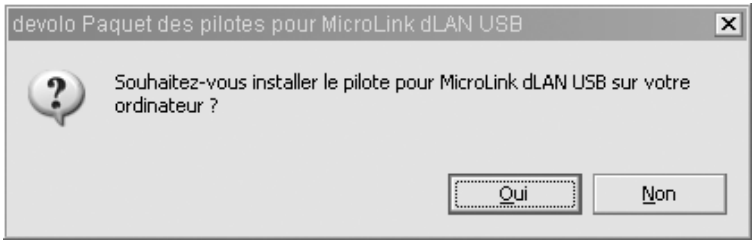


Figure 9.7
L'Assistant d'installation du pilote MicroLink dLAN USB

En cliquant sur Oui, l'Assistant lance l'installation du pilote USB, comme indiqué à la figure 9.8.

Figure 9.8
Installation des pilotes MicroLink dLAN USB

L'installation du périphérique USB-Powerline Bridge se déroule ensuite automatiquement, comme l'illustrent les figures 9.9 et 9.10. Ce périphérique est en fait la carte réseau virtuelle, qui permet de se connecter au réseau CPL *via* l'interface USB de l'ordinateur.

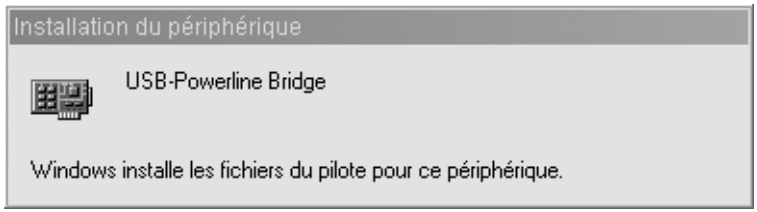


Figure 9.9
Installation du périphérique USB-Powerline Bridge

Figure 9.10
Installation du pilote USB réussie

L'installation est terminée. La nouvelle carte réseau, de type Connexion au réseau local, est visible dans la fenêtre des connexions réseau (*via* Démarrer, Panneau de configuration et Connexions réseau), comme l'illustre la figure 9.11.

Figure 9.11

Connexions réseau avec la nouvelle carte réseau MicroLink dLAN USB

Cette carte réseau étant virtuelle, nous constatons qu'elle disparaît de la fenêtre des connexions réseau dès que nous débranchons le câble USB qui relie l'ordinateur à l'équipement CPL, comme l'illustre la figure 9.12.

Figure 9.12

Disparition de la carte réseau USB après débranchement du câble USB

Une fois l'installation du périphérique USB effectuée, la configuration de l'équipement CPL se déroule de la même manière pour une interface USB ou Ethernet.

Configuration d'un équipement CPL Ethernet ou USB

Pour cet exemple de configuration d'un équipement CPL, nous retenons l'outil de configuration d'Oxance Power Packet Utility.

Une fois l'outil téléchargé, nous pouvons procéder à l'installation en lançant le programme **Install_Config_CPL.exe,** qui ouvre la fenêtre d'installation illustrée à la figure 9.13.

Figure 9.13
Fenêtre d'installation du programme de configuration CPL

Le programme d'installation propose un emplacement cible pour les fichiers de lancement du programme, comme illustré à la figure 9.14. Il est possible de choisir un emplacement différent de celui indiqué par défaut.

Le programme d'installation continue sa copie des programmes vers l'emplacement et toutes les opérations d'installation nécessaires, comme illustré à la figure 9.15.

Une fois l'installation terminée, une dernière fenêtre s'affiche, comme l'illustre la figure 9.16, indiquant la fin de l'installation. Il suffit de cliquer sur Terminer pour valider la fin de l'installation et lancer le programme Configuration_CPL.

Une fois l'installation achevée, le programme Configuration_CPL peut être lancé (*via* Démarrer, Programmes) en cliquant sur l'icône ci-contre. Le programme propose plusieurs onglets, correspondant aux différentes fonctionnalités disponibles, comme l'illustre la figure 9.17.

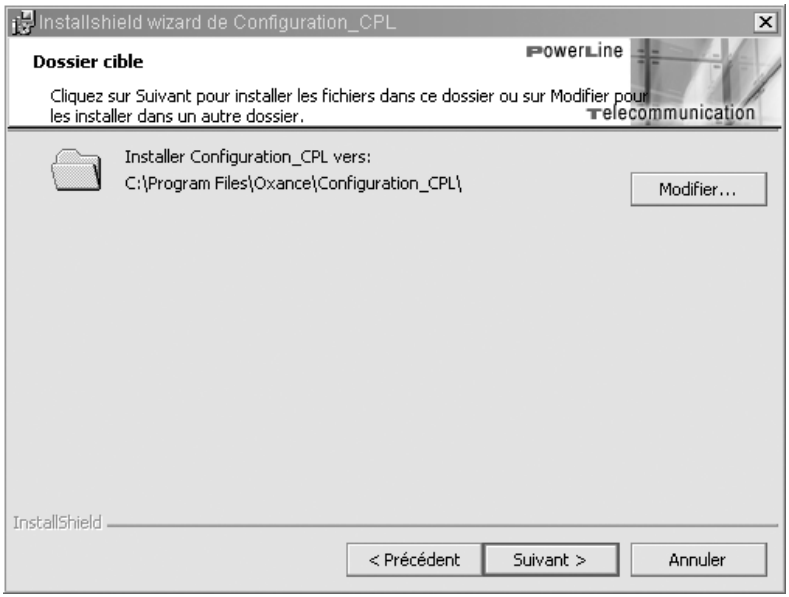


Figure 9.14
Dossier cible pour les fichiers programme

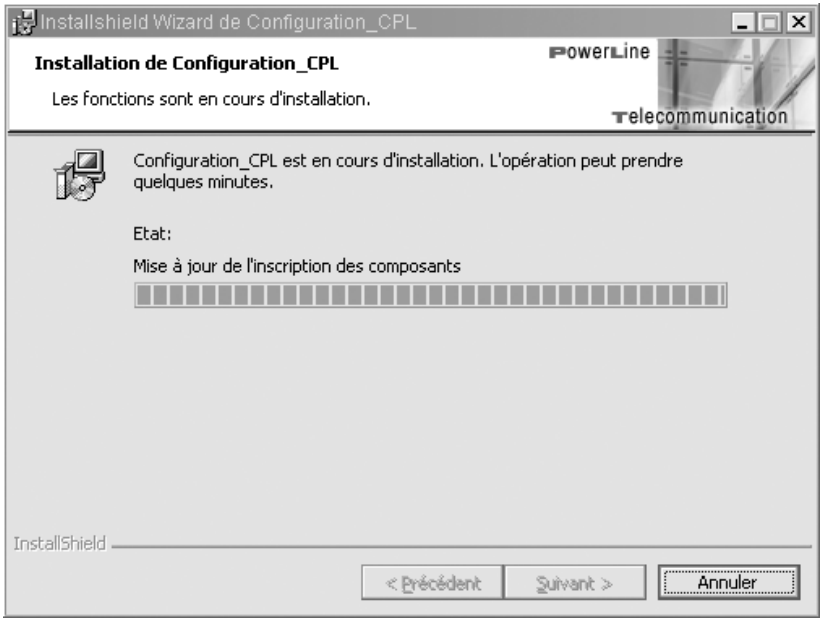


Figure 9.15
Copie des programmes vers l'emplacement cible

Figure 9.16
Fin du programme d'installation

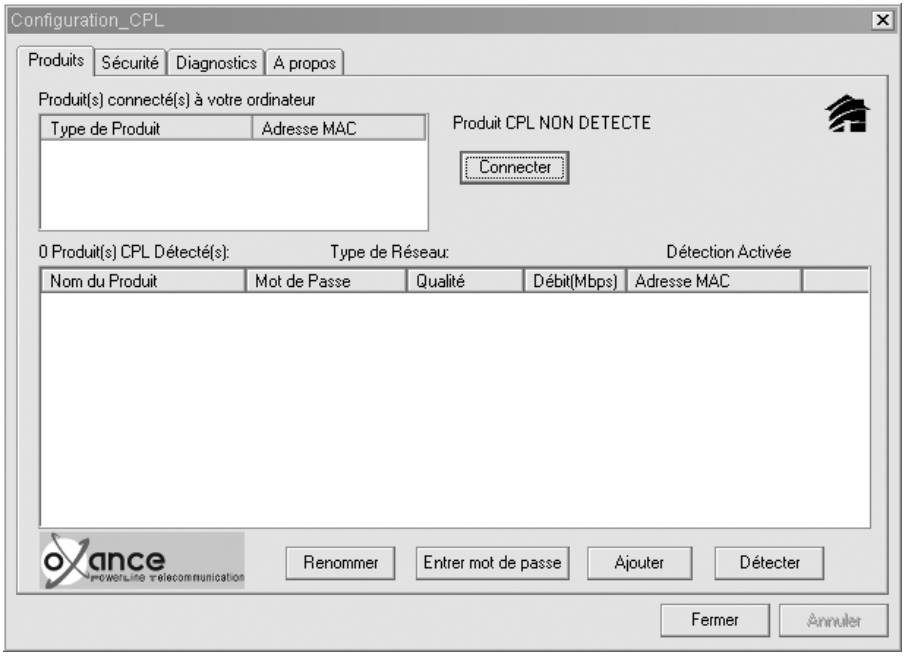


Figure 9.17
Onglet Produits de l'outil de configuration CPL

Pour constituer un réseau local CPL sécurisé, il faut commencer par configurer la clé NEK (Network Encryption Key) sur les différents équipements que nous désirons connecter au réseau.

Dans l'onglet Sécurité, nous commençons par entrer un nom de 4 à 24 caractères dans le champ Nom du réseau privé. Ce nom équivaut au mot de passe de la clé NEK commune à tous les équipements du réseau CPL. Par défaut, il a pour valeur **HomePlug.**

Tout équipement CPL au standard HomePlug acheté dans le commerce peut se connecter à un réseau CPL dont le mot de passe de la NEK a été laissé à sa valeur par défaut. Dans la mesure où le signal se propage au-delà du compteur électrique de l'habitation, toute personne peut donc se connecter en ce cas sur ce réseau local privé. C'est pourquoi il est très important pour la sécurité du réseau CPL de remplacer cette valeur par défaut. La figure 9.18 illustre le mot de passe par défaut.

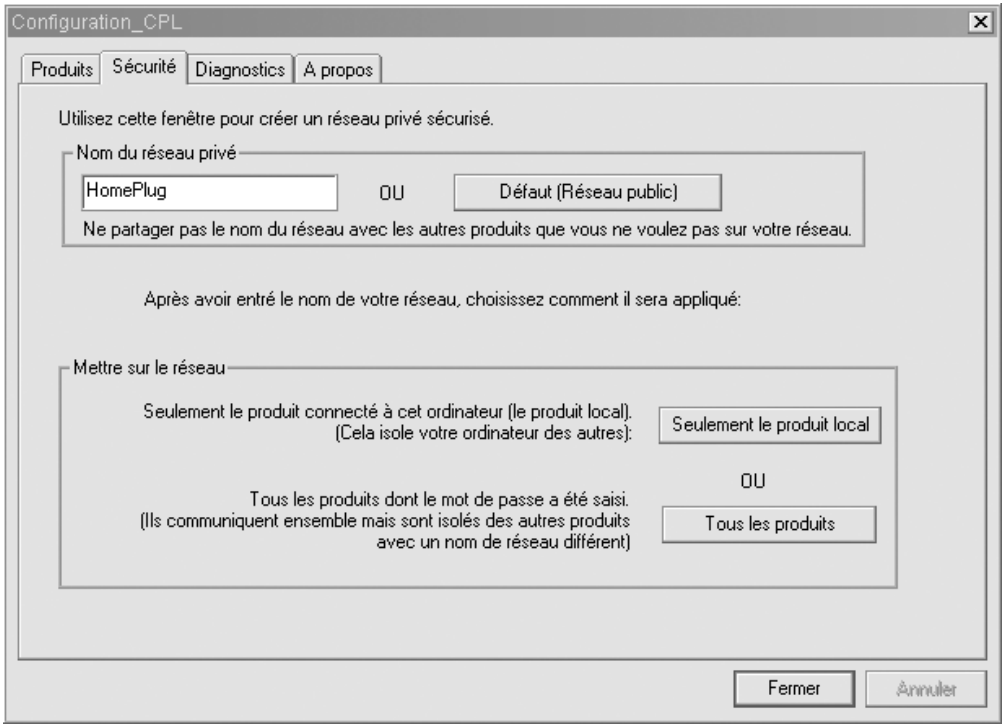


Figure 9.18
Onglet Sécurité de l'outil de configuration CPL

À la figure 9.19, le mot de passe de la clé NEK a été remplacé par la valeur **Mot2Passe.** Plus ce mot de passe est long et intègre des chiffres et des caractères spéciaux, plus il est difficile à percer pour une personne mal intentionnée désirant accéder au réseau CPL.

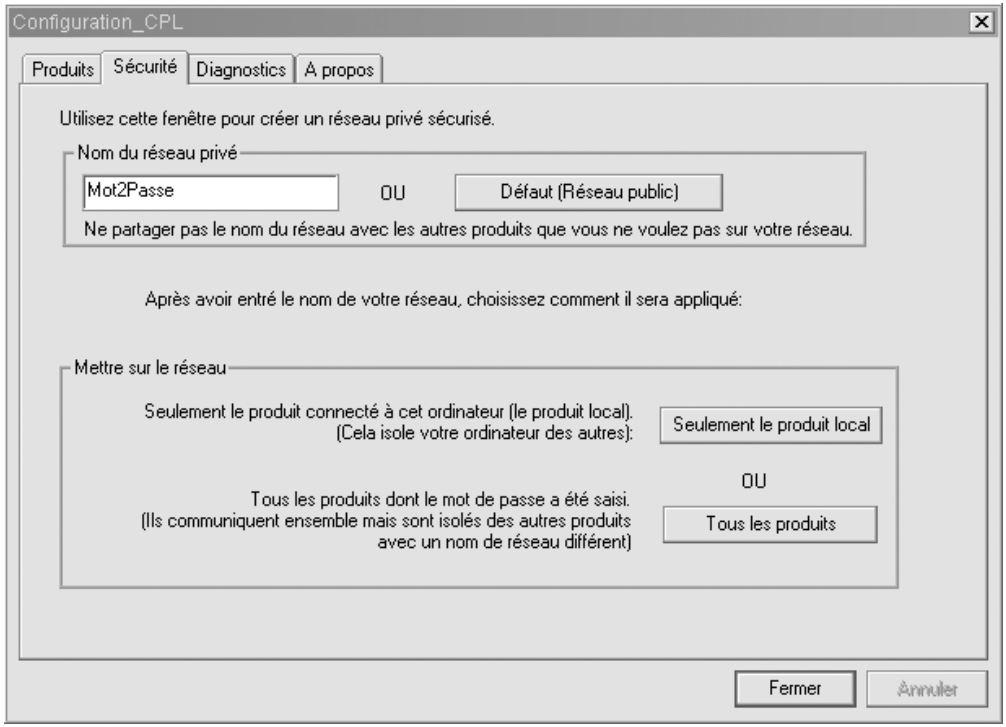


Figure 9.19

Configuration du mot de passe du réseau local CPL

Il est possible de configurer tous les équipements CPL connectés au réseau électrique, qu'ils soient ou non déjà présents dans le réseau local CPL, depuis cette interface de configuration. Il suffit pour cela de connaître la clé DEK des équipements distants connectés sur le réseau électrique.

La clé DEK est unique pour chaque équipement CPL, et son ID est indiquée au dos de l'équipement. Elle peut porter le nom de SecureID (Devolo), Password (Corinex et Oxance), Mot de passe (LEA), etc. Cette clé est codée sur 16 octets au format hexadécimal.

À la figure 9.20, la DEK a pour valeur JJMZ-QFDI-RVHE-OJRS et se situe au-dessus de l'adresse MAC de l'équipement CPL à configurer. La clé DEK est sécurisée.

Figure 9.20
Lecture de la clé DEK sur le boîtier d'un équipement CPL

Connaissant la valeur de la clé DEK, il suffit de cliquer sur Ajouter dans l'onglet Produits et d'entrer cette valeur dans le champ Mot de passe *(voir figure 9.21)*. Le champ Nom de l'adaptateur permet d'identifier l'équipement CPL (chambre ou bureau, par exemple).

Figure 9.21
Ajout d'un équipement CPL au réseau grâce à la valeur de la clé DEK

La figure 9.22 illustre la configuration d'un réseau local CPL à l'aide de clés DEK lues sur les équipements Salon et Cuisine connectés sur le même réseau électrique.

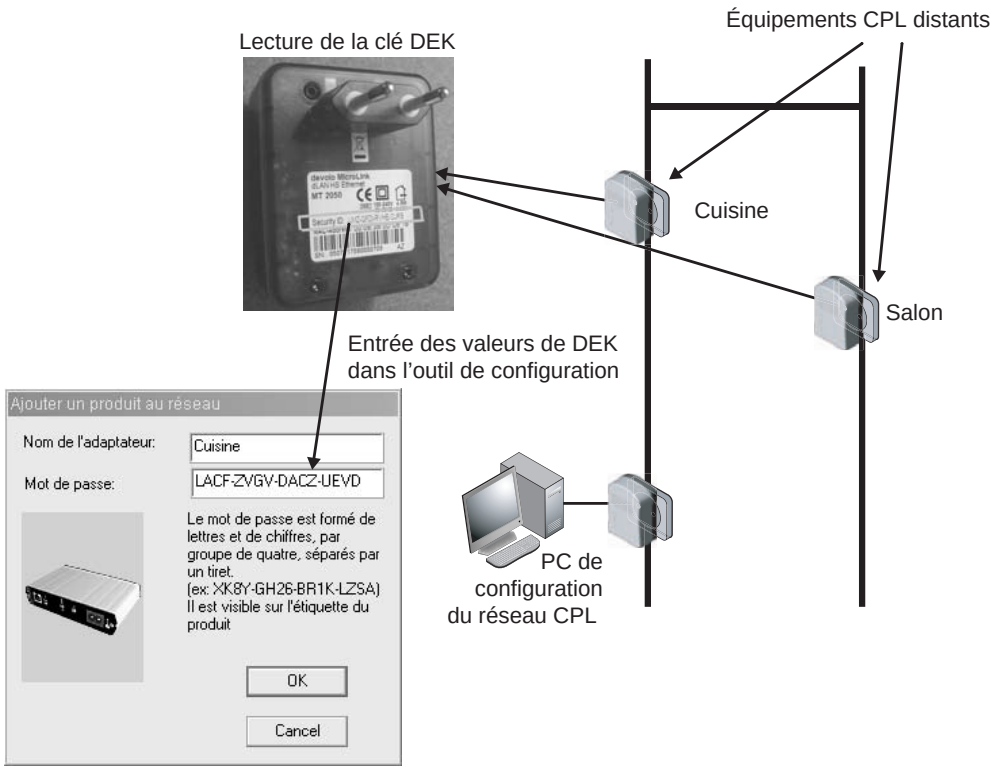


Figure 9.22

Configuration du réseau CPL à l'aide de la clé DEK

Une fois tous les équipements CPL du réseau configurés localement ou grâce à la clé DEK, il suffit de sélectionner l'onglet Produits pour vérifier l'état des liens CPL entre l'équipement sur lequel est connecté le PC et les autres équipements CPL raccordés au réseau électrique *(voir figure 9.23) :*

- Le volet « Produit(s) connecté(s) à votre PC » indique le ou les équipements CPL connectés directement en Ethernet au PC de configuration *via* la carte réseau du PC ainsi que son adresse MAC.
- Le volet « Produit(s) détecté(s) » liste les équipements CPL détectés sur le réseau électrique et disposant de la même clé NEK et indique leur débit estimé.

Il est possible de renommer les produits de la liste en cliquant sur Renommer et en indiquant un nom significatif pour retrouver l'équipement CPL dans l'architecture du réseau électrique. À la figure 9.23, nous avons renommé les équipements CPL **Cuisine** et **Chambre.**

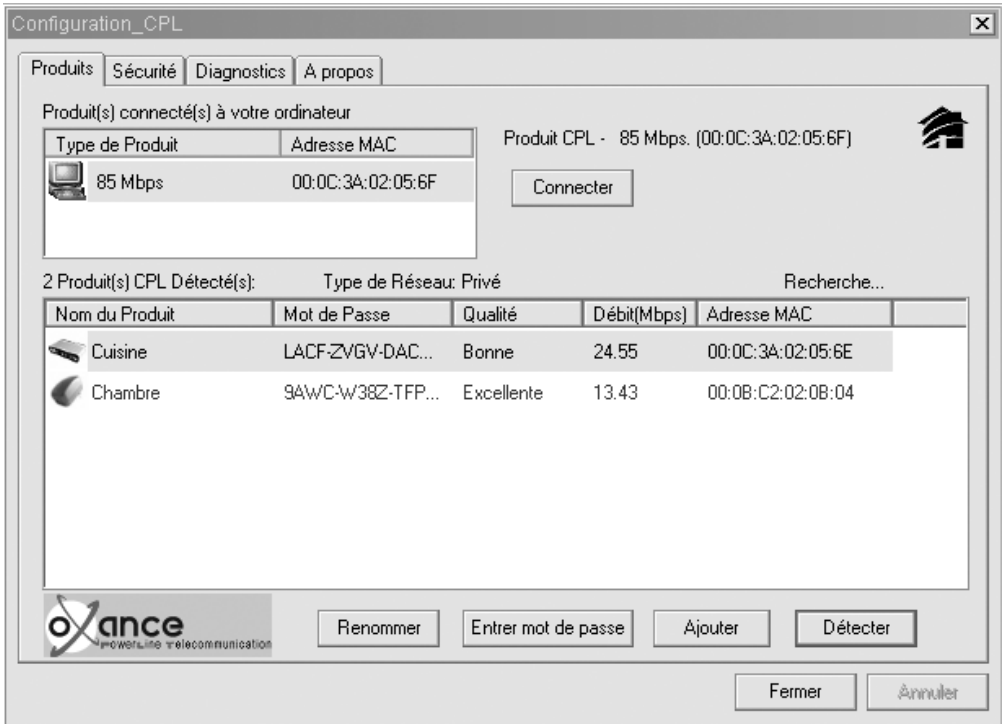


Figure 9.23
Diagnostic de l'état du réseau CPL

Cohabitation de plusieurs réseaux locaux CPL HomePlug sur un même réseau électrique

Il n'est pas possible de configurer plusieurs clés NEK sur un même équipement CPL HomePlug 1.0 et Turbo. Il n'est donc pas possible qu'un équipement appartienne à plusieurs réseaux locaux CPL. Dans le cadre de la spécification HomePlug AV, il sera possible d'avoir plusieurs clés de cryptage sur un même équipement CPL et donc d'avoir des équipements appartenant à plusieurs réseaux locaux CPL. Il est en effet possible d'avoir plusieurs réseaux locaux CPL sur un même réseau électrique. Il suffit que ces réseaux locaux CPL partagent la bande de fréquences (de 1 à 30 MHz) et divisent leur vitesse de transmission par le nombre de réseaux locaux CPL en présence.

La configuration du réseau CPL étant à présent terminée, il est possible de configurer le réseau IP et les applications adéquates pour les utilisateurs du réseau Ethernet constitué par le réseau CPL. Cette configuration du réseau IP est détaillée au chapitre 10.

En cliquant sur l'onglet Diagnostics, il est possible de visualiser des informations système sur le PC et sur l'équipement CPL directement connecté au PC en Ethernet, ainsi que des historiques des produits CPL précédemment détectés par l'outil de configuration.

La figure 9.24 illustre cet onglet pour l'équipement **Chambre,** correspondant au réseau CPL **Mot2Passe,** avec la date et l'heure de la dernière visualisation de cet équipement. Pour sauvegarder ou envoyer ces historiques à d'autres installateurs de réseaux CPL, il suffit de cliquer sur Imprimer.

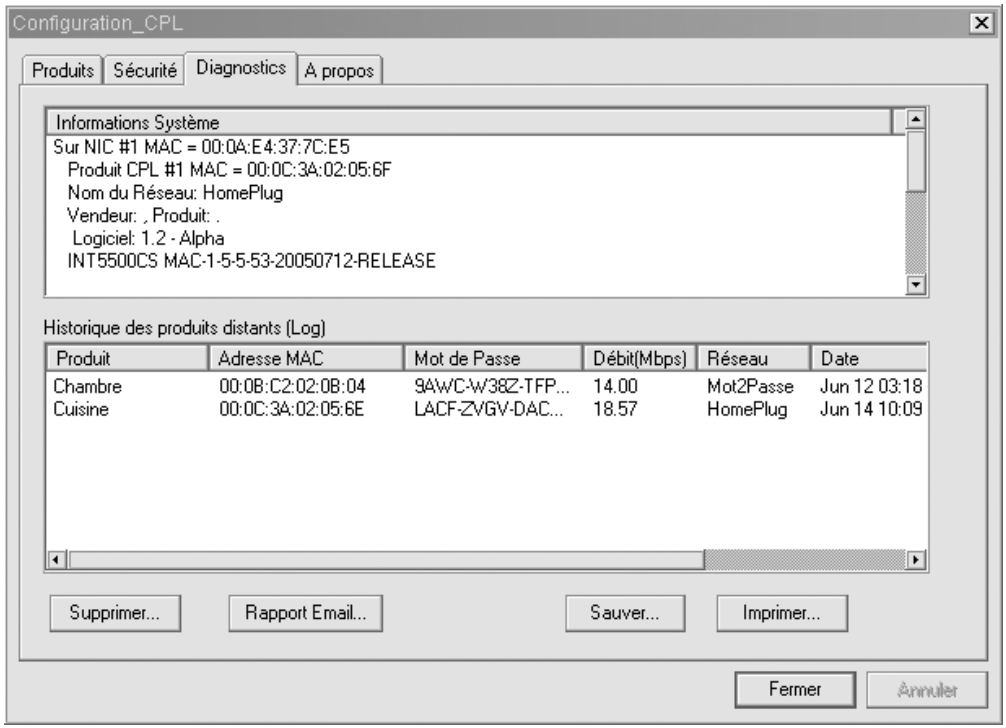


Figure 9.24

Onglet Diagnostics de l'outil de configuration

La figure 9.25 donne un exemple de fichier texte de sauvegarde des historiques de configuration.

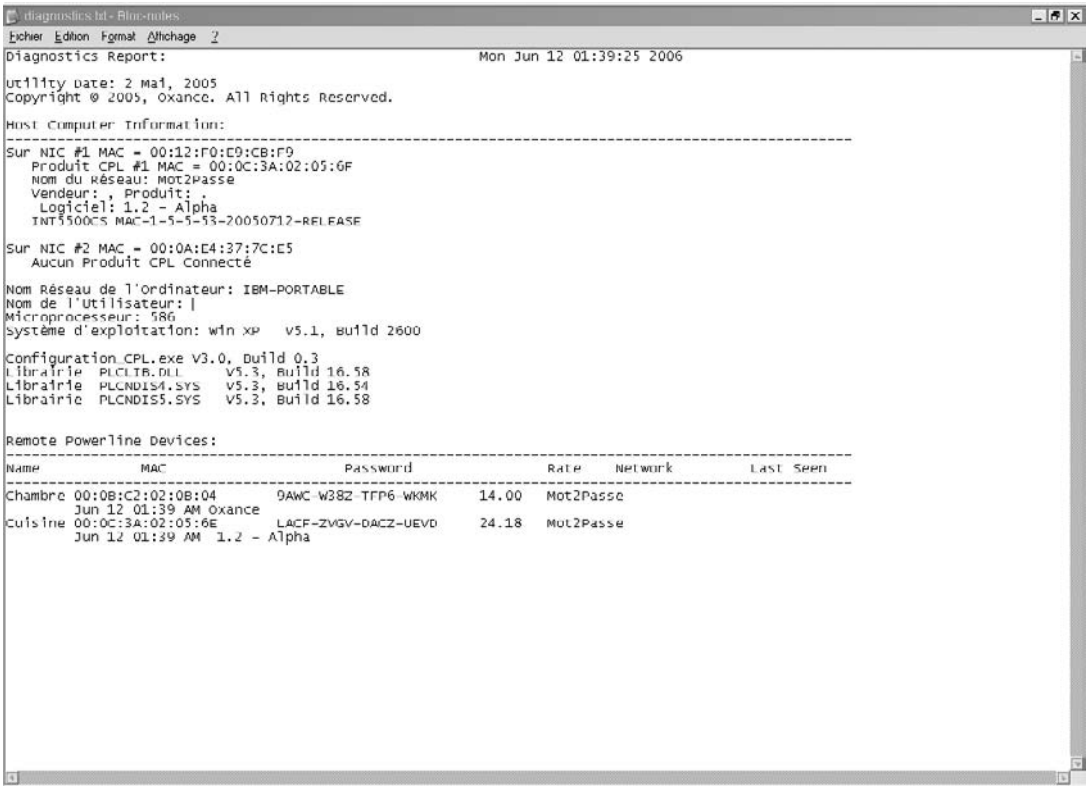


Figure 9.25

Sauvegarde des historiques de configuration des équipements détectés par l'outil de configuration CPL

Configuration d'un réseau CPL sous Linux

De la même manière que sous Windows, l'installation d'un réseau CPL sous Linux consiste à relier la carte réseau du PC à un des équipements CPL du réseau électrique et à utiliser un outil de configuration CPL pour Linux.

Dans le cas d'un équipement CPL avec interface USB, il faut installer le driver de l'interface virtuelle USB/Ethernet. Pour cela, il est nécessaire de récupérer l'archive comportant ce driver en le téléchargeant à l'adresse suivante (pour un équipement Devolo) :

http://download.devolo.biz/webcms/0607105001130251610/dLAN-linux-package-2.0.tar.gz

La figure 9.26 illustre la page du site de Devolo proposant les outils de configuration CPL des équipements dLAN duo.

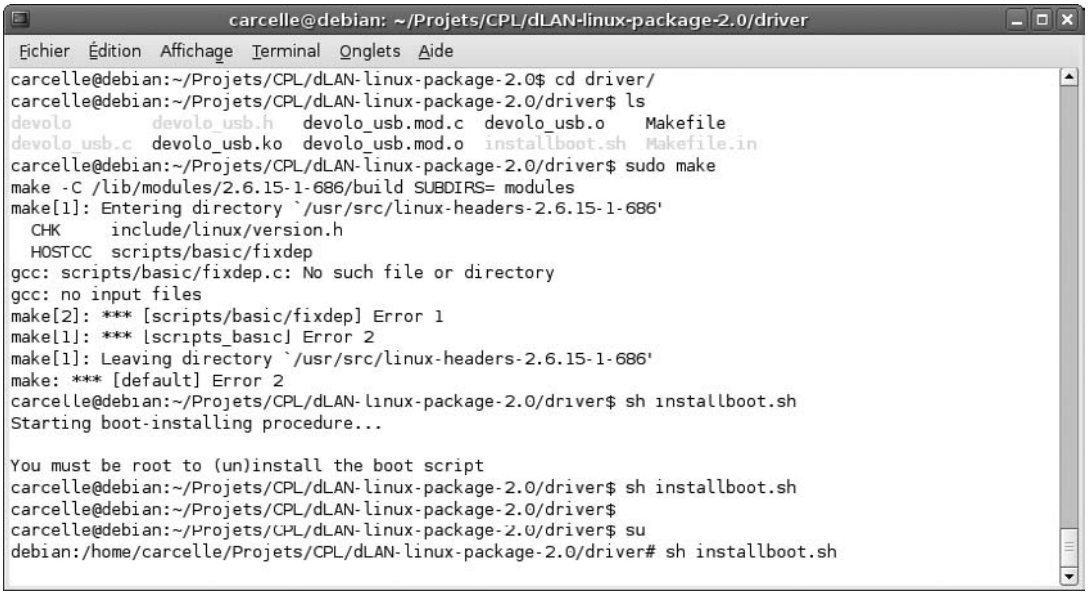


Figure 9.26

Page d'accueil des outils de configuration des équipements dLAN duo de Devolo

Il suffit de cliquer sur le lien Driver Linux pour le télécharger puis de sauvegarder le fichier à un emplacement sur le disque lorsque la fenêtre de téléchargement illustrée à la figure 9.27 s'affiche.

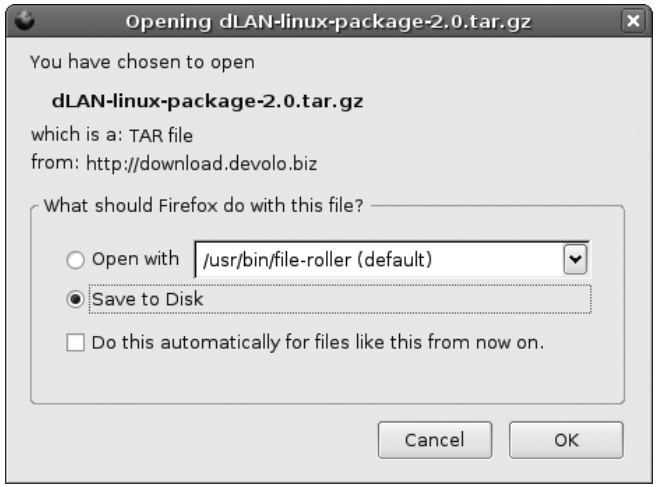


Figure 9.27

Fenêtre de téléchargement de l'outil CPL Linux

Dans notre exemple, nous sauvegardons le fichier sous :

```
carcelle@debian:~/Projets/CPL
```

Une fois le fichier téléchargé, il faut le décompresser deux fois grâce aux commandes suivantes :

```
carcelle@debian:~/Projets/CPL$gunzip dLAN-linux-package-2.0.tar.gz
carcelle@debian:~/Projets/CPL$tar -xvf dLAN-linux-package-2.0.tar
```

Il faut ensuite connecter l'équipement CPL USB à un port disponible du PC et vérifier que l'équipement est reconnu en lançant la commande suivante :

```
carcelle@debian:~/Projets/CPL$dmesg
```

La commande `dmesg` donne la sortie illustrée à la figure 9.28.

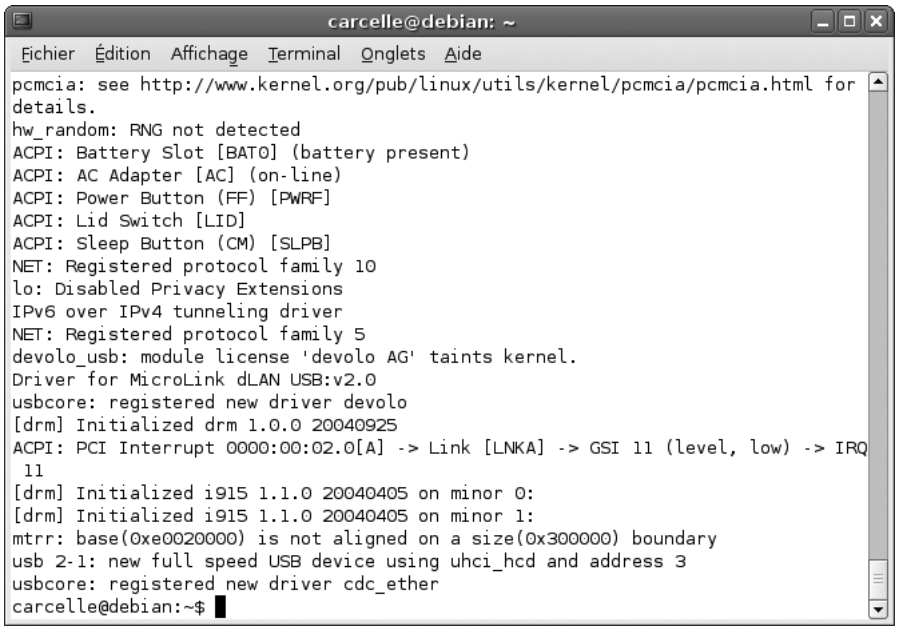


Figure 9.28
Sortie de la commande dmesg

Pour installer le driver ainsi téléchargé, il faut ouvrir le répertoire où l'outil CPL a été décompressé :

```
carcelle@debian:~/Projets/CPL$cd dLAN-linux-package-2.0/driver/
```

La figure 9.29 illustre les fichiers contenus dans ce répertoire.

À partir de cet instant, il faut passer en mode superutilisateur *(root)* puis lancer la commande d'installation `install.boot.sh` illustrée à la figure 9.30.

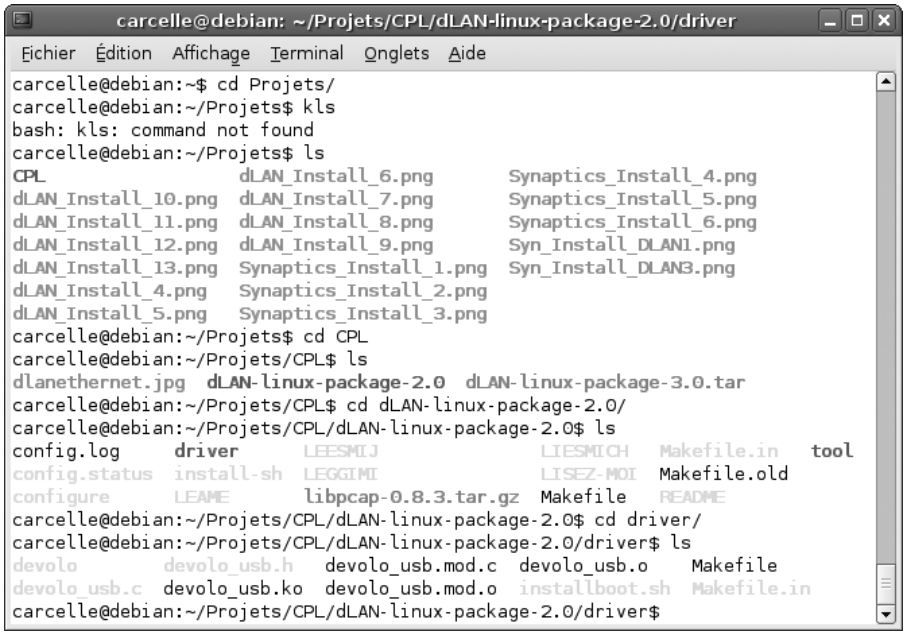


Figure 9.29

Contenu du répertoire des pilotes de l'équipement CPL USB

Figure 9.30

Lancement de la commande d'installation

Pour compiler le pilote USB, il faut ensuite lancer la commande `make usbdriver` suivante *(voir figure 9.31) :*

```
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$make usbdriver
```

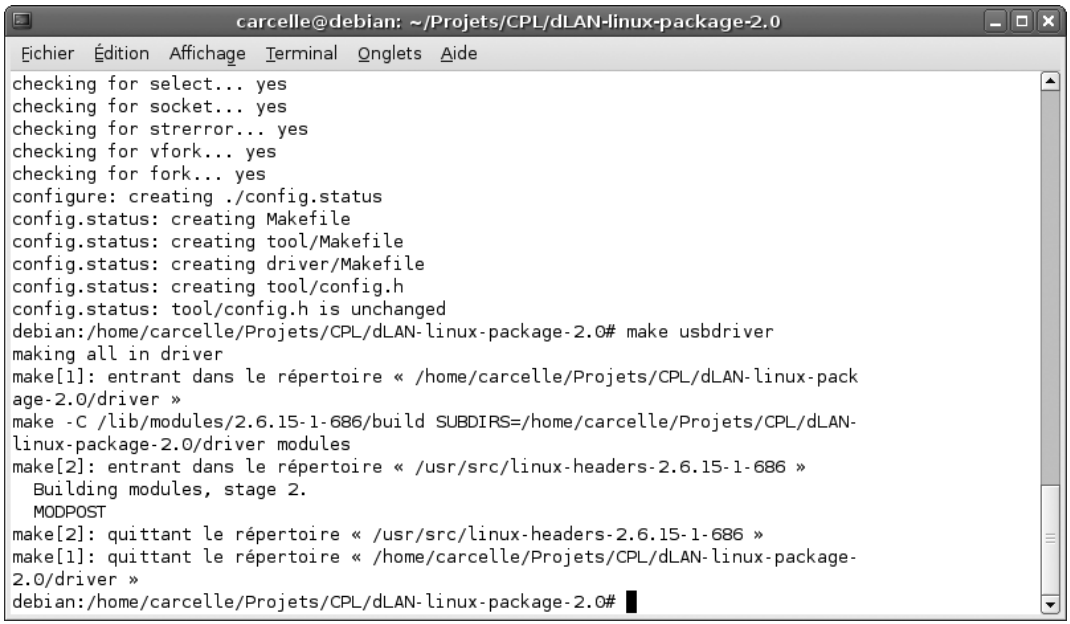


Figure 9.31

Lancement de la commande make usbdriver

Une fois la compilation terminée, la commande suivante, illustrée à la figure 9.32, permet d'installer le pilote aux emplacements disque adéquats *(voir figure 9.33) :*

```
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$make install-usbdrive
```

Enfin, la commande suivante :

```
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$make installboot
```

permet que le pilote USB soit chargé au démarrage.

Il suffit de redémarrer l'ordinateur pour valider l'ensemble des commandes.

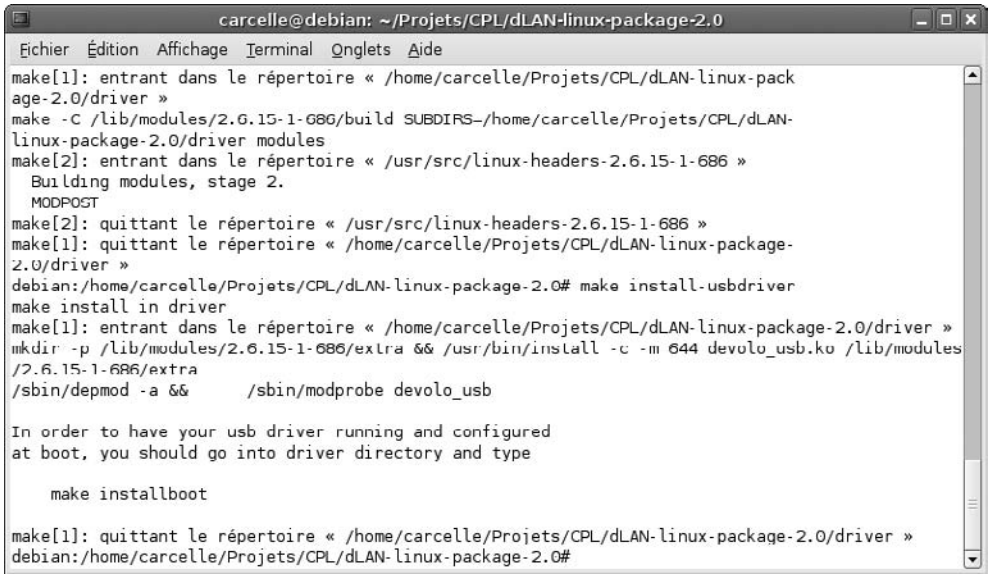


Figure 9.32

Lancement de la commande make install-usbdriver

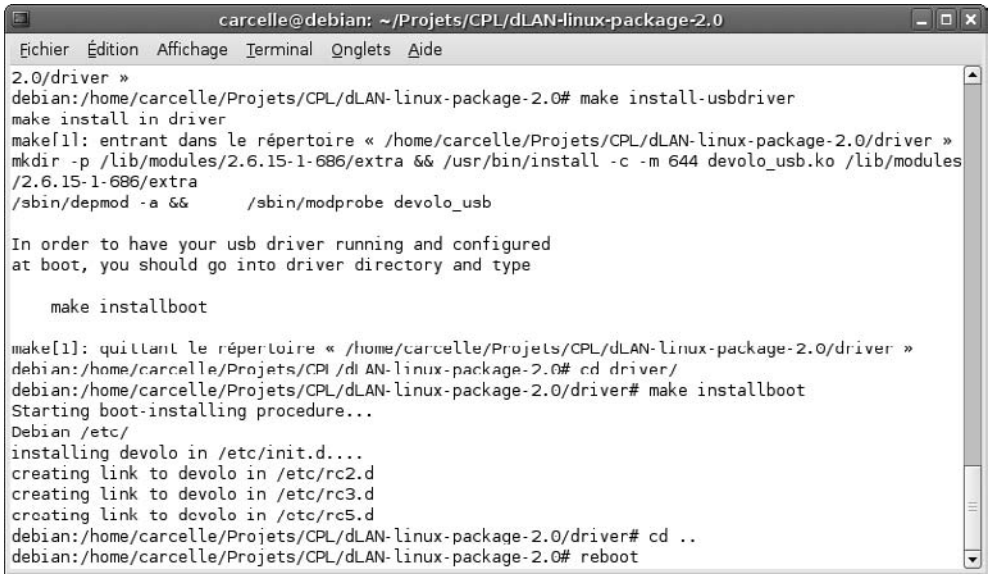


Figure 9.33

Lancement de la commande make install-boot

Une fois le redémarrage terminé, l'équipement doit rester branché sur le port USB afin de vérifier que la nouvelle carte virtuelle Ethernet/USB est installée, comme illustré à la figure 9.34.

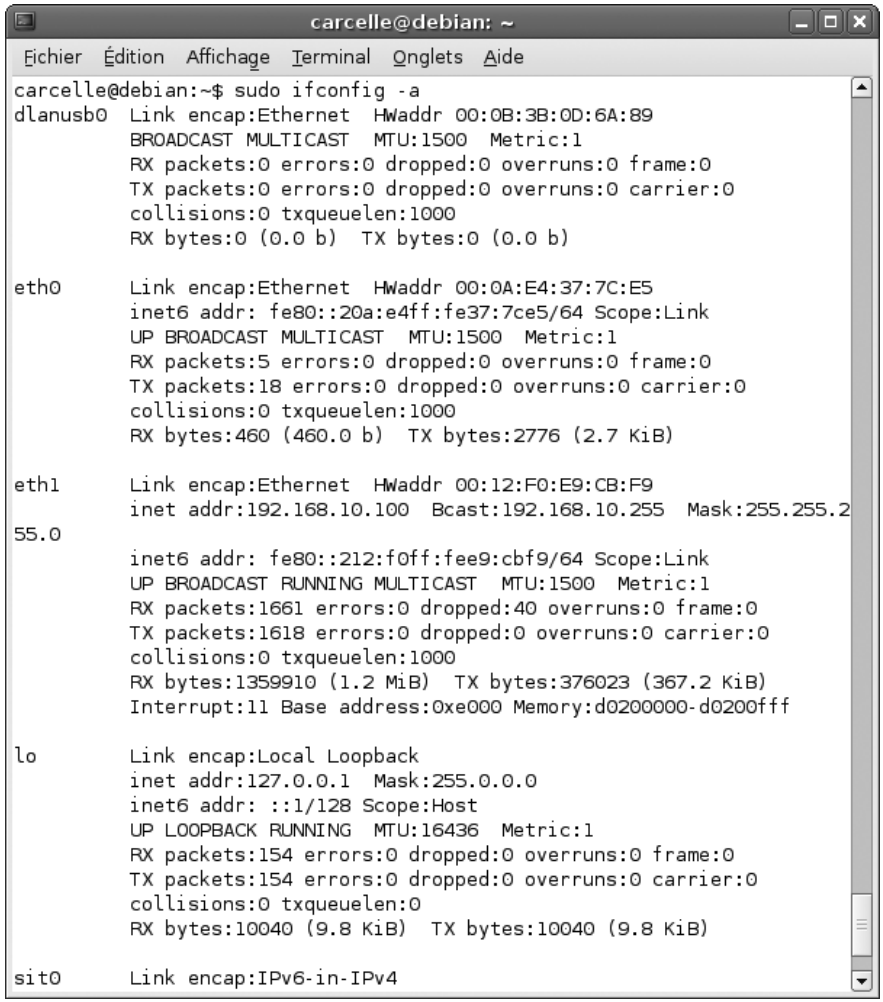


Figure 9.34

Vérification de l'installation de la carte virtuelle Ethernet/USB

La carte `dlanusb0` est bien installée. Nous pouvons commencer l'installation de l'utilitaire de configuration CPL.

L'outil de configuration sous Linux ayant été décompressé dans le même répertoire que le pilote USB, commençons par le placer dans le bon répertoire :

```
debian:home/carcelle/Projets/CPL/dLAN-linux-package-2.0#./configure
```

Nous pouvons commencer par configurer les paramètres de compilation, comme illustré à la figure 9.35.

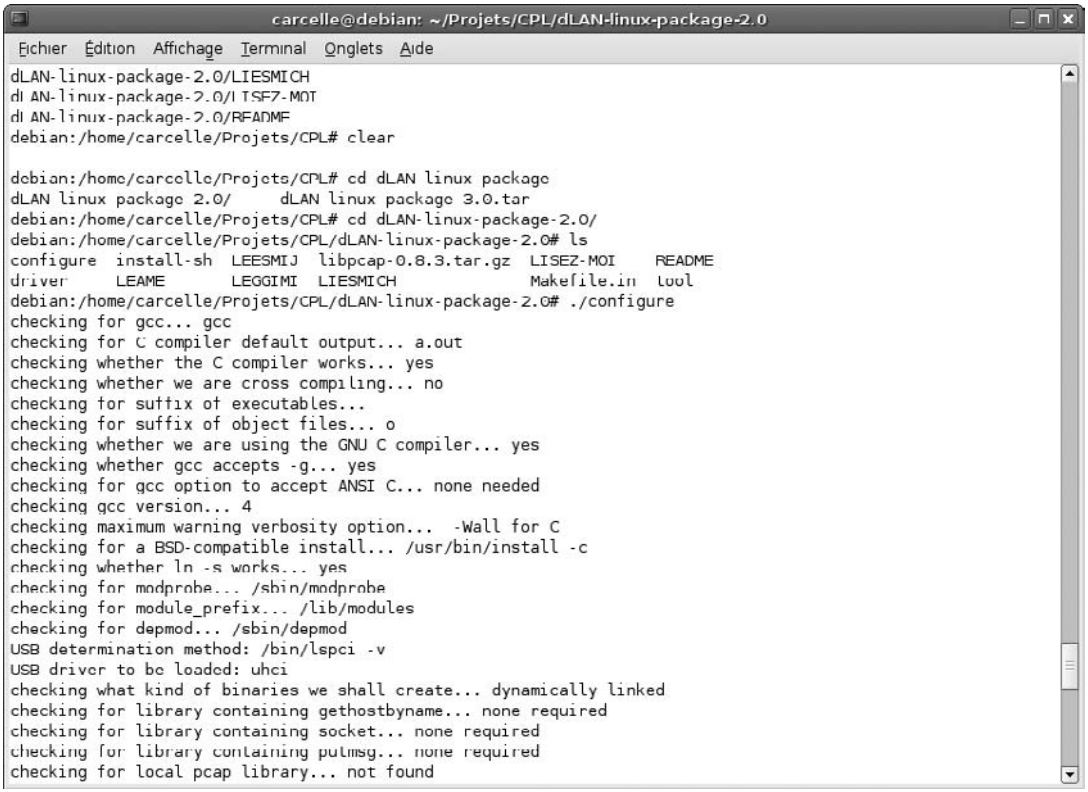


Figure 9.35

Configuration des paramètres de compilation

Nous pouvons ensuite lancer la compilation de l'outil de configuration CPL à l'aide de la commande `make`, comme illustré à la figure 9.36.

Une fois la compilation terminée, il faut installer les fichiers compilés dans les bons emplacements disques au moyen de la commande `make install`.

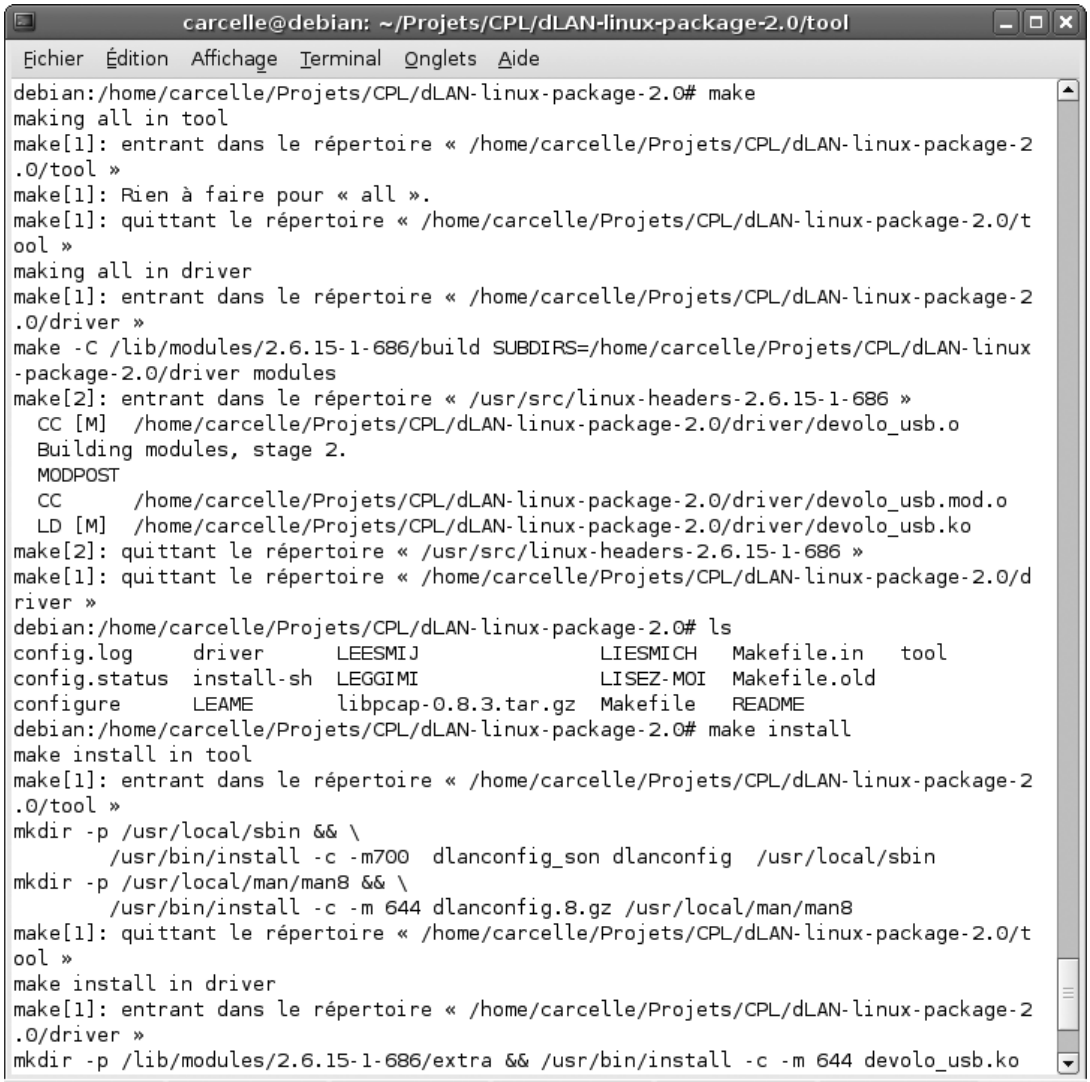


Figure 9.36

Compilation de l'outil de configuration CPL

Il est alors possible de lancer l'outil de configuration avec la carte virtuelle Ethernet/USB ou avec la carte Ethernet connectée à un équipement CPL USB ou Ethernet grâce à la commande suivante *(voir figure 9.37) :*

```
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0$sudo dlanconfig eth0
```

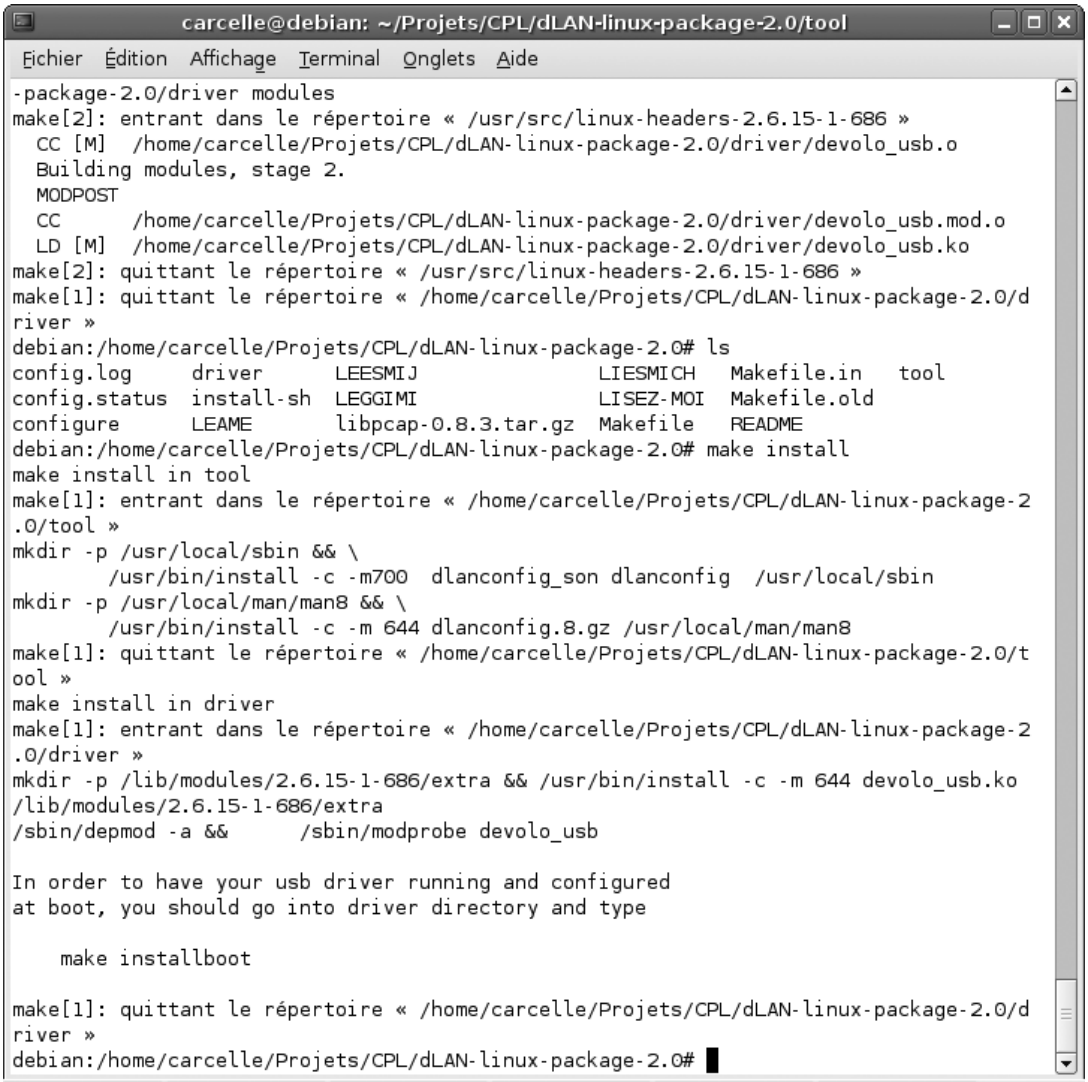


Figure 9.37

Installation de l'outil de configuration CPL

Il est possible de lancer l'outil sur l'interface `eth0` ou `dlanusb0`. La figure 9.38 illustre la détection des équipements CPL connectés au réseau CPL effectuée par l'outil de configuration.

Dans cet exemple, l'équipement CPL détecté correspond à la spécification HomePlug 1.0 puisque son débit physique estimé est de 12,829 Mbit/s.

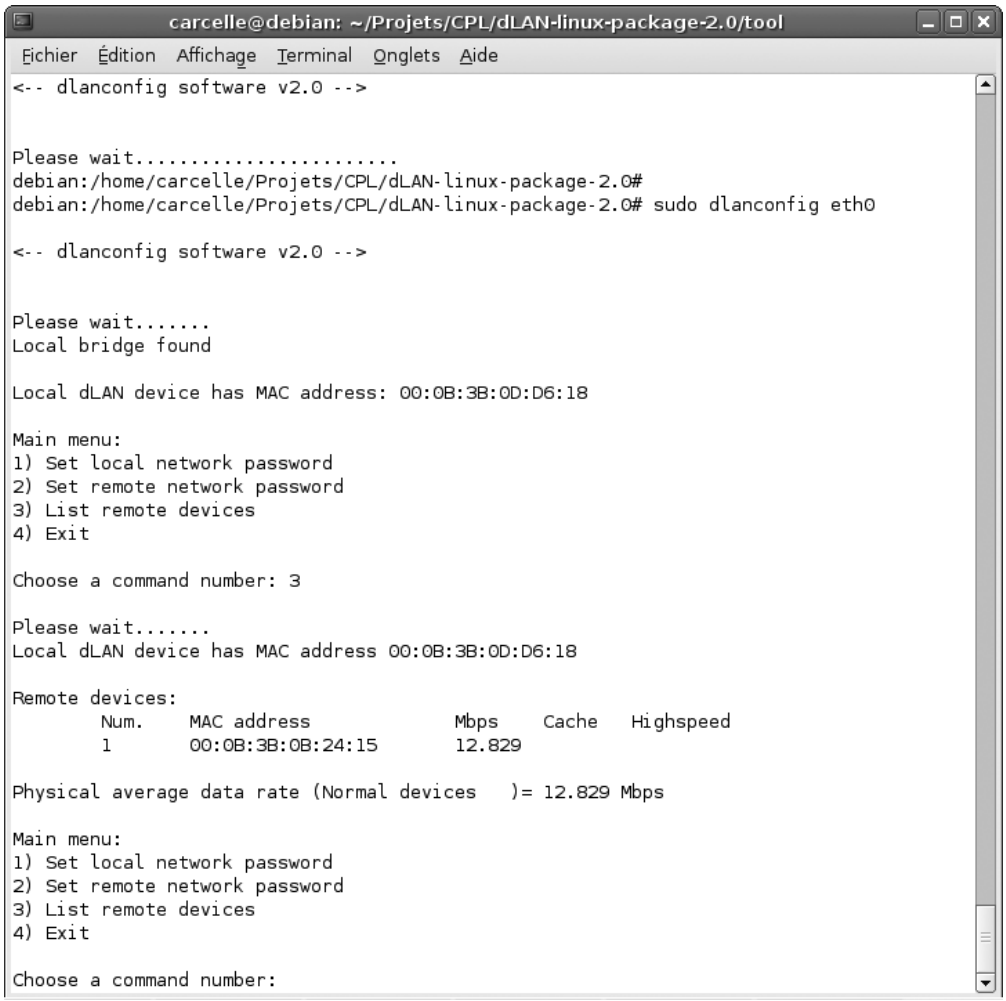


Figure 9.38

Détection d'un équipement CPL Ethernet à l'aide de l'outil de configuration CPL Linux

L'outil de configuration propose un menu dont les quatre fonctionnalités sont les suivantes :

- « Set local network password », qui permet de configurer la clé du réseau CPL (clé NEK) sur le ou les équipements CPL connectés directement en Ethernet au PC de configuration.

- « Set remote network password », qui permet de configurer la clé du réseau CPL sur les équipements CPL distants branchés sur le réseau électrique (clé DEK).
- « List remote devices », qui permet de donner la liste des équipements CPL connectés au réseau CPL et configurés avec la même clé réseau CPL.
- « Exit », qui permet de sortir de l'outil de configuration.

Configuration d'un réseau CPL sous FreeBSD

Le système d'exploitation FreeBSD n'offre pas beaucoup d'outils pour configurer des réseaux CPL. Nous allons détailler le programme plconfig, un des seuls disponibles actuellement pour ce type de plate-forme.

FreeBSD est un système d'exploitation proche de Linux, issu des travaux sur les noyaux Unix effectués au sein de l'Université de Berkeley, en Californie. S'il existe peu de différences avec les distributions Linux, les développements sur plate-forme FreeBSD diffèrent cependant légèrement.

FreeBSD est essentiellement utilisé comme système d'exploitation par les serveurs de courrier, Web et de sécurité. FreeBSD utilise un système de paquets, appelé « ports », représentant des programmes utilisables sous ce système d'exploitation. Ce système de ports est géré par un ensemble de développeurs répartis autour du monde qui en garantissent l'intégrité. Le nombre de ces développeurs est beaucoup moins important que pour Linux, ce qui rend FreeBSD à la fois plus stable et plus homogène.

Commençons par télécharger l'outil de Manuel Kasper, plconfig, à l'adresse *https://neon1.net/prog/plconfig-0.2.tar.gz.*

Dans une console en mode superutilisateur, nous décompressons ensuite le programme d'installation de l'outil, puis lançons l'installation au moyen de la commande `make`.

Le programme affiche un menu d'aide si aucune option ou interface réseau n'est indiquée comme paramètre à la commande *plconfig* :

```
#tar xfvz plconfig-0.2.tar.gz; cd plconfig-0.2
#make
#./plconfig
Syntax
Powerline Bridge config version 0.2 by Manuel Kasper <mk@neon1.net>

Usage:   plconfig [-pqrh] [-b device] [-s key] interface

         -s key            set network encryption key
                           (plaintext password or 8 hex bytes preceded by 0x)
         -b device         use device (default is /dev/bpf0)
         -p                don't switch interface to promiscuous mode
```

```
        -r              request parameters and statistics
        -q              request Intellon-specific network statistics
        -h              display this help

        If -s is not specified, plconfig will listen for management packets
        indefinitely (after requesting stats if -r is specified)
```

Comme l'indique ce menu d'aide, le programme propose les fonctionnalités réseau CPL suivantes :

- `-s`, qui permet de configurer la clé NEK sur les équipements connectés localement en Ethernet au PC de configuration.
- `-r`, qui permet d'interroger la puce HomePlug de l'équipement CPL connecté localement et de récupérer un certain nombre de paramètres et de statistiques. Cette option permet en outre de visualiser les équipements CPL du réseau électrique correctement configurés.
- `-q`, qui permet d'interroger la puce CPL et de récupérer des valeurs et statistiques propres au constructeur de puces Intellon.

Comme nous le voyons, ce programme n'est pas aussi complet que les outils sous Windows ou sous Linux mais propose tout de même les principales fonctionnalités exigées pour configurer un réseau CPL (configuration de la clé réseau et état des liens CPL au niveau physique).

Configuration d'un réseau DS2

Le constructeur espagnol DS2 est un acteur du marché concurrent de HomePlug, dont les produits ne sont pas compatibles avec les équipements HomePlug.

La configuration d'un réseau CPL DS2 à 200 Mbit/s s'effectue localement sur l'équipement par le biais d'une interface HTTP. Elle est donc identique pour Windows et Linux/FreeBSD.

Les équipements DS2 peuvent fonctionner dans trois modes réseau différents :

- HE : l'équipement est maître pour le réseau CPL.
- CPE : l'équipement est esclave pour le réseau CPL.
- TDREP : l'équipement sert de répéteur pour le réseau CPL.

Nous illustrons cette section par des équipements CPL Corinex AV, fondés sur des puces DS2 Wisconsin. Il existe deux types de firmwares dans ces équipements : *alma* et *spirit*. Nous avons retenu un équipement avec firmware *alma*, qui propose davantage de fonctionnalités.

Avant de se connecter sur l'interface HTTP, il faut placer l'équipement CPL et le PC de configuration dans le même plan d'adressage IP. Les équipements CPL Corinex AV ayant, par défaut, l'adresse IP 10.10.1.69, il faut configurer l'adresse IP du PC de configuration dans ce même plan d'adressage, par exemple en 10.10.1.10.

La figure 9.39 illustre les différents plans d'adressage qui vont coexister sur le réseau électrique.

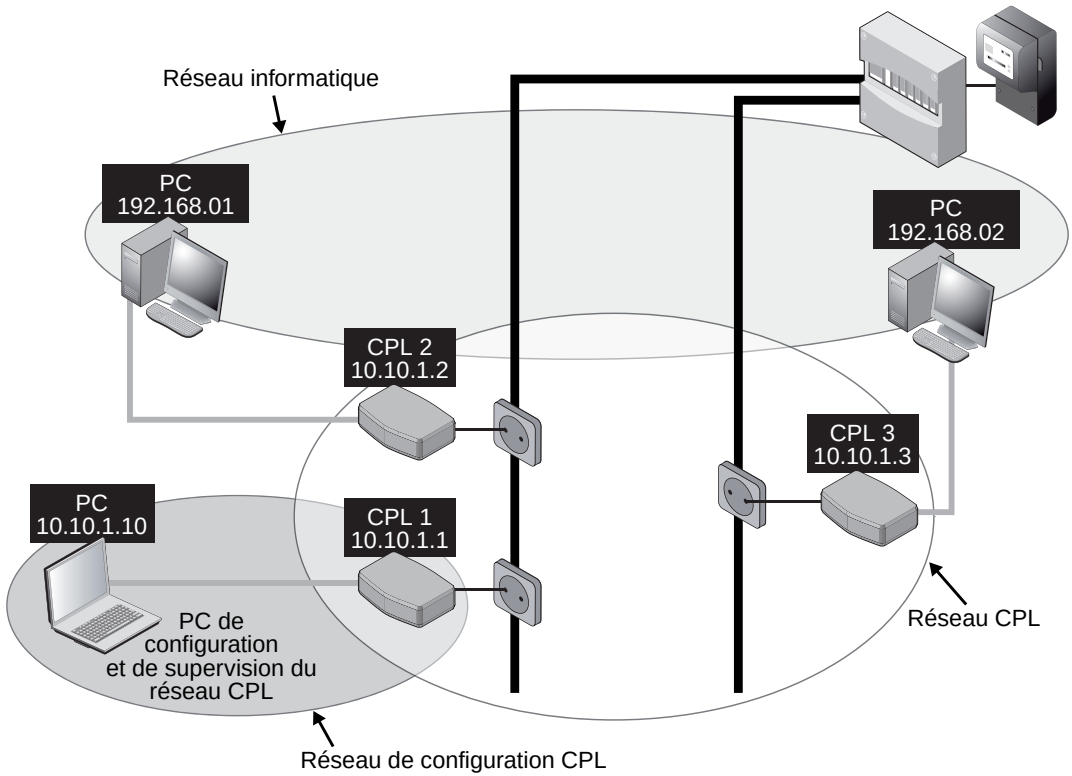


Figure 9.39

Plans d'adressages d'un réseau CPL DS2

Une fois connecté sur la page d'accueil, il faut entrer le mot de passe par défaut **paterna** pour ouvrir les pages de configuration, comme illustré à la figure 9.40.

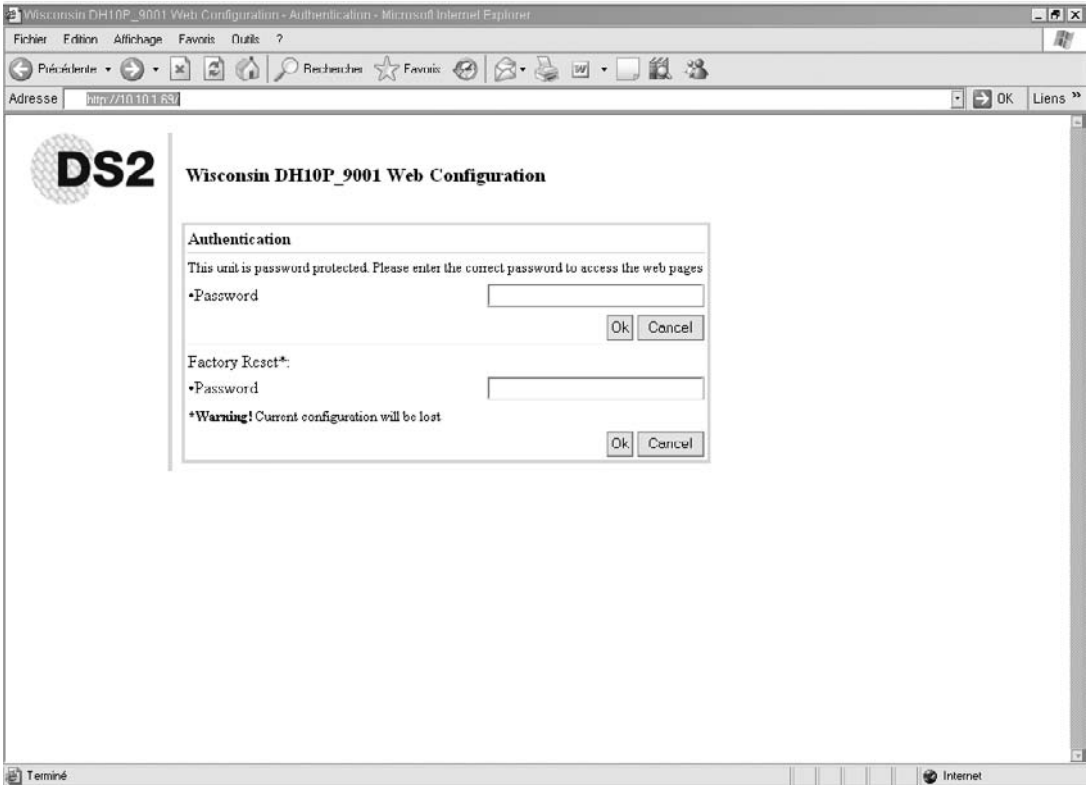


Figure 9.40
Page d'accueil de l'outil HTTP de configuration DS2

La première page de configuration offre une vision d'ensemble des principaux paramètres d'un équipement CPL DS2 *(voir figure 9.41)*, notamment les suivants :

- adresse IP de l'équipement CPL ;
- mode réseau MAC (HE, CPE, TDREP) de l'équipement CPL ;
- mode du lien physique CPL ;
- groupes multicast au niveau de la couche IP ;

- clé (ou mot de passe) permettant de sécuriser le réseau CPL ;
- priorités de certains flux de données entre équipements CPL.

Ces paramètres peuvent être configurés séparément puis validés et écrits dans la mémoire non volatile de l'ordinateur. Un reboot de l'équipement permet de prendre en compte les modifications apportées à la configuration d'ensemble.

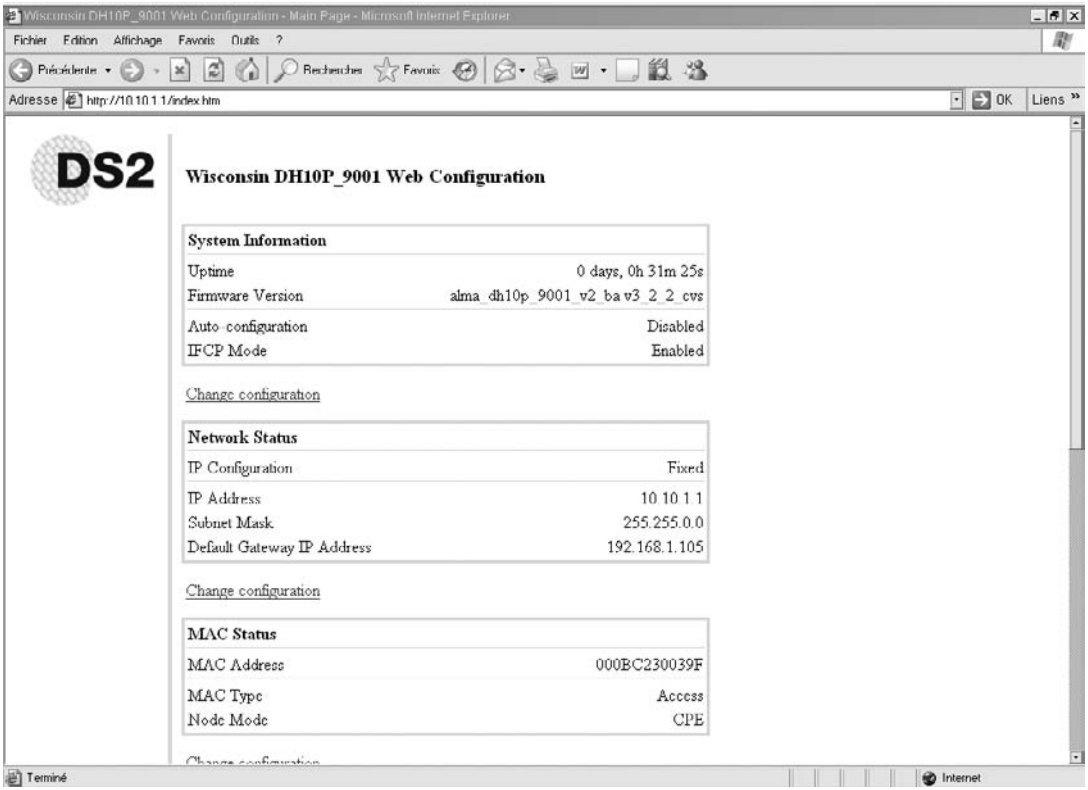


Figure 9.41

Paramètres de configuration de l'équipement CPL DS2

Il est possible de configurer l'adresse IP, le masque de sous-réseau et la passerelle par défaut de l'équipement en cliquant sur Change configuration, en dessous de Default Gateway IP Address. La page de configuration illustrée à la figure 9.42 s'affiche alors.

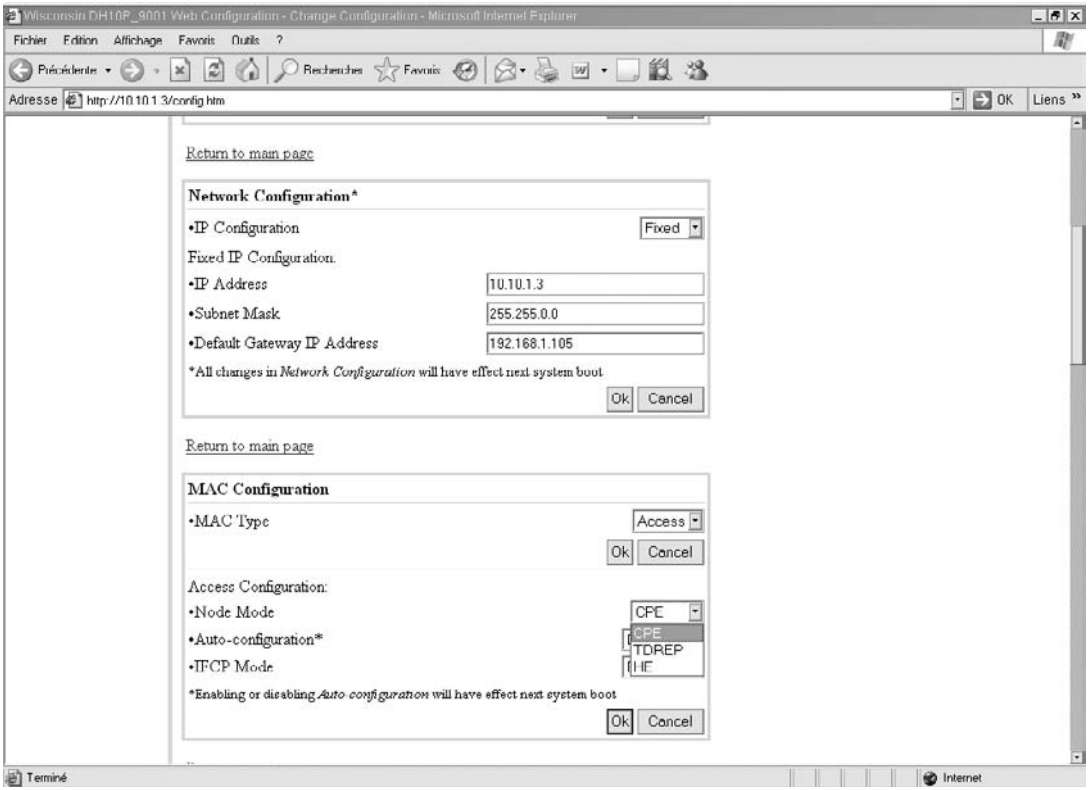


Figure 9.42

Configuration des paramètres réseau et MAC de l'équipement CPL DS2

Dans l'exemple de la figure 9.39, les équipements CPL1, CPL2 et CPL3 ont respectivement les adresses 10.10.1.1, 10.10.1.2 et 10.10.1.3, et le masque de sous-réseau est placé à 255.255.0.0. Dans ce cas, la passerelle par défaut n'est pas importante car le PC de configuration dispose d'une adresse dans le même plan d'adressage (10.10.1.10).

Une fois ces paramètres réseau configurés, il est important de configurer le mode réseau de chaque équipement CPL.

Comme l'illustre la figure 9.43, l'équipement le plus proche du tableau électrique est en mode maître (HE), les autres équipements étant en mode esclave (CPE) ou répéteur (TDREP). Ce dernier permet d'atteindre des équipements difficilement « connectables » du fait de la longueur du câble électrique ou d'autres contraintes de l'environnement électrique du bâtiment.

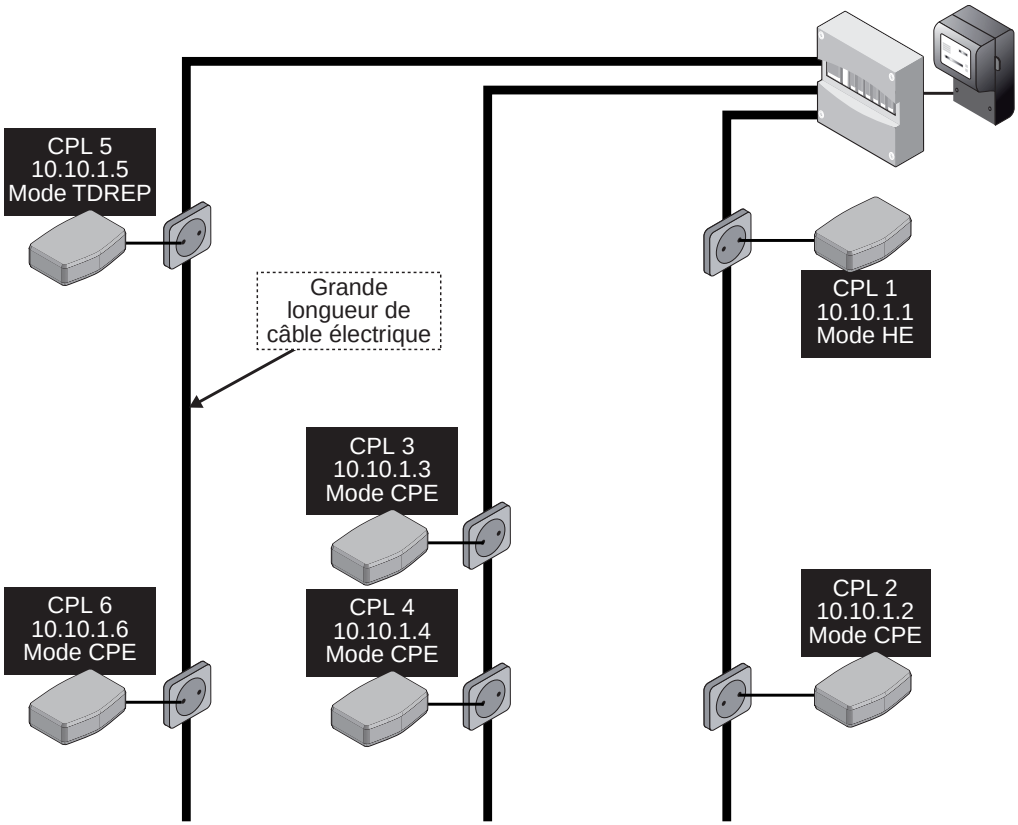


Figure 9.43

Configuration du mode réseau des équipements CPL DS2

Cette configuration s'effectue à la section Access configuration du volet MAC Configuration en sélectionnant Node Mode. Une fenêtre propose alors un choix parmi les trois modes possibles.

Les équipements CPL DS2 permettent de créer des groupes de type IP multicast, les trames IP étant envoyées depuis un équipement source vers plusieurs équipements destination appartenant au groupe multicast. Il est important de bien connaître les techniques de configuration des réseaux IP pour la mise en place des groupes « multicast » *(voir en fin de chapitre).*

Un des paramètres importants des réseaux CPL de tout type est la clé réseau, appelée **Password** dans l'outil de configuration DS2, qui permet de créer des réseaux CPL privés et de sécuriser les échanges de trames de données entre les éléments du réseau (équipements et terminaux connectés au réseau CPL). Cela s'effectue à la section

Security Configuration *(voir figure 9.44)* en entrant le nouveau de passe du réseau CPL propre à ce réseau. Ce paramètre est l'équivalent de la NEK pour les réseaux CPL HomePlug.

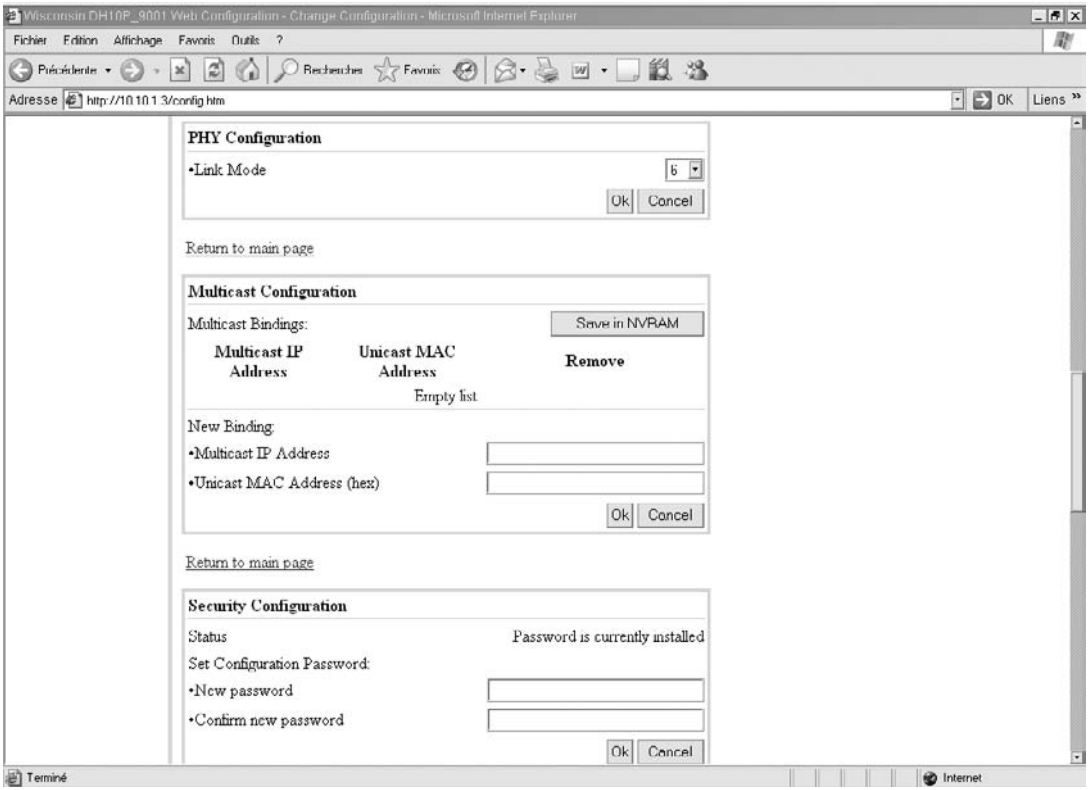


Figure 9.44

Configuration des paramètres PHY, multicast et sécurité d'un équipement CPL DS2

Il est alors possible de configurer la priorité de chacun des équipements CPL du réseau en plaçant le paramètre Default priority de la section Priority configuration entre 1 et 5, en fonction de la topologie du réseau et de la fonction de chacun des équipements.

Par exemple, sur la base de la topologie de la figure 9.43, l'équipement en mode maître peut être configuré avec une priorité « supérieure » (valeur 1) et certains des équipements CPL en mode CPE en priorité « moyenne » (valeur 2) si les terminaux connectés ont des applications temps réel. Les autres équipements peuvent être configurés en priorité « basse » (valeur 3 ou 4).

La figure 9.45 illustre la page HTML qui donne accès aux paramètres de configuration de sécurité du réseau CPL (mot de passe pour l'aller à l'interface de configuration, ID du réseau CPL, mot de passe pour la remise à zéro usine) et aux paramètres de configuration des priorités de chaque équipement sur le réseau CPL, spécialement le paramètre « default priority ».

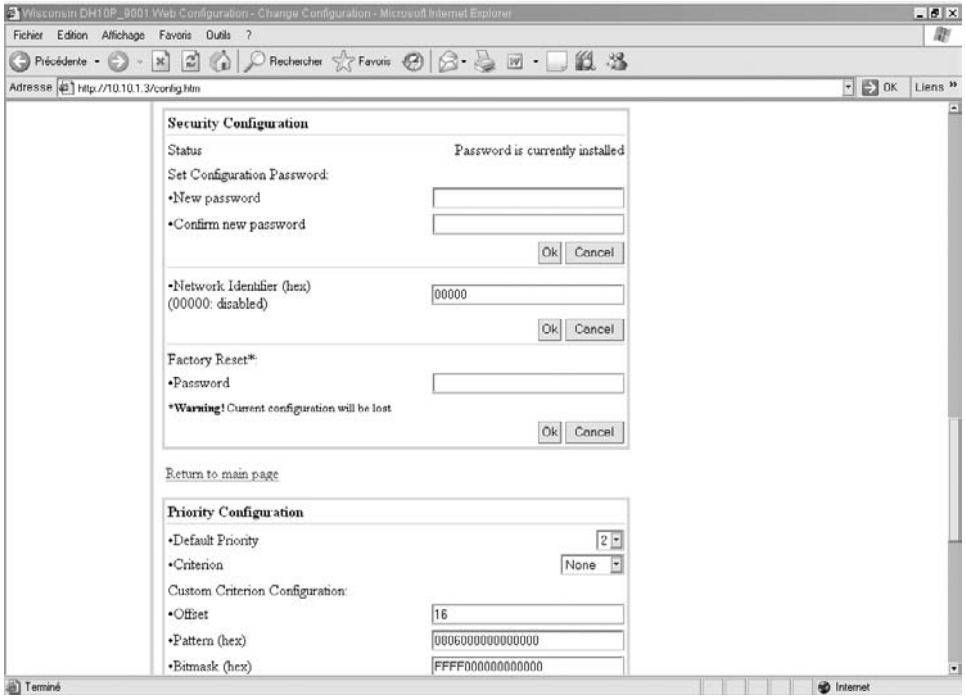


Figure 9.45

Configuration des paramètres de sécurité et de priorité d'un équipement CPL DS2

Il est également possible de configurer le réseau CPL DS2 en utilisant une console Telnet sur le port 40000 avec la commande :

```
C:\>telnet adresseIP_equipement_CPL 40000
```

`adresseIP_equipement_CPL` est l'adresse IP de l'équipement CPL que nous voulons configurer et qui est connecté par l'interface Ethernet au PC de configuration.

La configuration par le biais de la console Telnet donne accès à des fonctionnalités avancées, telles que la température de l'équipement CPL, le notching de certaines bandes fréquences, la fonction « bridge », le « roaming » entre réseaux CPL, etc.

Configuration des paramètres réseau

Pour achever la configuration d'un réseau CPL, il est encore nécessaire d'affecter à chaque équipement les bons paramètres de réseau, incluant la configuration de l'adresse IP, du masque de sous-réseau, de l'adresse de la passerelle par défaut et de l'adresse DNS.

Avant d'aborder ces étapes de configuration proprement dites, les sections qui suivent rappellent quelques notions essentielles sur la gestion des communications réseau, telles que adresses IP, masque de sous-réseau et DNS.

Rappels sur les paramètres réseau

La gestion des communications dans un réseau est régie par un nombre important de fonctionnalités liées aux standards utilisés. L'un d'eux, le protocole IP (Internet Protocol), définit la manière de communiquer par un système d'adressage et des mécanismes de routage particuliers.

Les adresses IP

Chaque machine connectée à un réseau local ou à Internet utilise la combinaison de deux protocoles, TCP (ou UDP) et IP, plus connue sous le nom TCP/IP ou UDP/IP. Pour communiquer, chaque machine possède une adresse IP unique. Les adresses IP sont de la forme *x.x.x.x,* où *x* correspond à un nombre compris entre 0 et 255.

Il existe deux versions du protocole IP, IPv4 et IPv6. L'adresse IPv4, que l'on utilise le plus souvent actuellement, est sur 4 octets et ne dispose que de fonctionnalités limitées, tournant essentiellement autour du routage. IPv6 est une évolution d'IPv4, qui se met peu en place dans les réseaux. Son adresse est sur 16 octets, et elle comporte de nombreuses fonctionnalités, comme la gestion de la mobilité, de la qualité de service et de la sécurité.

Structure d'une adresse IPv4

L'adresse IPv4 est sur 4 octets, soit 32 bits (1 octet équivaut à 8 bits).

Chaque adresse IP comporte deux parties :

- l'adresse réseau ;
- un numéro d'hôte correspondant à l'adresse de la machine elle-même.

Supposons un réseau constitué de trois machines, dont les adresses sont respectivement 145.41.12.1, 145.41.12.2 et 145.41.12.3. L'adresse réseau est en ce cas 145.41.12.x, 1, 2 et 3 correspondant aux adresses hôtes des machines.

Avec un tel plan d'adressage, le réseau peut connecter des machines ayant des adresses comprises entre 145.41.12.1 et 145.41.12.254. 145.41.12.255 est une adresse réservée, appelée adresse de broadcast ou adresse de diffusion, qui permet d'envoyer une information à toutes les stations du réseau. Un tel plan d'adressage n'offre que peu de possibilités en terme de connectivité au réseau, puisqu'il n'adresse que 254 machines potentielles.

Selon la taille de l'adresse réseau, le nombre de réseaux et donc le nombre d'hôtes associés peuvent être différents. Des classes d'adresses ont été définies pour tenir compte de cette différence.

Les classes d'adresses

Dans IPv4, les cinq classes d'adresses récapitulées au tableau 9.3 ont été définies.

Tableau 9.3 Classes d'adresses IPv4

Adresse	Plage d'adresses	Nombre de réseaux	Nombre d'hôtes par réseau
Classe A	1.0.0.0 à 126.0.0.0	126	16 777 214
Classe B	128.0.0.0 à 191.255.0.0	16 384	65 534
Classe C	192.0.0.0 à 223.255.255.0	2 097 152	254
Classe D	224.0.0.0 à 225.0.0.0	Adresses de groupes (multicast)	
Classe E	225.0.0.0 à 240.0.0.0	Expérimental	

Ces classes d'adresses principales sont définies en fonction du nombre d'octet utilisé pour l'adresse réseau :

- Pour les adresses de classe A, le premier octet (8 bits) est réservé pour l'adresse réseau avec le premier bit à zéro. Ainsi, l'adresse réseau est comprise entre 0000000 et 0111111 en format binaire. Sachant que les adresses 0.0.0.0. et 127.0.0.0 sont réservées, il y a donc $2^7 - 2$, soit 126 adresses réseau de classe A disponibles, allant de 1.0.0.0 à 126.0.0.0.
- Le nombre d'hôtes est défini sur 3 octets (24 bits). L'adresse de diffusion (x.x.x.255) et l'adresse x.x.x.0 étant réservées, cela donne $2^{24} - 2$, soit 16 777 214 hôtes possibles par adresse réseau de classe A.
- Pour les adresses de classe B, les deux premiers octets (16 bits) sont utilisés pour définir l'adresse réseau avec les deux premiers bits à 1 et 0. Il existe donc $2^{14} - 2$, soit 16 384 adresses réseau de classe B disponibles, allant de 128.0.0.0 à 191.255.0.0.
- Le nombre d'hôtes par adresse réseau est défini sur 2 octets. Comme pour les adresses de classe A, l'adresse de diffusion et l'adresse x.x.x.0 étant réservées, il y a donc $2^{16} - 2$, soit 65 534 hôtes possibles par adresse réseau de classe B.

- Pour les adresses de classe C, les trois premiers octets (24 bits) sont utilisés avec les trois premiers bits à 1,1 et 0, ce qui donne $2^{21} - 2$, soit 2 097 152 adresses réseau de classe C disponibles, allant de 192.0.0.0 à 223.255.255.0.

- Le nombre d'hôtes est défini sur un octet (8 bits). De même, l'adresse de diffusion et l'adresse x.x.x.0 étant réservées, il y a $2^8 - 2$, soit 254 hôtes par adresse réseau de classe C.

Les adresses de classes C et D sont réservées pour un adressage multicast expérimental.

L'affectation des adresses IP n'est pas automatique, et l'on ne peut pas affecter n'importe quelle plage d'adresses à un réseau. C'est l'IANA (Internet Assigned Numbers Agency) qui est en charge de fournir ces adresses à tout demandeur. Il faut toutefois remarquer que toutes les adresses de classes A et B disponibles sont déjà allouées.

Les adresses IP sont des adresses routables. Cela signifie qu'elles ne peuvent être utilisées pour un usage privé.

Afin d'éviter une utilisation abusive de l'adressage IP, l'IANA a réservé pour un usage strictement privé les trois plages d'adresses suivantes sur les trois principales classes :

- Classe A : 10.0.0.1 à 10.255.255.254

- Classe B : 172.16.0.1 à 172.63.255.254

- Classe C : 192.168.0.0 à 192.168.255.254

Pour se connecter à un réseau ayant un plan d'adressage différent ou à Internet, chaque station possédant une adresse IP privée doit spécifier une adresse de passerelle par défaut. Cette adresse correspond à une station qui prend en charge le routage du réseau et permet l'envoi comme la réception de requêtes d'un milieu non routable (réseau privé) vers un milieu routable (Internet).

Dans le cas d'un partage de connexion Internet par le biais d'une passerelle, c'est cette dernière qui a la charge d'envoyer les requêtes d'un environnement privé, donc non routable, vers Internet, environnement routable. L'adresse de la passerelle par défaut est dans ce cas l'adresse IP de la passerelle.

Masque de sous-réseau

Le masque permet, par une soustraction binaire entre ce dernier et l'adresse IP d'une machine, de connaître l'adresse réseau de cette machine.

Si l'adresse IP d'une machine est 192.168.0.1 et qu'on lui applique le masque 255.255.255.0, la soustraction binaire de ces deux adresses donne 192.0.0.0, soit l'adresse réseau.

De manière générale, les adresses de classe A ont pour masque 255.0.0.0, les adresses de classe B 255.255.0.0 et celles de classe C 255.255.255.0.

Lors de la configuration du masque de deux machines, si l'une a pour adresse IP 192.168.1.1, avec comme masque 255.255.255.0, et la seconde 192.168.1.10, avec comme masque 255.225.0.0, leurs adresses réseau (192.168.0.x et 192.168.1.x) ne sont pas identiques. Elles n'appartiennent donc pas au même réseau et ne peuvent communiquer entre elles.

DNS (Domain Name Service)

Le DNS est une structure hiérarchique composée d'un ensemble de serveurs permettant d'associer une adresse IP à un nom de domaine constitué d'un nom d'organisation (par exemple Google) et d'une classification (.fr, .com, etc.).

Il est de la sorte beaucoup plus facile de retenir des adresses de site Web, de messagerie ou encore FTP plutôt que leur adresse IP associée.

Il est toujours possible de connaître l'adresse IP d'un serveur particulier ou d'un site Web. Par exemple, un simple ping vers le site Web *www.google.fr* permet de connaître l'adresse IP de ce site, comme l'illustre la figure 9.46.

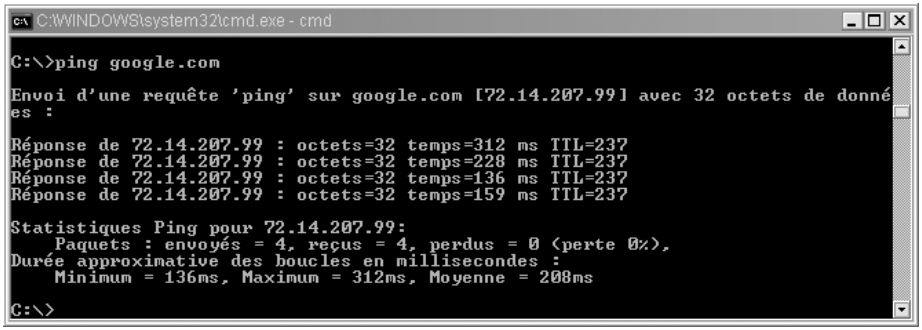


Figure 9.46
Adresse IP de www.google.fr

Généralement, deux adresses de serveur DNS sont demandées lors de la configuration des paramètres réseau afin de permettre d'accéder au réseau au cas où une panne surgisse sur un serveur. Les adresses DNS sont nécessairement des adresses IP.

Configuration des paramètres réseau sous Windows XP

Dans le Panneau de configuration, sélectionnez Réseau, puis, dans la zone des composants réseau, choisissez le composant TCP/IP de votre carte Wi-Fi, et cliquez sur Propriétés pour ouvrir la boîte de dialogue illustrée à la figure 9.47.

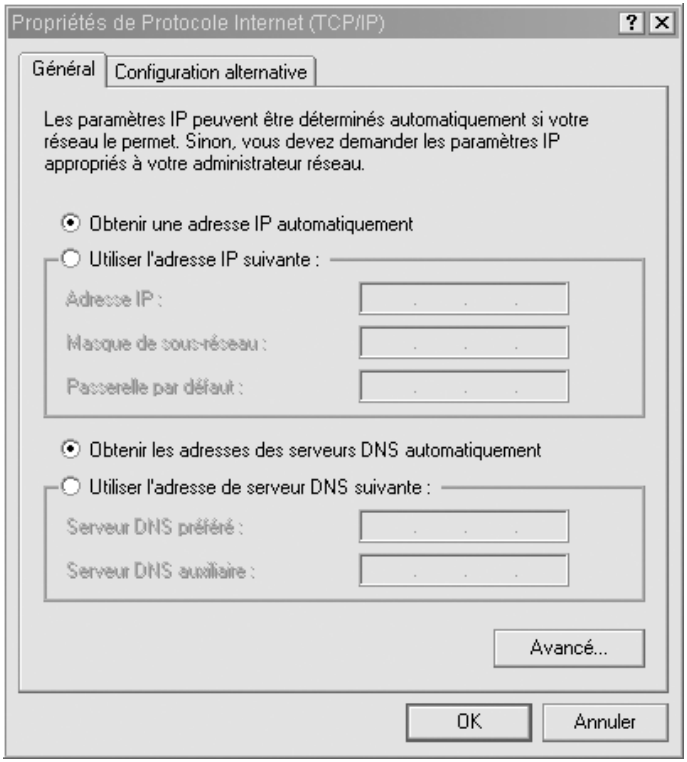


Figure 9.47
Paramétrage des propriétés TCP/IP de la carte

Renseignez les différents champs proposés en vous aidant le cas échéant des informations données par votre fournisseur d'accès :

- adresse IP correspondant à l'adresse IP de la machine ;
- masque de sous-réseau permettant de connaître l'adresse réseau et l'adresse de sous-réseau de l'adresse IP précédente ;
- passerelle par défaut correspondant à l'adresse de la machine du réseau connectée à Internet ;
- adresses DNS, généralement fournies par le FAI ou l'administrateur réseau.

Pour les versions de Windows autres que Windows 2000 et XP, un redémarrage est indispensable.

Dans le cas de Windows 2000 ou XP, l'activation des paramètres réseau définis par l'utilisateur peut prendre un temps de l'ordre d'une dizaine de secondes.

Configuration des paramètres réseau sous Linux

Pour configurer l'adresse IP et le masque de sous-réseau de la carte, saisissez dans un shell :

```
# ifconfig eth0 10.0.0.2 netmask 255.255.255.0
```

Pour configurer l'adresse de la passerelle (ici 10.0.0.1), entrez :

```
# route add default gw 10.0.0.1
```

La commande `route` permet de vérifier si l'adresse de la passerelle a bien été ajoutée dans la table de routage :

```
# route
Kernel IP Routing Table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
Default         10.0.0.1        0.0.0.0         UG    0      0        0 eth0
```

Pour configurer l'adresse du ou des serveurs de noms (DNS), il suffit d'éditer à l'aide de la commande `vi` le fichier `resolv.conf` se trouvant dans le répertoire `/etc` :

```
# vi/etc/resolv.conf
```

Voici un exemple pour le fichier `resolv.conf` :

```
nameserver adresse_IP_DNS
domain nom_de_domaine
```

`nameserver` permet de définir l'adresse du DNS primaire, tandis que `domain` définit le nom de domaine du réseau, si celui-ci possède un domaine. Tout comme les adresses DNS, le nom de domaine est fourni par le FAI. S'il existe plusieurs adresses DNS, il suffit d'ajouter une ligne avec `nameserver adress_IP_DNS` pour chaque adresse DNS supplémentaire.

Cette configuration peut aussi se faire de manière semi-automatique en configurant le fichier `/etc/pcmcia/network.opts` dans le cas où la carte réseau est une carte PCMCIA ou le fichier `/etc/network/interfaces` pour une carte PCI ou Mini-PCI.

10

CPL domestique

Malgré le coût encore relativement élevé des équipements CPL, de plus en plus de particuliers sont tentés par l'installation d'un réseau domestique sur courant porteur. L'absence de câbles à poser semble être le facteur déterminant d'un tel choix.

Il est vrai que l'installation d'un réseau CPL dans une maison ou dans un appartement est des plus simple. Il suffit de brancher les équipements CPL sur le réseau électrique et de les configurer. L'idéal est de disposer d'une connexion Internet *via* un modem ADSL, câble, satellite ou même 56 K, qu'il suffit de raccorder à un équipement CPL faisant office de passerelle pour fournir un accès Internet à toutes les prises électriques du réseau électrique.

De nouvelles offres d'accès Internet sont proposées par les opérateurs au moyen de deux boîtiers : un modem ADSL, qui se connecte à la prise téléphonique France Télécom, et un boîtier décodeur vidéo, qui reçoit le flux vidéo IP d'Internet et le diffuse vers une TV ou un écran HDTV. Certains FAI ajoutent à ces boîtiers deux équipements CPL pour les relier. Cette tendance va s'accentuer avec le développement des services de vidéo sur IP en HD (haute définition) pour les clients domestiques, qui permettront de diffuser les flux vidéo vers les différents écrans TV de l'habitation. Les CPL sont une des meilleures solutions pour diffuser ces flux IP, que ce soit en terme de débit ou de zone de couverture du signal.

La topologie d'un réseau domestique CPL peut varier en fonction des besoins et des architectures du réseau électrique, ainsi que des équipements choisis et du mode de fonctionnement réseau utilisé.

La figure 10.1 illustre un réseau domestique CPL dans lequel l'équipement CPL est connecté à Internet par le biais d'un modem, permettant le partage de la connexion.

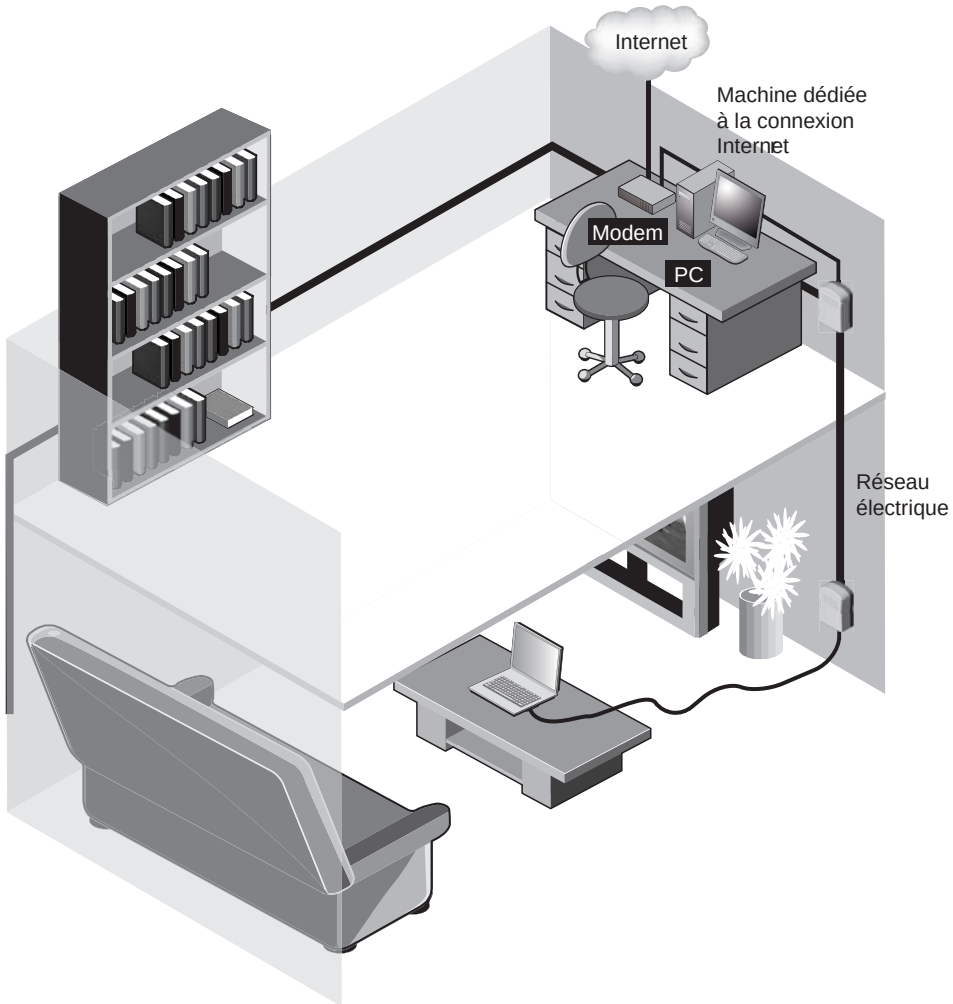


Figure 10.1
Réseau domestique CPL avec partage de la connexion Internet

Ce chapitre traite de la manière optimale d'installer un réseau CPL domestique, depuis le choix des équipements jusqu'à leur installation et leur configuration. L'installation d'un réseau domestique n'est pas une tâche très ardue, mais elle requiert de respecter certaines règles, concernant notamment le réseau électrique et la sécurité.

Sécurité électrique

La technologie CPL utilise comme support de communication le réseau électrique BT 220 V/50 Hz. Ce réseau présentant des dangers réels pour la sécurité des personnes, il est important de respecter quelques règles élémentaires de sécurité afin d'éviter tout risque d'électrocution.

La figure 10.2 illustre un panneau caractéristique symbolisant le risque électrique.

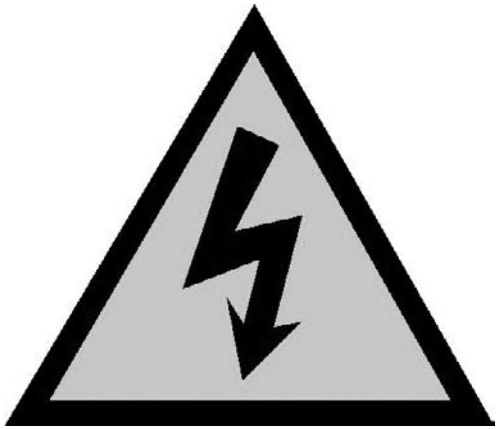


Figure 10.2
Panneau symbolisant le risque électrique

Les principales règles de sécurité électrique à respecter sont les suivantes :

- installer un disjoncteur différentiel 500 mA pour se protéger de tout court-circuit ;
- protéger les prises électriques par un disjoncteur ou un fusible ne dépassant pas 16 A ;
- ne pas exposer les équipements au soleil ou à la chaleur ;
- ne pas nettoyer les équipements à l'aide de détergents ou d'aérosols ;
- ne pas démonter les équipements sans les débrancher et attendre quelques minutes le déchargement des composants électroniques ;
- ne pas installer d'équipement à proximité d'arrivées d'eau (baignoire, douche, machine à laver, lavabo, piscine, etc.) ;
- ne pas surcharger les multiprises ou les rallonges afin de ne pas augmenter les risques d'électrocution ou d'incendie ;

- respecter les modes d'utilisation des équipements CPL ;
- ne pas tenter de mettre en place des systèmes d'injecteurs CPL sur les câbles électriques sans l'aide d'un électricien habilité.

En cas de doute sur l'une quelconque de ces règles ou concernant l'état du réseau électrique sur lequel on souhaite installer le réseau CPL, il est conseillé de s'adresser à un électricien professionnel ou à un spécialiste CPL.

Choix de la technologie CPL

Comme nous l'avons vu au cours des chapitres précédents, il existe plusieurs technologies et spécifications CPL dans la mesure où aucun standard IEEE n'est encore disponible. Même si elles partagent certaines fonctionnalités communes, ces spécifications présentent des caractéristiques différentes. Seul le consortium HomePlug se présente comme un standard CPL de fait, puisque la très grande majorité des équipements disponibles dans le commerce répondent à cette spécification.

Le tableau 10.1 récapitule les critères de choix des différentes technologies CPL disponibles actuellement.

Tableau 10.1 Éléments de choix des technologies CPL

Technologie CPL		Utilisation privilégiée et champ d'application
HomePlug	1.0, Turbo, AV	Réseaux domestiques, diffusion d'Internet, flux vidéo IP (HomePlug AV), diffusion audio
	Oxance	Réseaux professionnels, applications industrielles, qualité de service améliorée
	BPL	CPL pour les réseaux électriques MT (moyenne tension) des collectivités locales
DS2		Réseaux professionnels, réseaux domestiques haut débit (voix, données, vidéo IP haute définition)
Spidcom		Réseaux professionnels, applications industrielles, CPL pour le véhicule
Main.net		CPL pour les réseaux électriques des collectivités locales

Choix du matériel

Les prix des produits HomePlug 1.0 ont beaucoup baissé depuis l'arrivée des produits HomePlug Turbo, qui proposent des débits en accord avec les besoins actuels des applications. L'arrivée prochaine des équipements HomePlug AV devrait entraîner à son tour une baisse des prix des équipements HomePlug 1.0 et Turbo.

Pour les besoins des applications actuelles (diffusion des flux Internet voix, données et IPTV dans l'habitation), les équipements HomePlug Turbo semblent répondre au meilleur ratio débit/budget attendu des utilisateurs domestiques.

Les demandes grandissantes de débit des applications réseau, que ce soit entre terminaux d'une installation domestique (jeux en réseau, diffusion de flux de données, voix, vidéo entre serveurs multimédias et postes de réception ou de visualisation) ou pour recevoir de tout endroit d'une installation les services proposés par les opérateurs d'accès à Internet, nécessite des équipements dont le débit se situe autour de 200 Mbit/s au niveau de la couche physique, ce qui est le cas des équipements HomePlug AV.

Dans la mesure où les équipements HomePlug sont tous compatibles entre eux, il y aura pendant un certain temps coexistence des différents produits HomePlug adaptés aux utilisations suivantes :

- HomePlug 1.0 : navigation Web, messagerie électronique ;
- HomePlug Turbo : Internet, téléphonie IP, données (échange de fichiers volumineux), images (IPTV ou vidéo à la demande en MPEG-2 ou MPEG-4) ;
- HomePlug AV : vidéo HD numérique au format IP (MPEG-2 haute définition, par exemple) diffusées vers plusieurs postes de visualisation.

Placement des équipements sur le réseau électrique

Pour obtenir une qualité réseau et des performances permettant la diffusion des flux Internet (voix, données, IPTV), il est important de placer au mieux les équipements CPL sur le réseau électrique en fonction des critères suivants :

- topologie du réseau électrique de l'installation ;
- place des PC et terminaux IP censés être connectés aux flux en provenance du modem Internet.

La place idéale des équipements CPL est la suivante :

- Près du tableau électrique depuis lequel partent les différents câbles électriques qui alimentent les prises, les équipements électriques et les lumières de l'habitation.
- Près du modem Internet connecté au réseau RTC (réseau téléphonique commuté) public sur la prise téléphonique.

La figure 10.3 illustre un schéma électrique classique d'installation domestique avec accès à Internet. Les équipements CPL sont placés sur les prises électriques situées à proximité de la prise téléphonique qui connecte l'habitation à Internet.

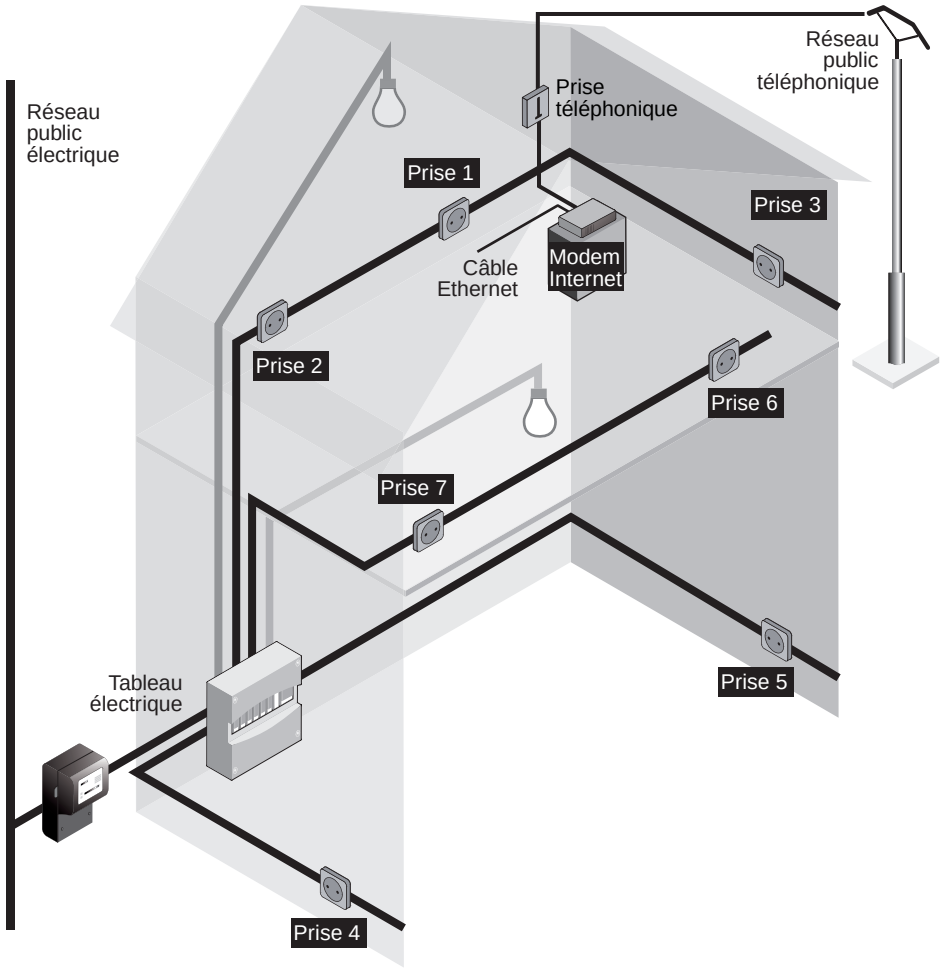


Figure 10.3
Schéma électrique classique d'une installation domestique avec accès à Internet

Dans une telle installation, il est possible d'utiliser trois équipements CPL pour recevoir le flux Internet avec une bonne couverture :

- Un équipement CPL passerelle connecté à la prise Ethernet du modem Internet et à la prise électrique Prise 1.
- Un équipement CPL pour PC fixe (Prise 3), qui peut se trouver sur le même câble électrique.
- Un équipement CPL pour PC portable (Prise 5 ou 6), qui peut être placé à un étage différent afin d'offrir la mobilité à l'installation domestique.

En milieu domestique, cette configuration réseau à trois équipements est la plus répandue. De plus en plus de foyers sont équipés d'au moins deux PC et d'une connexion Internet haut débit de type InternetBox.

La figure 10.4 illustre ce même réseau domestique avec tous les équipements en place pour la diffusion des différents flux Internet vers les prises du réseau électrique.

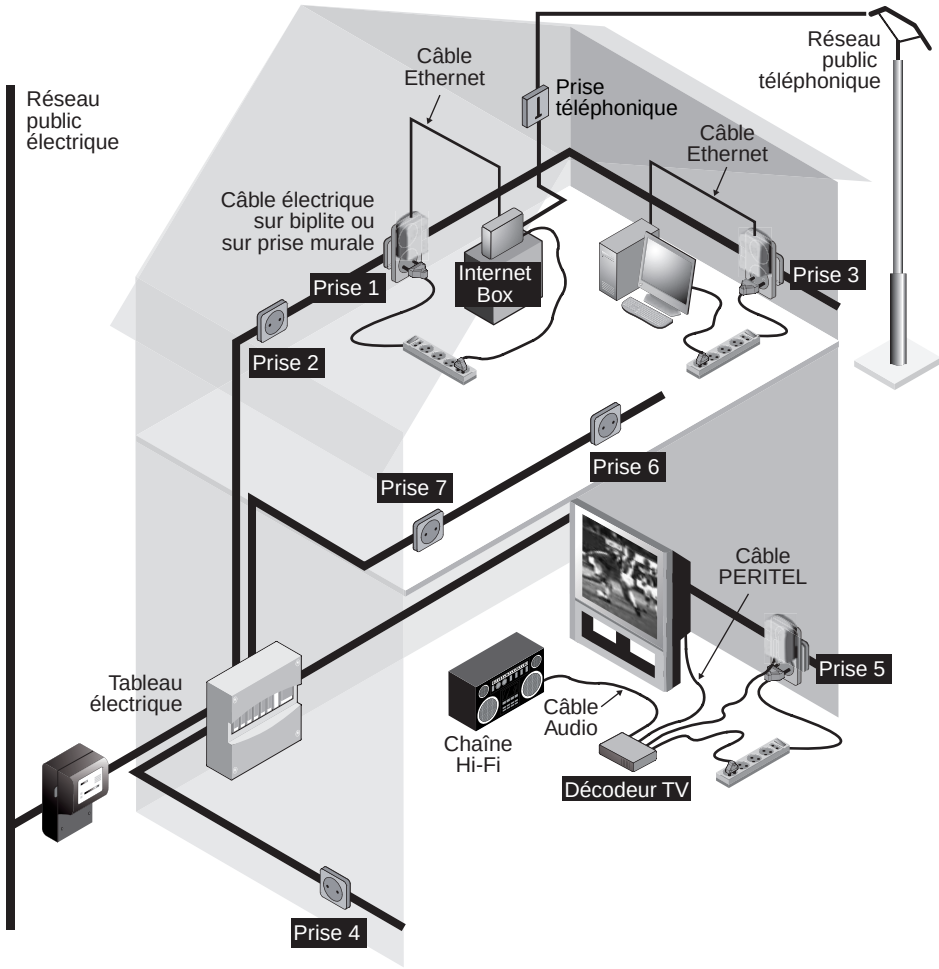


Figure 10.4

Place des équipements CPL dans l'installation domestique

L'équipement CPL positionné sur la prise 3 permet à l'ordinateur de se connecter à Internet *via* les prises électriques (Prise 3 vers Prise 1). Il est donc important de trouver le bon compromis entre le débit souhaité, la position du PC dans l'habitation et la qualité des liens de communications CPL entre Prise 3 et Prise 1.

Avec des équipements HomePlug Turbo, il convient de trouver, à l'aide d'outils de configuration CPL, tels que l'outil Configuration_CPL d'Oxance décrit au chapitre 9, une prise électrique dont le débit se situe entre 12 et 75 Mbit/s, ce qui est généralement le cas des prises situées à un même étage dans des pièces adjacentes.

L'équipement CPL positionné sur la prise 5 permet au décodeur TV de se connecter à l'InternetBox *via* le réseau électrique et de récupérer les flux vidéo provenant de la connexion Internet. Ces flux vidéo demandent au minimum 1 Mbit/s de débit utile stable pour que l'affichage TV soit fluide. Il est important de ne pas trop dégrader le signal vidéo sur le réseau électrique, au risque de perdre des images. Cette contrainte suppose que le lien de communication CPL entre Prise 5 et Prise 1 offre un débit utile de 1,5 Mbit/s. Il est possible de vérifier ce débit au moyen d'un outil de configuration CPL. L'équipement concerné doit être directement branché sur une prise murale ou sur une biplite, mais pas sur une multiprise.

Le tableau 10.2 recense, pour un équipement HomePlug Turbo, les correspondances entre les débits affichés par l'outil de configuration et les débits utiles disponibles pour les applications du réseau IP qui s'appuient sur le réseau CPL. Au vu de ce tableau, il est important de trouver une prise 5 qui donne au minimum un débit affiché de 10 Mbit/s.

Tableau 10.2 Débits CPL HomePlug Turbo affiché et utile

Débit affiché (Mbit/s)	Débit utile (Mbit/s)
85	12,5
75	11,8
55	9,42
45	8,79
35	8,23
25	7
14	4,5
12,83	3,5
11	3,2
10,16	2,9
8,36	2,4
6,35	2
4,04	1,22
3	0,89
1	0,33
0,9 (mode ROBO)	0,2

Il est également possible de diffuser sur le réseau électrique le flux de téléphonie analogique provenant de la connexion Internet et disponible sur la prise RJ-11 de l'InternetBox connectée à la prise téléphonique.

Les équipements CPL Wingoline de Niroda, par exemple, fonctionnent dans la bande de fréquences de 3,3 à 8,2 MHz, selon un protocole de communication propriétaire différent de celui des équipements HomePlug. Le réseau CPL créé par les équipements Niroda n'est donc pas interopérable avec un réseau CPL HomePlug. Il est possible de placer jusqu'à 24 équipements CPL Niroda sur le même réseau électrique pour déporter des lignes téléphoniques analogiques.

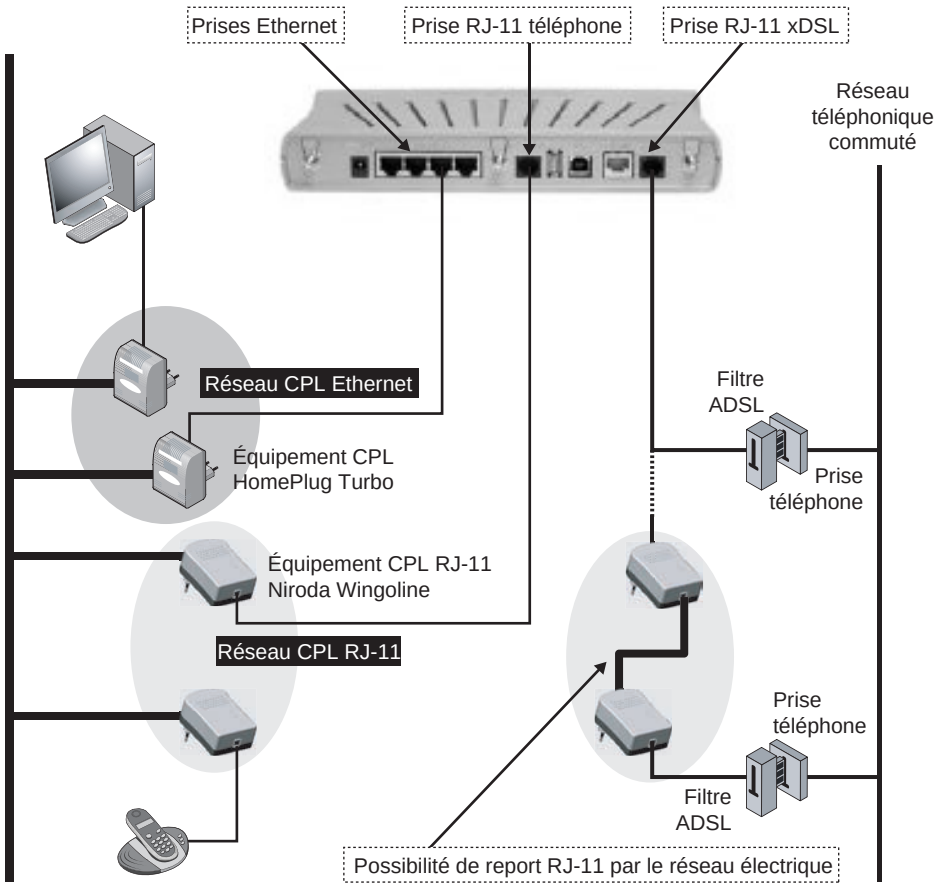


Figure 10.5

Réseaux CPL différents connectés à une InternetBox

La figure 10.5 illustre les connectivités possibles depuis l'InternetBox fournie par le FAI avec les réseaux CPL suivants :

- Réseau CPL Ethernet HomePlug, qui permet de connecter les terminaux IP de l'habitation aux prises Ethernet de l'InternetBox.

- Réseau CPL RJ-11, qui permet de connecter les équipements téléphoniques analogiques sur la prise téléphonique de l'InternetBox.
- Réseau CPL RJ-11, qui permet de connecter l'InternetBox à la prise téléphonique France Télécom à travers le réseau électrique de l'habitation.

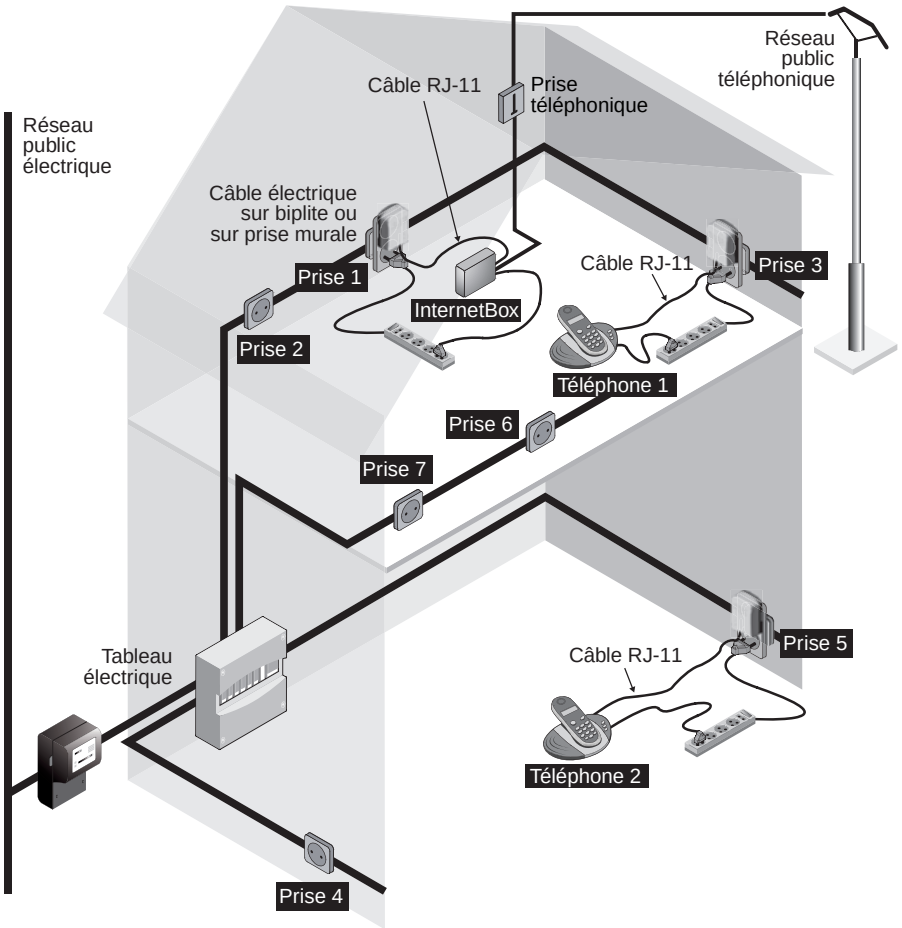


Figure 10.6

Place des équipements permettant de diffuser la téléphonie IP sur le réseau électrique domestique

Les équipements Niroda suivants du réseau CPL RJ-11 peuvent être placés comme indiqué à la figure 10.6 :

- InternetBox connectée au réseau électrique sur la prise 1 *via* son connecteur téléphonique RJ-11 ;
- téléphone 1 connecté sur la prise 6 par le biais d'un équipement Niroda au réseau CPL « téléphonique » ;

- téléphone 2 connecté sur la prise 5 de la même manière.

Les débits nécessaires à la téléphonie étant de l'ordre de 20 Kbit/s, il est tout à fait réaliste de l'envisager sur l'installation électrique d'une habitation de taille moyenne (trois ou quatre pièces).

La figure 10.7 illustre les flux ou signaux suivants, qui circulent sur les réseaux électriques et téléphoniques de l'installation domestique :

- signal téléphonique analogique entre les téléphones et la connectique RJ-11 de l'InternetBox ;
- flux de données IP provenant de la connexion Internet ADSL.

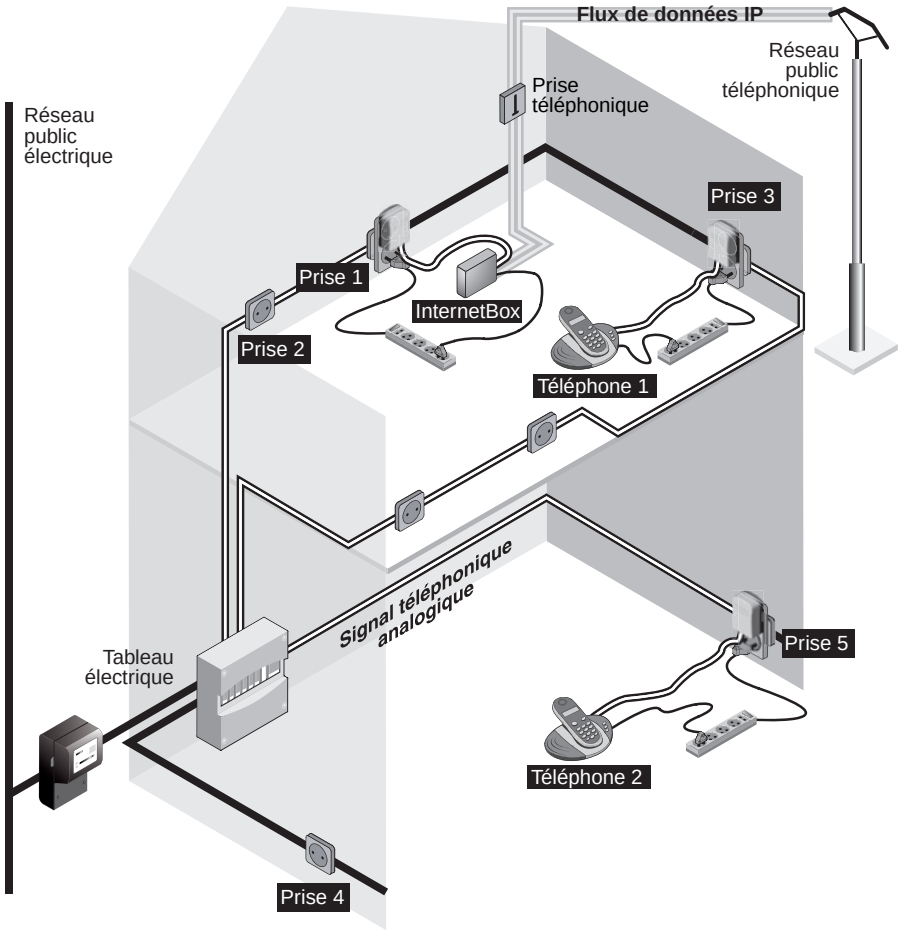


Figure 10.7

Diffusion du signal téléphonique analogique sur le réseau électrique domestique

Paramétrage de la sécurité

Même dans un cadre domestique, la sécurisation d'un réseau CPL est une étape importante. L'utilisation des câbles électriques implique que le réseau arrose une zone de couverture plus ou moins large, pouvant s'étendre au-delà du périmètre du domicile. Cela permet à quiconque d'accéder au réseau et, par exemple, d'en utiliser la connexion Internet.

Les réseaux CPL offrent des mécanismes de sécurité susceptibles de prévenir l'écoute clandestine par une gestion des mots de passe adéquate.

Pour sécuriser le réseau de manière encore plus fiable, d'autres solutions existent, à base de pare-feu, de serveur d'authentification et de réseau privé virtuel.

Configuration de la passerelle CPL

La notion de passerelle peut paraître ambiguë puisqu'il existe potentiellement plusieurs passerelles dans un même réseau, déterminées par les éléments suivants :

- La passerelle Internet, modem ou InternetBox, qui permet de connecter l'habitation domestique au réseau Internet, généralement par le biais de la prise téléphonique, avec une connexion xDSL.
- La passerelle Ethernet, qui permet de connecter le modem, un routeur ou l'InternetBox au réseau local et de configurer les paramètres de sécurité que nous détaillons dans les sections suivantes.
- La passerelle CPL, qui permet de connecter la passerelle Internet au réseau électrique et de diffuser dans tout le réseau les flux IP provenant d'Internet.

La figure 10.8 illustre la place de ces différents types de passerelles dans une installation domestique.

Pour un équipement HomePlug Turbo, la passerelle CPL ne nécessite pas de configuration spécifique par rapport aux autres équipements CPL du réseau puisque HomePlug Turbo fonctionne en mode pair-à-pair. La spécificité de la passerelle CPL vient du fait que cet équipement est connecté à la passerelle Internet et que tous les flux IP sortants vers Internet passent par cet équipement.

Le seul paramètre HomePlug Turbo à configurer de manière spécifique sur la passerelle CPL est la priorité (paramètres CA0, CA1, CA2 et CA3 précisant quatre niveaux de priorités). Le tableau 10.2 récapitule les caractéristiques de ces niveaux de priorité pour HomePlug 1.0 et Turbo.

Tableau 10.3 Niveaux de priorité des trafics de données pour la passerelle CPL

Priorité pour le traffic de données	Priorité HomePlug 1.0 et Turbo	
0	CA0	Priorité basse
1		
2	CA1	
3		

Tableau 10.3 Niveaux de priorité des trafics de données pour la passerelle CPL *(suite)*

Priorité pour le traffic de données	Priorité HomePlug 1.0 et Turbo	
4	CA2	Priorité haute
5		
6	CA3	
7 (plus prioritaire)		

Ces huit classes de priorités sont héritées de la description des classes du standard IEEE 802.1D en simplifiant les huit classes 802.1D en quatre classes CPL.

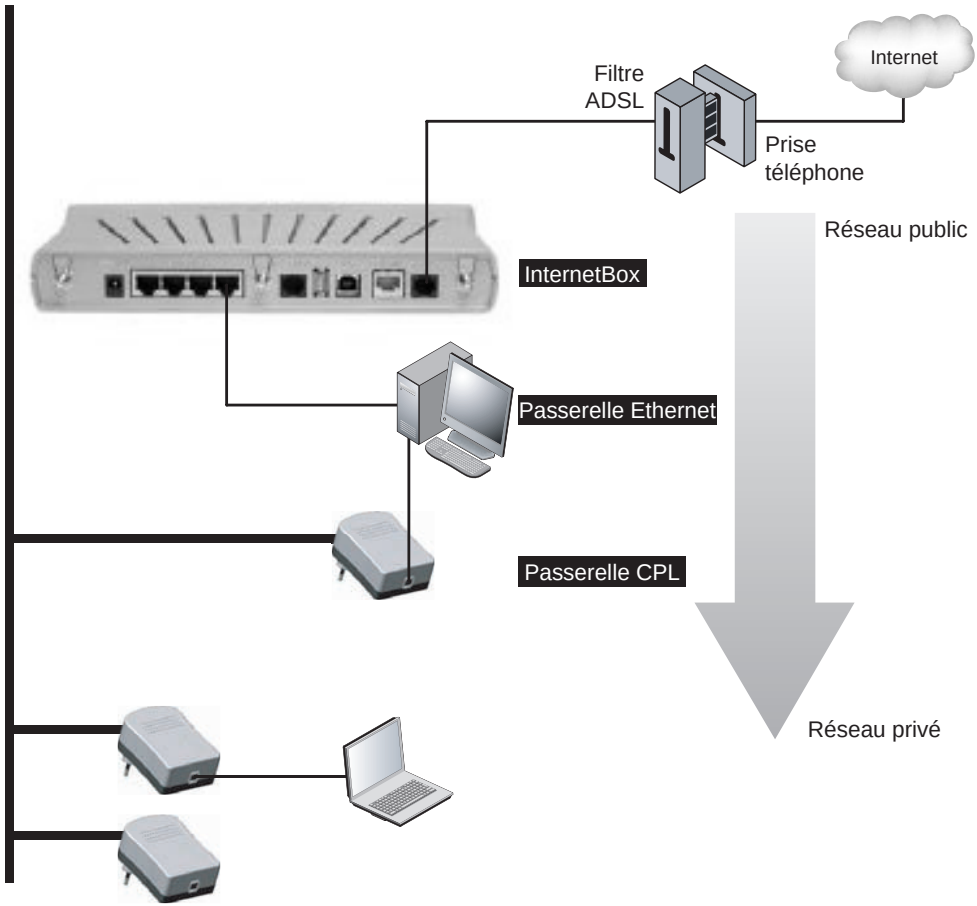


Figure 10.8
Emplacement des différentes passerelles depuis le réseau public vers le réseau privé

Pour configurer les valeurs des paramètres de priorité CA sur la passerelle CPL, il suffit de placer la valeur à CA3 afin de permettre une priorisation des trafics entrants et sortants de l'équipement CPL, cet équipement pouvant constituer le goulet d'étranglement du réseau CPL.

Dans la mesure où les outils de configuration CPL ne permettent pas de configurer ce paramètre, j'ai développé un outil spécifique pour système d'exploitation Windows, qui se lance en exécutable. Ce programme est disponible à l'adresse *http://carcelle.fu8.com/ConfigurationPrioriteCPL.zip.*

Il est nécessaire d'avoir installé au préalable l'outil WinPCap, qui permet de gérer les entrées/sorties sur la carte réseau. Cet outil est généralement préinstallé par les outils de configuration CPL. Si ce n'était pas le cas, il est possible de le télécharger à l'adresse *http://www.winpcap.org/install/bin/WinPcap_3_1.exe.*

Une fois l'outil WinPCap téléchargé et installé, il suffit de procéder de la façon suivante pour installer l'outil ConfigurationPrioritéCPL :

1. Téléchargez le fichier **ConfigurationPrioriteCPL.zip,** puis décompressez-le dans un répertoire local.
2. Lancez l'outil en double-cliquant sur le fichier **ConfigurationPrioritéCPL.exe.**

Une fois l'outil lancé, une fenêtre DOS propose le choix d'une des priorités 0(CA0), 1(CA1), 2(CA2), 3(CA3), comme l'illustre la figure 10.9.

Figure 10.9

Lancement de l'outil de configuration des priorités CPL

Une fois le choix de la priorité effectué, l'outil propose de choisir la carte réseau Ethernet du PC connecté à l'équipement CPL localement. L'information des adresses IP permet

de reconnaître la bonne carte réseau. Dans le cas de la figure 10.10, la carte connectée à la passerelle CPL est la carte 3, qui dispose de l'adresse IP 192.168.0.10.

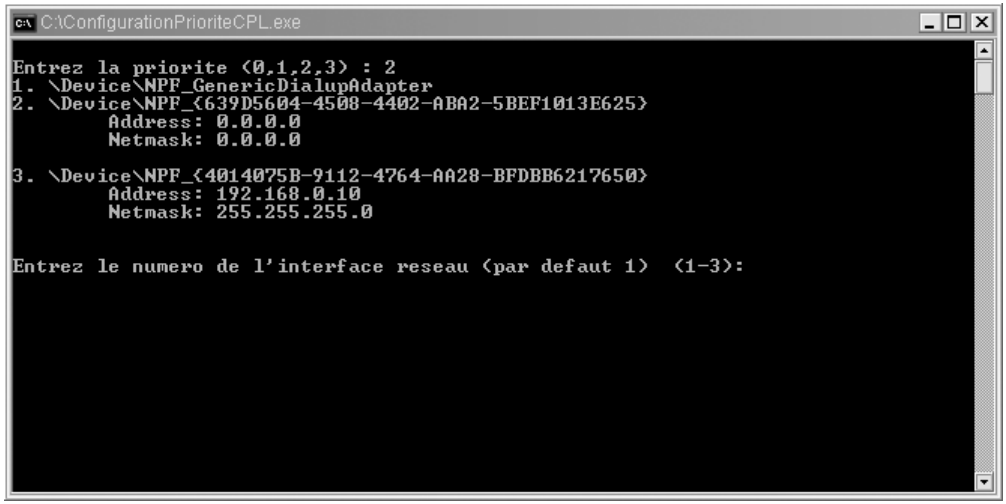


Figure 10.10

Configuration de la carte Ethernet connectée à l'équipement CPL

Une fois le choix de la carte réseau effectué, la fenêtre DOS se referme, indiquant que la configuration de la priorité est terminée.

Il est important de repérer l'équipement CPL qui dispose de la priorité supérieure et de le maintenir connecté à la passerelle Internet ou à l'InternetBox.

Configuration de la sécurité CPL

La configuration de la sécurité CPL est une partie importante de la mise en place du réseau CPL, qui permet de sécuriser les échanges de données entre les équipements CPL du réseau électrique. Le signal CPL se propageant au-delà de la limite du compteur électrique de l'habitation, toute personne malveillante peut intercepter les données, pour peu que les équipements CPL soient simplement configurés avec les paramètres par défaut de la clé réseau NEK.

La configuration de la sécurité permet en outre de mettre en place plusieurs réseaux CPL sur le même réseau électrique en configurant différentes clés réseau NEK sur les équipements HomePlug connectés.

Comme nous l'avons vu au chapitre 9, dédié à la configuration des équipements CPL HomePlug, la clé NEK (Network Encryption Key) doit être configurée sur tous les équipements CPL à installer grâce à des outils de configuration tels que Configuration_CPL d'Oxance.

Cet outil (disponible à l'adresse *http://www.oxance.com/download/Install-Config/Install_Config_CPL.exe*) permet de configurer la clé NEK sur les différents équipements CPL. Il suffit pour cela de connecter un à un les équipements CPL au PC sur lequel est installé l'outil de configuration par le biais d'un câble réseau (Ethernet ou USB, selon les modèles d'équipements CPL).

Une fois l'équipement connecté au PC, l'outil de configuration se lance *via* le menu Démarrer. La fenêtre illustrée à la figure 10.11 s'ouvre alors. L'équipement connecté localement au PC est décrit dans le volet « Produit(s) connecté(s) à votre ordinateur » de l'onglet Produits (il s'agit sur la figure d'un équipement CPL HomePlug Turbo à 85 Mbit/s).

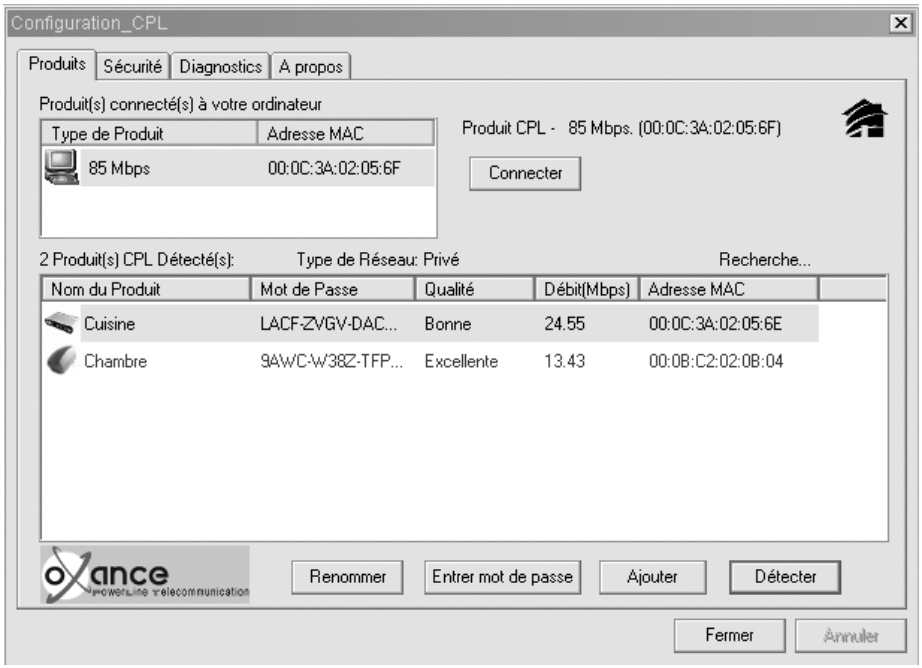


Figure 10.11
Onglet Produits de l'outil de configuration CPL d'Oxance

L'onglet Sécurité permet de modifier la clé réseau, placée par défaut à la valeur **HomePlug,** et de lui attribuer une valeur spécifique pour le réseau de l'installation domestique.

Cette clé doit comporter entre 4 et 24 caractères et inclure si possible des chiffres et des lettres (minuscules et majuscules), par exemple **Mot2Passe.** Il suffit de cliquer sur « Seulement le produit local » pour configurer l'équipement local.

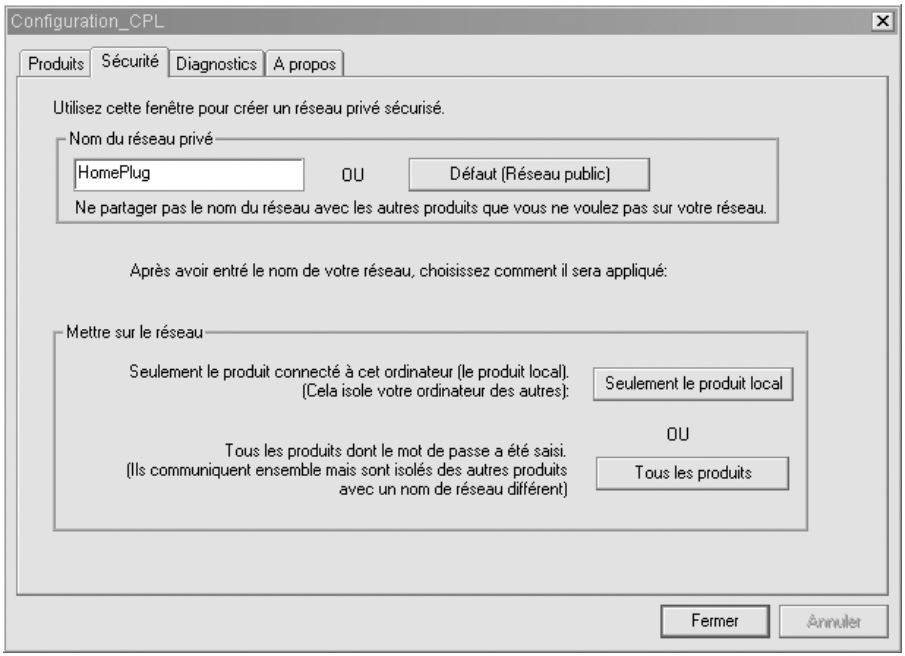


Figure 10.12

Configuration de la clé NEK dans l'onglet Sécurité

Pour effectuer la même opération sur tous les équipements CPL, il suffit de les connecter au PC de configuration.

Une fois tous les équipements CPL correctement configurés, l'onglet Produits permet de vérifier que tous les équipements CPL sont vus de la passerelle CPL.

La figure 10.13 illustre un réseau CPL avec trois équipements CPL et les liens CPL suivants :

- équipement MAC=00-0C-3A-02-05-6F vers équipement Cuisine : qualité « bonne », avec un débit affiché de 24,55 Mbit/s ;
- équipement MAC=00-0C-3A-02-05-6F vers équipement Chambre (HomePlug 1.0) : qualité « excellente », avec un débit affiché de 13,43 Mbit/s.

La sécurité du réseau CPL étant configurée, il est possible de configurer la sécurité des terminaux eux-mêmes.

Nombre maximal d'équipements CPL sur un même réseau

Les spécifications HomePlug 1.0 et Turbo précisent qu'un réseau CPL ayant une même clé réseau peut disposer au maximum de 15 équipements. Étant donné qu'il n'est pas possible, avec les équipements HomePlug 1.0 et Turbo, de configurer plusieurs clés réseau NEK, un équipement ne peut appartenir qu'à un seul réseau CPL à la fois. Ce problème est résolu avec le standard HomePlug AV, qui permet différentes configurations réseau et plusieurs clés réseau pour un même équipement.

Tests de fonctionnement CPL

Une fois les configurations effectuées sur les différents équipements CPL du réseau, il est recommandé de vérifier le bon fonctionnement des liens réseau de l'installation domestique en effectuant un test avec l'outil de configuration CPL (onglet Produits).

Pour tester le bon fonctionnement du réseau CPL, il peut en outre être utile de lancer des commandes ping depuis les PC connectés au réseau CPL vers l'InternetBox, comme illustré à la figure 10.13.

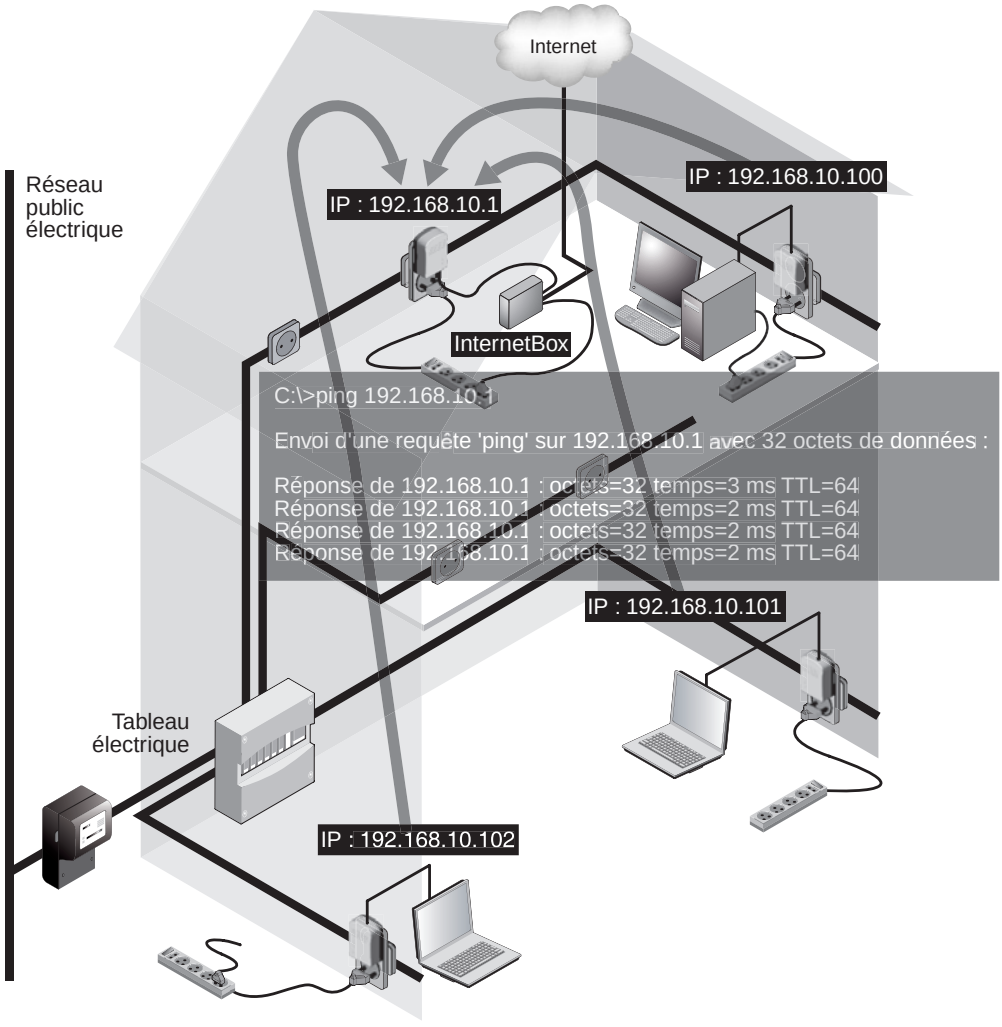


Figure 10.13

Test de bon fonctionnement du réseau CPL au niveau IP

Il faut pour cela que tous les PC ou terminaux soient dans le même plan d'adressage que l'InternetBox (par exemple, pour un réseau IP de type 192.168.10.x, l'InternetBox est en IP=192.168.10.1 et les autres équipements en IP=192.168.10.100, 101, 102, etc.). La configuration de l'adresse réseau (ou IP) d'un PC est détaillée au chapitre 9.

Pour lancer la commande ping, il suffit de procéder de la façon suivante :

1. Cliquez sur Démarrer puis sur Exécuter.
2. Saisissez **cmd.** Une fenêtre DOS s'ouvre.
3. Entrez la commande suivante :

```
C:\>ping 192.168.10.1

Envoi d'une requête 'ping' sur 192.168.10.1 avec 32 octets de données :

Réponse de 192.168.10.1 : octets=32 temps=3 ms TTL=64
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=64
```

Si cette commande renvoie des réponses, cela veut dire que les liens réseau sont configurés et prêts à être utilisés par les applications.

Pare-feu

La connexion au réseau Internet peut offrir aux personnes malintentionnées une porte d'accès au réseau domestique. La seule solution pour prévenir ces attaques est d'utiliser un pare-feu, ou firewall. Le rôle d'un firewall est de n'autoriser que certains protocoles dans le réseau domestique en fonction du numéro de port utilisé.

Chaque protocole utilise un numéro de port spécifique, par exemple le port 80 pour HTTP (HyperText Transfer Protocol), qui lui permet d'être reconnu en tant que tel par le réseau. En n'autorisant que certains ports et donc certaines applications, comme la messagerie électronique, HTTP ou FTP, tous les autres ports sont interdits.

Parmi les nombreux firewalls commercialisés, il en existe des gratuits, comme celui disponible dans les distributions Linux utilisant un noyau 2.4 ou 2.6.

Windows XP permet d'instaurer des règles de firewalling logiciel de la connexion réseau d'une station, mais non de tout le réseau, à la différence des firewalls matériels, qui peuvent interdire un protocole sur tout un réseau.

Pour accéder au firewall logiciel de Windows XP, il suffit de procéder de la façon suivante :

1. Dans le Panneau de configuration, sélectionnez Connexion réseau pour afficher la fenêtre illustrée à la figure 10.14.

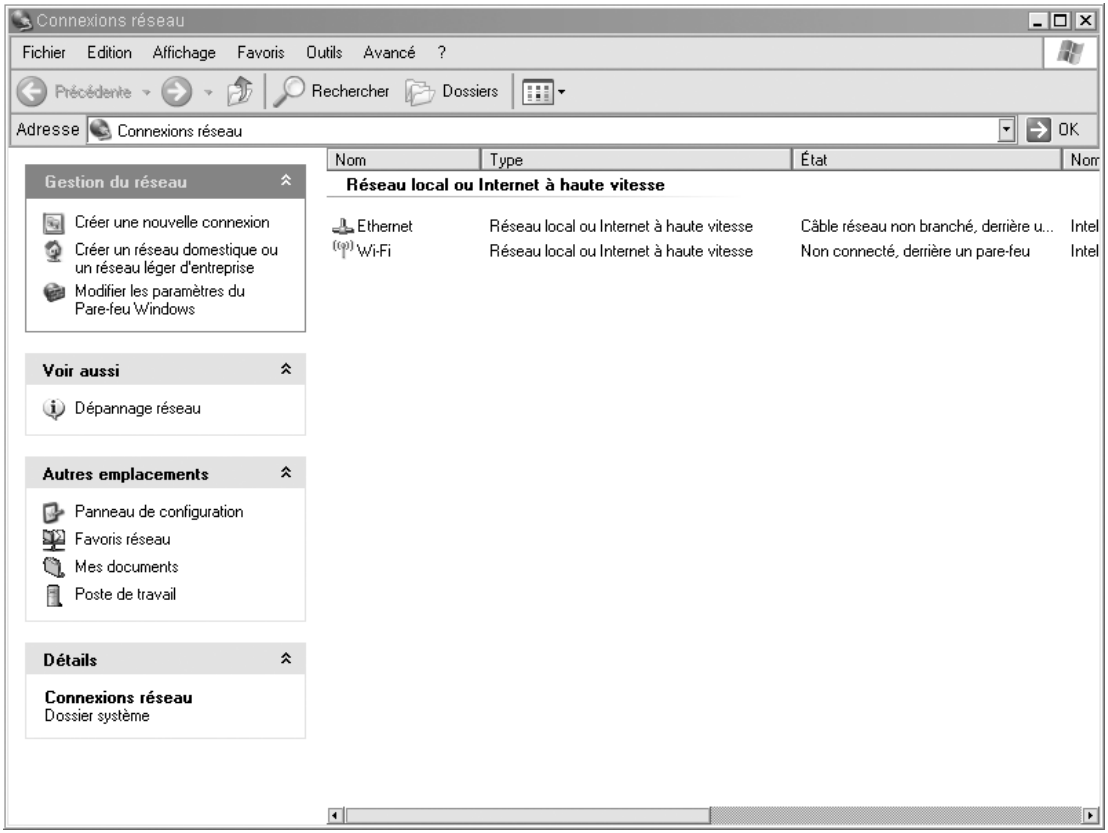


Figure 10.14

Fenêtre des connexions réseau de Windows XP

2. Choisissez Connexion réseau Ethernet pour afficher la boîte de dialogue illustrée à la figure 10.15.
3. Cliquez sur l'onglet Avancé, comme illustré à la figure 10.16.
4. Dans la zone Pare-feu Windows, cliquez sur Paramètres, et cochez la case Activé (recommandé).

Figure 10.15
Boîte de dialogue Propriétés de Ethernet

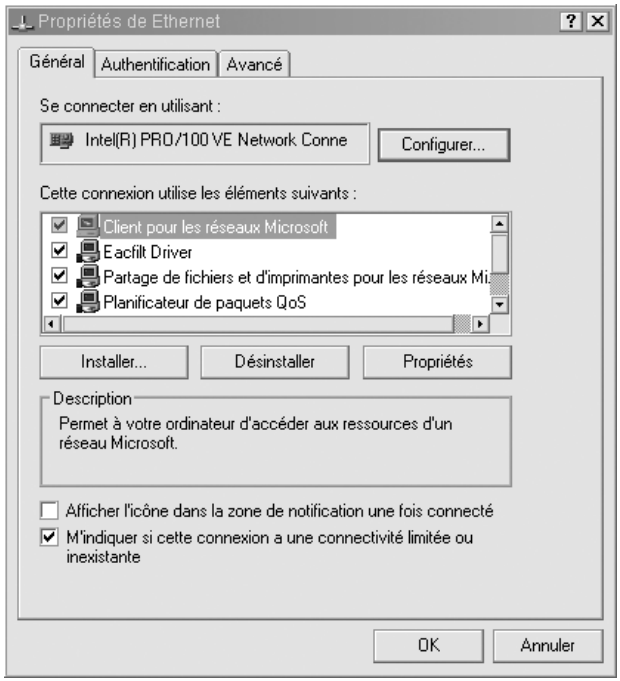
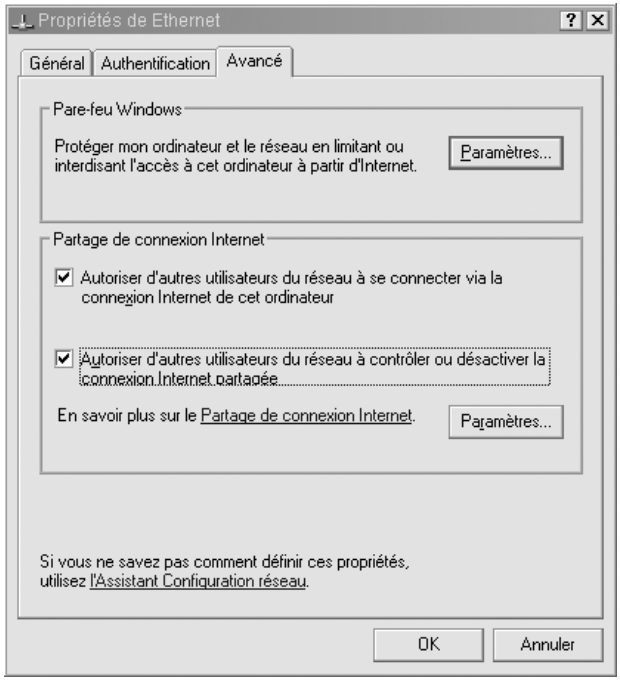


Figure 10.16
Paramètres de configuration avancés de la connexion



L'installation d'un firewall matériel doit se faire sur la machine connectée à Internet, l'idéal étant une machine dédiée, telle la passerelle d'accès définie précédemment *(voir figure 10.17)*.

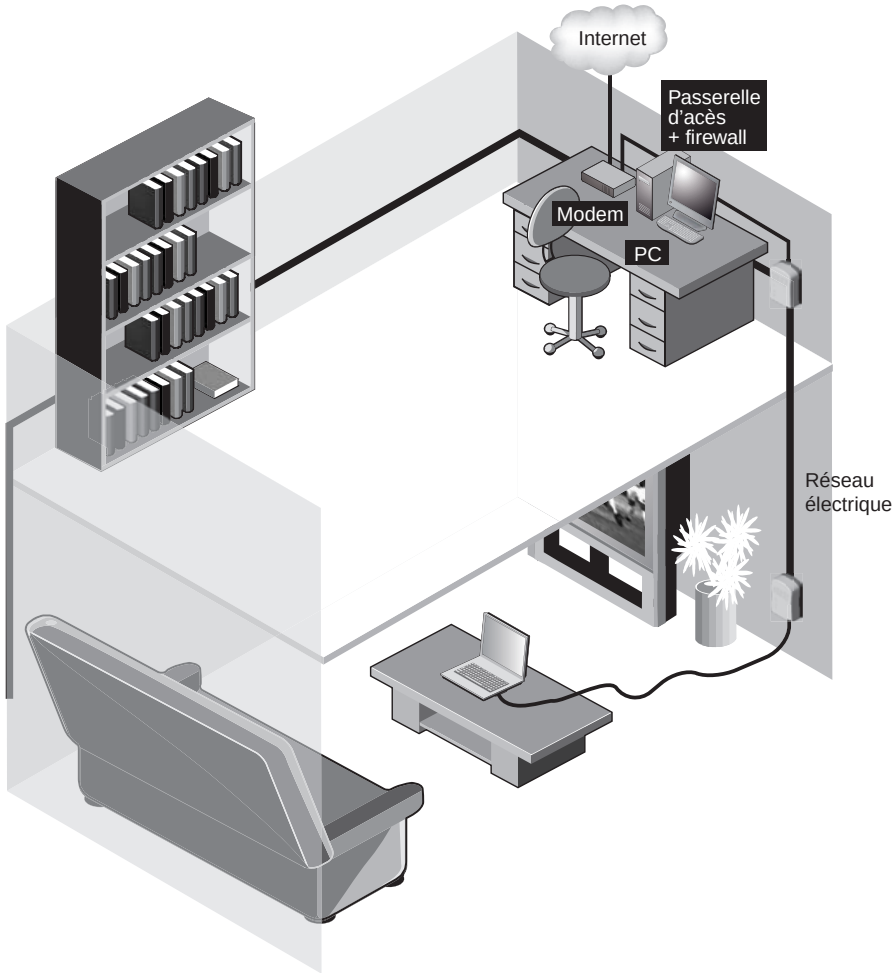


Figure 10.17
Réseau CPL avec passerelle d'accès sécurisée par firewall

VPN et PPPoE

Le seul moyen de garantir une totale sécurité d'un réseau CPL consiste, comme expliqué au chapitre 4, à recourir à un VPN (Virtual Private Network).

L'utilisation d'un serveur d'authentification n'est nécessaire que dans le cas où le réseau doit être fortement sécurisé. L'authentification permet, comme son nom l'indique,

d'authentifier de manière fiable tout utilisateur voulant se connecter au réseau. Le protocole d'authentification le plus utilisé est RADIUS (Remote Authentication Dial-In User Server), dont une version gratuite, appelée freeradius, est disponible à l'adresse *http://www.freeradius.org.*

Pour sécuriser un réseau de manière encore plus fiable, un VPN est indispensable. Par le biais de mécanismes d'authentification et de chiffrement, le VPN permet de sécuriser complètement les liaisons du réseau CPL. IPsec est le protocole le plus utilisé actuellement dans les VPN. L'utilisation d'un VPN IPsec demande toutefois des machines assez puissantes. Elle exige en outre des machines clientes qu'elles disposent de la configuration nécessaire de leur client VPN.

L'utilisation de serveurs d'authentification ou de serveurs VPN nécessite l'ajout des fonctionnalités correspondantes au niveau d'une passerelle spécifique, dans le cas où la passerelle d'accès à Internet incorpore déjà un serveur DHCP et un routeur NAT, comme illustré à la figure 10.18.

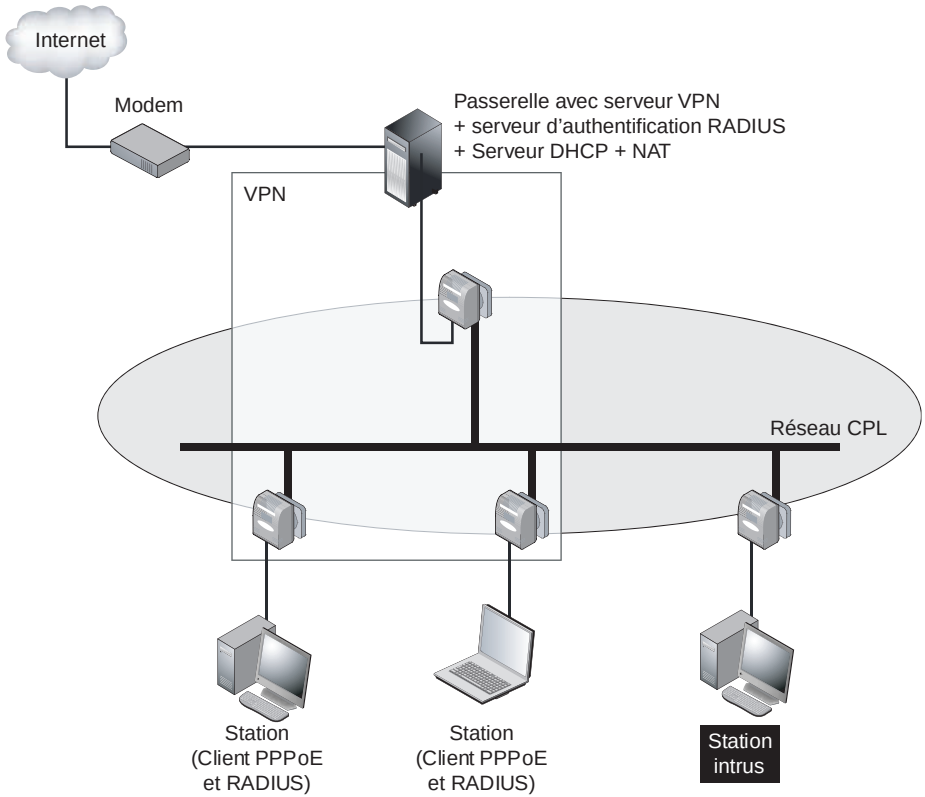


Figure 10.18

Réseau CPL avec passerelle sécurisée par VPN ou RADIUS

Une autre méthode permettant d'améliorer la sécurité du réseau CPL et du réseau local IP consiste à mettre en place un serveur PPPoE et un serveur RADIUS associé. Cette technique permet de mettre en place des « tunnels » IP entre les machines connectées au réseau local CPL et à la passerelle Internet, ces clients étant authentifiés sur le serveur RADIUS.

Si un intrus parvient à se connecter à un réseau local CPL, il ne peut utiliser le réseau local tant qu'il n'est pas connecté au serveur PPPoE et au serveur RADIUS sur la passerelle. La station de l'intrus ne peut donc ni accéder aux autres machines connectées au réseau CPL, ni accéder à Internet par l'intermédiaire de la passerelle du réseau CPL.

La figure 10.19 illustre la notion de tunnels PPPoE, constitués entre les machines clientes et la passerelle Internet, qui permettent de sécuriser les échanges entre la passerelle (et Internet) et ces machines clientes.

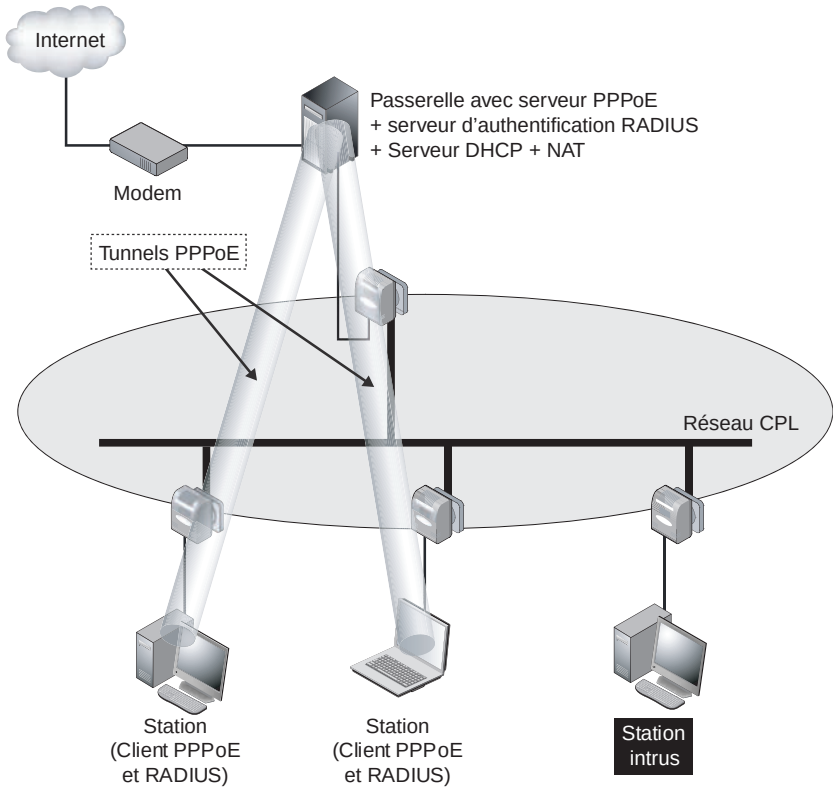


Figure 10.19

Réseau CPL avec passerelle sécurisée par serveurs PPPoE et RADIUS

Cette technique de sécurisation fondée sur les tunnels PPPoE est largement utilisée par les FAI pour garantir la séparation entre les différents clients d'accès à Internet, mais elle peut être tout aussi bien appliquée à un réseau CPL domestique ou professionnel.

Configuration d'une passerelle Internet

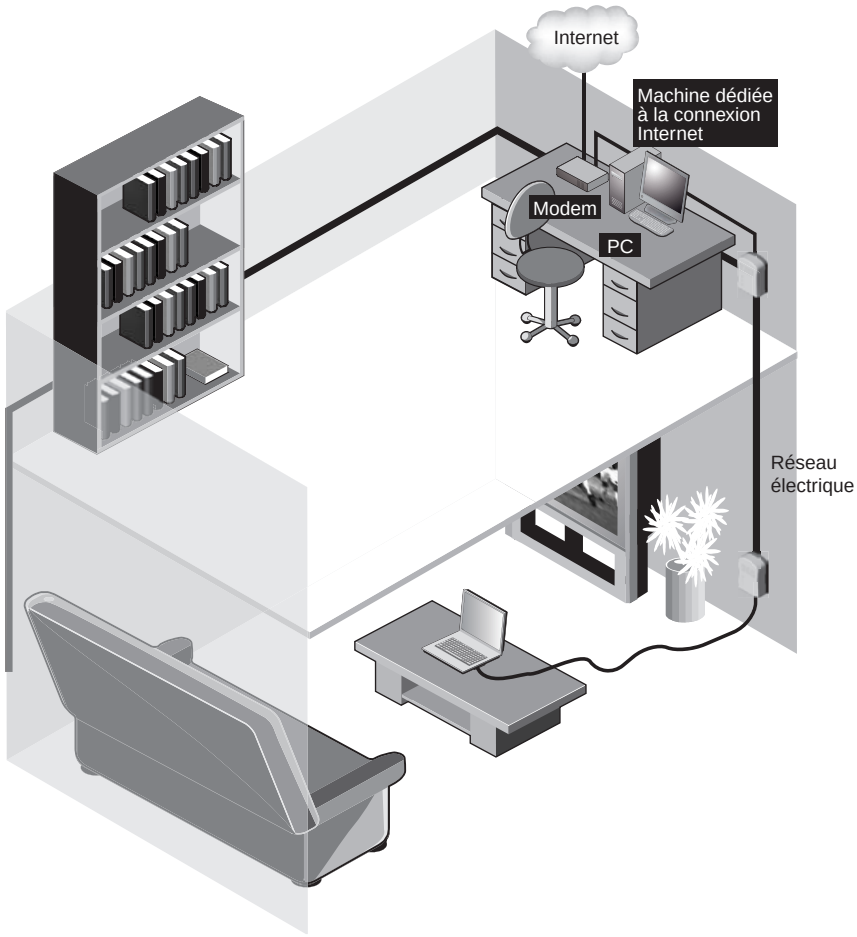
Dans un réseau CPL, toute connexion Internet peut être utilisée : modem 56 K, RNIS, câble, ADSL, ADSL2+, satellite ou FTTH (Fiber to the Home). Étant donné que la vitesse de transmission d'un réseau CPL est comprise entre 1 et 14 Mbit/s pour HomePlug 1.0, 1 à 85 Mbit/s pour HomePlug Turbo et 1 à 200 Mbit/s pour HomePlug AV, les débits des connexions Internet actuellement disponibles sont largement couverts.

Les performances de HomePlug 1.0 peuvent engendrer des débits utiles inférieurs à ceux des dernières technologies ADSL, comme l'ADSL2+ (20 Mbit/s), mais dès que l'on passe à HomePlug Turbo (25 Mbit/s), ce n'est plus un problème.

La connexion à Internet peut se faire de deux manières : soit en utilisant une machine dédiée, soit en connectant directement l'équipement CPL au modem d'accès à Internet ou à l'InternetBox, soit en utilisant directement un modem-routeur CPL.

Dans le premier cas, une machine partage sa connexion, comme illustré à la figure 10.20.

Figure 10.20
Connexion Internet par l'intermédiaire d'une machine dédiée



La figure 10.21 illustre un réseau domestique CPL dans lequel c'est un équipement multifonction (routeur/modem xDSL/CPL) qui est connecté à Internet.

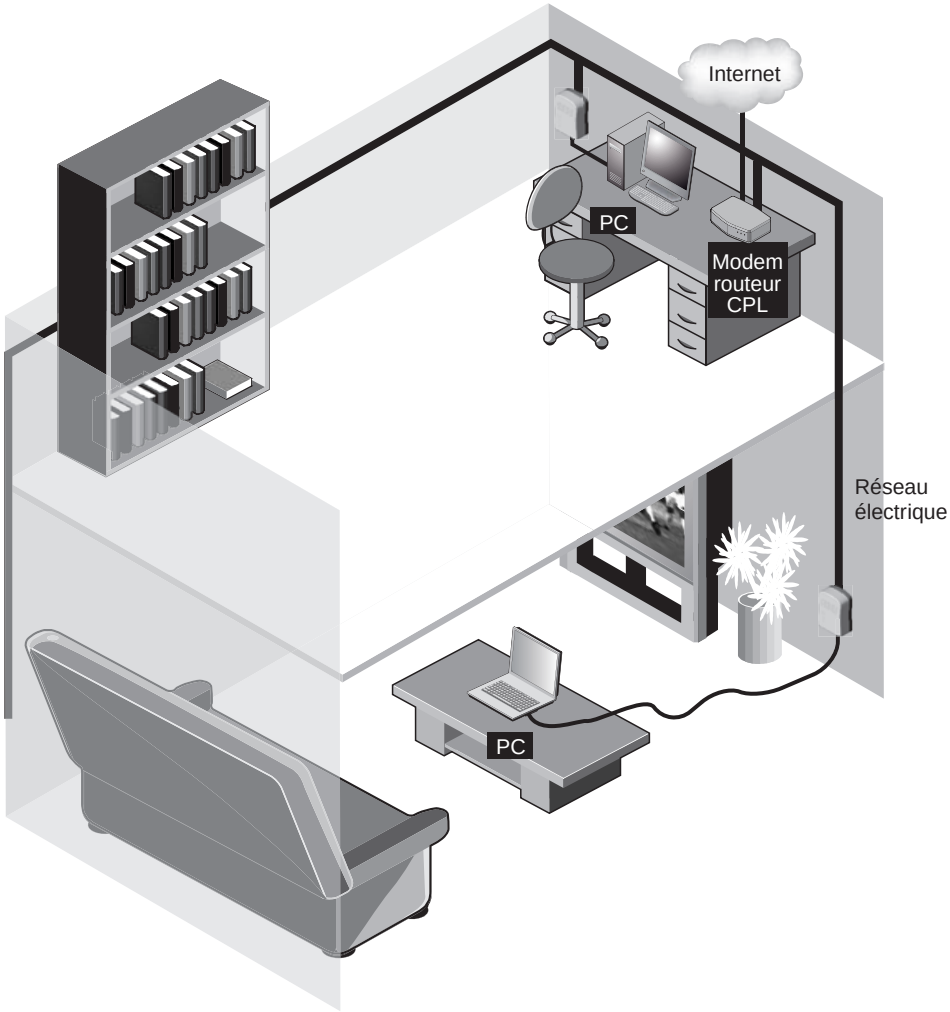


Figure 10.21
Connexion Internet par l'intermédiaire d'un modem-routeur CPL

L'inconvénient de ce dernier type de topologie est que l'équipement CPL ne possède que rarement un pare-feu, permettant de bloquer différents types de trafics et d'empêcher les attaques sur le réseau, ou un VPN. Dans la topologie où une machine dédiée est utilisée pour la connexion à Internet, n'importe quel logiciel de firewalling ou de serveur VPN peut être installée pour protéger le réseau.

Partage de la connexion Internet

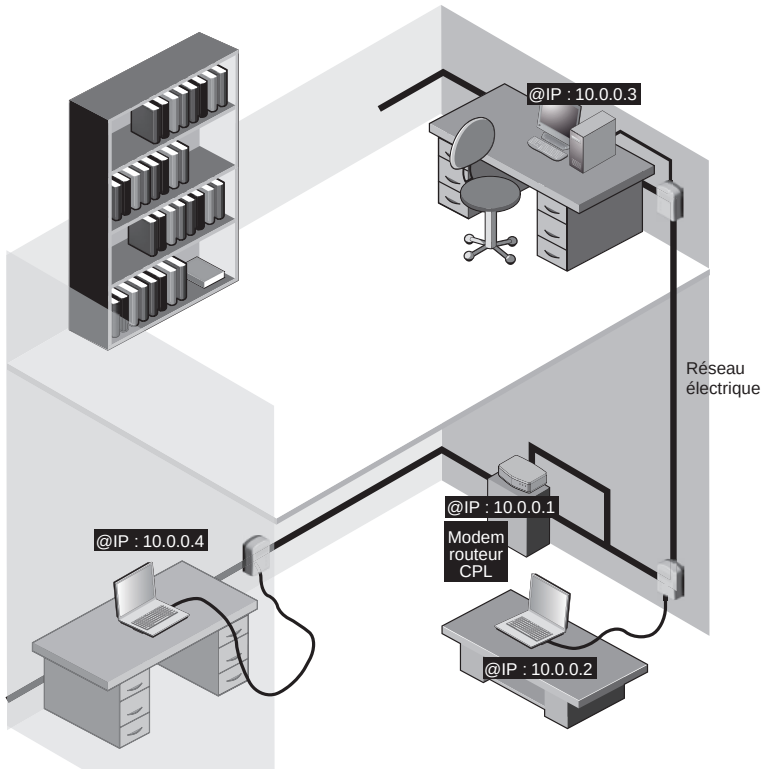
Pour partager une connexion Internet, deux protocoles sont utilisés, le NAT (Network Address Translation) et DHCP (Dynamic Host Configuration Protocol) :

- NAT permet de partager une connexion Internet entre plusieurs stations tout en utilisant l'adresse IP donnée par le fournisseur d'accès (FAI). Une autre caractéristique de NAT est qu'il permet de prévenir certaines attaques. Certains modems Internet dotés de fonctionnalités de routeurs incorporent le NAT, mais il est possible de l'installer sur une machine dédiée, connectée à Internet.
- DHCP est un protocole client-serveur qui permet d'allouer dynamiquement et pendant un certain temps (*lease time*, ou bail) les paramètres TCP/IP nécessaires à une station pour se connecter au réseau. Les paramètres fournis par le serveur DHCP auprès de la station sont l'adresse IP de la machine, le masque de sous-réseau, l'adresse de la passerelle par défaut et les adresses des serveurs de noms (DNS). DHCP offre une manière conviviale de configurer les stations, mais cette configuration peut aussi bien être effectuée manuellement en modifiant directement les paramètres de la carte.

En ce qui concerne les adresses IP, toutes les stations du réseau doivent avoir la même adresse de réseau, par exemple 192.168.0.*x* ou 10.0.*x*.*x*, avec *x* compris entre 1 et 254 dans les deux cas, comme l'illustre la figure 10.22.

Figure 10.22

Configuration des adresses IP du réseau domestique



Adresses DNS

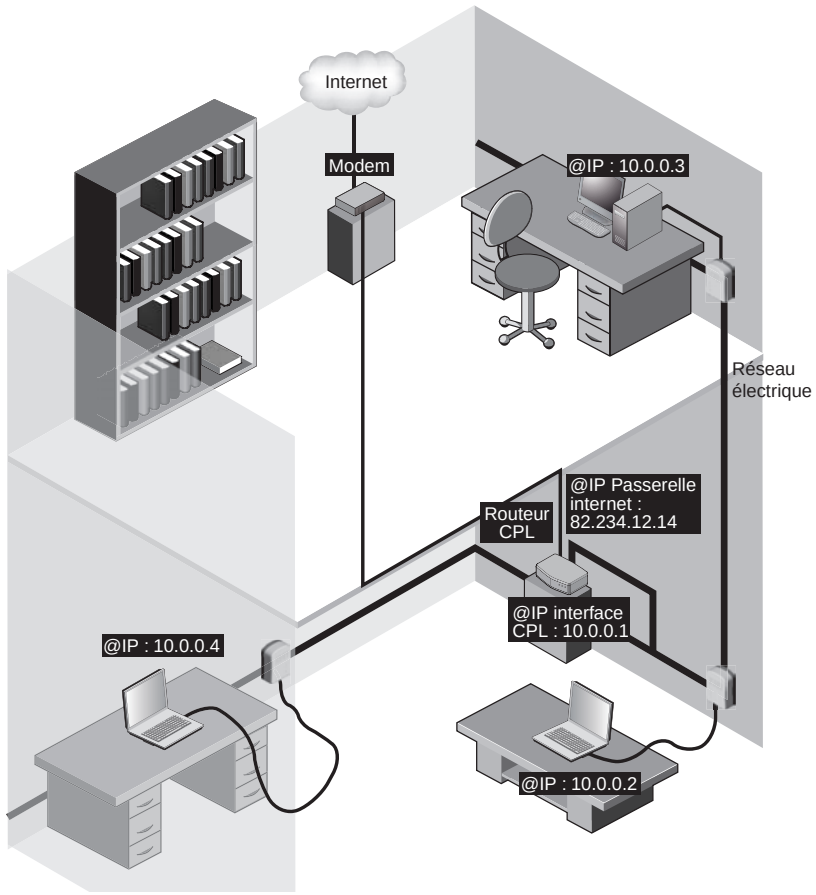
Les adresses DNS sont données par le fournisseur d'accès Internet, sauf dans le cas où un DNS local est présent dans le réseau domestique.

Configuration de NAT et DHCP

L'architecture idéale d'un réseau domestique CPL est celle où le routeur CPL fait à la fois office de routeur NAT et de serveur DHCP, le NAT permettant de partager la connexion Internet avec tous les équipements connectés au réseau et le DHCP fournissant tous les paramètres permettant à chaque équipement d'être connecté au réseau. Ces fonctionnalités sont présentes dans la plupart des modems-routeurs CPL destinés au marché domestique.

Cette architecture idéale est illustrée à la figure 10.23.

Figure 10.23
Architecture idéale d'un réseau CPL domestique



Dans le cas où les fonctionnalités NAT et DHCP ne sont pas incorporées dans le modem Internet ou l'InternetBox qui sert de passerelle d'accès à Internet, il est toujours possible de les utiliser mais en configurant une machine dédiée jouant le rôle de passerelle, comme illustré à la figure 10.24.

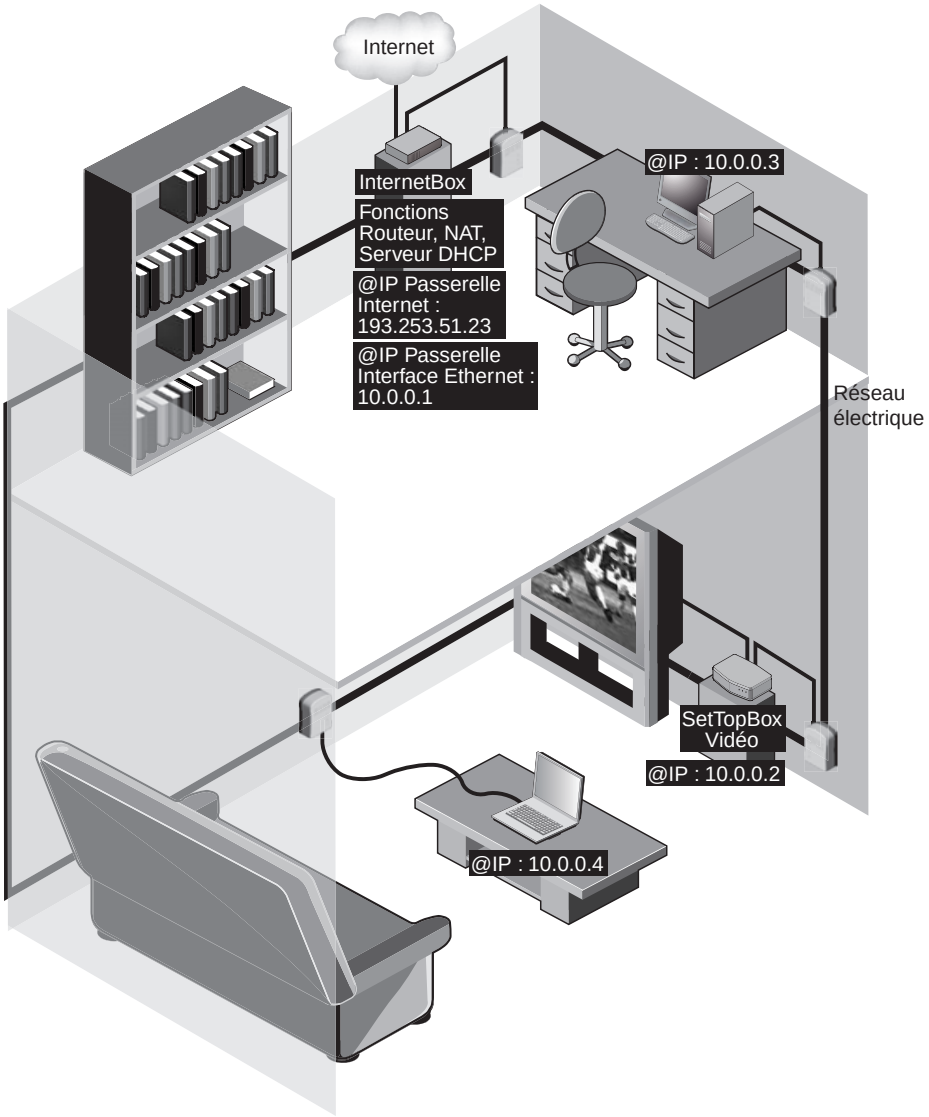


Figure 10.24

Architecture d'un réseau CPL domestique avec passerelle d'accès à Internet dédiée

L'idéal pour configurer une telle machine dédiée est d'utiliser Linux, dont les différentes distributions fournissent les fonctionnalités NAT et DHCP, alors que, sous Windows, il faut recourir à des logiciels payants. L'autre avantage de Linux est que le système n'exige pas d'énormes ressources.

Pour configurer une machine faisant du NAT et incorporant un serveur DHCP, un processeur de la génération 486 et 32 Mo de mémoire suffisent largement. Autre avantage, cette machine peut rester allumée en permanence sans le moindre bogue.

DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP permet de fournir dynamiquement des paramètres IP aux stations qui se connectent au réseau. Ce protocole est de plus en plus utilisé, car il facilite l'administration du réseau, surtout quand ce dernier est composé d'un nombre assez important de machines.

DHCP a été conçu au départ pour compléter un autre protocole, BOOTP (BOOTstrap Protocol), qui est utilisé dans le même esprit. Les messages BOOTP sont compatibles avec DHCP, mais pas l'inverse. La différence entre DHCP et BOOTP est que DHCP peut fournir à une station une certaine plage d'adresses et que chacune de ces adresses est négociée et n'est valable que pour une certaine période de temps.

Architecture de DHCP

Le protocole DHCP s'appuie sur une architecture client-serveur. Dans le cas des réseaux CPL, le client DHCP est l'équipement connecté au réseau CPL et le serveur DHCP le modem-routeur CPL.

L'exemple illustré à la figure 10.25 ne comporte qu'un seul serveur DHCP situé au niveau de l'InternetBox, pour les offres des FAI récentes, ou du modem Internet, mais un réseau peut être composé de plusieurs passerelles d'accès à Internet, et donc de plusieurs serveurs DHCP. Le fait d'utiliser plusieurs serveurs DHCP n'entraîne aucune contrainte réseau.

Lorsqu'une station initie le protocole DHCP, ce dernier lui fournit les paramètres suivants :

- adresse IP ;
- masque de sous-réseau ;
- passerelle par défaut ;
- adresse DNS ;
- nom de domaine.

Une fois ces paramètres reçus, l'ordinateur peut dialoguer librement avec d'autres machines du réseau ou accéder à Internet, s'il existe un partage de la connexion. Ce

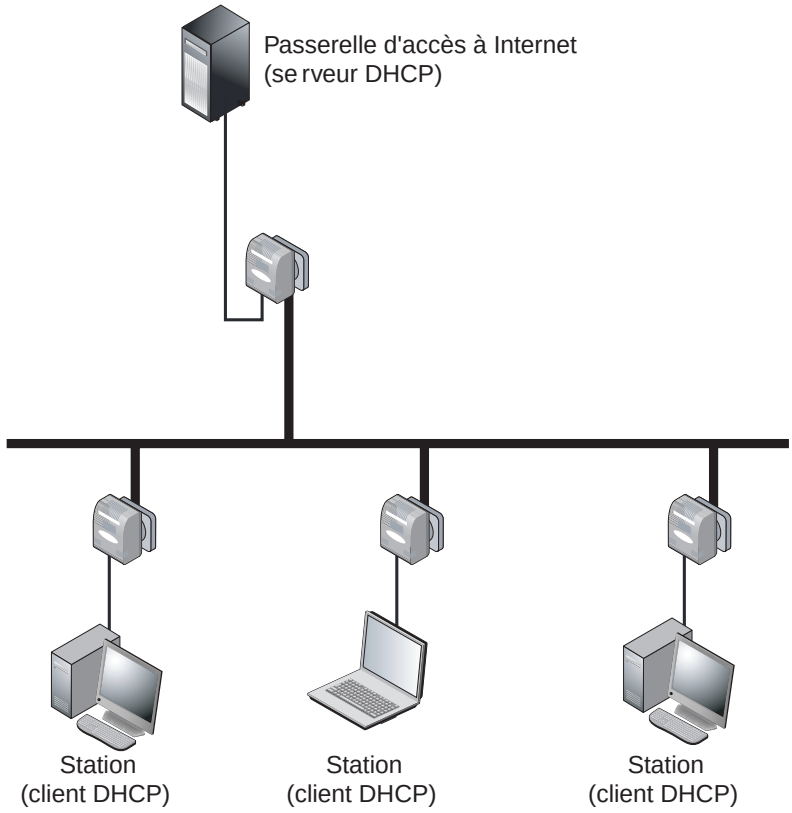


Figure 10.25
Architecture DHCP

mécanisme est transparent aux yeux de l'utilisateur et ne prend pas plus d'une seconde.

Une autre caractéristique de DHCP est le bail *(lease)*. Comme expliqué précédemment, les paramètres qui sont fournis à une station du réseau ne sont valables que pour une certaine période de temps. Ce bail est négocié entre la machine et le serveur lors de la demande de paramètres. À l'expiration de ce bail, celui-ci peut toujours être renégocié par la machine.

Configuration dynamique d'un client DHCP

La configuration dynamique d'une machine qui se connecte s'effectue en quatre phases, comme illustré à la figure 10.26 :

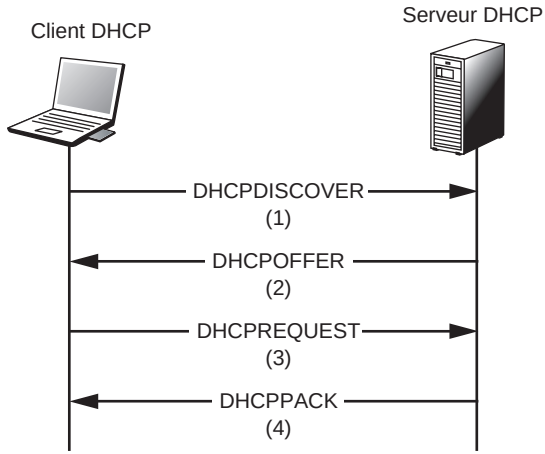


Figure 10.26
Configuration dynamique d'une machine via *le protocole DHCP*

1. Lorsqu'un client DHCP accède à un réseau, aucune adresse ne lui est allouée, et il a comme adresse IP 0.0.0.0.
2. Pour se configurer, le client envoie une requête DHCPDISCOVER en broadcast – avec une adresse IP 255.255.255.255 – sur le réseau, dans laquelle il insère son adresse MAC.

> **Adresse MAC**
> L'adresse MAC est une adresse fixe affectée à chaque carte Ethernet des terminaux connectés au réseau CPL.

3. Le serveur DHCP lui répond avec un DHCPOFFER, toujours émis en broadcast puisque le client n'a pas encore d'adresse IP. Le DHCPOFFER est composé de l'adresse MAC du client, de la durée du bail ainsi que de l'adresse IP du serveur.

   Il est possible d'avoir plusieurs serveurs DHCP, mais nous n'en utilisons qu'un dans le contexte de cet ouvrage.
4. Si le client accepte cette offre, il envoie un DHCPREQUEST pour recevoir les paramètres.
5. Le serveur envoie un DHCPACK confirmant que le client accepte.

Configuration sous Windows XP

La configuration d'un client DHCP sous Windows XP est très simple :

1. Lorsqu'on insère une carte Ethernet sous Windows, elle est automatiquement configurée en tant que client DHCP par défaut.
2. Si la carte a déjà été configurée précédemment avec une adresse IP fixe, ouvrir le Panneau de configuration, et sélectionnez Connexion réseau. La fenêtre illustrée à la figure 10.27 s'affiche.

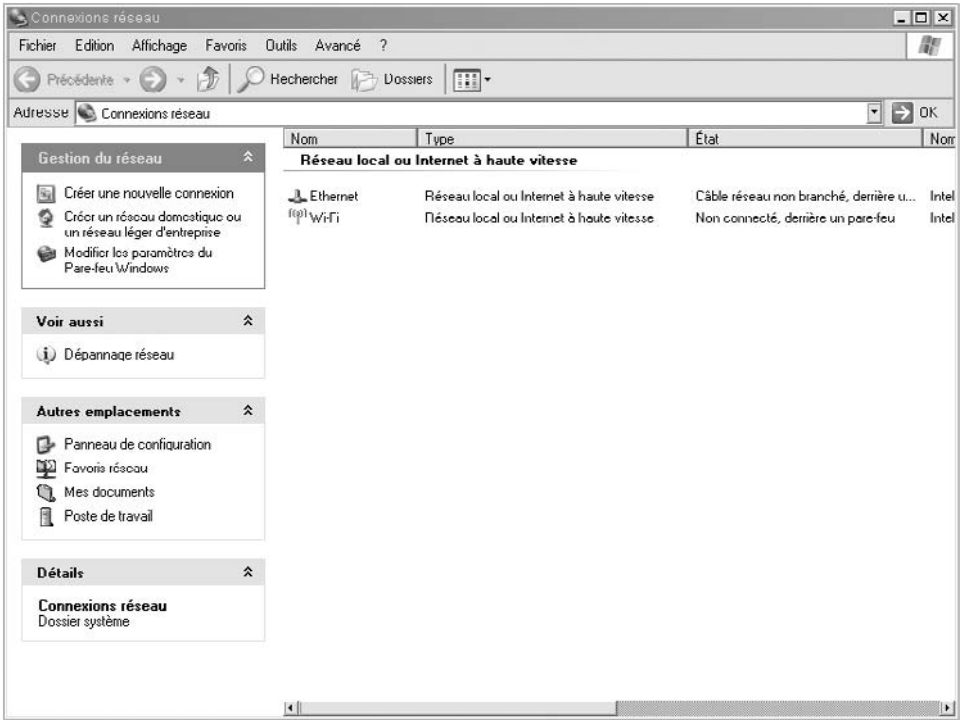


Figure 10.27

Configuration du réseau (ici, le PC dispose également d'une connexion Wi-Fi)

3. Choisir Connexion au réseau local pour afficher la boîte de dialogue illustrée à la figure 10.28.
4. Cliquer sur Propriétés pour afficher les propriétés de la connexion au réseau local, comme illustré à la figure 10.29.
5. Cocher la case Protocole Internet (TCP/IP). La boîte de dialogue Propriétés de Protocole Internet (TCP/IP) s'affiche, comme illustré à la figure 10.30.
6. Cocher la case Obtenir une adresse IP automatiquement. L'ordinateur est maintenant configuré en DHCP.

Figure 10.28
État de la connexion au réseau local

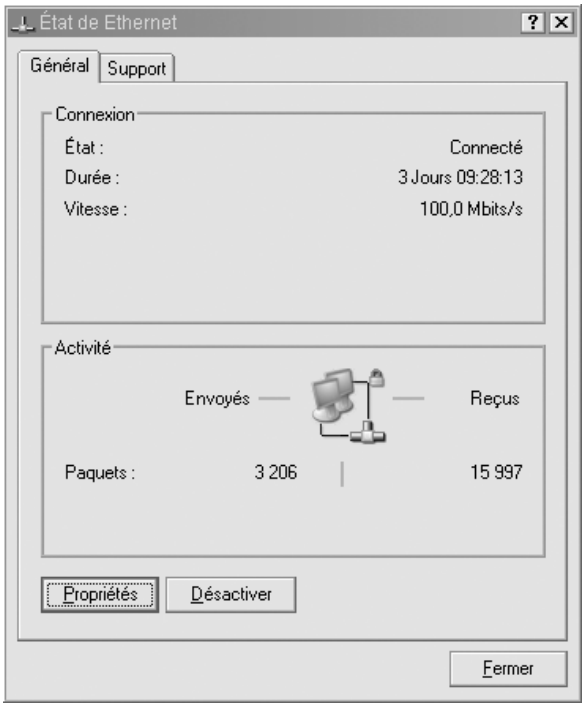


Figure 10.29
Propriétés de la connexion au réseau local

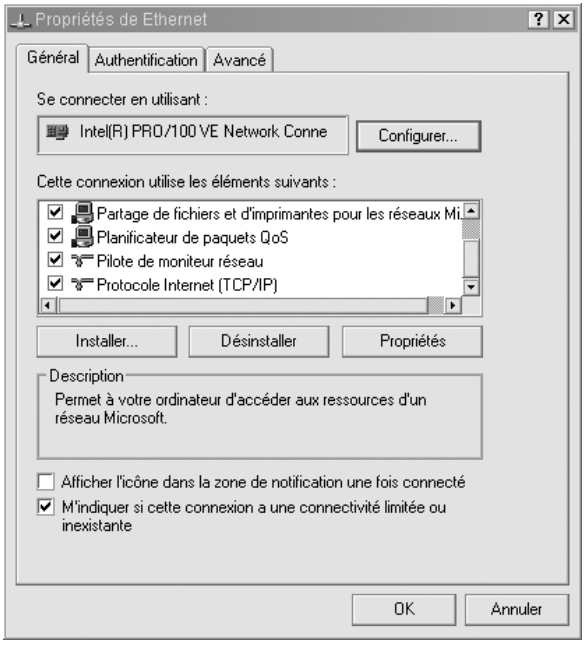
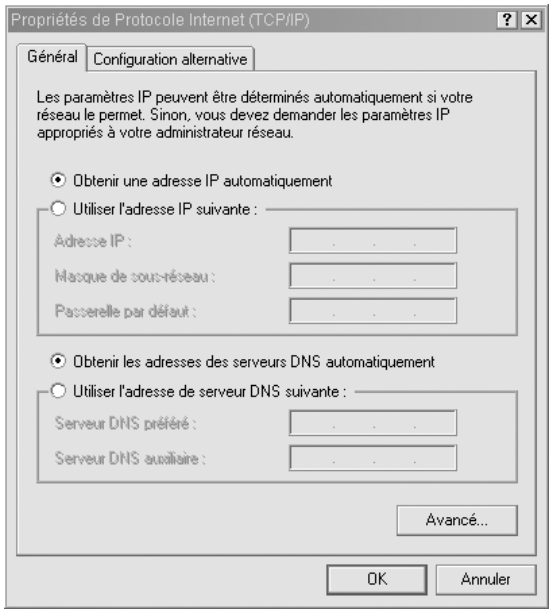


Figure 10.30
Configuration des paramètres TCP/IP de la carte Ethernet réseau local

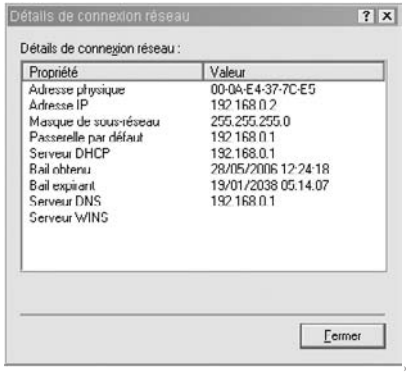


Sous Windows 2000/XP, pour vérifier que la carte est bien configurée, il suffit de vérifier sa prise en charge dans la boîte de dialogue État de Connexion réseau local, comme illustré à la figure 10.31 *(voir l'étape 1 ci-dessus pour accéder à cette boîte de dialogue).*

Figure 10.31
Paramètres TCP/IP de la carte Ethernet réseau local

Le bouton Détails donne plus de renseignements sur les paramètres de la carte *(voir figure 10.32).*

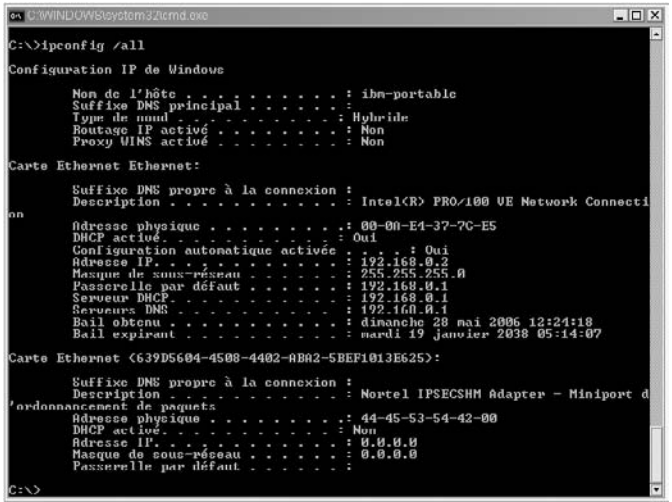
Figure 10.32
Paramètres TCP/IP détaillés de la carte Ethernet réseau local



Il est possible de vérifier la configuration de la carte par l'intermédiaire de la commande `ipconfig` :

1. Dans le menu Démarrer, cliquez sur le bouton Exécuter, et entrez **cmd** pour ouvrir la commande MS-DOS.
2. À l'invite, saisissez **ipconfig /all** pour afficher toutes les informations concernant la carte réseau et vérifier qu'elle a bien été configurée. Nous constatons à la figure 10.33 que les informations sont les mêmes que celles obtenues précédemment.

Figure 10.33
Paramètres TCP/IP de la carte par ipconfig



Il se peut que la carte n'ait pas été configurée par le serveur DHCP. Si tel est le cas, Windows attribue à la carte une adresse IP par défaut, de type 169.254.*x.x.* Pour réinitialiser une demande de requête au serveur DHCP, il suffit d'entrer **ipconfig /release** puis **ipconfig /renew.**

11

CPL d'entreprise

Les CPL pénètrent de plus en plus dans le monde de l'entreprise, et plus généralement dans les réseaux des bâtiments professionnels et industriels, où ils se placent comme compléments ou remplaçants de réseaux Wi-Fi ou Ethernet.

Les performances et les distances de propagation des réseaux électriques permettent de considérer les réseaux CPL comme des dorsales non seulement pour les locaux d'une PME, mais aussi pour les bâtiments professionnels (hôtels, hôpitaux, salles de concert, grandes surfaces, etc.) et industriels (usines, entrepôts, grues, etc.).

Les CPL peuvent donc être vus de par leurs performances et leur stabilité comme une technologie de remplacement, de complément ou de desserte d'autres technologies réseau d'entreprise, notamment les suivantes :

- Dorsale en remplacement du réseau Ethernet pour des raisons de coût ou pour des bâtiments dans lesquels les travaux sont impossibles (bâtiments classés ou sécurisés, hôpitaux, etc.), ou dorsale d'un réseau Wi-Fi pour relier les différentes cellules du réseau radio.
- Complément du réseau Ethernet pour satisfaire aux besoins d'extension d'un réseau existant (coûts inférieurs, facilité de déploiement, etc.), ou encore en cas de déplacement d'une entreprise.
- Réseau temporaire pour couvrir des événements tels que concert, conférence, etc.).
- Création de plusieurs réseaux séparés sur un même réseau électrique (administration, entreprise publique, laboratoire, etc.).

Le prix des équipements CPL n'est pas très élevé, surtout dans le cas d'une entreprise passant complètement en CPL, pour peu que l'on raisonne à long terme et que l'on prenne en compte l'économie liée au matériel filaire (câbles, prises, switchs, etc.).

Au sein d'une entreprise, le réseau CPL peut être considéré soit comme un réseau d'exploitation, soit comme un réseau dit d'invités, permettant, par exemple, aux visiteurs d'accéder à Internet. Dans ce dernier cas, il est préférable de séparer ce réseau de celui de l'entreprise.

Comme au chapitre précédent, consacré à l'installation d'un réseau CPL domestique, nous décrivons dans le présent chapitre les étapes nécessaires à l'installation et à la configuration d'un réseau CPL d'entreprise, en insistant plus particulièrement sur l'accès au réseau électrique.

Architecture réseau

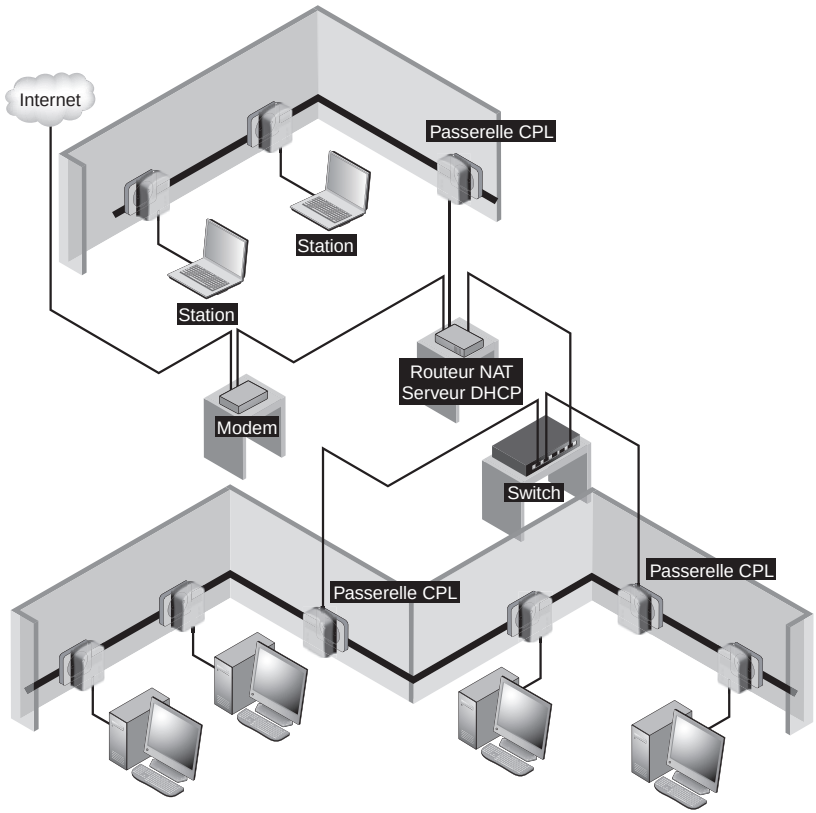
Dans une entreprise, l'architecture d'un réseau CPL peut différer grandement suivant la taille du réseau, le nombre de postes à connecter et les objectifs assignés à ce dernier.

L'architecture réseau d'une petite entreprise, comprenant un petit nombre de PC (moins de dix postes) et une connexion Internet par modem câble ou ADSL ne diffère pas de celle d'un réseau domestique.

Les seules options possibles tiennent à la gestion des fonctionnalités de serveur DHCP, de routeur NAT et de connexion Internet, qui s'effectue au niveau d'une passerelle dédiée. Par l'intermédiaire d'un switch, il est ensuite toujours possible d'ajouter une ou plusieurs passerelles CPL afin de constituer différents réseaux CPL sur le même réseau électrique.

Figure 11.1

Architecture d'un réseau CPL comprenant plusieurs passerelles CPL reliées à un switch

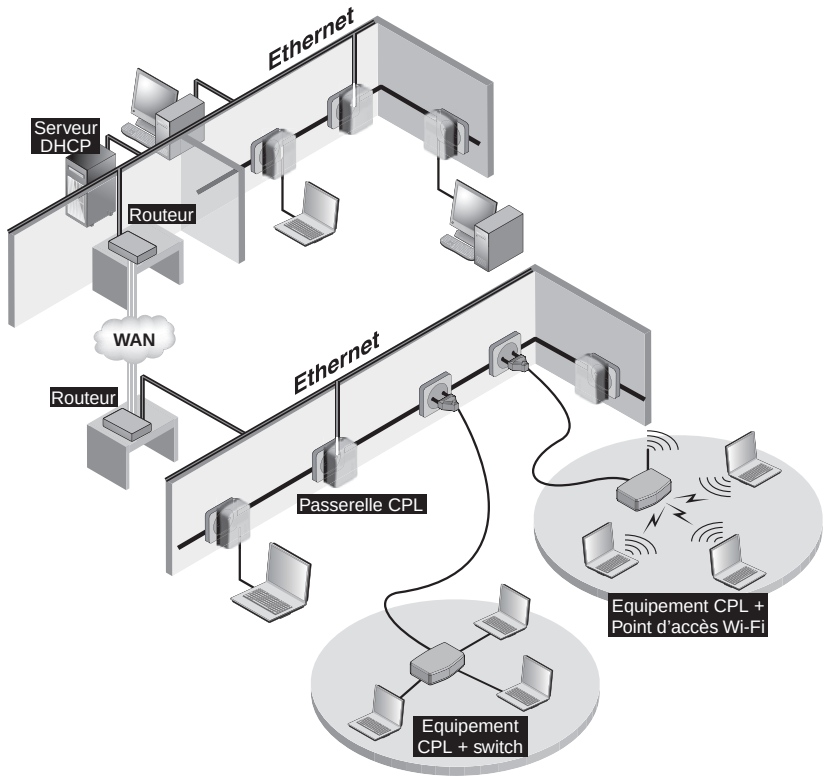


La figure 11.1 illustre une architecture où le serveur joue le rôle de serveur DHCP et de routeur NAT et où un switch lui est connecté pour permettre l'ajout de nouvelles passerelles CPL d'accès à l'architecture.

Le plus souvent, le réseau CPL se greffe à un réseau Ethernet existant dans l'entreprise, lequel possède déjà certaines fonctionnalités, telles que DHCP, la connexion Internet et NAT.

La figure 11.2 illustre un réseau d'entreprise constitué de deux sous-réseaux connectés entre eux *via* un WAN (Wide-Area Network) par l'intermédiaire de routeurs. Les routeurs sont eux-mêmes connectés au réseau Ethernet de chaque partie du réseau d'entreprise. Sur ces réseaux Ethernet, sont connectés les réseaux CPL permettant de connecter les terminaux des différentes salles de l'entreprise.

Figure 11.2
Architecture de réseau d'entreprise avec routeurs incorporant des réseaux CPL



Il est possible de connecter les terminaux aux équipements CPL du réseau des différentes manières suivantes :

- Terminaux connectés directement à un équipement CPL branché sur le réseau électrique.

- Terminaux connectés à un équipement CPL switch, qui se connecte au réseau CPL et distribue les connexions dans la pièce *via* sa fonction switch.
- Terminaux connectés *via* leur interface radio à un point d'accès Wi-Fi doté d'une fonctionnalité CPL lui permettant de se connecter au réseau CPL.

Supervision de réseau CPL

Les réseaux d'entreprise professionnels et industriels demandent certaines fonctionnalités que ne requièrent pas les réseaux domestiques, notamment la supervision, afin de s'assurer du bon fonctionnement du réseau en permanence et de remonter des alertes vers les administrateurs en cas de panne de certains équipements.

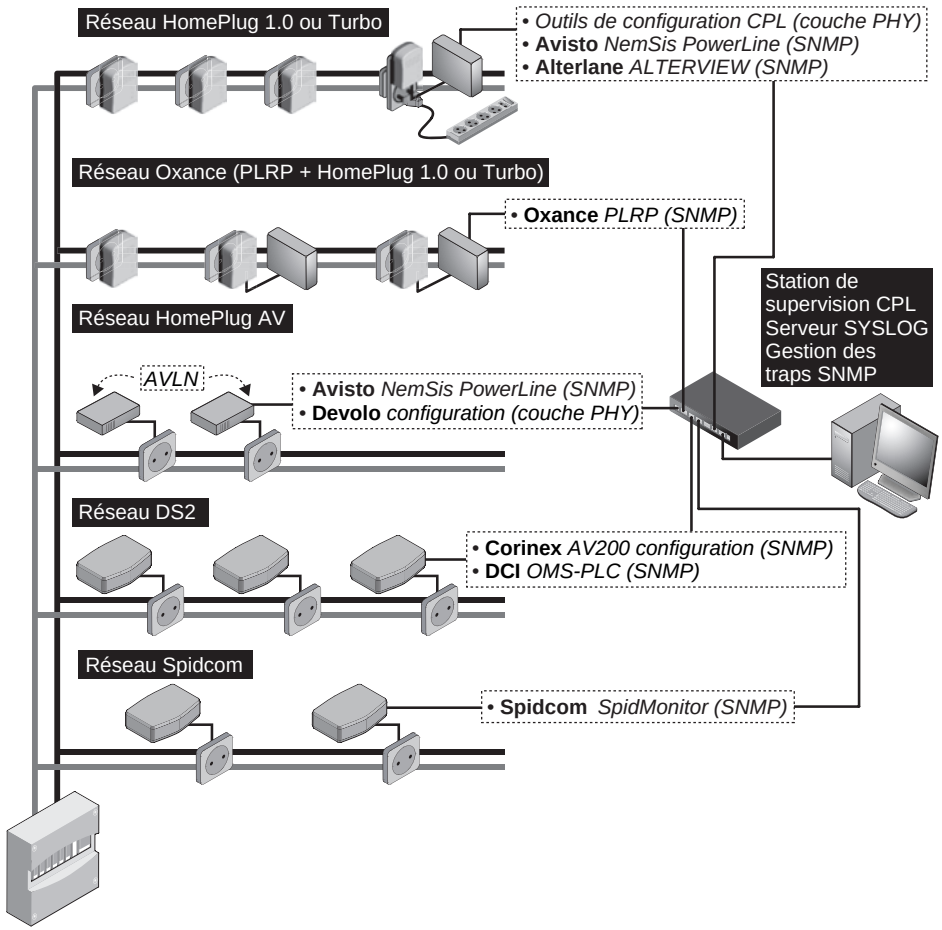


Figure 11.3

Outils de supervision des différentes technologies de réseaux CPL

Parmi les protocoles standardisés pour la supervision, SNMP (Simple Network Management Protocol) en versions v1, v2 et v3 s'est largement imposé dans les équipements réseau, qui sont désormais largement équipés d'une brique logicielle SNMP. Cette brique logicielle permet d'interroger un équipement réseau à distance et d'obtenir la valeur d'un certain nombre de paramètres réseau et système (paquets perdus, paquets reçus, température des cartes, sollicitation CPU, etc.).

Les technologies CPL fonctionnant au niveau de la couche liaison de données (couche MAC), elles ne permettent pas directement une interrogation SNMP à distance. Un certain d'outils matériels et logiciels permettent cependant de superviser l'ensemble des réseaux CPL.

La figure 11.3 illustre la supervision de plusieurs réseaux CPL de technologies différentes. Oxance, DS2 et Spidcom implémentent directement dans leurs équipements une interface HTTP et une pile SNMP (avec une MIB correspondante).

Les technologies HomePlug (1.0, Turbo et AV) ne proposant pas de pile SNMP dans leurs équipements, il est nécessaire d'utiliser ou de développer des outils de supervision au niveau MAC et d'utiliser les outils de configuration CPL qui donnent l'état des liens CPL au niveau PHY.

Choix du standard

Contrairement aux CPL à usage domestique, pour lesquels le prix des équipements est le critère essentiel, les réseaux d'entreprise professionnels et industriels nécessitent souvent des fonctionnalités qui impliquent le choix d'une technologie plus professionnelle, tout en s'efforçant de retenir un standard le plus ouvert possible afin de permettre des évolutions futures.

Le tableau 11.1 recense les critères de choix d'une technologie CPL d'entreprise.

Tableau 11.1 Critères de choix des technologies CPL d'entreprise

Technologie CPL		Critère de choix
HomePlug	1.0, Turbo	Faible coût, idéal pour les PME, peu de fonctionnalités avancées, sécurité DES-56 bits, facilité de déploiement, peu de possibilités d'administration
	AV	Technologie de pointe, important débit utile, coût plus élevé, fonctionnalités avancées de gestion de réseau, QoS garantie
	Oxance	Compatible HomePlug 1.0 et Turbo, fonctionnalités avancées (interface HTTP, administration SNMP par une adresse IP unique, sécurité renforcée par des clés sur le protocole Oxance PLRP, etc.), systèmes de couplage électrique professionnels, répéteurs CPL
DS2 AV200		Débit élevé et stable, architecture maître-esclave, administration centralisée, non compatible HomePlug, intégration des produits dans des boîtiers professionnels, fonctionnalités avancées de configuration (sécurité, filtrage, QoS, VLAN, etc.)
Spidcom		Débit élevé et stable, configuration très avancée (configuration possible de chacune des sous-bandes de fréquences utilisées), administration centralisée (SNMP, HTTP, etc.), expérience de projets innovants dans le domaine des CPL

La société Oxance développe des produits destinés aux professionnels fondés sur la spécification HomePlug, ce qui rend ces produits interopérables avec les équipements HomePlug 1.0 et Turbo. Cette société propose en outre des produits et accessoires particulièrement permettant d'optimiser le réseau CPL (répéteurs, filtres, systèmes de couplage).

La société Devolo développe des produits HomePlug (1.0, Turbo et AV) à destination des professionnels en les intégrant dans des boîtiers en métal dotés de systèmes de fixation adaptés aux locaux techniques proches des équipements électriques d'un bâtiment d'entreprise ou industriel.

Choix des équipements réseau et électriques

Certains des critères de choix des équipements CPL pour les réseaux domestiques peuvent être repris ici, à condition de leur en adjoindre un certain nombre d'autres, notamment les suivants :

- gestion de plus de 15 équipements (limite du standard HomePlug 1.0 et Turbo pour un réseau simple CPL) ;
- monitoring du réseau (SNMP typiquement) ;
- administration et configuration centralisées (HTTP, Telnet, SSH, etc.) ;
- boîtiers métalliques isolés, permettant la dissipation de chaleur des composants électroniques CPL ;
- interface CPL et alimentation 220 V/50 Hz séparée ;
- répétition possible du signal CPL ;
- intégration de fonctions réseau avancées (routeur NAT, serveur DHCP firewall, switch, Wi-Fi, etc.).

Concernant les équipements électriques CPL (filtres, systèmes de couplage, injecteurs de signal CPL, etc.), il est recommandé de faire appel à des produits professionnels et de les installer avec l'aide d'électriciens agréés par EDF afin de garantir le respect des normes de sécurité et d'obtenir une installation pérenne.

Qualité de service

L'intégration de la qualité de service, ou QoS (Quality of Service), dans les différentes technologies CPL est nécessitée par le développement des applications temps réel, telles que la vidéo à la demande, la diffusion de flux vidéo HDTV, la téléphonie IP, le travail collaboratif, la vidéoconférence, etc.

Les contraintes réseau de telles applications peuvent être difficiles à concilier avec le fait que les technologies CPL utilisent comme médium de communication le réseau électrique, qui subit les interférences des autres équipements branchés sur le réseau.

Le tableau 11.2 récapitule les fonctionnalités implémentées dans les différentes technologies CPL afin de répondre à ces contraintes.

Tableau 11.2 Fonctionnalités de QoS des technologies CPL

Technologie CPL		Fonctionnalité de QoS
HomePlug	1.0, Turbo	Priorités CA (intervalles PRS dans les trames) en correspondance avec les étiquettes VLAN du standard IEEE 802.1Q
	AV	Classes de priorités utilisateur (0 à 7), en correspondance avec les classes de trafic du standard IEEE 802.1D, Synchro AC, TDMA, propagation des QMP, utilisation des étiquettes VLAN du standard IEEE 802.1Q
	Oxance	Priorités CPL (VLAN, fixed, fairness), niveaux de priorité (0 à 5), limitation par source (IP ou MAC), par destination (IP ou MAC) en débit ascendant et descendant
DS2 AV200		Paramètres Default priority, Criterion, utilisation des Offset, Pattern, Bitmask, utilisation des étiquettes VLAN du standard IEEE 802.1Q
Spidcom		Utilisation des standards IEEE 802.1Q (étiquettes VLAN) et IEEE 802.1P pour la QoS des applications temporellement critiques

Parmi ces technologies, HomePlug 1.0 et Turbo sont peut-être celles qui ont le moins de garantie de QoS, tandis que HomePlug AV présente des garanties de QoS optimales, dans la mesure où le signal CPL s'appuie sur le signal 220 V/50 Hz transporté sur les câbles électriques pour synchroniser les différents équipements du réseau CPL.

La QoS dans HomePlug AV

La spécification HomePlug AV bénéficie de nombreux développements et ajouts de fonctionnalités par rapport à HomePlug 1.0 et Turbo. Parmi eux, la QoS a été implémentée au moyen de classes de trafic aux performances garanties. Le nom même d'AV correspond à Audio et Vidéo, deux types d'applications dans lesquels les contraintes de QoS (débit important garanti, délai de propagation, jitte) sont cruciales pour le bon fonctionnement des transmissions sans perte de données.

Ces contraintes peuvent être supportées par l'implémentation des fonctionnalités suivantes *(voir le chapitre 3) :*

- Synchronisation du signal CPL sur le 50/60 Hz afin de garantir les espaces de temps TDMA et CSMA/CA avec les CP (Contention Period) et les CFP (Contention Free Period).
- Paramètres QMP (QoS and Mac Parameters) dans les équipements CM (Connection Manager), CCo (Central Coordinator) et STA (Station).
- Propagation des paramètres QMP entre les différents équipements du réseau afin de maintenir l'homogénéité du réseau CPL en terme de QoS et de performances.

☞

La QoS dans HomePlug AV *(suite)*

Parmi les paramètres QMP, le tableau 11.3 récapitule ceux qui sont les plus importants pour la gestion de la QoS. Pour rappel, la MSDU (MAC Service Data Unit) est la trame de données au niveau MAC dans la couche de liaison de données.

Tableau 11.3 Principaux paramètres QMP de QoS de HomePlug AV

Paramètre QMP	Description
Delay Bound	Temps maximal mesuré en microsecondes pour transporter une MSDU entre le moment où elle est délivrée à la sous-couche de convergence SAP (Service Access Point) au niveau de la couche liaison de données de la station émettrice et celui où elle est reçue au niveau de la couche SAP de la station réceptrice.
Jitter Bound	Décalage maximal mesuré en microsecondes du temps de propagation d'une MSDU entre la couche SAP de l'émetteur et la couche SAP du récepteur
Nominal MSDU	Valeur nominale de la partie données de la trame MSDU en octets fondée sur le standard IEEE 802.3 (valeur comprise entre 46 et 1 500 octets)
Max MSDU	Valeur maximale de la partie données de la trame MSDU
Min MSDU	Valeur minimale de la partie données de la trame MSDU
Average Data rate	Vitesse de transmission moyenne mesurée en unités de 10 Kbit/s spécifiée au niveau de la sous-couche de convergence SAP pour transporter les trames MSDU sur un lien CPL. Cela n'inclut pas les en-têtes MAC et PHY nécessaires au transport des MSDU.
Max Data rate	Vitesse de transmission maximale spécifiée au niveau de la sous-couche de convergence SAP pour transporter les trames MSDU sur un lien CPL
Min Data rate	Vitesse de transmission minimale spécifiée au niveau de la sous-couche de convergence SAP pour transporter les trames MSDU sur un lien CPL
Max Burst size	Taille maximale exprimée en octets d'une surcharge lors d'un envoi en continu de trames MSDU généré par une application à la vitesse de transmission maximale
MSDU Error rate	Taux d'erreur sur une trame MSDU exprimé sous la forme $x \times 10^{-y}$, où *x* est spécifié dans les 8 bits de poids fort en format *unsigned integer,* et *y* dans les 8 bits de poids faible au même format.
Inactivity Interval	Temps maximal mesuré en millisecondes pendant lequel une connexion est autorisée à être maintenue inactive (sans transport de données utiles) avant que l'équipement CM (Connection Manager) n'autorise à nouveau la transmission.
CLST (Convergence Layer SAP Type)	Compatibilité de la sous-couche de convergence SAP avec d'autres couches que celle spécifiée dans le standard IEEE 802.3
CDESC (Connection Descriptor)	Champs optionnels provenant des couches applicatives supérieures, ou HLE (High Layers Entities), utilisés, par exemple, pour la QoS dans le mode UPnP (Universal Plug-and-Play), ou d'autres couches applicatives supérieures. Ces champs sont les suivants : version d'IP (v4 ou v6), IP source, IP destination, port source IP, port destination IP, protocole IP (UDP ou TCP).

☞

Tableau 11.3 Principaux paramètres QMP de QoS de HomePlug AV *(suite)*

Paramètre QMP	Description
ATS Tolerance	Variance tolérée mesurée en microsecondes sur l'écart d'horodatage ATS (Arrival Time Stamp) entre l'horloge de synchronisation du réseau CPL, ou NTS (Network Time Base), et le marquage des trames MSDU avec l'horodatage ATS
Average Number of PBs (PHY Blocks) per TXOP (time allowed between two Transmisson Opportunities)	Nombre moyen de blocs de données PHY (au niveau de la couche physique) en bloc de 520 octets par intervalle entre deux opportunités de transmission pour transporter une trame MSDU sur un lien CPL
Minimum Number of PBs per TXOP	Nombre minimal de blocs de données PHY (en bloc de 520 octets) nécessaires pour transporter une trame MSDU sur un lien CPL
Maximum Number of PBs per TXOP	Nombre maximal de blocs de données PHY (en bloc de 520 octets) nécessaires pour transporter une trame MSDU sur un lien CPL

Comme nous le pouvons le voir, la gestion de la QoS dans HomePlug AV est particulièrement complexe et fait appel à un grand nombre de paramètres échangés en permanence entre les équipements CPL du réseau.

Cette gestion de la QoS garantit aux applications les contraintes réseau qui leur sont nécessaires. HomePlug AV spécifie huit classes d'applications correspondant à différentes priorités utilisateur, comme indiqué au tableau 11.4.

Tableau 11.4 Classes d'applications en fonction des priorités utilisateur

Priorité utilisateur	Classe d'application
7	Contrôle du réseau (caractérisé par des paquets ayant la garantie d'être reçus afin de maintenir l'infrastructure du réseau)
6	Voix (délai de propagation de moins de 10 ms et jitte maximale connue – situation envisagée : traversée d'un LAN d'un campus)
5	Vidéo et Audio (délai de propagation de moins de 100 ms)
4	Trafic réseau contrôlé (typiquement pour des applications professionnelles avec contrôle d'admission et réservation de bande passante garantie pendant certaines périodes de transmission)
3	Platinium (typiquement pour des applications de type « best effort » pour certains utilisateurs privilégiés du réseau CPL)
1, 2	Trafic de fond (typiquement pour des transferts de fichiers et autres trafics importants mais n'impactant pas le reste des applications du réseau CPL)
0	Best effort (typiquement le trafic LAN classique : courriel, navigation Web, FTP, IRC, etc.)

Accès au média électrique

Comme nous l'avons vu aux chapitres 7 et 10, les deux méthodes d'accès principales au média électrique sont les suivantes :

- Couplage capacitif, qui consiste à brancher l'équipement CPL (passerelle ou équipement du réseau) sur une prise électrique, comme on branche un équipement électrique domestique *(voir figure 11.4).*

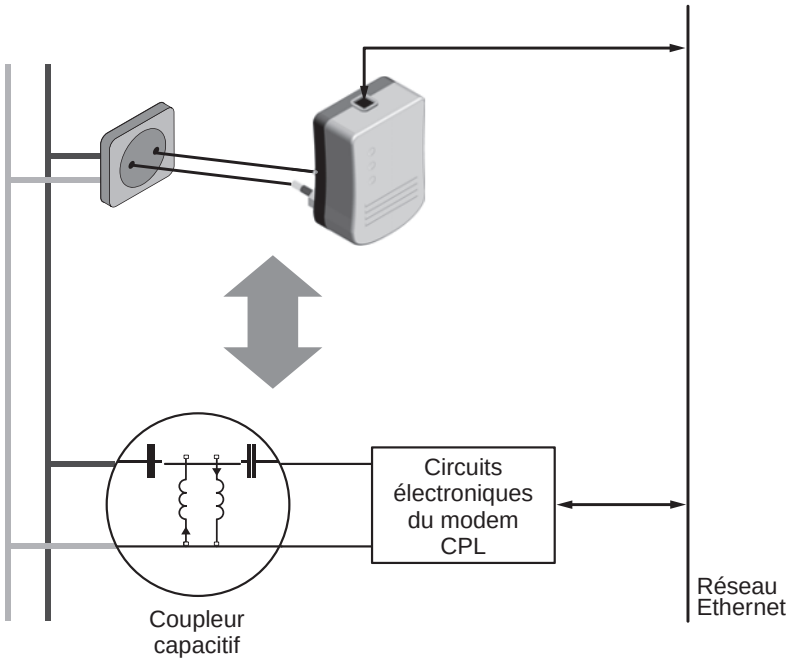


Figure 11.4
Principe du couplage capacitif d'un équipement CPL sur le réseau électrique

- Couplage inductif, qui est plus efficace pour diffuser le signal CPL sur les câbles et permet de meilleures performances. Cependant, il nécessite d'avoir accès aux câbles électriques, ce qui n'est possible qu'au niveau du tableau électrique puis en utilisant des coupleurs/injecteurs sur chaque câble, sur un seul câble ou sur plusieurs câbles en même temps.

La figure 11.5 illustre le principe de chaque type d'injection du signal CPL sur les câbles électriques au niveau du tableau électrique. Pour placer les systèmes d'injection du signal CPL, il est préférable de retirer le boîtier du tableau électrique afin d'accéder aux différents départs électriques vers les prises du bâtiment. Pour cette opération, il est nécessaire d'être habilité à intervenir sur des réseaux électriques ou de faire appel à un électricien agréé.

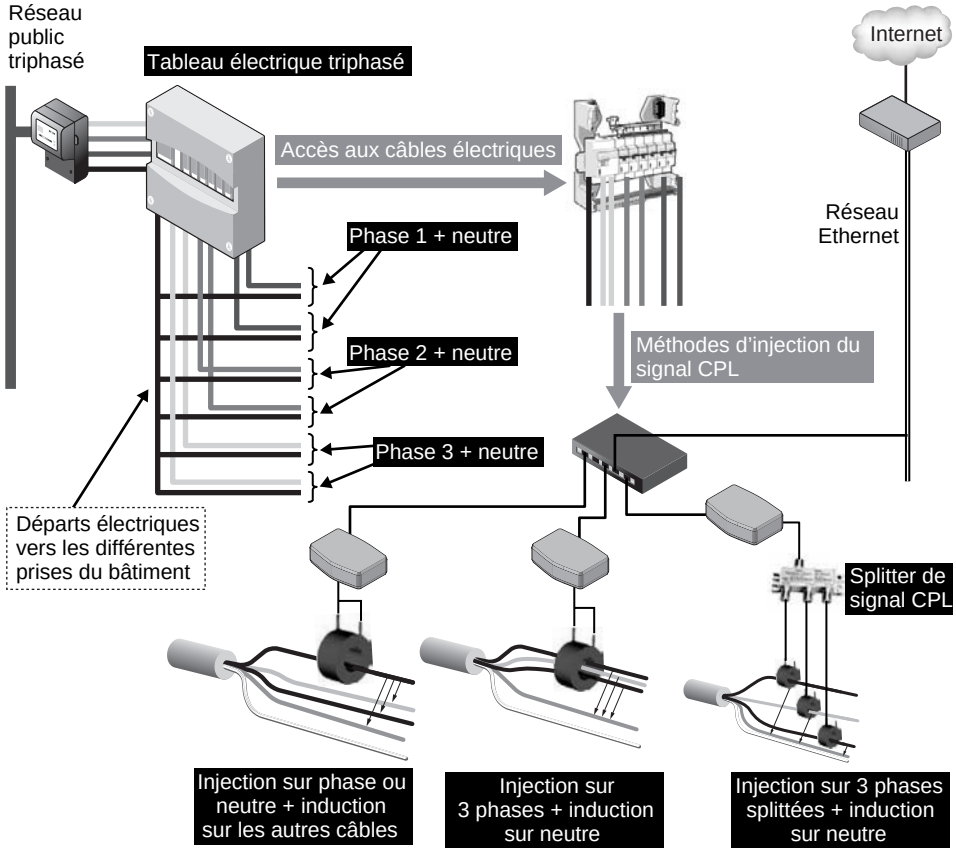


Figure 11.5

Méthodes de couplage inductif des équipements CPL sur les câbles électriques

Les phénomènes d'induction mutuelle entre câbles électriques d'un réseau, en particulier au niveau du tableau électrique, où les câbles sont proches les uns des autres, permettent d'envisager le système des différentes manières suivantes :

- Un seul câble (ou une seule phase ou le câble neutre), avec une induction sur les autres câbles.
- Plusieurs câbles en même temps, avec un seul injecteur qui englobe tous les câbles, l'induction mutuelle se faisant vers le câble neutre.
- Chaque phase (chaque câble), avec trois injecteurs différents reliés à l'équipement CPL câble TV *via* un splitter de signal TV « un vers trois ». L'induction se fait depuis les trois phases vers le câble neutre.

Placement des équipements

L'emplacement des équipements CPL sur le réseau électrique influence évidemment la propagation du signal CPL sur les différents câbles électriques parcourant un bâtiment. Il est donc important de choisir un emplacement qui favorise au mieux la propagation vers le maximum de prises électriques du réseau, comme l'illustre la figure 11.6.

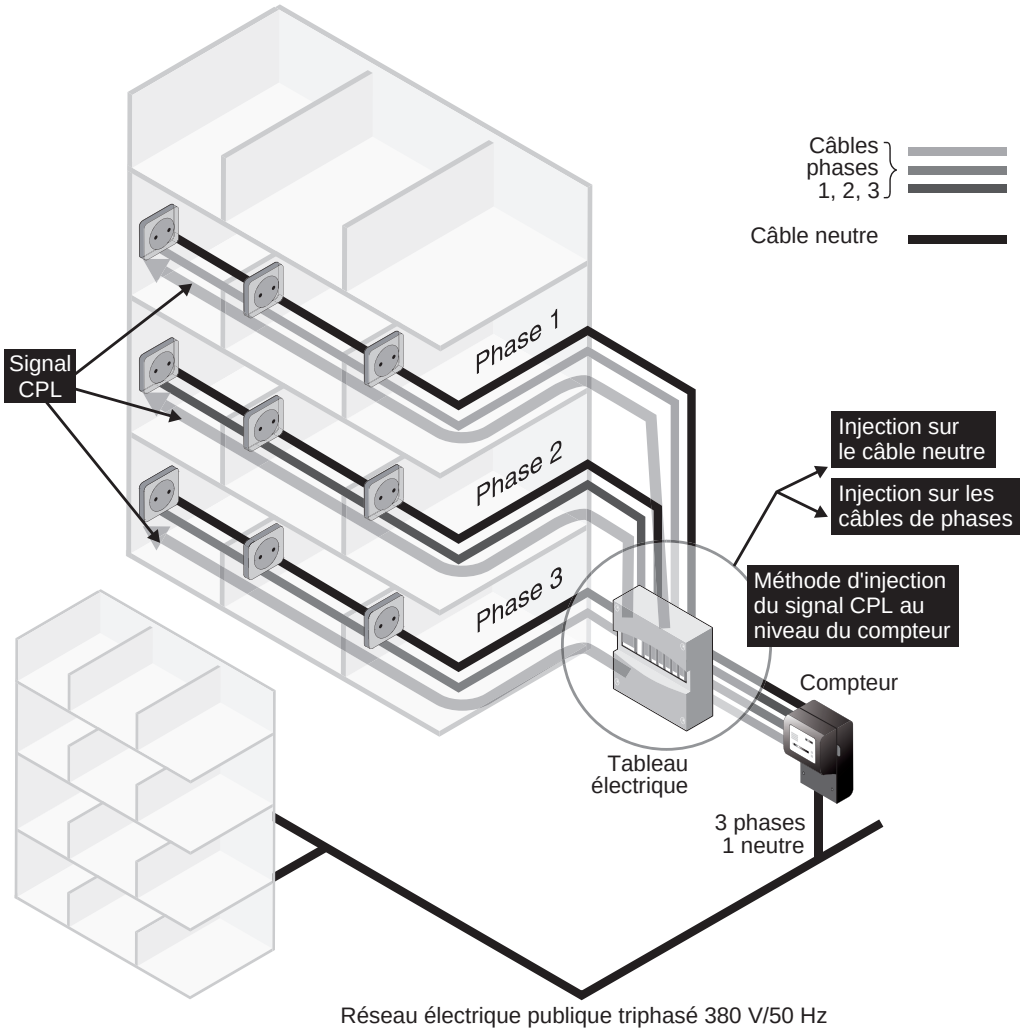


Figure 11.6

Injection du signal CPL au niveau du tableau électrique d'un bâtiment

Le tableau électrique est un endroit stratégique du réseau électrique puisqu'il peut être vu comme le « hub » du réseau, où tous les câbles se connectent pour récupérer l'électricité

provenant du compteur. Ce « hub » électrique est donc l'endroit idéal pour placer les équipements CPL qui vont faire office de passerelle, c'est-à-dire qui seront connectés à la fois au réseau LAN Ethernet de l'entreprise et au réseau électrique pour diffuser les trames Ethernet (Internet ou LAN) vers les différents équipements CPL branchés sur les prises.

Il est important de pouvoir récupérer un schéma de câblage du bâtiment afin de connaître la topologie du réseau électrique et de voir les différentes répartitions de phases (dans le cas d'une topologie triphasée).

Choix de l'architecture réseau

Comme nous avons pu le voir aux chapitres 3 et 10, il existe plusieurs types d'architectures réseau selon les technologies CPL utilisées.

Dans le cas d'une topologie pair-à-pair (HomePlug 1.0 ou Turbo), un des équipements fait office de passerelle entre le réseau Ethernet et le réseau électrique mais n'a pas de place spécifique dans le réseau CPL. Ce genre d'architecture est pertinent pour des réseaux de type LAN reliés entre eux par une dorsale Ethernet filaire.

Chaque équipement ayant le même niveau hiérarchique dans le réseau, il est important de ne pas trop éloigner les équipements CPL les uns des autres sur le réseau électrique (un équipement par pièce adjacente).

Dans le cas d'une architecture en mode maître-esclave (DS2 ou Spidcom), un des équipements (le maître) jouit d'une place privilégiée dans le réseau et doit pouvoir visualiser les différents équipements CPL esclaves. À nouveau, le tableau électrique est un emplacement central idéal pour diffuser le signal CPL vers une majorité de prises électriques du réseau électrique. Cet emplacement central peut être situé dans le local technique, au plus près des équipements réseau Ethernet du LAN.

Dans le cas d'une architecture en mode centralisé (HomePlug AV), les équipements de l'architecture sont le CCo (Central Coordinator) et les STA (stations). Il n'y a qu'un CCo par AVLN (AV Logical Network) pour gérer les liaisons CPL entre équipements CPL du réseau. De par ses fonctionnalités, HomePlug AV spécifie que l'équipement le « mieux » placé du réseau électrique, c'est-à-dire celui qui peut visionner les autres équipements, se configure automatiquement en CCo. Il est donc judicieux de placer cet équipement au point le plus central du réseau électrique, le tableau électrique, d'où il peut visualiser l'ensemble des équipements STA du réseau CPL HomePlug AV.

Nous illustrons ces différentes options d'architecture réseau dans l'exemple d'implémentation proposé en fin de chapitre.

Paramétrage de la sécurité

Comme nous l'avons vu au chapitre précédent consacré aux réseaux domestiques, il est important de configurer correctement les clés des réseaux CPL, afin qu'aucune personne malveillante ne puisse s'y introduire et récupérer les trames qui circulent sur le réseau électrique.

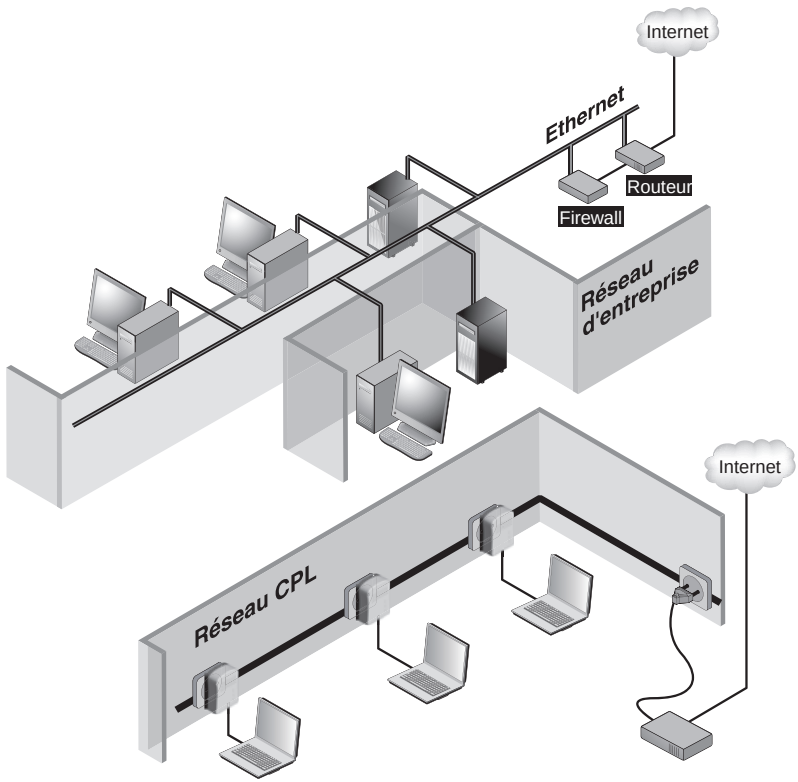
Précisons que, contrairement aux technologies Wi-Fi, qui utilisent l'air, et sont donc potentiellement écoutables, comme support physique, les technologies CPL rendent extrêmement difficile de se connecter sur le média électrique pour essayer de récupérer ces trames.

Dans le cas d'une entreprise, il est cependant nécessaire de veiller à bien configurer les pare-feu d'accès à Internet et à séparer correctement les différents réseaux logiques de l'entreprise afin de protéger ses données. Les sections qui suivent présentent les principaux axes à respecter pour cela.

Topologies de sécurité

Il existe des moyens radicaux pour sécuriser un réseau CPL d'entreprise, comme d'installer le réseau entièrement à l'extérieur du réseau de l'entreprise ou de sécuriser l'accès entre la partie CPL et le reste du réseau.

Figure 11.7
Exemple d'architecture de réseau CPL non connecté au réseau d'entreprise



La figure 11.7 illustre la première solution. L'installation d'un réseau CPL à l'extérieur du réseau de l'entreprise est généralement coûteuse, que ce soit en temps ou en achat de matériels. L'entreprise se retrouve de surcroît avec deux réseaux à gérer et donc deux connexions Internet, deux serveurs DHCP, etc., dont l'administration demande évidemment plus de temps.

Dans la seconde solution, illustrée à la figure 11.8, la connexion entre le réseau CPL et le réseau de l'entreprise est sécurisée de la même manière qu'une connexion Internet, par l'intermédiaire d'un firewall.

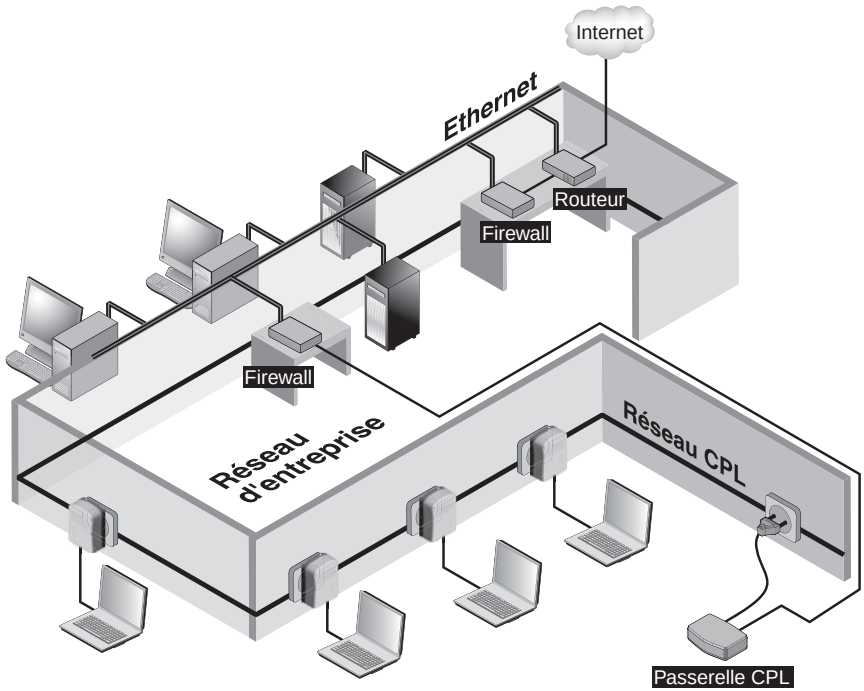


Figure 11.8

Architecture d'un réseau CPL connecté au réseau d'entreprise par l'intermédiaire d'un firewall

La société Asoka USA propose un switch CPL, qui permet de gérer plusieurs réseaux CPL HomePlug 1.0 et Turbo. Tous les équipements HomePlug 1.0 et Turbo ne supportant qu'une seule clé réseau à la fois, ils ne peuvent faire partie de plusieurs réseaux CPL en même temps.

Par ailleurs, il n'est pas possible de dissocier plusieurs équipements CPL HomePlug 1.0 et Turbo dans un même réseau électrique s'ils ont la même clé réseau. Le seul moyen de les dissocier est d'entrer une clé réseau différente sur chacun d'entre eux et un équipement CPL en passerelle capable de gérer toutes ces clés réseau. C'est ce que fait le

Switch 8330 d'Asoka, qui est capable de gérer jusqu'à 22 clés réseau CPL en même temps. Des informations sur ce produit sont disponibles à l'adresse suivante :

http://asokausa.com/cms/asokausa/pdf/switch8330pb050205%20%5BConverted%5D.pdf

Gestion de plusieurs réseaux CPL et séparation des clients CPL dans HomePlug AV

Parmi les fonctionnalités offertes par HomePlug AV et non disponibles dans HomePlug 1.0 et Turbo, la gestion de plusieurs clés réseaux dans un même équipement permet à un réseau CPL de configurer l'équipement central (CCo) avec plusieurs clés réseau et chacun des autres équipements CPL du réseau avec une seule clé réseau. Cela implique que les équipements CPL ne se voient pas les uns les autres et ne voient que l'équipement central, qui fait office de passerelle de niveau 2 pour les éléments CPL du réseau. Il est ainsi possible de constituer une architecture de type FAI, dans laquelle chaque élément du réseau n'a accès qu'à Internet et pas aux autres éléments du réseau électrique local. De par sa flexibilité, ce type de réseau CPL peut être modifié pour permettre aux éléments du réseau de se mettre sur le même réseau IP tout en ayant accès à Internet.

Configuration de la sécurité

La base de la sécurité d'un réseau d'entreprise repose avant tout sur la collecte d'informations et le monitoring, qui permet de déterminer l'origine d'une attaque.

Le point important de la sécurité des réseaux CPL réside dans la configuration d'une bonne clé réseau pour l'encryptage optimal des données échangées sur le réseau électrique (dans le cas de produits HomePlug, la clé NEK doit être longue et mélanger des caractères en majuscules et minuscules et des chiffres sur 20 caractères).

Suivant les constructeurs d'équipements CPL et les technologies CPL, il est plus ou moins possible de configurer des fonctionnalités de sécurité avancées. Le tableau 11.5 récapitule les principales fonctionnalités de sécurité des différentes technologies CPL.

Tableau 11.5 Fonctionnalités de sécurité des technologies CPL

Technologie CPL		Fonctionnalité de sécurité
HomePlug	1.0, Turbo	Clé NEK (DES 56 bits)
	AV	Clé NEK, clé NMK, clé DAK (AES-128 bits + rotation des clés)
	Oxance	Clé NEK, filtrage par adresse MAC et adresse IP des équipements connectés au réseau CPL, mot de passe PLRP (AES-128 bits), mot de passe sur l'interface de configuration HTTPS
DS2		Échange de clés maîtres-esclaves, filtrage d'adresses MAC et IP, mot de passe sur l'interface de configuration HTTP
Spidcom		Échange de clés maîtres-esclaves

VLAN (Virtual LAN)

Comme son nom l'indique, un VLAN (Virtual LAN) permet de définir des réseaux locaux virtuels. Apparue depuis plusieurs années dans les réseaux Ethernet sous le standard IEEE 802.1Q, cette technologie permet de faire cohabiter plusieurs réseaux locaux virtuels sur une même connexion Ethernet.

La plupart des switchs d'entreprise proposent cette solution, qui est à considérer pour greffer un réseau CPL à un réseau Ethernet existant. En créant deux réseaux locaux virtuels, l'un pour le réseau Ethernet et l'autre dédié spécifiquement au CPL, cette solution aboutit à la topologie illustrée à la figure 11.8, dans laquelle les deux réseaux sont séparés par un firewall.

Le VLAN CPL repose sur l'utilisation de multiples clés réseau (clés NEK dans le cas de HomePlug) ou de réseaux de différentes technologies (un réseau HomePlug et un réseau DS2, par exemple). HomePlug supporte la propagation des étiquettes VLAN, lesquelles peuvent être configurées sur les switchs du réseau Ethernet de l'entreprise.

Les réseaux privés virtuels (VPN)

Comme nous l'avons vu pour les réseaux CPL domestiques, les VPN (Virtual Private Network) représentent la manière la plus fiable de sécuriser un réseau CPL d'entreprise. Ils s'appuient pour cela sur une architecture client-serveur, dans laquelle le client est la station connectée à l'équipement CPL et le serveur une machine dédiée.

Cette solution étant détaillée au chapitre 10, nous n'y revenons pas ici. Bien que le projet soit maintenant arrêté, FreeS/WAN est la solution VPN Open Source de référence. Elle est disponible à l'adresse *http://www.freeswan.org.*

Installation et configuration d'un répéteur (bridge) CPL

Comme indiqué précédemment, le signal CPL se propage sur les câbles électriques et subit une atténuation significative du fait de la résistance des câbles et des perturbations électromagnétiques engendrées par les équipements électriques branchés sur le réseau électrique. Pour remédier à ce problème d'atténuation et obtenir une couverture optimale et complète d'un bâtiment en signal CPL, il peut être utile d'installer des équipements dits « répéteurs », afin d'étendre le réseau CPL aux zones du réseau électrique ou le signal CPL est trop atténué.

Nous donnons dans cette section un exemple de configuration d'un équipement répéteur de marque Oxance permettant d'étendre le réseau CPL installé. La notion d'équipement répéteur est corrélée avec celle de segment de réseau CPL.

L'architecture illustrée à la figure 11.9 inclut les équipements CPL suivants :

- CPL1 et CPL2 sont des produits Oxance PLT300 actifs en mode PLRP, propre à Oxance, administrables par le biais d'une interface Web sur l'interface réseau Ethernet.
- CPL3 est un produit Oxance PLT320 actif en mode PRLP qui a pour fonction de répéter le signal CPL sur le réseau électrique. Il dispose pour cela de deux interfaces CPL HomePlug, mais pas d'interface Ethernet, et est administrable par le biais de l'interface Web de CPL1 ou CPL2.
- CPL4 et CPL5 sont des produits CPL HomePlug passifs classiques, qui ne peuvent être connectés à CPL1 et CPL2 sans système de répétition.

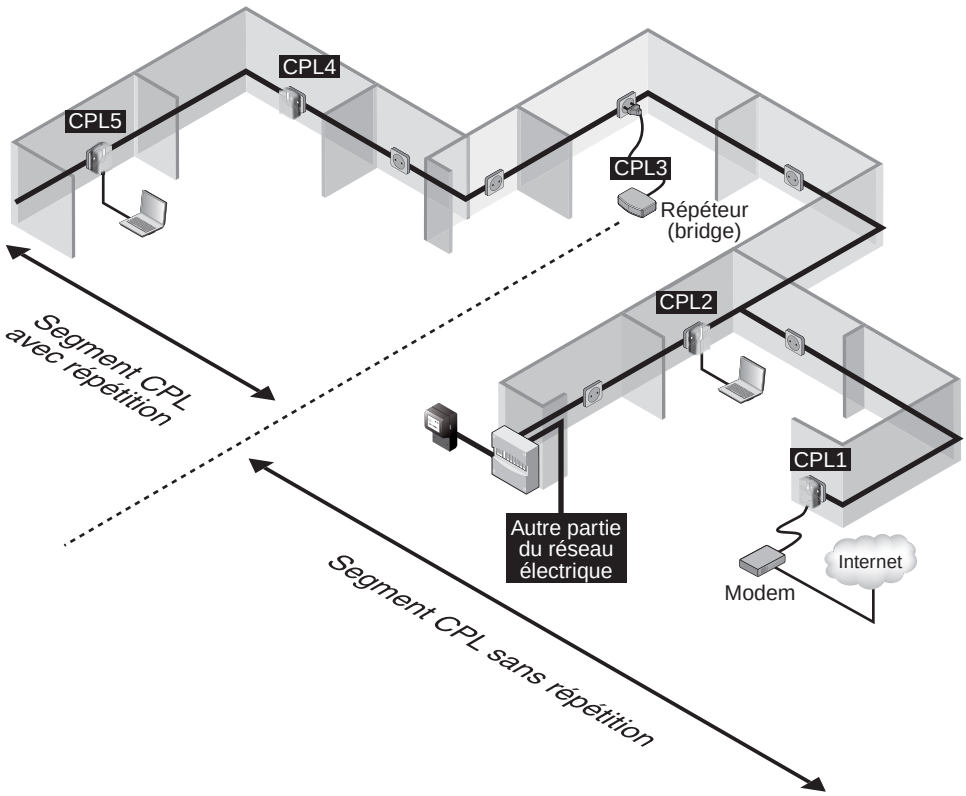


Figure 11.9

Exemple d'architecture réseau nécessitant une répétition du signal CPL

La figure 11.10 donne une représentation logique de ce réseau, avec les différents segments du réseau connectés les uns aux autres afin d'offrir une continuité de ce réseau CPL sur l'ensemble du réseau électrique.

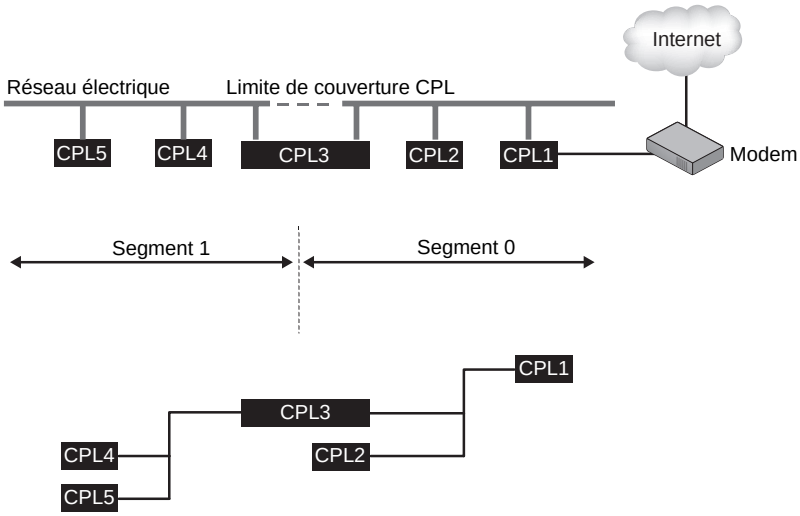


Figure 11.10

Représentation logique de la répétition du CPL sur deux segments

Le PLT320 dispose en sortie d'usine de l'adresse IP 192.168.1.251. Une fois, le PC de configuration correctement réglé pour être sur le même réseau IP (192.168.1.100, par exemple), il est possible de se connecter avec le mot de passe réseau (vide par défaut en sortie d'usine).

La figure 11.11 illustre la page d'accueil de l'outil de configuration telle qu'elle s'affiche sur le PC de configuration auquel est connecté un PLT300 lui-même connecté au PLT320.

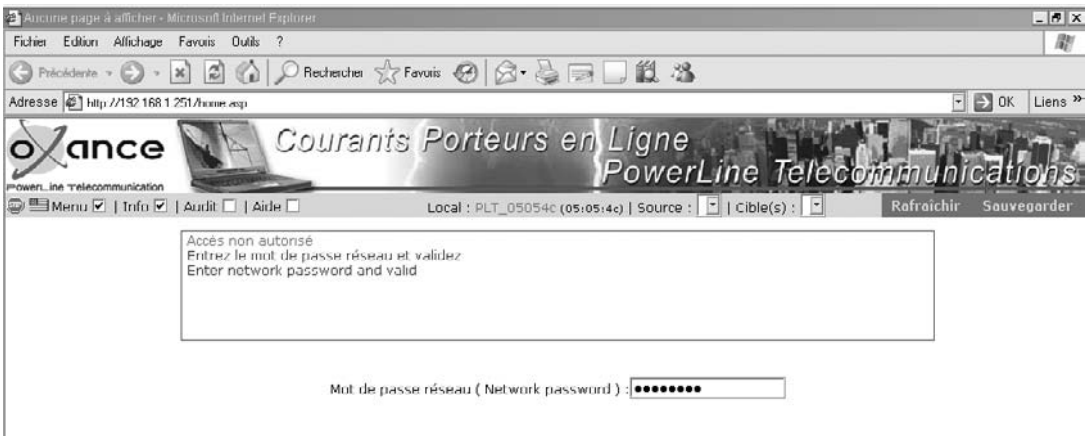


Figure 11.11

Page d'accueil de l'outil de configuration d'un équipement Oxance PLT300

Pour permettre aux équipements CPL Oxance actifs de se comporter en répéteur (ou bridge), il faut activer une option en se connectant au PLT320 *via* l'interface disponible sur le PLT300 et en entrant l'adresse MAC du PLT320 dans le menu Source de la barre de menus Oxance. Une liste déroulante affiche les équipements identifiés. Ces identifiants commencent par PLT et finissent par des caractères hexadécimaux correspondant à la fin de l'adresse MAC (adresse MAC égale à 0c000b0507e8 pour l'équipement identifié par PLT_0507e8).

Il est donc d'important de bien lire l'adresse MAC sur le boîtier de l'équipement à configurer et de la repérer dans le menu déroulant Source afin de pouvoir s'y connecter et modifier ses paramètres de configuration. Dans le cas présent, nous repérons l'équipement PLT320.

Une fois connecté au PLT320, il suffit de sélectionner le menu Configuration, puis Mode avancé et Options pour afficher la liste des options disponibles dans cet équipement, comme illustré à la figure 11.12. Pour activer une nouvelle option, comme « homeplug », qui permet de rendre l'équipement compatible avec les autres équipements CPL, il est nécessaire d'avoir une clé d'activation.

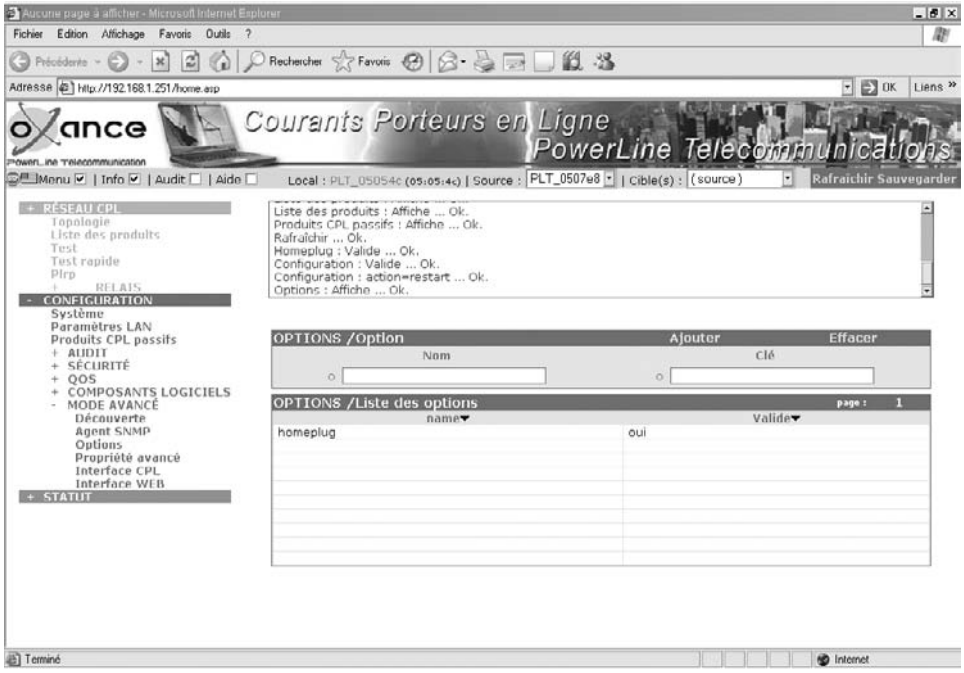


Figure 11.12

Équipement Oxance PLT320 avec la clé d'option « homeplug » validée

La clé doit être générée par la société Oxance pour permettre aux produits d'être compatibles avec les produits HomePlug passifs du marché. Cette clé sur 32 bits doit être entrée dans le champ Clé et son nom exact dans le champ Nom, en respectant la casse.

Une fois cette opération effectuée, il suffit de cliquer sur Ajouter pour afficher la nouvelle clé dans la liste des options du volet inférieur.

Il est possible d'ajouter des équipements CPL passifs (HomePlug 1.0 ou Turbo, sans le protocole PLRP d'Oxance), comme illustré à la figure 11.13, en sélectionnant le menu Produits CPL passifs et en entrant le mot de passe de la clé réseau DEK sous l'option HomePlug. Il correspond sur la figure à celui indiqué au dos du boîtier.

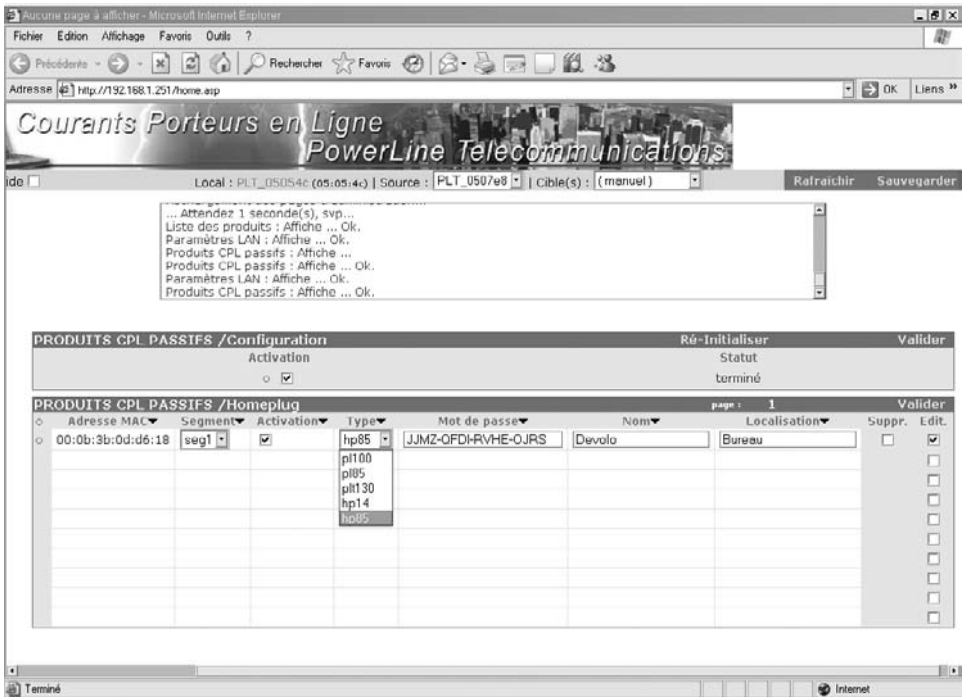


Figure 11.13

Ajout d'un équipement CPL passif au réseau CPL Oxance

Pour enregistrer ces paramètres, il faut cliquer sur Valider, à droite du volet PRODUITS CPL PASSIFS /Homeplug, puis sur Valider et sur Ré-Initialiser dans le volet PRODUITS CPL PASSIFS /Configuration et enfin sur Sauvegarder dans la barre de menus Oxance *(voir figure 11.14)*.

En sélectionnant le menu Statut du volet de gauche puis en cliquant sur « Visu. CPL direct », il est possible de vérifier que le nouvel équipement ajouté au réseau CPL par le biais du répéteur est visible au niveau de la couche MAC. À la figure 11.15, l'équipement nommé « Devolo » et le débit CPL estimé ne sont pas visibles (paramètre « unknown ») depuis cette version de l'outil Oxance (2.0.4).

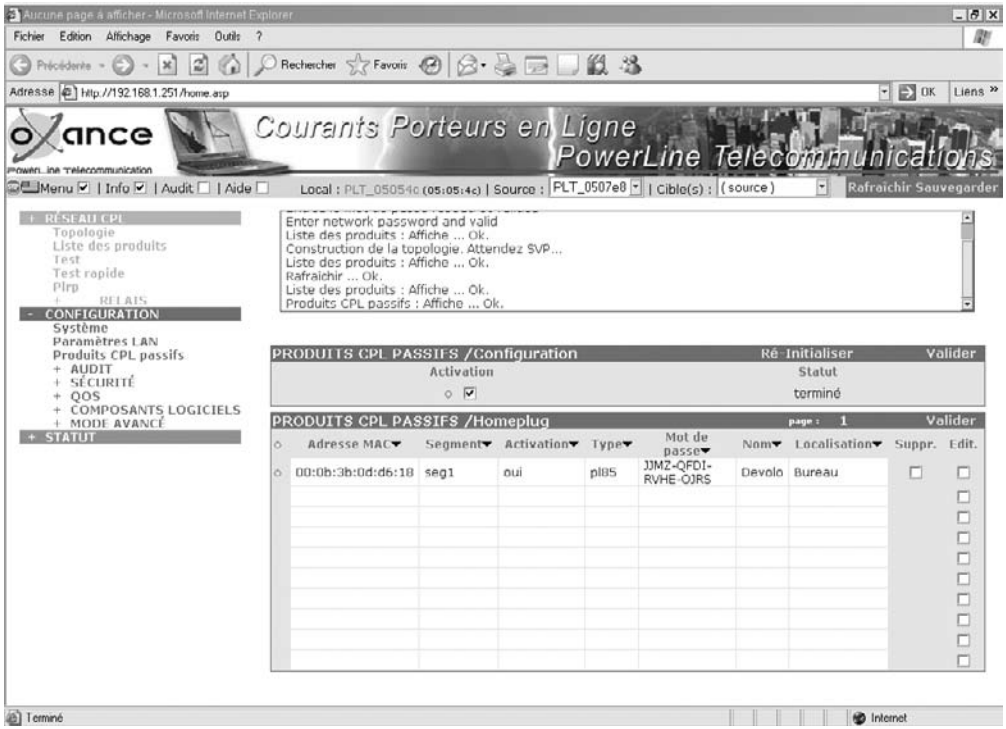


Figure 11.14

Vue d'ensemble des produits CPL passifs ajoutés au réseau CPL « répété »

Il faut maintenant se reconnecter sur l'équipement « local », c'est-à-dire l'équipement PLT300, puis sélectionner le menu Configuration dans le volet de gauche, cliquer sur RESEAU CPL /Liste des produits et cliquer sur Découvrir dans le volet du bas pour voir si l'équipement CPL passif est visible dans les équipements détectés. Si c'est le cas, une ligne supplémentaire donne des détails sur l'équipement en question.

Dans l'exemple de la figure 11.16, il s'agit d'un équipement Devolo HomePlug Turbo. Pour valider la liste des équipements CPL détectés, cliquer alors sur Valider.

Une fois cette étape réalisée, il est possible de visualiser l'ensemble des équipements CPL (PLT300, PLT320, HomePlug passifs) présents sur le réseau électrique en sélectionnant Réseau CPL puis Topologie dans le volet de gauche, comme illustré à la figure 11.17. Nous retrouvons bien notre topologie, le réseau CPL étant constitué de deux segments, Seg0 et Seg1, reliés par le répéteur PLT320.

Finalement, la figure 11.18 illustre l'affichage de l'architecture CPL que nous venons de configurer. Nous pouvons vérifier que les deux segments du réseau CPL (segment 0 et segment 1) sont bien reliés par l'équipement répéteur PLT320 repéré par le nom PLT_0507e8.

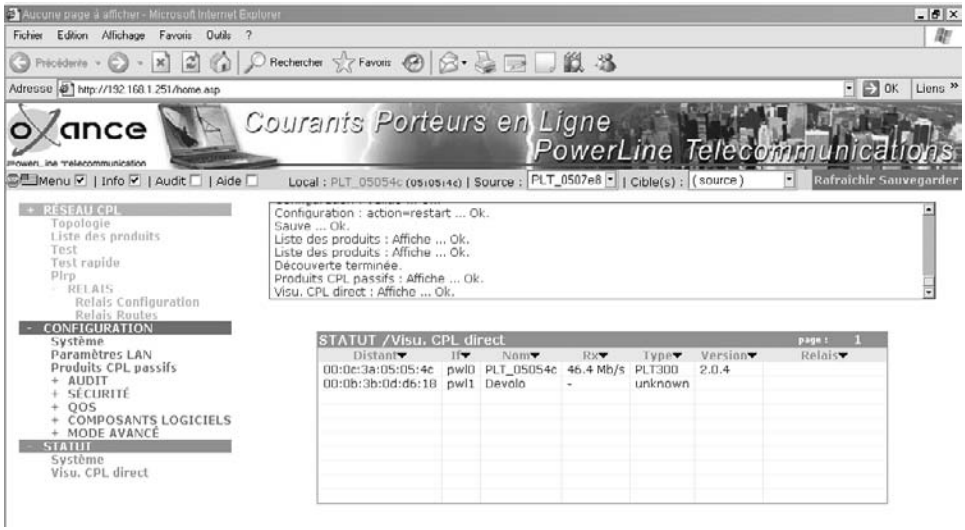


Figure 11.15

Visualisation directe des équipements CPL au niveau de la couche MAC

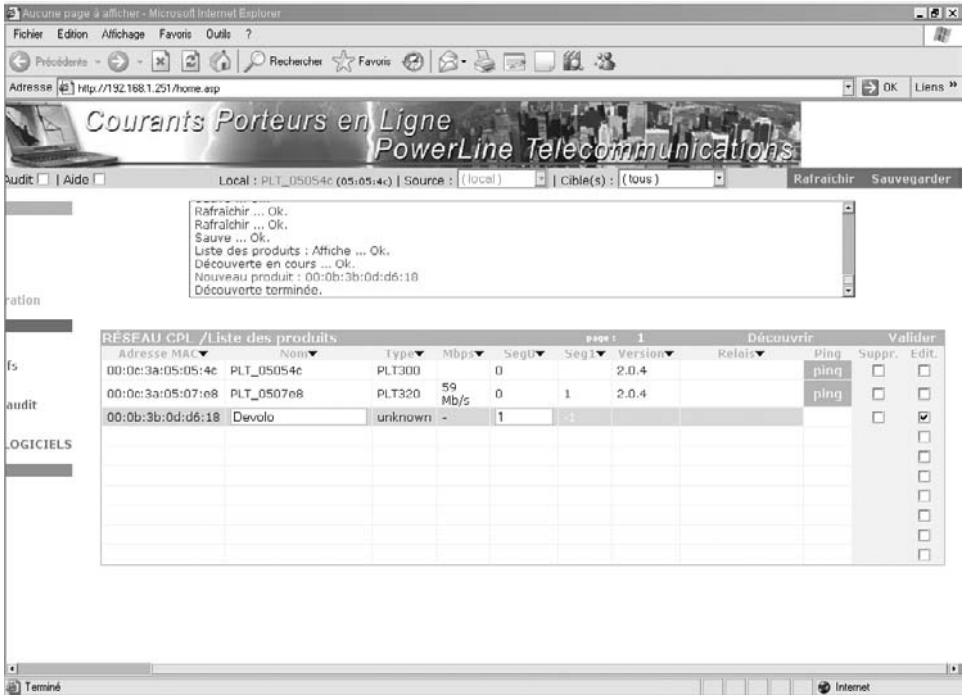


Figure 11.16

Visualisation des produits CPL présents sur le réseau électrique

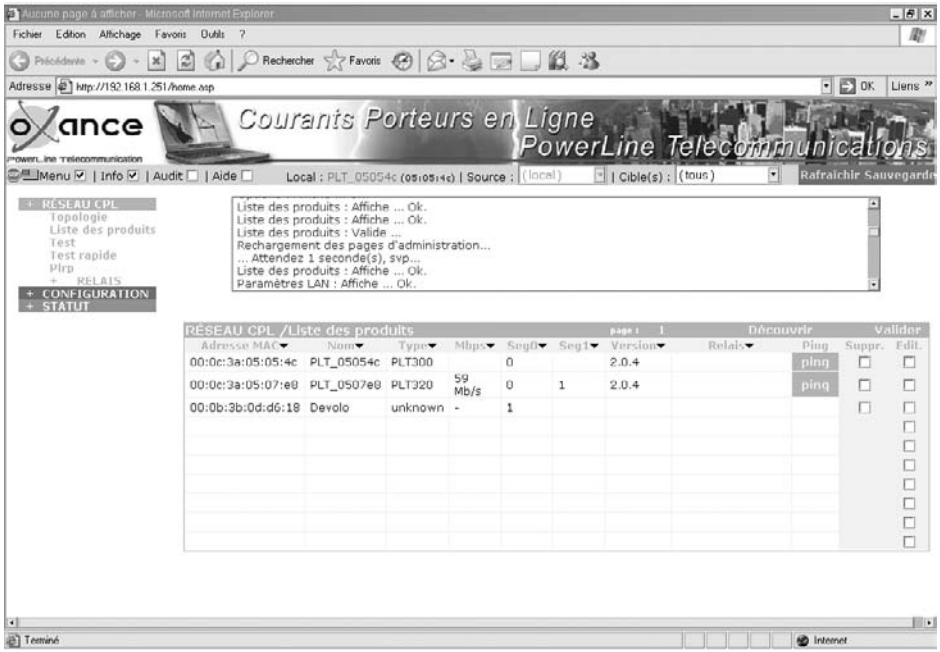


Figure 11.17
Visualisation de la liste des produits actifs et passifs du réseau local CPL

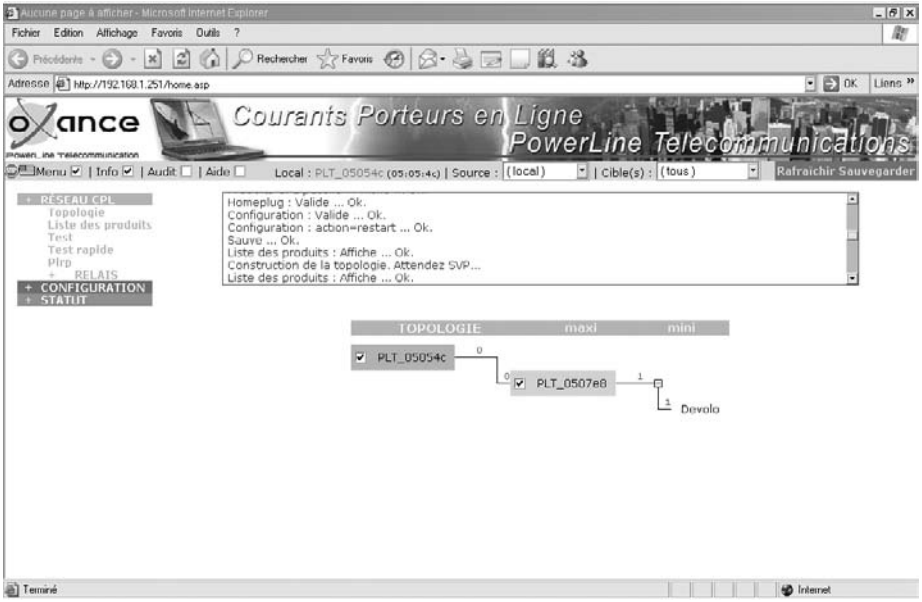


Figure 11.18
Visualisation de la topologie de réseau avec bridge

La téléphonie IP CPL

Les réseaux CPL pouvant être vus comme des réseaux Ethernet sur le réseau électrique, il est possible d'y connecter des téléphones IP au sein de l'entreprise. Ces téléphones sont configurés de manière à pouvoir se connecter sur un PABX (autocommutateur) de type IP. Ce dernier récupère les flux au protocole SIP (Session Initiation Protocol) provenant des téléphones et sert de passerelle vers le RTC, c'est-à-dire le réseau de téléphonie analogique classique.

L'outil libre de droit Asterisk, disponible à l'adresse *http://www.asterisk.org,* peut être installé sur le réseau d'entreprise afin de gérer le parc de téléphones IP sur CPL.

L'avantage de cette solution est qu'elle permet de déplacer les téléphones IP sur tout le réseau électrique. La figure 11.19 en donne un exemple d'architecture.

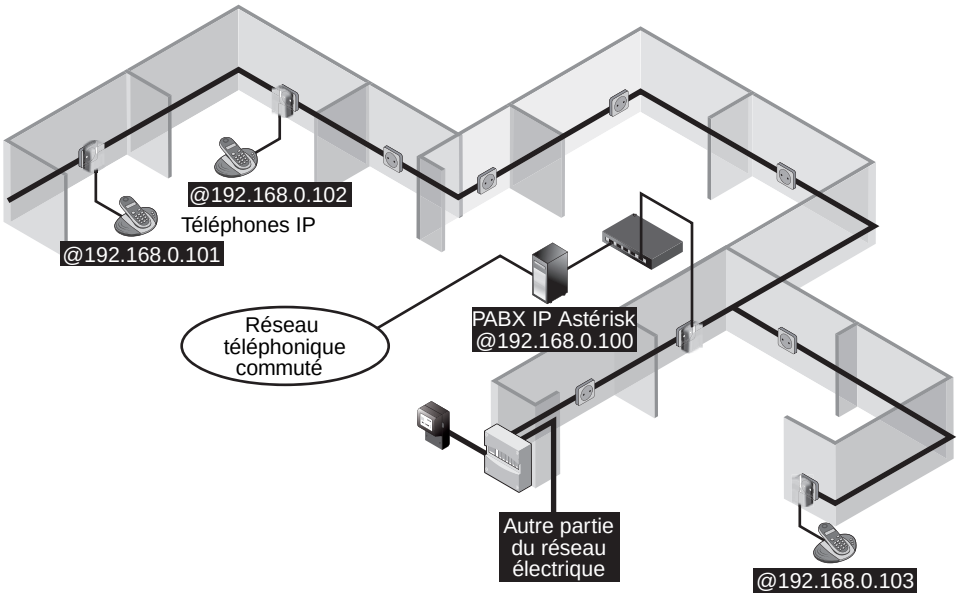


Figure 11.19

Infrastructure de téléphonie IP sur réseau CPL

Exemple de mise en œuvre de réseau CPL dans un hôtel

Un hôtel désire s'équiper d'un réseau informatique multiusage pour les différents services qu'il propose à ses clients et décide d'installer un réseau CPL.

La figure 11.20 illustre l'architecture réseau de l'hôtel, avec deux bâtiments alimentés par un compteur et deux tableaux électriques (un pour chaque bâtiment).

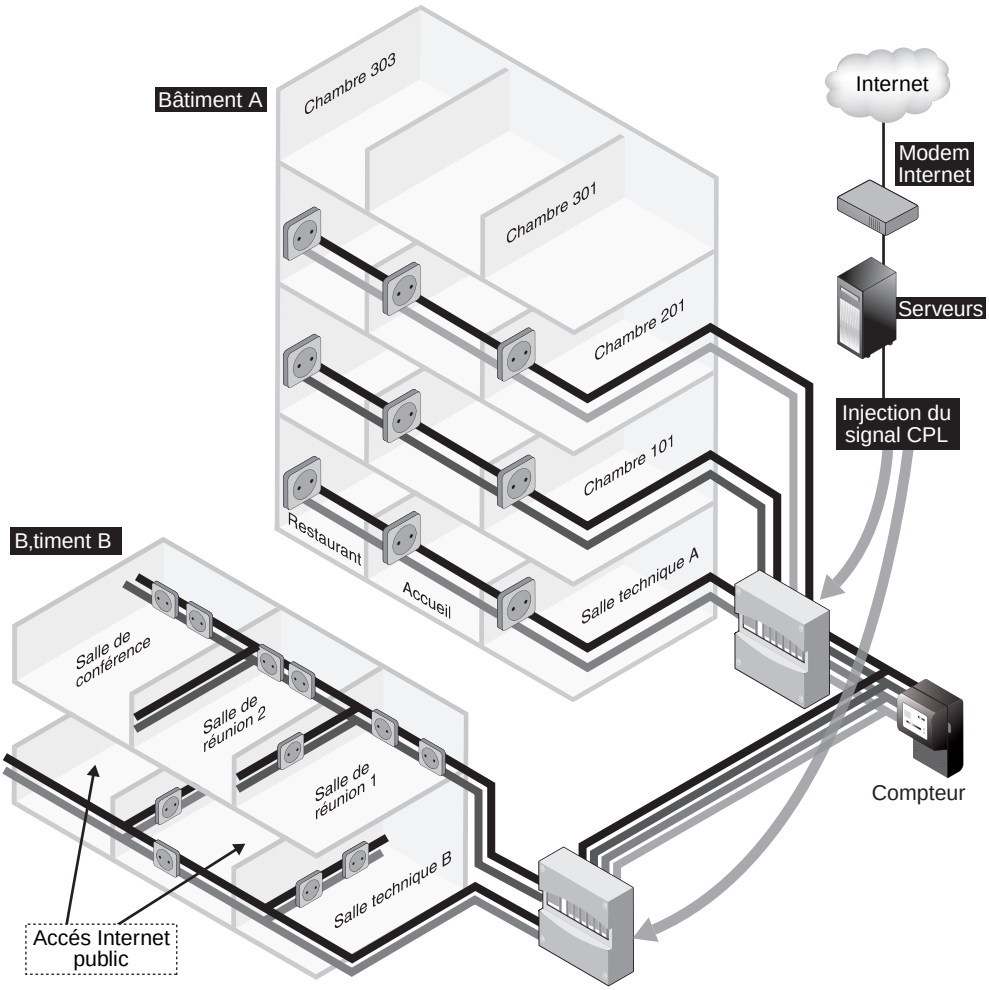


Figure 11.20
Architecture du réseau CPL de l'hôtel

Au sein de ces deux bâtiments, le gestionnaire de l'hôtel désire les services suivants :

- Bâtiment A :
  - Accès Internet avec confidentialité des données dans chaque chambre.
  - Accès Internet et raccordement des caisses du restaurant au système d'information de l'hôtel.
- Bâtiment B :
  - Salle de réunion 1, qui propose un réseau local Ethernet sur CPL afin de permettre des échanges entre ordinateurs connectés, ainsi qu'un accès Internet sécurisé.

– Salle de réunion 2, qui propose les mêmes services que la salle de réunion 1, mais avec respect de la confidentialité des données échangées entre les réseaux des deux salles.

– Deux salles avec accès Internet public ouvert aux clients de l'hôtel.

– Salle de conférence avec solution de vidéoconférence IP par le réseau CPL.

Mise en œuvre du réseau

La mise en œuvre de ce réseau demande de bien visualiser l'ensemble des réseaux logiques connectés ou non les uns avec les autres dans les deux bâtiments.

L'architecture réseau doit prendre en compte les éléments suivants, comme illustré à la figure 11.21 :

- place et configuration des différentes passerelles CPL et de l'injection du signal CPL ;
- accès Internet de l'hôtel ;
- clés réseau des différents CPL, qu'ils soient ou non séparés les uns des autres ;
- liens réseau entre les bâtiments.

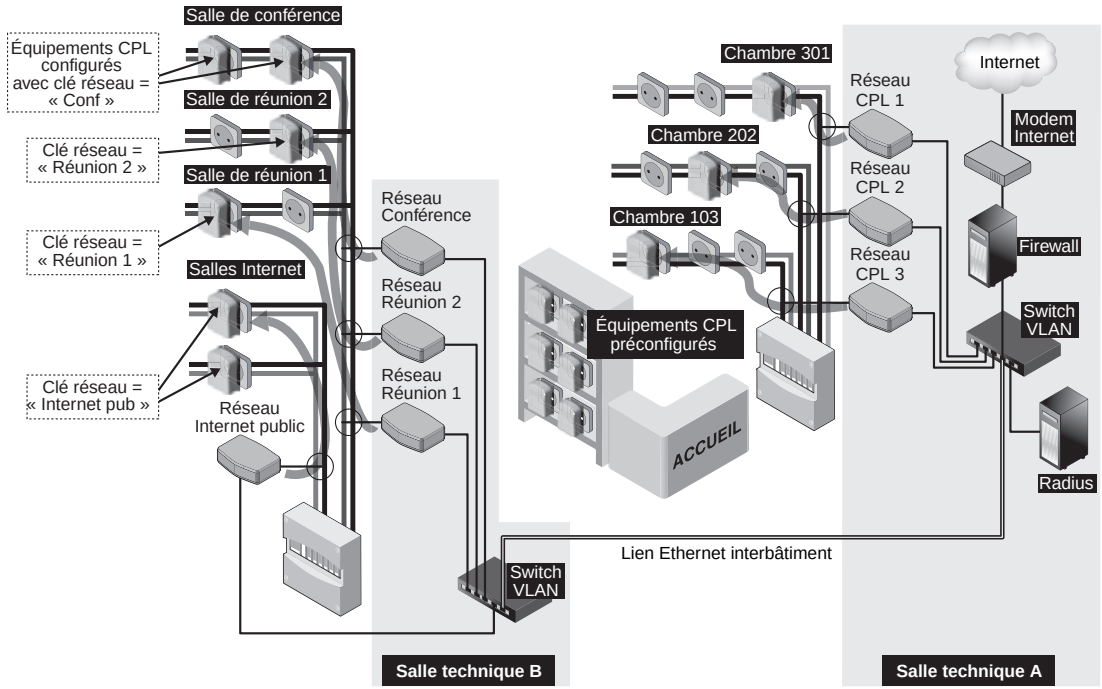


Figure 11.21

Architecture complète des réseaux CPL de l'hôtel

La figure 11.22 illustre l'architecture logique d'ensemble à mettre en œuvre. Elle comporte des parties en Ethernet câblé, comme le lien entre les deux bâtiments, puisqu'on souhaite maintenir de bonnes performances en terme de débit et un service garanti afin d'éviter de dégrader le service IP dans le bâtiment B.

Afin de séparer les différents réseaux CPL, il est important de les mettre si possible sur des phases différentes (trois câbles de phase et un câble de neutre dans le cas d'une installation triphasée) et surtout de configurer des clés réseau différentes pour chaque service désiré. En terme de sécurité, il peut être envisagé de mettre en place un serveur RADIUS afin d'authentifier les clients du réseau CPL.

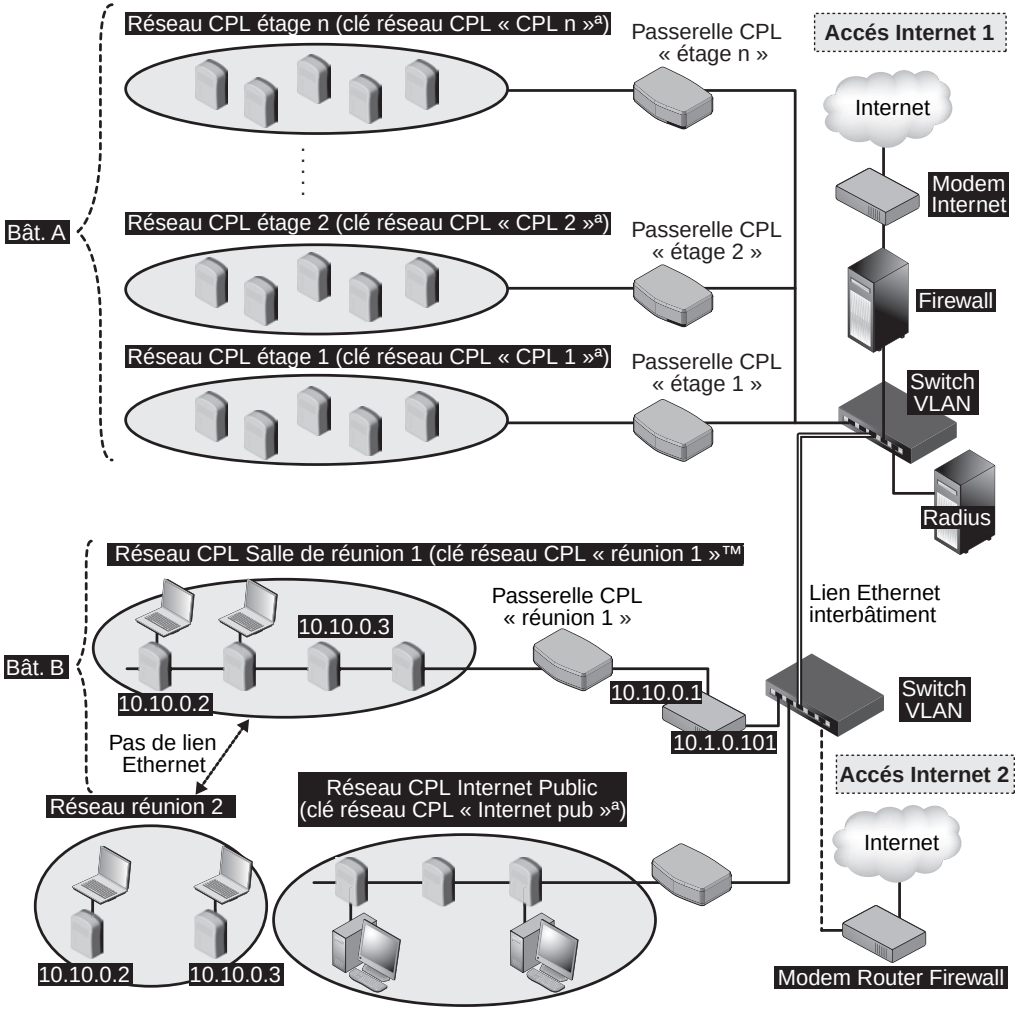


Figure 11.22

Architecture logique d'ensemble des réseaux CPL de l'hôtel

Cette figure montre les connexions des réseaux CPL au système d'information, notamment les accès Internet dans les chambres de l'hôtel et les configurations avec un routeur NAT pour les salles de réunion permettant de sécuriser les PC des clients mais aussi le réseau d'entreprise vis-à-vis des réseaux CPL administrés.

Réseaux CPL d'étage de l'hôtel

L'hôtel propose aux clients de se connecter à Internet dans leur chambre *via* un prêt d'équipement CPL à brancher sur les prises de la chambre. Cette connexion à Internet doit se faire de manière authentifiée, sécurisée et confidentielle. Les équipements CPL disponibles à l'accueil de l'hôtel sont donc préconfigurés pour être capables de se connecter sur le réseau CPL d'étage.

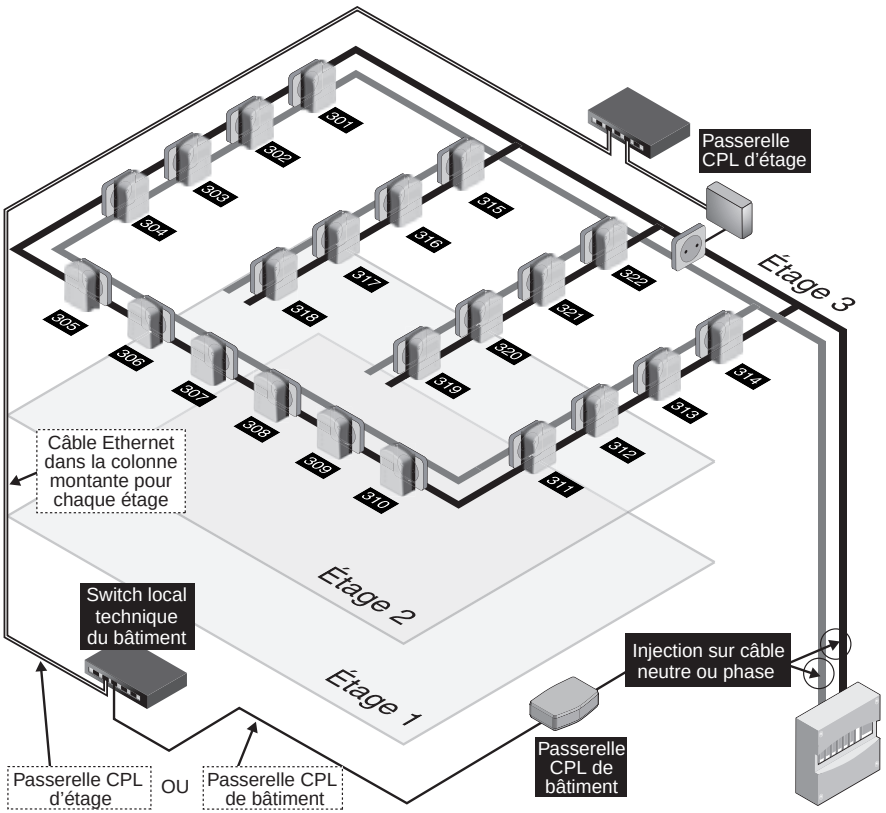


Figure 11.23

Gestion du réseau CPL d'étage avec plus de 15 équipements

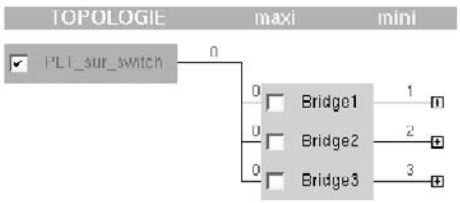
Le problème technique posé vient de ce que HomePlug 1.0 et Turbo spécifient une limite de 15 équipements par réseau CPL derrière une passerelle CPL. La figure 11.23 illustre le plan d'un étage, comportant plus de 15 équipements CPL potentiellement connectables au réseau d'entreprise Chambres de l'hôtel, qui compte 22 chambres. Le signal CPL est amené

soit par injection depuis le tableau électrique du bâtiment, soit, s'il y a trop de distance, en tirant un câble Ethernet à chaque étage et en incluant une passerelle CPL par étage.

En utilisant les produits Oxance PLT300, il est possible d'ajouter des extensions de réseau CPL au-delà de la limite des 15 équipements en créant des « segments », c'est-à-dire des zones CPL de 15 équipements. Pour 22 chambres, il suffit d'avoir deux segments (un de 15 et un de 7) pour couvrir les besoins de l'étage.

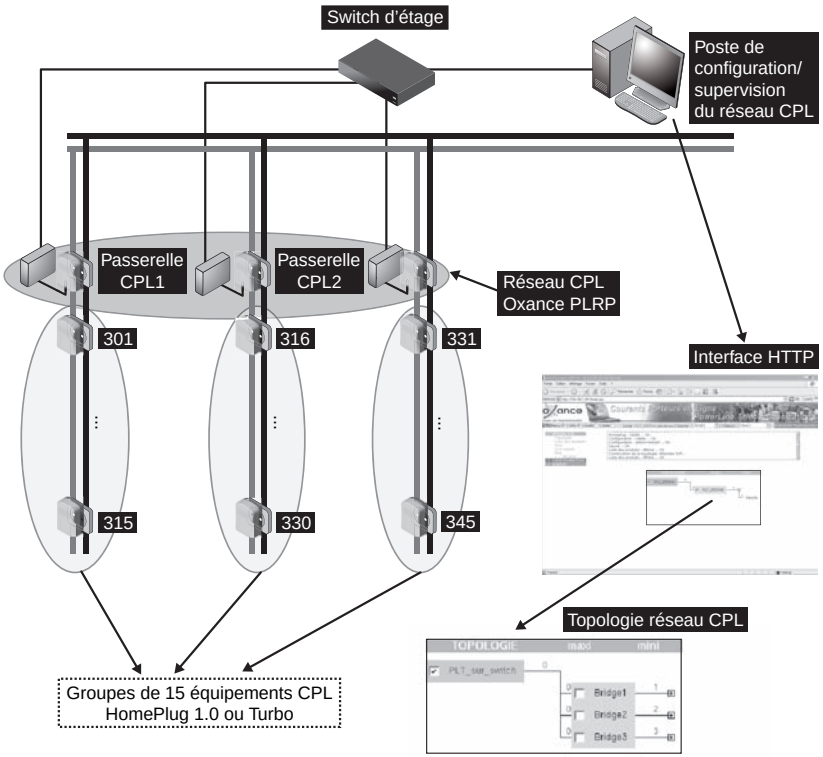
L'interface d'administration Oxance en HTTP illustrée à la figure 11.24 donne une vision des « bridges » CPL et des segments avec 3 segments potentiels de 15 équipements CPL.

Figure 11.24
Topologie du réseau CPL Oxance avec bridges



La figure 11.25 illustre l'architecture CPL à configurer au niveau de l'équipement CPL Oxance PLT300 permettant de gérer ces 3 segments de 15 équipements CPL.

Figure 11.25
Architecture réseau d'étage avec plusieurs segments CPL



Accès Internet avec confidentialité entre ordinateurs

Un des inconvénients des réseaux CPL HomePlug 1.0 et Turbo vient du fait que le support est partagé et qu'il peut donc y avoir des connexions réseau entre équipements CPL du réseau, et donc entre chambres, comme le montre le cas des trois chambres illustré à la figure 11.26.

La confidentialité des données est cependant possible avec les équipements PLT300 d'Oxance, qui permettent de mettre en place des règles de blocage entre ordinateurs du réseau CPL.

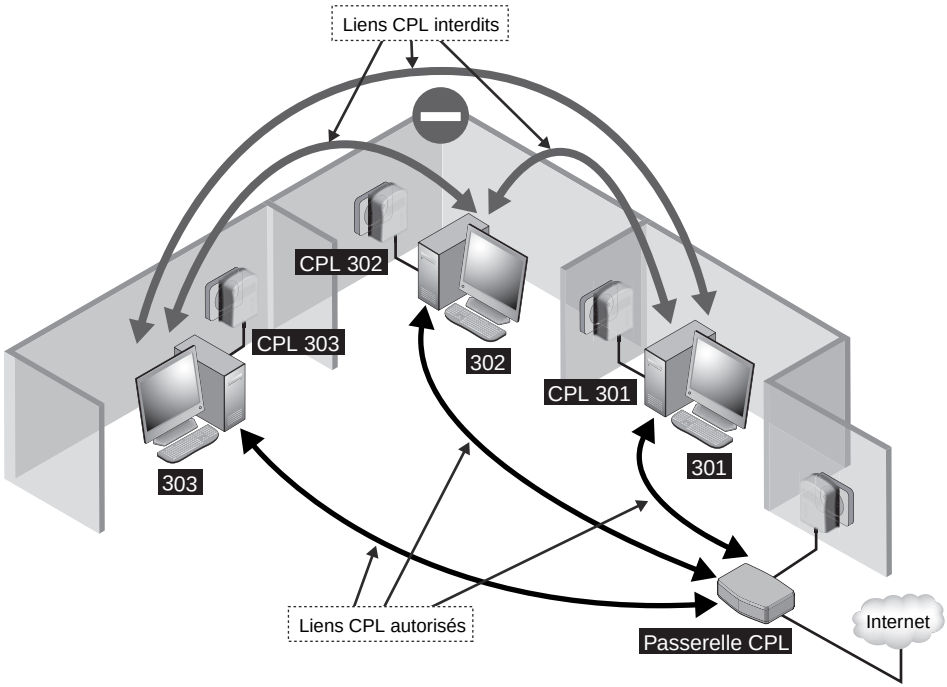


Figure 11.26

Accès Internet avec confidentialité entre ordinateurs

Supposons que le réseau des chambres soit en 192.168.0.1/24. La configuration de ces règles s'effectue à l'aide de l'interface HTTP par le biais du menu Sécurité en sélectionnant le sous-menu Filtrage des données et en cochant la case Edit. La nouvelle règle de filtrage doit évidemment indiquer les adresses IP source et destination de toutes les stations à filtrer.

La règle à mettre en place doit bloquer les trafics IP bidirectionnels de toute machine du réseau 192.168.1.0/24 vers toute autre machine de ce même réseau. Une règle supplémentaire est nécessaire pour autoriser tout trafic bidirectionnel vers les réseaux extérieurs.

La figure 11.27 illustre les deux nouvelles règles mises en place dans le sous-menu Filtrages de données. La première bloque les trafics entre les machines du même réseau afin d'isoler les machines entre elles. La seconde permet le trafic sortant vers d'autres réseaux IP, telle la connexion à Internet.

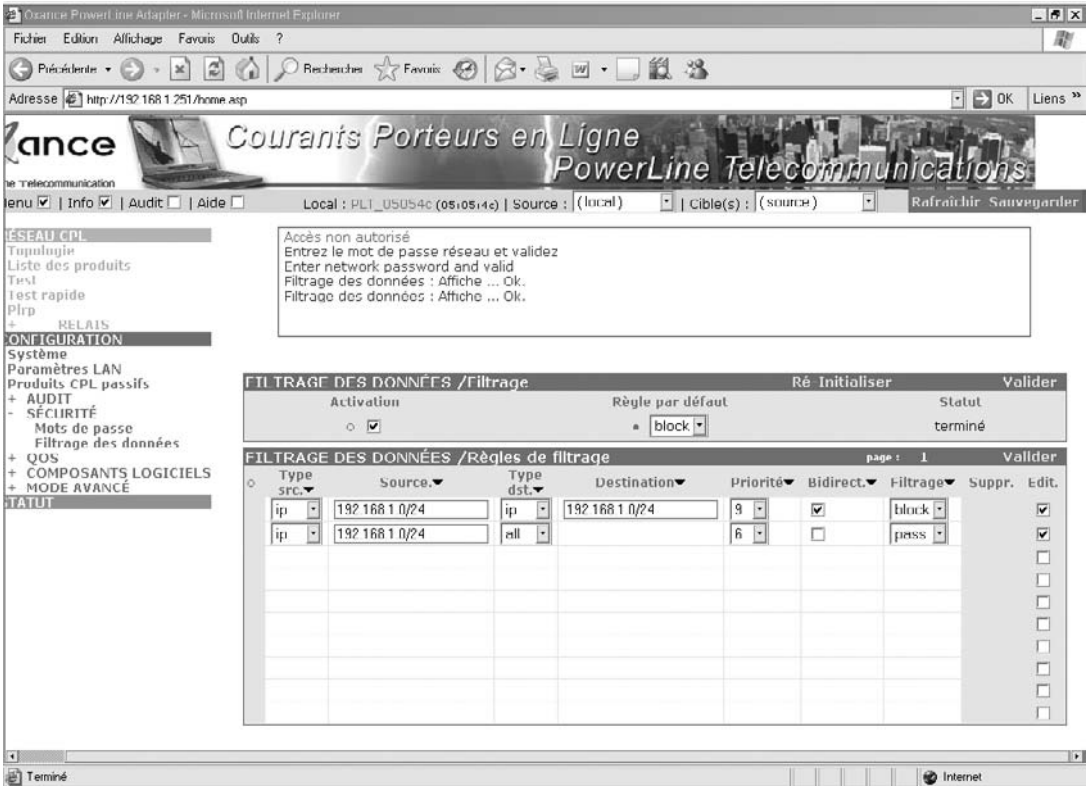


Figure 11.27

Configuration de la confidentialité entre ordinateurs

Il est possible que le réseau CPL Oxance et celui des terminaux portables des clients de l'hôtel aient des plans d'adressage différents sans que cela perturbe le réseau IP, puisque les communications se déroulent au niveau Ethernet.

Configuration d'un client DHCP sous Linux

Il est de plus en plus fréquent de trouver des systèmes Linux dans les réseaux d'entreprise, que ce soit sur les serveurs ou les postes client. Il est donc important pour les administrateurs de réseaux professionnels de savoir comment configurer un client DHCP sous Linux.

Avant de commencer la configuration du client DHCP, il convient de s'assurer que la carte Ethernet fonctionne sous Linux. Si ce n'est pas le cas, il faut installer les drivers pour cette carte.

Sous Linux, il existe deux clients DHCP très répandus : dhclient et pump, qui sont disponibles dans toutes les distributions Linux.

La configuration d'un client DHCP peut se faire de manière manuelle, en saisissant **dhclient eht0** ou **pump eht0,** suivant le client concerné, `eth0` étant l'interface réseau, ou automatiquement, en modifiant le fichier **/etc/pcmcia/networks.opts.**

Comme dans le cas de Windows, il suffit de saisir **ifconfig eth0** pour connaître l'état des paramètres de la carte et savoir si cette dernière est bien configurée. Si la carte n'a pas été configurée par le serveur DHCP, aucune adresse IP n'apparaît :

```
# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:02:2D:4C:05:B8
          inet addr:10.0.0.2  Bcast:10.0.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:3 Base address:0x100
```

Configuration du serveur DHCP/NAT

La plupart des distributions Linux proposent un serveur DHCP, nommé dhcpd.

La configuration du serveur DHCP ne demande que la création d'un fichier de configuration **dhcpd.conf,** qui sera placé dans le répertoire **/etc.**

Voici un exemple de fichier **dhcpd.conf :**

```
subnet 10.0.0.0 netmask 255.255.255.0 {
range 10.0.0.2 10.0.0.50;
option routers 10.0.0.1;
option domain-name-servers 10.0.0.60;
default-lease-time 1000
max-lease-time 3600
}
```

- `subnet` permet de définir l'adresse réseau utilisée par les adresses IP.
- `netmask` définit le masque de sous-réseau.
- `range` définit la plage d'adresses fournie par le serveur dhcpd.
- `option routers` définit l'adresse IP de la passerelle par défaut.
- `option domain-name-servers` définit l'adresse DNS.
- `default-lease-time` définit la durée du bail par défaut, ici 1 000 secondes.
- `max-lease-time` définit la durée maximale du bail.

Le serveur dhcpd peut être lancé chaque fois que la passerelle Internet est allumée en entrant la ligne :

```
# dhcpd eth0
```

où `eth0` est l'interface Ethernet connectée à la passerelle.

Il peut aussi être lancé de manière automatique en créant un script dans le répertoire **/etc/rc** et en incorporant la commande suivante :

```
/usr/sbin/dhcpd eth0
```

NAT (Network Address Translation)

Le NAT est une technique qui permet de connecter à Internet plusieurs machines sur une même adresse IP. Le NAT a été et reste largement utilisé pour pallier le faible nombre d'adresses IP disponibles.

Supposons un réseau CPL dans lequel un modem-routeur CPL est connecté à Internet, comme illustré à la figure 11.28.

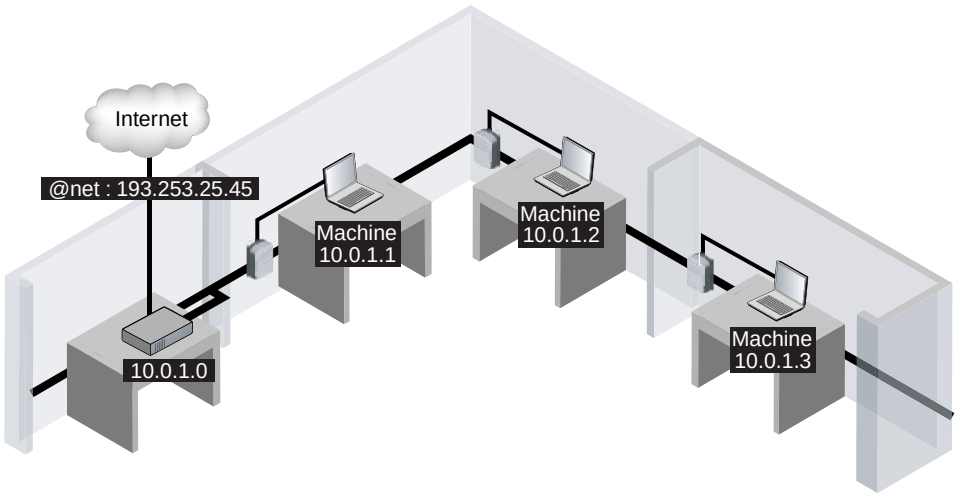


Figure 11.28
Réseau CPL connecté à Internet

Les machines du réseau ne peuvent accéder à Internet que si le modem Internet ou une autre entité dans le réseau incorpore des fonctions de routage NAT et est connecté à Internet. La plupart d'entre eux incorporent le NAT.

Le routage NAT permet de n'utiliser qu'une seule adresse routable sur Internet pour un ensemble de machines possédant des adresses privées fixes, non routables.

Lorsqu'une machine envoie des données qui ne sont pas destinées au réseau local, le routeur NAT – ici le modem Internet – remplace l'adresse IP de l'expéditeur par l'adresse IP de connexion donnée par le fournisseur d'accès Internet (@net sur la figure). Dans le même temps, le modem Internet inscrit dans une table de correspondance les informations de la connexion (adresse IP de l'expéditeur, protocole utilisé).

Lorsque le modem Internet reçoit des données provenant d'Internet, il vérifie dans sa table de correspondance à qui ces données sont destinées en comparant le type des données reçues aux informations contenues dans la table. Une fois le destinataire trouvé, l'adresse IP @net est remplacée par celle du destinataire. De la sorte, toutes les machines du réseau utilisent la même adresse IP pour accéder à Internet.

Grâce à ce système d'adressage, le NAT peut filtrer les paquets entrants et éviter les attaques externes. Si les machines ne sont pas à l'initiative de la connexion, les paquets extérieurs ne peuvent être traités par le routeur NAT.

Configuration du NAT

Contrairement au serveur DHCP, le NAT dépend du noyau utilisé, 2.2 ou 2.4/2.6. Dans les deux cas, et comme pour le serveur DHCP, il est possible soit de lancer le NAT manuellement après avoir allumé la passerelle, soit d'écrire un script dans le répertoire **/etc/rc** de façon à automatiser l'exécution du NAT lors du démarrage de la passerelle.

Quel que soit le noyau utilisé, il faut commencer par modifier le fichier **/etc/network/options,** à l'aide de la commande **vi,** par exemple, et modifier la ligne `ip_forward=no` en `ip_forward=yes`.

Pour les noyaux 2.2, la commande **ipchains** permet de gérer le NAT :

```
/sbin/ipchains -A forward -i ppp0 -s 10.0.0.0/24 -j MASQ
```

`ppp0` est l'interface reliée à Internet.

Pour les noyaux 2.4 et 2.6, il faut utiliser la commande **iptables :**

```
/sbin/iptables -t nat -A POSTROUTING -o ppp0 -s 10.0.0.0/24 -j MASQUERADE
```

`ppp0` est l'interface reliée à Internet.

Comme indiqué précédemment, le réseau CPL peut être vu comme une infrastructure de niveau 2 (Ethernet) permettant de connecter les différents terminaux IP entre eux. La configuration IP des équipements connectés à ce réseau est donc celle que l'on retrouve classiquement dans tous les réseaux IP (adressage IP, fonctionnalités DHCP et NAT, etc.).

12

CPL de collectivité locale

Les accès Internet haut débit proposés par les FAI ont connu ces dernières années un développement spectaculaire, offrant à la fois des débits plus importants et de nouveaux supports pour atteindre de plus en plus de clients (câble téléphonique, câble TV, radio, etc.).

Dans ce cadre, le réseau électrique paraît promis à un grand avenir pour acheminer le signal Internet au plus près des terminaux qui désirent qui se connecter, par le biais de l'ensemble des prises électriques d'un bâtiment ou d'un logement.

L'utilisation du réseau électrique public comme support de communication, et particulièrement comme médium de diffusion du signal Internet, vers les clients finals présente l'évident avantage que le réseau électrique est présent partout. Cependant, l'utilisation de ce support, avant tout conçu pour le transport et la distribution du signal électrique, comme médium de télécommunications requiert un certain nombre de précautions.

Nous détaillons dans ce chapitre les contraintes et les choix des équipements permettant de mettre en place un réseau CPL jusqu'à chaque usager du réseau électrique d'une collectivité locale. L'installation d'une infrastructure de ce type est d'ores et déjà l'un des projets majeurs en cours de mise en œuvre d'un opérateur de télécommunications.

Les réseaux électriques des collectivités locales

Comme nous l'avons vu au cours des chapitres précédents, les réseaux électriques au sens large peuvent être vus comme plusieurs sous-réseaux connectés les uns aux autres, avec différents niveaux de tension, différentes responsabilités, différents gestionnaires et différents niveaux de sécurité.

Ces sous-réseaux sont réglementés en France par la CRE (Commission de régulation de l'électricité), depuis les lignes THT (très haute tension), que nous voyons parcourir le pays pour relier les grands sites de production d'électricité aux différentes collectivités locales, jusqu'aux prises électriques dont nous disposons dans les bâtiments (habitations, entreprises, etc.) pour alimenter les appareils électriques que nous utilisons tous les jours.

La figure 12.1 représente schématiquement ces différents sous-réseaux, avec leurs niveaux de tension respectifs et les types de lignes associés, ainsi que leur raccordement au réseau électrique privé, en aval du compteur électrique, qui permet de relier en électricité un bâtiment au réseau public. Le réseau d'une collectivité locale s'étend du transformateur HTB/HTA jusqu'aux compteurs des bâtiments de la collectivité.

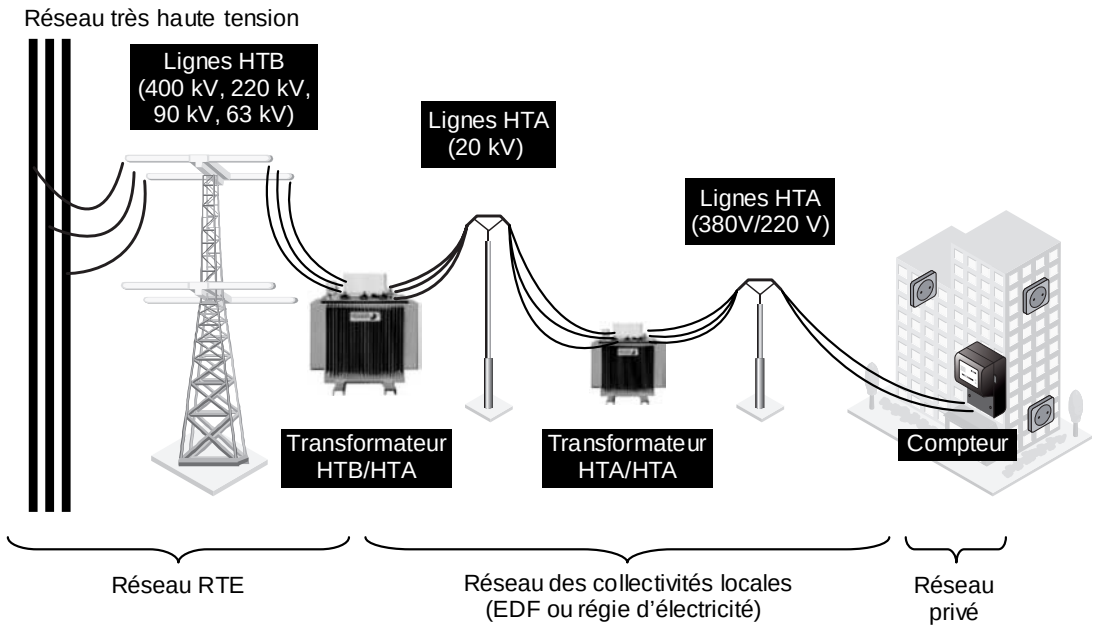


Figure 12.1
Architecture des sous-réseaux électriques français

Responsabilités des sous-réseaux

Les différents sous-réseaux du réseau électrique français diffèrent en partie par la nature du propriétaire du réseau, d'une part (câbles, pylônes, équipements d'infrastructures, etc.), qui est généralement la collectivité locale pour les réseaux électriques HTA, et celle de l'opérateur du réseau, d'autre part, c'est-à-dire celui qui utilise, alimente, entretient et maintient le réseau et les équipements d'infrastructure qui le composent, généralement EDF ou une régie d'électricité pour les réseaux électriques HTA.

La figure 12.2 illustre ce partage de responsabilités pour un réseau HTA au niveau de la connexion du réseau électrique privé au réseau électrique public incarnée par le compteur électrique.

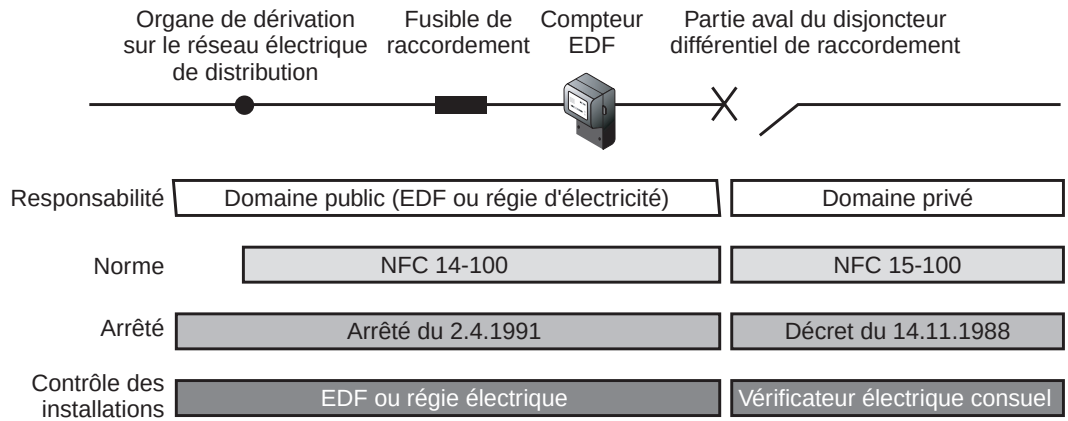


Figure 12.2

Partage des responsabilités pour un réseau électrique de distribution

Ce partage des responsabilités est important à connaître en cas de déploiement d'un réseau CPL, puisqu'il est nécessaire d'installer les équipements CPL sur les différentes parties du réseau électrique pour permettre au signal CPL de se propager depuis le point de connexion à un réseau IP jusqu'aux prises électriques des usagers du réseau public d'électricité.

Les opérateurs des réseaux électriques

Pour un opérateur de réseau électrique, qu'il soit local ou national, voire international, qui dispose de réseaux électriques dans certains lieux géographiques seulement ou répartis dans toute la France, la mise en place d'un réseau CPL en fait un opérateur de télécommunications, à l'image d'un FAI pour les accès Internet. Cela implique qu'il assume

les métiers d'installateur et de gestionnaire d'un réseau de télécommunications dans le cadre d'un réseau électrique, lequel comporte des règles de sécurité différentes de celles des réseaux en paire torsadée, câble TV ou fibre optique.

Le paysage électrique français peut être découpé de la façon suivante :

- vingt et une régies d'électricité locales, couvrant 5 % du territoire ;
- EDF Distribution, couvrant 95 % du territoire.

Pour les régies d'électricité qui gèrent les réseaux électriques locaux (communautés de villages, petites villes, agglomérations, syndicats de communes, etc.), les CPL peuvent constituer une technologie de choix pour connecter à Internet les collectivités locales situées en zones blanches.

Les derniers déploiements de réseaux CPL, qu'ils soient expérimentaux (avec le soutien de la DATAR) ou opérationnels (comme certaines communes du département de la Seine-et-Marne), ont démontré que cette technologie pouvait aider efficacement les collectivités locales à acheminer l'accès à Internet à des foyers qui en étaient privés. Ces déploiements s'appuient souvent sur des opérateurs de télécommunications locaux par le biais d'architectures réseau utilisant le meilleur de chaque technologie disponible actuellement (BLR, Wi-Fi, CPL, réseau Mesh, etc.).

L'opérateur national, EDF, a préféré se cantonner aux métiers de la production, du transport et de la distribution de l'énergie électrique, qu'elle connaît, et ne pas se placer comme potentiel opérateur de télécommunications pour les quelque trente millions de compteurs électriques connectés à son réseau. Cette décision s'appuie par ailleurs sur les directives de la Commission européenne concernant le principe de spécialisation de chacun des grands groupes européens ou nationaux dits de réseaux (électricité, télécommunications, transport, etc.).

Topologie des réseaux électriques

Plusieurs règles de construction président à la mise en œuvre d'un réseau électrique dit de distribution, c'est-à-dire connecté aux grands réseaux à haute tension, ou HTB, alimentant les bâtiments d'une collectivité locale en fournissant l'électricité aux compteurs des abonnés.

On distingue d'abord trois types de réseaux électriques MT et BT, selon la densité d'habitation et la zone géographique considérée *(voir figure 12.3) :* rurale, semi-urbaine et urbaine.

Les spécificités de ces réseaux électriques concernent les éléments suivants :

- topologie du réseau ;

- distance entre pylônes ;
- distance entre le transformateur et les différents compteurs qu'il alimente ;
- nombre de compteurs derrière un transformateur de distribution MT/BT.

Pour chacun de ces réseaux, trois topologies du réseau électrique MT sont possibles : en étoile, en anneau ou en maillage. La topologie la plus fréquemment utilisée est le maillage, qui présente l'avantage de sécuriser l'ensemble du réseau électrique contre d'éventuels défauts électriques à certains points du réseau. Si un défaut, comme un court-circuit, fragilise le réseau en un point, d'autres lignes électriques prennent le relais, la topologie présentant des liens secours du fait du maillage. Aucun point du réseau électrique n'est alimenté par une ligne électrique unique.

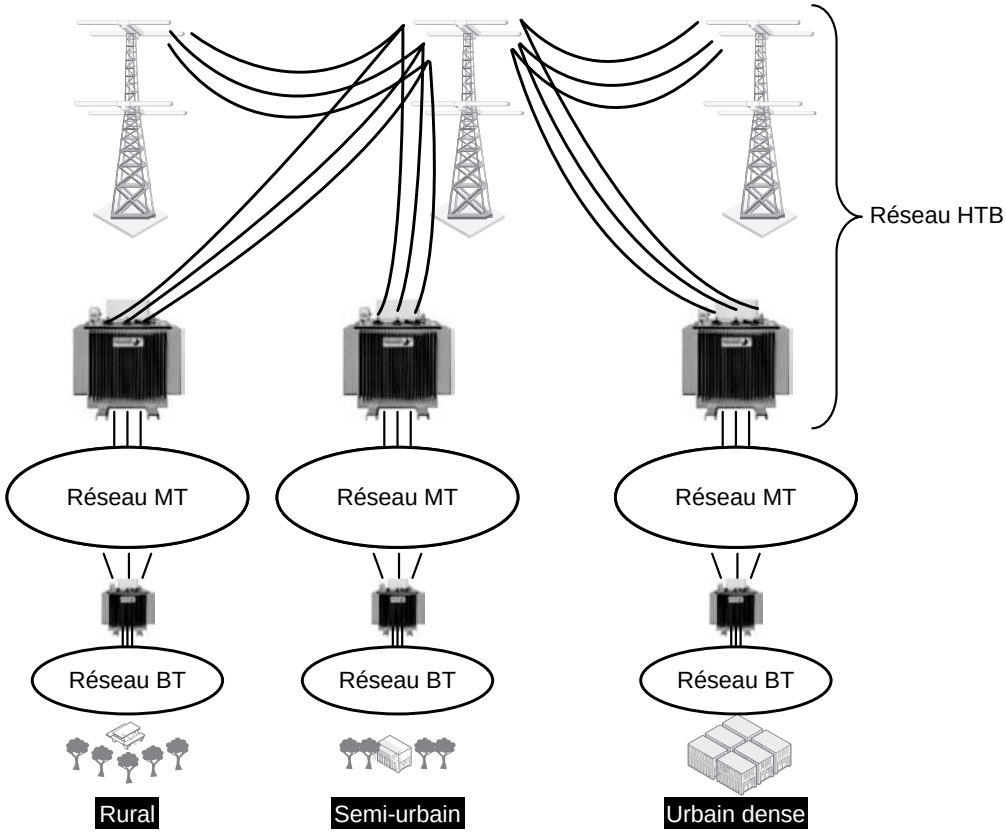


Figure 12.3
Réseaux électriques MT et BT

Topologie des réseaux MT

Dans les zones rurales, la topologie en étoile de type « branches d'arbre » est privilégiée. Dans les zones semi-urbaines, on retrouve des topologies en étoile de type « branches d'arbre » et en anneau avec plusieurs points de connexion au réseau haute tension.

Dans les zones urbaines denses, la topologie privilégiée est le maillage, mais fonctionnant en étoile sous tension. Les liens de maillage sont des liens de secours, pour le cas où l'un des liens principaux viendrait à être coupé.

Les figures 12.4 à 12.6 illustrent ces différentes topologies des réseaux MT.

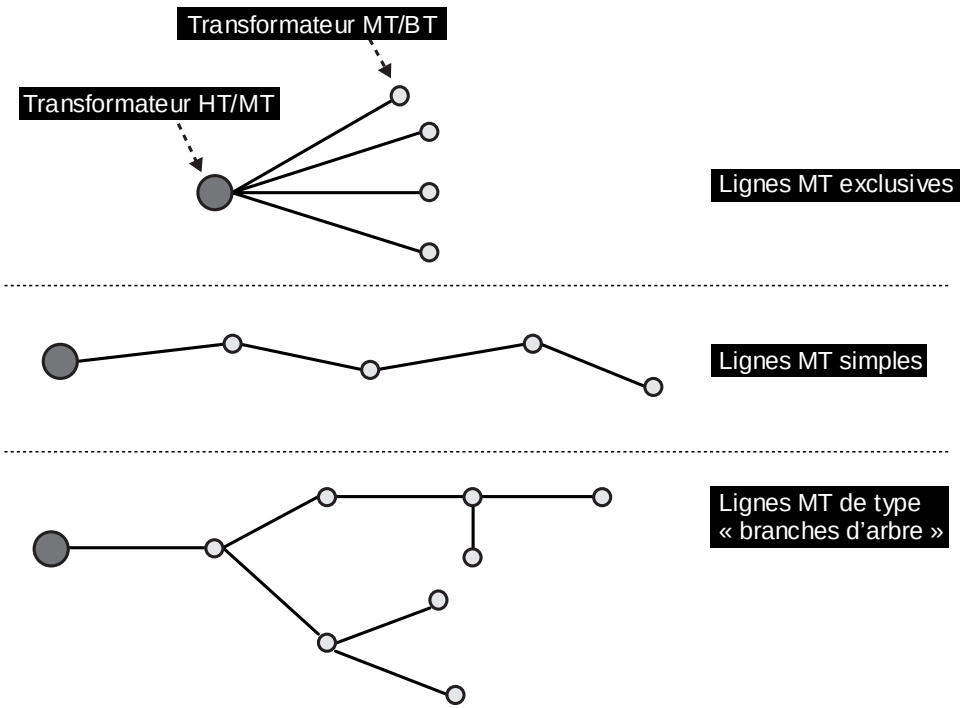


Figure 12.4
Topologie en étoile

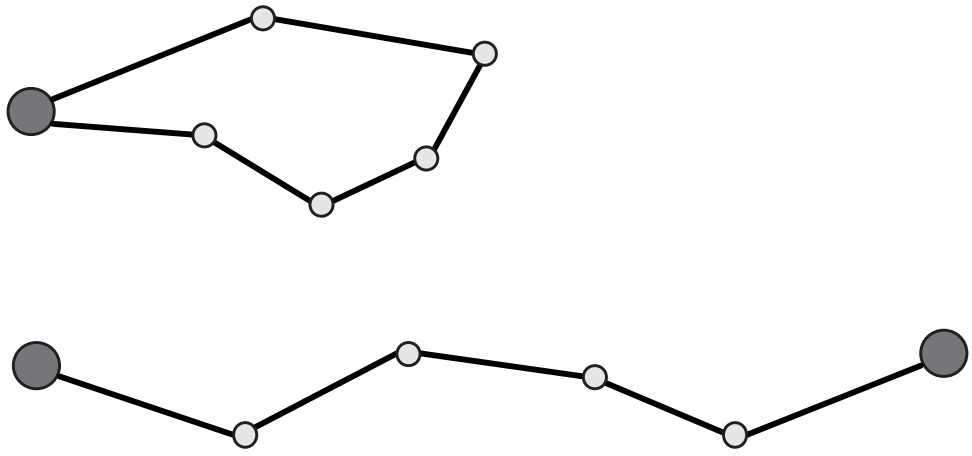


Figure 12.5
Topologie en anneau

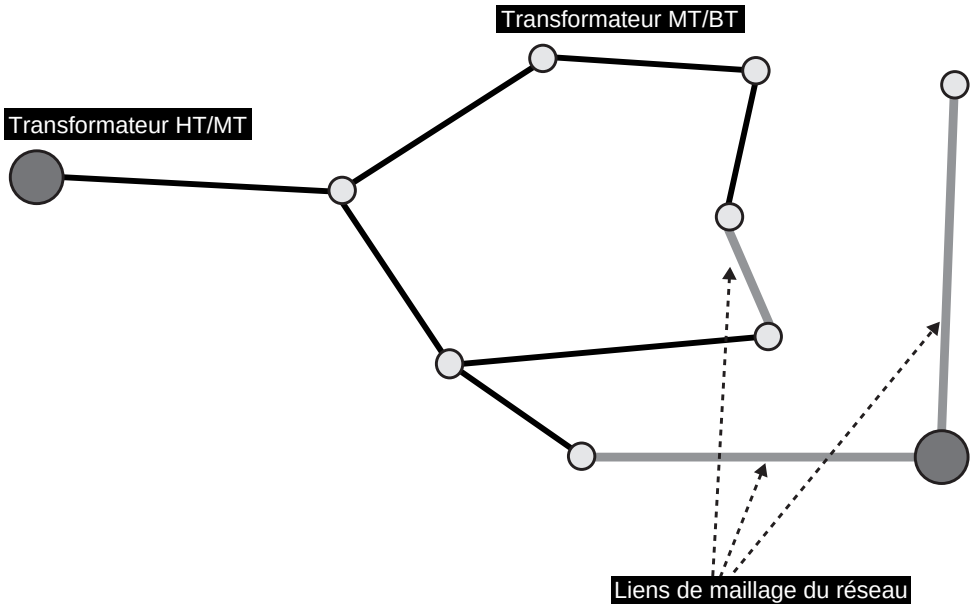


Figure 12.6
Topologie maillée

Topologie des réseaux BT

En France, la topologie des réseaux électriques BT est en étoile de type « branches d'arbre », permettant ainsi des liens par maillage entre certaines branches du réseau électrique. Ces liens de maillage restent cependant trop rares pour définir la topologie du réseau comme un véritable maillage.

Les règles de construction des réseaux électriques déterminent l'ingénierie CPL à mettre en œuvre pour obtenir la meilleure couverture et les meilleures performances du réseau IP vers les abonnés et les prises électriques des bâtiments de la collectivité locale.

La figure 12.7 illustre un réseau électrique représentatif d'une collectivité locale depuis le transformateur HTB/HTA vers les différentes branches du réseau BT HTA basse tension qui alimentent les compteurs des abonnés.

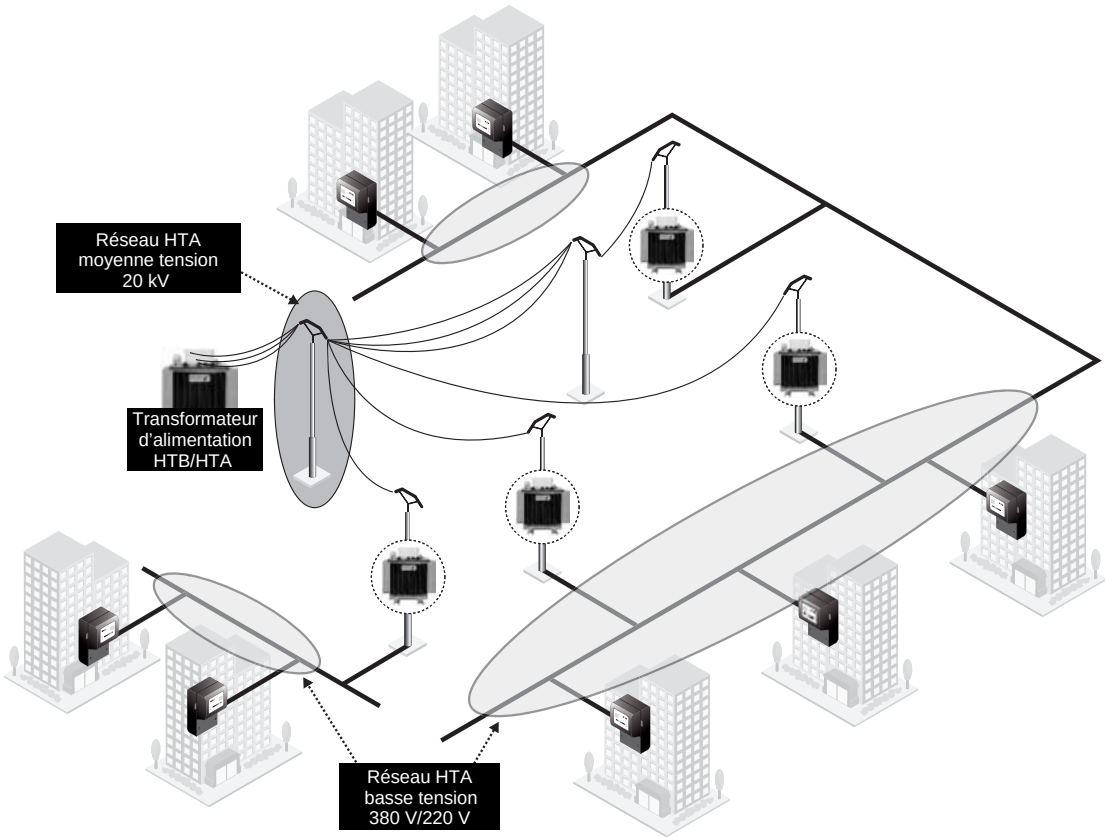


Figure 12.7

Exemple de réseau électrique de distribution dans une collectivité locale

Si nous regardons de plus près la topologie et les équipements électriques d'un réseau de distribution électrique en milieu urbain dense, par exemple l'alimentation des compteurs d'un immeuble d'habitation, nous retrouvons la situation illustrée à la figure 12.8. Cette figure très complète montre les différents éléments du réseau électrique, depuis le poste électrique de quartier jusqu'au compteur d'un appartement. Se superposent à cette installation électrique les équipements CPL permettant la diffusion du signal de données depuis le poste électrique jusqu'à l'équipement CPL esclave présent dans l'appartement.

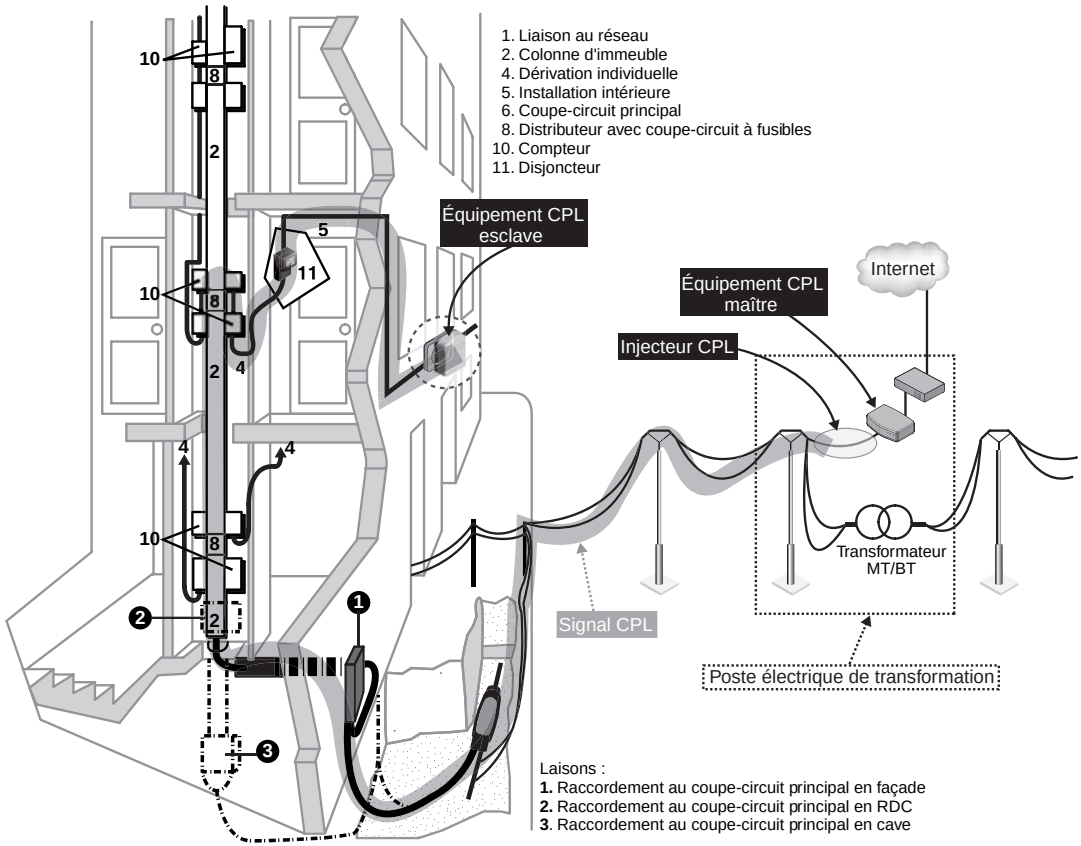


Figure 12.8

Topologie et équipements électriques dans une zone urbaine dense d'immeubles

Mise en place d'un réseau CPL dans une collectivité locale

Différentes problématiques doivent être prises en compte lors de l'installation d'un réseau CPL dans une collectivité locale. Cela commence par la constitution d'une équipe projet, avec une partie MOA (maîtrise d'ouvrage), en l'occurrence la collectivité locale, qui définit les besoins en terme d'accès Internet et de réseau IP afin d'élaborer le cahier des charges, et une partie MOE (maîtrise d'œuvre), qui définit l'ingénierie et l'infrastructure CPL en collaboration avec les équipes opérationnelles de la régie d'électricité locale.

L'équipe de MOE est constituée d'ingénieurs électricité pour le respect des règles de sécurité et d'ingénieurs télécoms/réseaux pour l'utilisation de l'infrastructure électrique et la mise en œuvre des services Internet répondant aux besoins des habitants.

Architecture réseau et place des CPL

Les réseaux de télécommunications peuvent être vus comme une grande pyramide de réseaux constituée, du haut en bas, des sous-réseaux suivants :

- **Très grands réseaux.** Relient les villes et les continents en très haut débit, classiquement en fibre optique, à l'image d'Ebone ou d'Europanet en Europe. Les technologies CPL ne permettent pas de constituer de tels types de réseaux.
- **Dorsales inter-POP.** Relient les différents points de présence IP très haut débit aux DataCenters des grandes villes. Ces réseaux en fibre optique peuvent être situés entre les villes ou dans les agglomérations. Ces dorsales relient les points de présence aux centraux (téléphonique, câble TV, satellite, WiMax, BLR, Mesh, etc.) des FAI. Les technologies CPL ne permettent pas pour l'instant de constituer ce type de réseau, mais les débits offerts par HomePlug AV et HomePlug BPL pourront permettre dans certains cas de constituer des parties de ce type de réseau.
- **Réseaux de desserte.** Permettent de connecter les centraux des FAI et les abonnés à Internet et aux réseaux IP en général. Ces réseaux sont constitués de tous les supports utilisables pour atteindre les abonnés qui se trouvent à quelques kilomètres des centraux des FAI. Les technologies CPL sont évidemment idéales pour les réseaux de desserte dans la mesure où la topologie des réseaux électriques permet d'atteindre l'ensemble des bâtiments et potentiellement chacune des prises d'un bâtiment d'une collectivité locale.
- **Réseaux locaux (LAN ou interbâtiment).** Classiquement Ethernet ou Wi-Fi, ils sont susceptibles d'être remplacés ou complétés par la technologie CPL, aux avantages non négligeables (débit, sécurité, facilité de déploiement, présence pervasive des prises électriques).

La problématique d'une collectivité locale illustrée dans ce chapitre est de constituer un réseau de desserte avec les technologies CPL, ou selon une architecture hybride mêlant plusieurs technologies, permettant de proposer un accès Internet haut débit à l'ensemble des bâtiments de la collectivité.

La figure 12.9 illustre cette pyramide des réseaux de télécommunications dans laquelle les technologies CPL peuvent se placer au niveau des réseaux LAN et des réseaux de desserte dans le cas des collectivités locales.

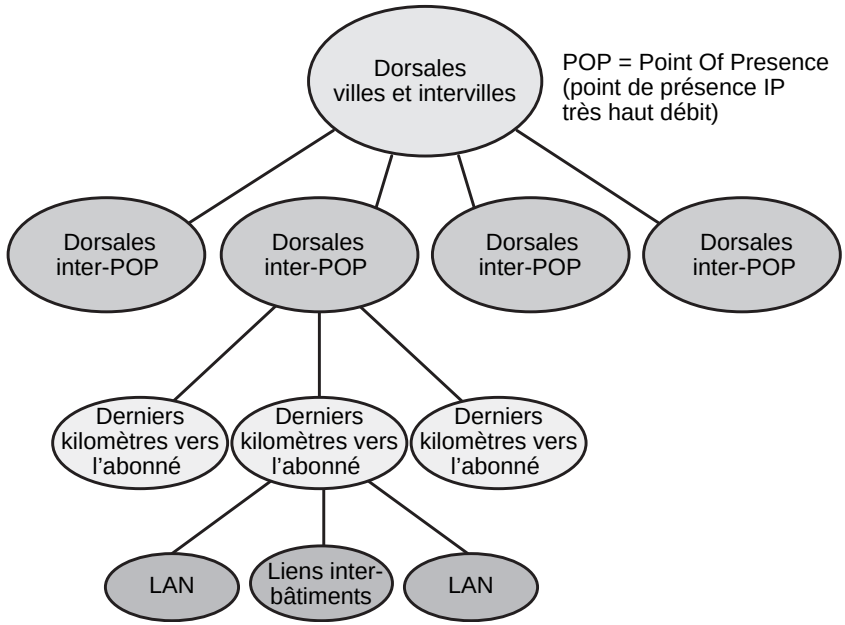


Figure 12.9

Pyramide des réseaux de télécommunications

Contraintes du réseau électrique pour l'architecture CPL

Les principales contraintes influençant l'architecture d'un réseau CPL dans un réseau électrique basse tension sont les suivantes :

- **Zone géographique.** Les caractéristiques du réseau sont différentes dans un milieu résidentiel, d'entreprises (comportant généralement une plus forte densité de compteurs) ou industriel (généralement plus exigeant en terme de qualité de service).
- **Nombre de compteurs par réseau basse tension.** Forte différence de densité entre zones rurales et zones d'immeubles de bureaux denses.
- **Longueurs de câbles.** Classiquement, la longueur des câbles pour atteindre les abonnés varie de 50 m (milieu urbain dense) à 300 m (milieu rural faiblement dense).
- **Topologie du réseau.** Un réseau électrique est constitué de câbles électriques reliant les transformateurs du réseau et les points de livraison, dont le nombre varie selon la zone considérée.

Architecture CPL

L'utilisation des technologies CPL comme réseau de desserte pour une collectivité locale afin d'offrir un accès Internet demande une architecture de réseau CPL différente de celle que nous avons vue aux chapitres 10 et 11, consacrés aux réseaux CPL domestiques et d'entreprise.

La topologie du réseau électrique HTA basse tension de la collectivité locale depuis le transformateur MT/BT vers les différents compteurs des bâtiments est en étoile. De plus, le réseau de desserte impose une isolation entre clients du réseau CPL, afin d'empêcher toute interception des communications de données circulant entre un client du réseau CPL et Internet.

Cela implique une architecture CPL de type maître-esclave, dans laquelle le maître du réseau :

- Contrôle, administre et supervise les différents équipements du réseau.
- Assure la sécurité et la confidentialité des connexions vers Internet et entre chacun des clients du réseau CPL.
- Assure la fonctionnalité de passerelle vers les autres réseaux IP, et plus particulièrement vers le point de transit IP disponible dans la collectivité locale (satellite, point de présence IP, fibre optique, BLR, WiMax, Mesh, etc.).

La figure 12.10 illustre un exemple d'architecture CPL dans une collectivité locale depuis le transformateur MT/BT vers les différentes branches du réseau en étoile desservant en électricité les bâtiments de la collectivité locale.

Les points clés de cette architecture sont les suivants :

- Passerelle CPL, qui permet la connexion vers d'autres réseaux IP.
- Injecteurs CPL, utilisés dans les installations de réseau électrique public de la façon illustrée à la figure 12.11.
- Répéteurs CPL, qui permettent d'offrir une continuité du signal CPL sur toute la longueur du câble jusqu'à l'abonné, pouvant atteindre 200 à 300 m. L'avantage du réseau CPL pour les collectivités est que le réseau électrique est beaucoup moins sujet aux perturbations qu'un réseau domestique ou d'entreprise.
- Passerelle, située dans le poste électrique où se trouve le transformateur MT/BT ou HT/MT permettant l'injection du signal CPL au nœud de la topologie en étoile du réseau électrique public.

Cette architecture d'un réseau de desserte en technologies CPL est finalement assez simple et généralement sans surprise, contrairement à celle d'un réseau domestique ou d'entreprise, où les plans du réseau électrique font souvent défaut, ce qui demande des tests avant installation.

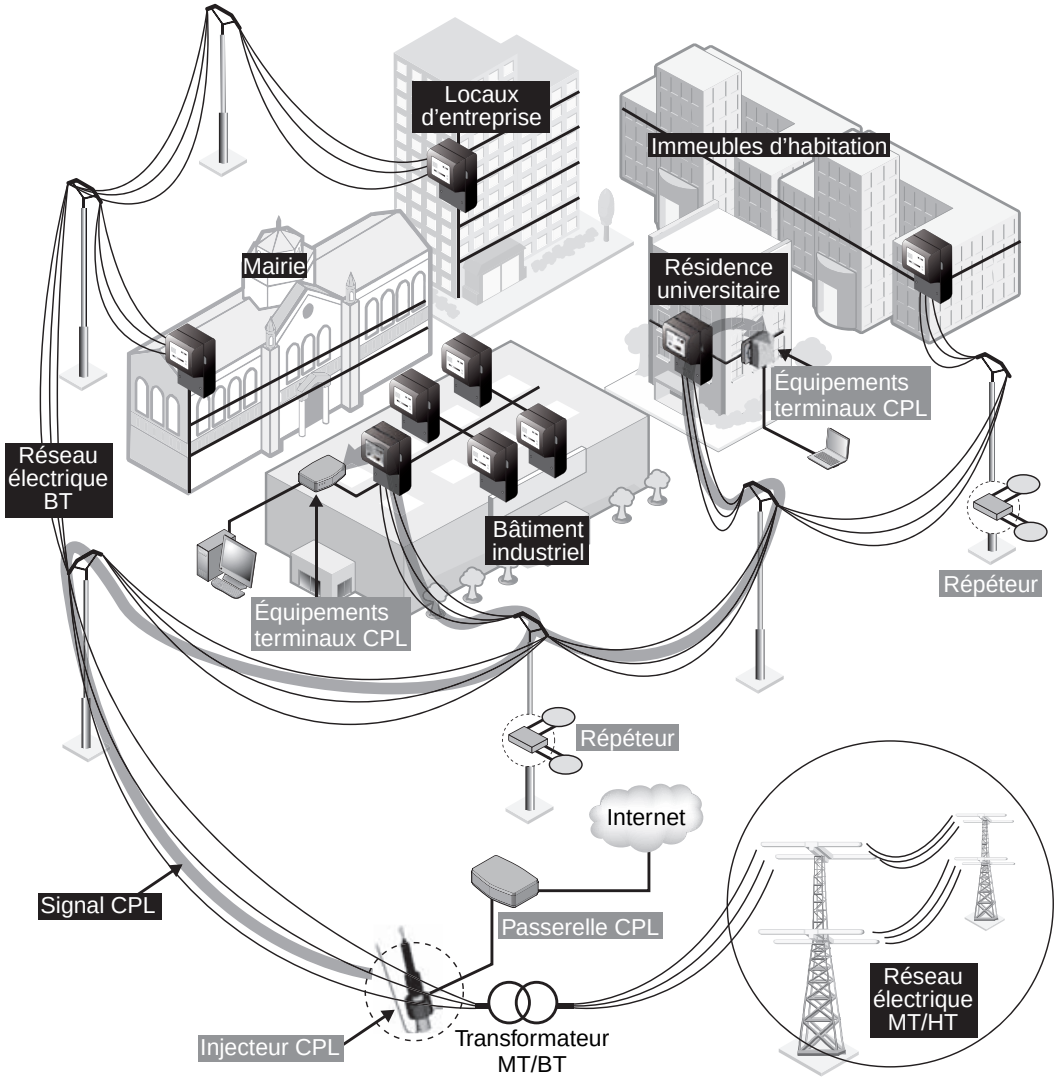


Figure 12.10

Exemple d'architecture CPL pour une collectivité locale

Dans le cas du réseau de la collectivité locale, la régie d'électricité dispose de toutes les informations concernant le réseau électrique (types de câbles, longueur des câbles, nombre d'abonnés sur chaque branche du réseau électrique, type de transformateur, position adéquate des répéteurs, etc.) permettant d'optimiser l'ingénierie de la MOE.

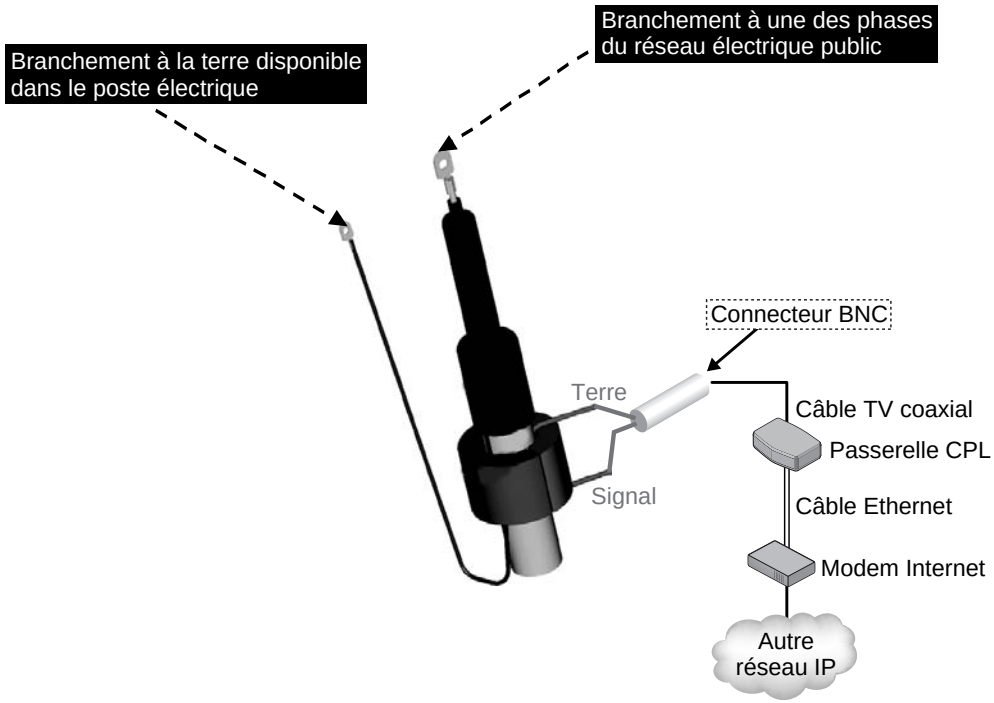


Figure 12.11

Exemple de connexion d'un injecteur CPL de marque Eichhoff

Problématiques des réseaux électriques

Le fait d'installer un équipement de télécommunications sur un réseau électrique public s'accompagne d'un certain nombre de règles de sécurité, qui doivent être respectées par tous les intervenants sur les équipements du réseau électrique, notamment les opérateurs et les agents techniques de la régie électrique.

Concernant les réseaux CPL, ces règles sont les suivantes :

- parfaite isolation des équipements de couplage et de répétition ;
- maintenance des équipements CPL transparente pour le fonctionnement du réseau électrique ;
- intervention sur les équipements CPL par des personnes habilitées.

Les habilitations à intervenir sur un réseau électrique (hors tension, à proximité ou sous tension) s'obtiennent par le biais de formations spécifiques et d'agréments par des organismes *ad hoc*.

Le tableau 12.1 recense les différentes habilitations pour les différentes classes d'intervenants techniques sur un réseau électrique en fonction des travaux à effectuer.

Tableau 12.1 Habilitations électriques

Habilitation	Hors tension		Proximité		Sous tension	
	BT	HT	BT	MT	BT	MT
Non électricien	B0	H0	BOV	HOV	-	-
Exécutant électricien	B1	H1	B1V	H1V	B1T	H1T
Chargé de travaux	B2	H2	B2V	H2V	B2T	H2T

La mise en place d'équipements de télécommunications et plus généralement d'équipements électriques sur l'infrastructure d'un réseau électrique public pose par ailleurs un certain nombre de questions, notamment les suivantes :

- Alimentation électrique des équipements CPL (mise en place d'un compteur d'alimentation, facturation de l'alimentation électrique des équipements, CPL, etc.).
- Non-perturbation du fonctionnement du réseau électrique et de ses équipements de contrôle/commande.
- Identification éventuelle de réseaux CPL bas débit existants sur le réseau électrique de la régie de la collectivité locale et de l'emplacement de ces équipements (poste électrique, pylône, etc.).
- Coexistence éventuelle des réseaux CPL de la collectivité locale et de réseaux CPL domestiques ou d'entreprise privés. Nous reviendrons sur cette coexistence entre réseaux CPL, et donc entre technologies CPL, au chapitre 13, dédié aux réseaux hybrides.

Choix des équipements et des technologies

Le choix des équipements CPL pour un réseau de collectivité locale est particulièrement important dans la mesure où l'architecture maître-esclave que nécessite ce type de réseau demande l'utilisation d'une technologie CPL incompatible avec les autres.

Le projet Opera (Open PLC Research Alliance) n'ayant pas encore abouti à la mise au point d'un standard CPL et l'alliance HomePlug n'ayant pas encore finalisé, en septembre 2006, la version HomePlug BPL (Broadband PowerLine) dédiée aux réseaux CPL des collectivités, les technologies CPL pour les réseaux des collectivités locales sont spécifiques à chaque constructeur, même si certains d'entre eux se fondent sur HomePlug, comme Oxance, qui propose des produits CPL pour réseaux de desserte des collectivités locales.

Il est donc important de comparer les différentes technologies capables de répondre aux besoins d'une architecture maître-esclave sur le réseau électrique public. Le tableau 12.2 récapitule à cet effet les avantages et inconvénients de chaque technologie CPL pour un réseau de desserte.

Tableau 12.2 Avantages et inconvénients des technologies CPL pour réseau de desserte

Technologie CPL de desserte	Équipement et fonctionnalité	Avantage	Inconvénient
Main.net	– Maître CuPLUS – Répéteur RpPLUS – Esclave NtPLUS	– Technologie éprouvée dans différents projets CPL – Bonne portée du signal CPL – Outil de supervision (NmPLUS)	– Technologie un peu dépassée
Oxance	– Maître BPL 380-IC avec injection inductive ou BPL 380-CC avec injection capacitive – Répéteur BPL320 – Esclave PL85	– Fondée sur HomePlug – Bonne portée du signal CPL – Filtrage des adresses MAC – Confidentialité entre clients du réseau CPL	– Pas totalement compatible avec les équipements HomePlug
Spidcom	– Maître Head-end – Répéteur (Repeater) – Esclave CPE	– Possibilité de configuration avancée (notching, densité spectrale de puissance, etc.) – Fort appui de l'ingénierie – Outil SPiDMonitor pour l'administration/supervision – 224 Mbit/s de débit au niveau PHY	– Peu déployé en France – Administration complexe
DS2	– Maître HE – Esclave de type immeuble collectif HG – Esclave de type appartement CPE	– Débit stable sur les réseaux publics – Interface de gestion simple par HTTP – Outil OMS-PLC pour l'administration/supervision – Intégration des produits par l'équipementier Corinex	– Non compatible avec les produits HomePlug
Ascom	– Maître – Esclave	– Interface Telnet facile – Mise à jour logicielle facile	– Débit faible – Technologie dépassée

Les informations de ce tableau ne sont qu'indicatives, mais elles devraient permettre aux ingénieurs d'étude de choisir la technologie CPL la mieux adaptée au cahier des charges de la collectivité locale.

Supervision du réseau de desserte CPL

De la même manière que les réseaux CPL d'entreprise, les réseaux CPL de desserte nécessitent un système de supervision des équipements de l'infrastructure.

L'architecture d'un réseau CPL de desserte comporte les éléments suivants :

- Réseau CPL de desserte, constitué d'équipements CPL en mode maître-esclave et utilisant le réseau électrique public jusqu'à l'abonné final.
- Connexion du réseau CPL de desserte à d'autres réseaux IP (*via* des accords dits de peering) constitutifs d'Internet ou directement vers Internet *via* un FAI.
- NOC (Network Operation Center), centrale où sont regroupées les stations de supervision des différents réseaux CPL de desserte, qui permettent de vérifier l'état des équipements CPL constitutifs du réseau, par le biais notamment de fonctionnalités de cartographie GPS, permettant de donner la position de chacun des équipements.

La figure 12.12 illustre un exemple d'architecture de réseau CPL de desserte implémentant des tunnels VPN reliant le NOC aux passerelles CPL présentes dans les postes électriques, avec des liens dédiés pour la supervision des équipements de tête de réseau.

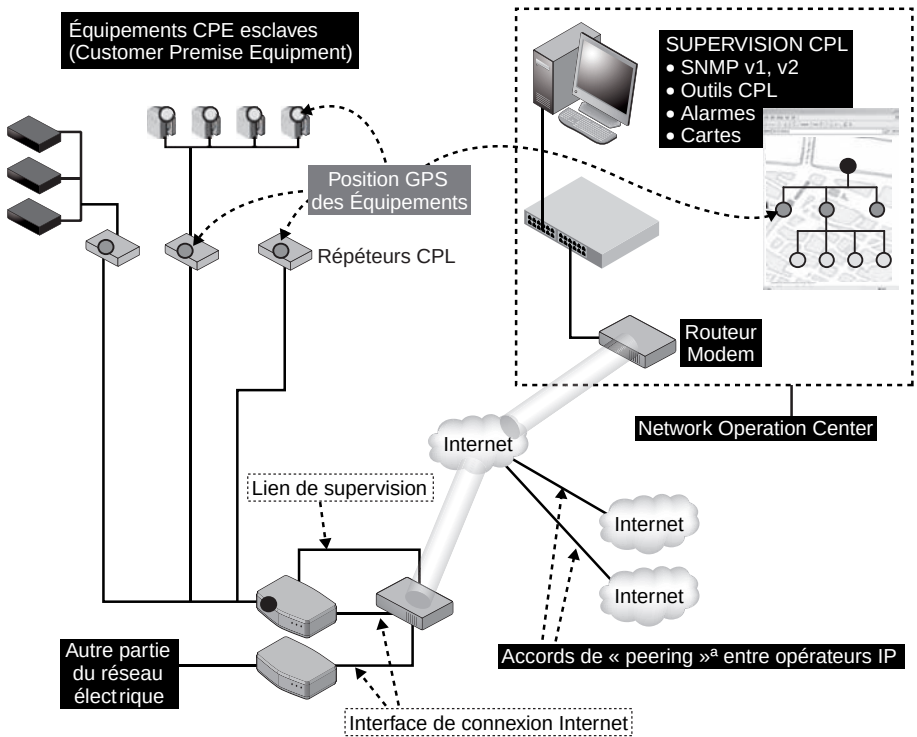


Figure 12.12

Architecture de supervision d'un réseau CPL de desserte

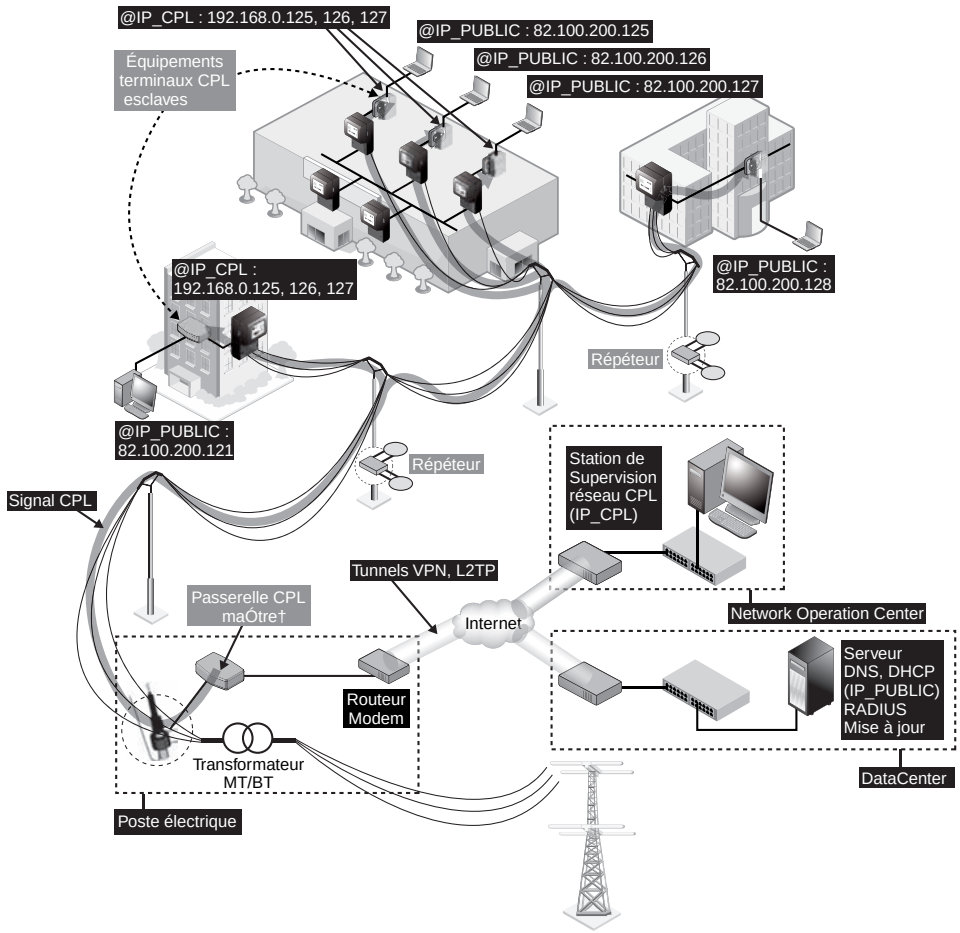
Les équipements de l'infrastructure sont tous supervisables en SNMP à l'aide d'outils permettant de remonter les informations (débits, états des interfaces, températures, taux d'erreur binaire, etc.) et de déclencher des alarmes sur des seuils. L'outil HP OpenView, par exemple, permet de centraliser les données SNMP remontées.

Pour les paramètres purement CPL des équipements du réseau, il est nécessaire d'utiliser des outils spécifiques à chaque technologie déployée. Par exemple, les produits DS2 disposent de l'outil OMS-PLC, développé par la société Dynamic Consulting International, qui permet de gérer la supervision d'un réseau de desserte en technologie DS2.

Configuration du réseau

Comme nous l'avons vu, il est possible d'utiliser différentes technologies pour constituer un réseau CPL de desserte, charge à l'équipe de MOE de choisir la mieux adaptée aux besoins de l'architecture.

Figure 12.13
Exemple d'architecture de réseau de desserte CPL



L'exemple d'architecture complète d'un réseau de desserte d'une collectivité locale illustré à la figure 12.13 comporte les éléments suivants :

- Réseaux IP en amont du réseau CPL, avec le DataCenter, qui regroupe les serveurs d'authentification, d'adresses et de noms et le NOC (Network Operation Center), qui s'occupe de la supervision et de l'administration de réseaux à distance, comme les réseaux CPL de desserte.

- Réseau CPL de desserte, avec la ou les passerelle CPL maître au niveau du poste électrique (hébergeant le transformateur MT/BT), les répéteurs et les équipements CPL esclaves (CPE en anglais). Les équipements esclaves se connectent à l'équipement maître et sont accessibles par leur adresse IP, qui se trouve dans un plan d'adressage IP privé différent de celui des adresses IP publiques délivrées aux abonnés de la collectivité locale.

- Injecteurs CPL, qui permettent de connecter les équipements CPL aux réseaux électriques publics BT ou MT au niveau du poste électrique ou sur un point d'un pylône électrique à proximité des abonnés finals.

Comme il n'est évidemment pas possible de donner la configuration de tous les équipements de toutes les technologies, nous nous contentons d'indiquer au tableau 12.3 les principaux paramètres à configurer pour chaque type d'équipement de l'infrastructure du réseau de desserte.

Tableau 12.3 Paramètres à configurer pour chaque type d'équipement de l'infrastructure CPL du réseau de desserte

Type d'équipement de l'infrastructure	Paramètre à configurer
Maître	– Paramètres de connexion Internet – Liste des équipements esclaves autorisés – Filtrage d'adresses MAC et IP – Confidentialité des équipements esclaves entre eux – Configuration des serveurs d'authentifications (RADIUS, PPP, etc.) – NAT et pare-feu pour les interfaces de gestion
Répéteur	– Segmentation des parties du réseau CPL – Clés réseau CPL – Répétition physique ou logique
Esclave	– Clés réseau CPL – Authentification auprès de l'équipement maître – Adressage IP CPL pour la gestion/supervision – Gestion des priorités (QoS) et des classes de services IP (voix, données, vidéo)

Position GPS des équipements CPL de l'infrastructure du réseau de desserte

Pour optimiser la supervision et la gestion des interventions de maintenance sur les équipements du réseau électrique, il est possible de repérer chaque équipement à l'aide de sa position GPS. Cette position GPS permet en outre de positionner facilement les éléments de l'architecture sur une cartographie disponible dans les outils de supervision du NOC (Network Operation Center).

Pour exemple, les produits Oxance permettent de configurer cette position pour chaque équipement *via* l'interface HTTP de l'équipement maître du réseau de desserte, comme l'illustre la figure 12.14.

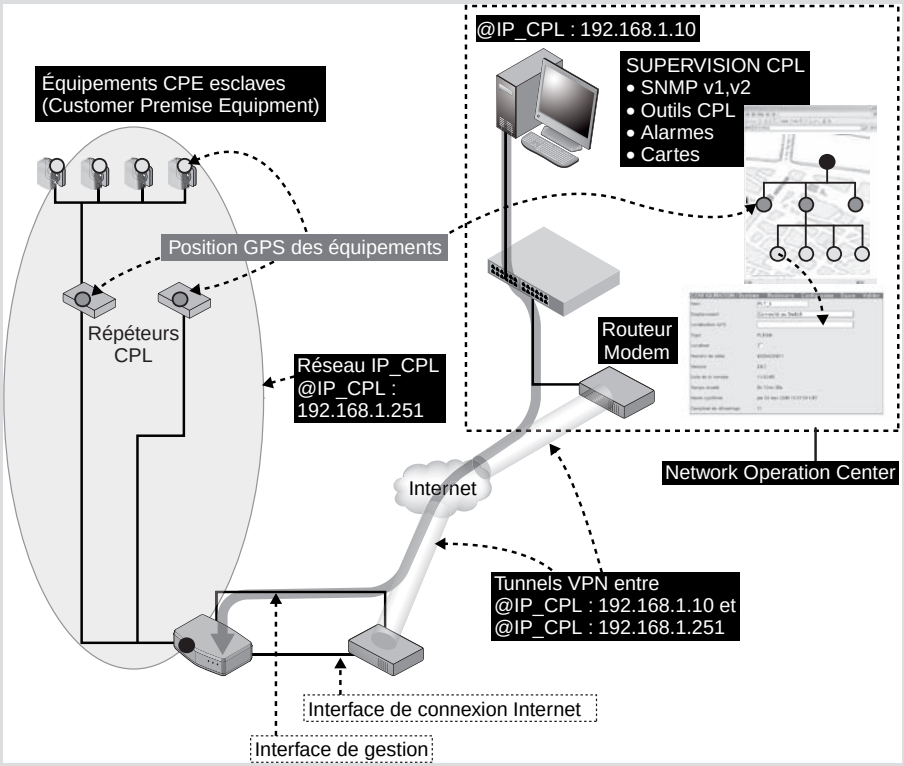


Figure 12.14

Architecture de configuration des équipements CPL pour le positionnement GPS des équipements du réseau de desserte

Il faut pour cela se connecter à l'interface de configuration HTTP des produits Oxance *via* les tunnels VPN entre le NOC et les équipements CPL de l'infrastructure qui permettent de voir le NOC et le réseau CPL dans le même réseau local avec un plan d'adressage commun. Par exemple, à la figure 12.14, la station de supervision est en 192.168.1.10 et le réseau CPL en 192.168.1.251.

☞

Une fois connecté à l'interface, comme illustré à la figure 12.15, il suffit de sélectionner l'équipement que l'on désire dans le menu Source de la barre de menus (équipements esclaves ou répéteurs, ces équipements sont repérés par leur adresse MAC au niveau de l'interface).

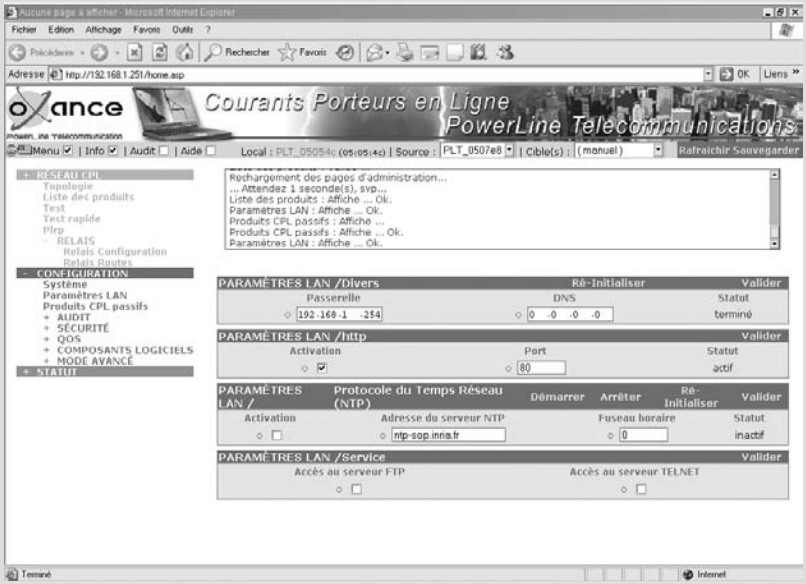


Figure 12.15
Interface de configuration du réseau CPL Oxance

Une fois connecté à l'équipement, il suffit de sélectionner les menus Configuration puis Système et de renseigner les informations voulues *(voir figure 12.16) :* nom de l'équipement, emplacement (poste électrique, switch, partie du réseau électrique, etc.), localisation GPS (par exemple 1,443 32 et 43,610 34, correspondant à la longitude et à la latitude de la position géographique de l'équipement). Il suffit ensuite de cocher la case Localiser pour activer la localisation.

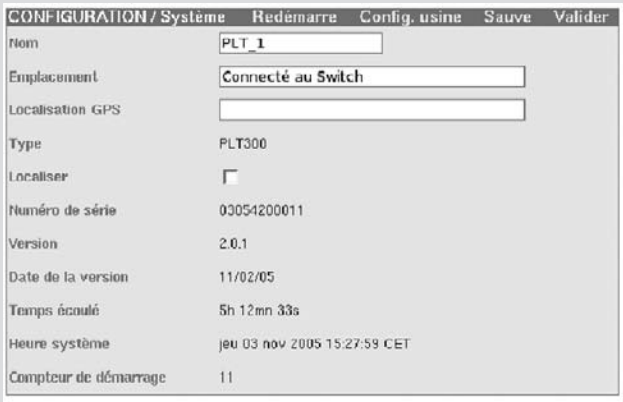


Figure 12.16
Configuration de la position GPS des équipements CPL Oxance

Exemples de réseaux CPL de petite, moyenne et grande taille

Plusieurs déploiements de réseaux CPL sur des réseaux électriques de collectivités locales ont été expérimentés ces dernières années.

Ces développements ont permis aux centres de recherche et développement des opérateurs de tester leurs technologies *in situ* sur des cas réels de réseaux et d'abonnés. Des collectivités locales, appuyées par des opérateurs alternatifs, des régies électriques, etc., ont ensuite élaboré de premières offres d'abonnement Internet par CPL.

D'autres avancées ont été effectuées aux États-Unis, en Espagne et en Suisse, où des déploiements de CPL de desserte ont été effectués dans des villes entières. Dernièrement, la Chine a mené avec l'opérateur FibrLink des déploiements CPL pour des dizaines de milliers d'habitants de constructions neuves.

La récente acquisition de Current Technologies par Google montre que, pour certains acteurs majeurs d'Internet, les CPL incarnent une technologie de desserte appelée à se développer.

Réseaux CPL de petite taille

Dans le cadre de ses missions, le département recherche et développement d'EDF a déployé en 2002 un réseau CPL de desserte dans la commune de Courbevoie, dans les Hauts-de-Seine, avec l'appui du FAI Tiscali pour la connexion Internet.

Ce réseau de desserte avait pour objectif de tester la qualité d'un accès Internet sur le réseau de distribution d'EDF basse tension en milieu urbain dense (topologie de réseau électrique en étoile de type branches d'arbre).

L'architecture de cette infrastructure se composait d'un accès Internet très haut débit, avec une fibre optique au niveau du poste électrique de quartier, lequel alimentait entre 100 et 200 abonnés EDF.

Au niveau du poste électrique, les équipements CPL permettaient d'injecter le signal CPL dans les câbles électriques partant du transformateur et desservant les appartements des différents immeubles du quartier. Ces équipements CPL du poste électrique étaient des maîtres.

Les équipements CPL esclaves connectés au réseau CPL étaient situés dans les appartements. Ils disposaient des autorisations logiques adéquates pour récupérer le signal Internet provenant du FAI Tiscali. Ce FAI gérait les authentifications des utilisateurs et l'attribution des adresses IP à chaque client du réseau de desserte CPL.

Réseaux CPL de taille moyenne

Dans le cadre de la politique de réduction de la fracture numérique concernant l'accès Internet haut débit en milieu rural, le conseil général de Seine-et-Marne a déployé des technologies réseau Wi-Fi, CPL et satellite dans les communes de Villeneuve-Saint-Denis et Villeneuve-le-Comte.

Le déploiement de réseaux de desserte en CPL a permis d'amener le haut débit dans des zones dites blanches, non desservies par des offres ADSL. Ces deux communes ont ainsi pu être desservies en Internet haut débit depuis un point de présence à proximité des communes, au travers d'une architecture CPL complète.

Réseaux CPL de grande taille

Hors de France, des déploiements de réseaux CPL de desserte de grande taille ont été réalisés en Espagne (Saragosse et Barcelone) par la société DS2 et aux États-Unis par Current Technologies, qui a déployé des réseaux CPL dans les États du Maryland et du Texas pour une offre d'accès Internet symétriques à 4 Mbit/s, visant potentiellement deux millions de personnes.

La ville de Fribourg, en Suisse, a été parmi les premières à déployer un réseau CPL de desserte avec la technologie Ascom en 2001 avec le FAI Swisscom.

En France, un des grands projets de réseau CPL de desserte est porté par le Sipperec, un groupement intercommunal dans le domaine de l'énergie et des communications en Île-de-France.

Projet de réseau CPL de desserte en Île-de-France du Sipperec

Le Sipperec est un groupement intercommunal dans le domaine de l'énergie et des communications de quatre-vingt-six communes d'Île-de-France. À l'horizon de cinq ans, 1,5 million de foyers devrait être relié à l'Internet haut débit et/ou au téléphone grâce aux courants porteurs en ligne. Le coût global de ce chantier s'élève à 155 millions d'euros. La société française Mecelec a été retenue comme prestataire global de déploiement de ce réseau CPL. Le projet est d'une ampleur inégalée en France et dans le monde en matière de CPL outdoor sur la boucle locale en zone urbaine.

Les équipements CPL seront déployés dans plus de 7 700 transformateurs électriques dans le but de permettre le raccordement de 130 000 immeubles. Les conditions de location de ce réseau à des opérateurs/fournisseurs tiers sont d'ores et déjà publiées. Mecelec devra leur louer ses capacités pour 15 euros par mois au maximum par liaison, avec un plafond fixé à 10 euros pour le service téléphonique seul.

La société prévoit d'autres applications pour le réseau, notamment la vidéosurveillance en milieu urbain.

(http://www.sipperec.fr/presse/Communique_presse_MECELEC_300306.pdf)

13

CPL hybride

Les récents développements des supports de communication informatiques ont multiplié les médias réseau (Ethernet câblé, Wi-Fi, CPL, fibre optique, câble TV, etc.), offrant aux applications de nouvelle génération les débits, couverture et temps de transit adéquats.

Aucun de ces supports n'offrant en lui-même les capacités idéales, des réseaux hybrides ont fait leur apparition afin de tirer le meilleur parti de ces technologies. Une bonne connaissance de ces dernières est cependant nécessaire afin d'optimiser l'architecture et la configuration de ces nouveaux réseaux.

Les réseaux Ethernet câblés sont aujourd'hui ceux qui reviennent le plus cher, notamment en raison des travaux liés au câblage. Ils restent cependant ceux qui offrent les meilleures performances et une garantie de service à près de 100 %. Lorsqu'il n'est pas possible de bâtir de tels réseaux, il peut se révéler intéressant de s'appuyer sur des technologies complémentaires.

Ce chapitre vise à mettre en perspective l'intérêt des technologies CPL actuelles vis-à-vis des autres technologies réseau. Avec l'apparition de la spécification HomePlug AV, les technologies CPL ajoutent aux avantages des CPL (facilité de déploiement, faible coût, évolutivité, sécurité), des performances globales capables de rivaliser avec ces autres technologies.

Cohabitation des différents réseaux

La cohabitation entre technologies réseau, qu'elles soient filaires ou sans fil, engendre des perturbations. Par exemple, la propagation des signaux CPL sur les câbles électriques émet un champ électromagnétique susceptible de perturber non seulement les autres systèmes de communication, comme les réseaux radio, mais aussi les différentes technologies CPL elles-mêmes.

L'un des développements importants en matière de cohabitation réseau étant précisément la juxtaposition des CPL et de Wi-Fi, il est important de comprendre et maîtriser ces perturbations.

CPL entre eux

Comme nous l'avons vu tout au long de cet ouvrage, il n'existe pas encore de standard CPL IEEE. En conséquence, un certain nombre de technologies CPL coexistent sur les réseaux électriques publics et privés.

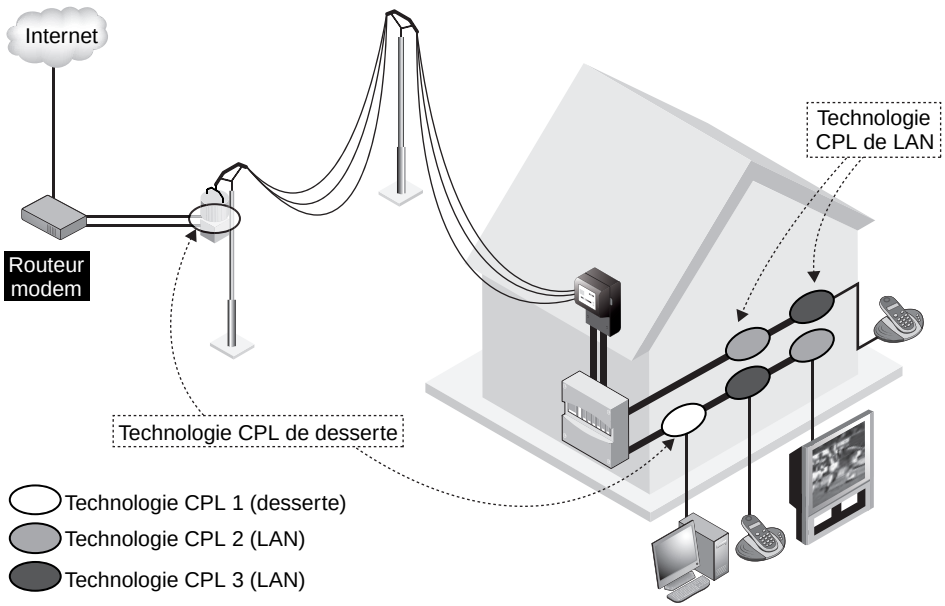


Figure 13.1

Cohabitation entre technologies CPL sur le même réseau électrique

La figure 13.1 illustre une habitation dans laquelle coexistent les trois technologies CPL suivantes :

- desserte CPL de collectivité locale pour fournir un accès Internet ;
- LAN de diffusion des flux vidéo provenant de l'InternetBox vers des équipements CPL proches des terminaux vidéo dispersés dans l'habitation ;

- LAN de diffusion du signal téléphonique IP et des signaux domotiques (télécommandes, informations de capteurs, etc.) et domestiques (babyphones, vidéosurveillance, etc.) dans l'habitation.

Ces trois technologies étant à haut débit, elles fonctionnent toutes dans la bande de fréquences des 2-30 MHz, mais avec des techniques d'accès au média et d'utilisation de la bande de fréquences distinctes. En l'absence de standard et de norme d'interopérabilité, ces technologies CPL se sont développées en parallèle, sans souci de coexistence mutuelle.

L'alliance CEPCA (Consumer Electronics Powerline Communication Alliance) travaille actuellement à la mise au point d'un guide d'interopérabilité entre technologies CPL *(voir ci-dessous)*, qui devrait permettre d'optimiser l'utilisation de cette bande de fréquences.

Alliance CEPCA et interopérabilité des technologies CPL

Dans l'attente d'un standard CPL, l'alliance CEPCA a élaboré une proposition technique afin de gérer la coexistence des technologies CPL. Cette proposition se fonde sur une fonction CDCF (Commonly Distributed Coordination Function), qui permet de gérer les espaces temporels et fréquentiels de manière répartie entre les différentes technologies.

Cette répartition s'appuie sur les éléments suivants :

- gestion des accès hybrides entre FDMA (Frequency Division Multiple Access) et TDMA (Time Division Multiple Access) ;
- gestion de la QoS par un système d'espaces temporels TDMA, comme dans HomePlug AV pour les applications de vidéo HD.

Comme l'illustre la figure 13.2, ces deux principes devraient permettre d'éviter les interférences mutuelles et d'optimiser l'utilisation du média de communication commun.

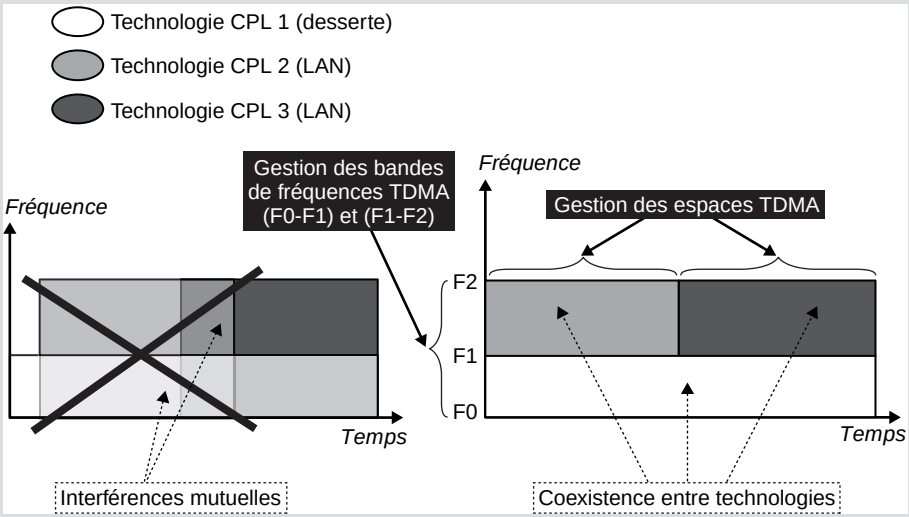


Figure 13.2

Proposition de gestion des interférences mutuelles entre technologies CPL

Le principal problème de coexistence entre technologies CPL vient de l'absence de normalisation dans l'utilisation de la bande de fréquences. Cela entraîne une diminution de la bande passante disponible pour chaque technologie. Les communications de données fonctionnent encore, mais dans des modes dégradés, voire très dégradés, qui nuisent à l'acheminement des services offerts aux couches supérieures (IP, TCP, etc.) et empêchent le bon fonctionnement des applications.

De même qu'il faut éviter d'avoir trop d'équipements CPL sur un même réseau électrique (les spécifications de HomePlug 1.0 et Turbo limitent ce nombre à 16 équipements), il faut éviter d'implémenter plusieurs technologies CPL sur un même réseau électrique (HomePlug, DS2, Spicom, etc.).

Les propositions de l'alliance CEPCA sont proches des celles implémentées dans HomePlug AV, qui offre un mécanisme de cohabitation des réseaux HomePlug 1.0, Turbo et AV grâce à une allocation d'espaces de temps TDMA *(voir les chapitres 3 et 5)*.

La figure 13.3 illustre schématiquement ce système de cohabitation, dans lequel certaines périodes de temps sont allouées aux échanges de données entre équipements HomePlug 1.0 et d'autres aux échanges entre équipements d'autres spécifications HomePlug.

Ce type de gestion intelligente de la cohabitation entre équipements de différentes technologies HomePlug devrait être étendu aux autres technologies par la mise au point attendue d'un standard IEEE.

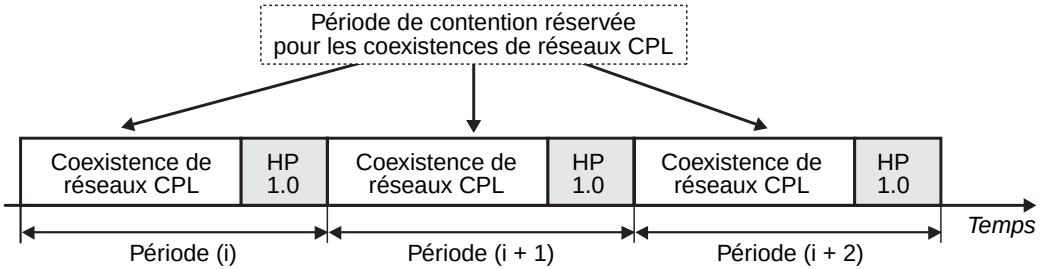


Figure 13.3

Gestion de la coexistence de réseaux CPL HomePlug par la spécification HomePlug AV

Comme indiqué au tableau 13.1, les développements des différentes spécifications HomePlug ont toujours cherché à favoriser leur interopérabilité, et donc l'évolutivité des réseaux CPL. En revanche, les autres technologies CPL ne sont pas interopérables avec HomePlug, ni entre elles d'ailleurs, ce qui restreint grandement l'évolutivité de ces réseaux.

Tableau 13.1 Interopérabilité entre technologies CPL

Technologie CPL A		Technologie CPL B						
		HomePlug					DS2	Spidcom
		1.0, Turbo	AV	Oxance	BPL	CC		
HomePlug	1.0, Turbo							
	AV							
	Oxance							
	BPL							
	CC							
DS2 AV200								
Spidcom								

CPL et Wi-Fi

La cohabitation entre technologies CPL et Wi-Fi ne pose aucun problème, puisque les bandes de fréquences utilisées sont différentes, les CPL opérant dans la bande des 1 à 30 MHz et les différentes standards IEEE 802.11 dans celle des 2,4 et 5 GHz.

En terme d'architecture, la cohabitation de ces deux technologies ne pose aucun problème non plus, ce qui permet d'utiliser le meilleur des deux technologies. De nombreux équipements hybrides CPL/Wi-Fi devraient donc voir le jour pour bâtir des architectures alliant une dorsale CPL et une desserte IP de type radio avec Wi-Fi.

La société Lite-On a d'ores et déjà annoncé la sortie prochaine d'un équipement CPL/Wi-Fi de type ampoule pour douille de plafonnier. Cet équipement permettra d'utiliser le réseau électrique qui alimente les ampoules pour véhiculer le signal CPL tout en dotant cette nouvelle génération d'ampoule, dite « intelligente », de fonctionnalités CPL et de points d'accès Wi-Fi.

Le placement d'un point d'accès Wi-Fi au niveau du plafond d'une pièce est idéal pour une couverture radio optimale.

La figure 13.4 illustre un exemple d'architecture CPL/Wi-Fi, avec un accès Internet relié à un équipement passerelle CPL diffusant le signal CPL sur le réseau électrique. Ce signal est récupéré par des équipements CPL/Wi-Fi qui utilisent leur interface radio 802.11 pour créer des cellules Wi-Fi dans les différentes pièces.

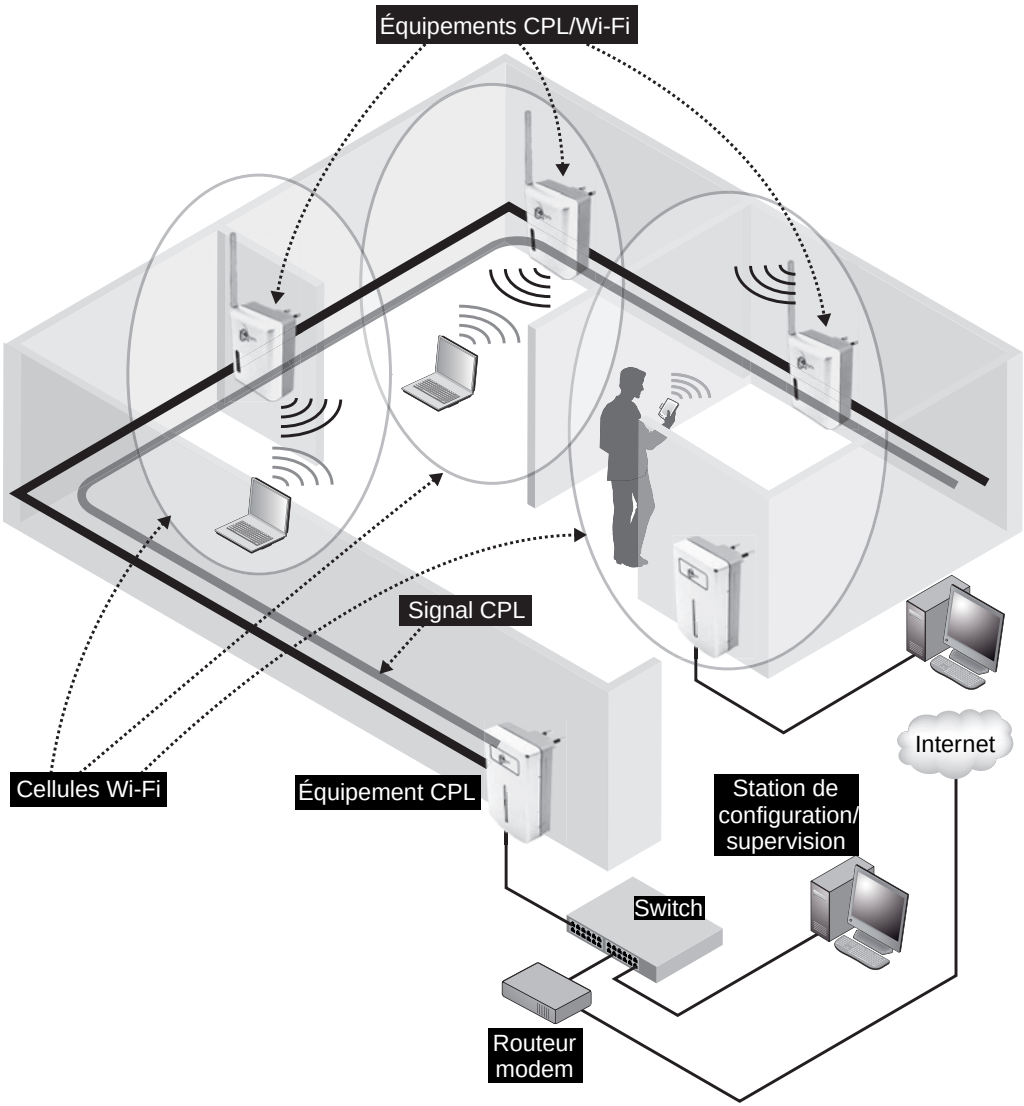


Figure 13.4
Exemple d'architecture hybride CPL/Wi-Fi

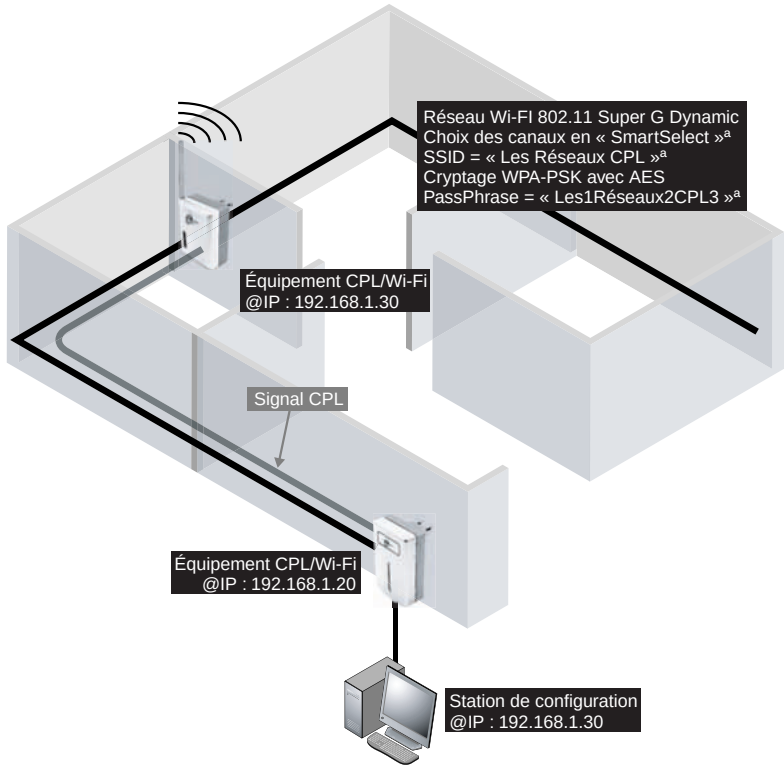
Pour illustrer la configuration d'une telle architecture, nous utiliserons les équipements NetPlug Turbo de Thesys illustrés à la figure 13.5.

Thesys propose un kit comprenant un équipement CPL doté d'une interface Ethernet et un équipement CPL/Wi-Fi comportant une prise électrique et une antenne pour l'interface IEEE 802.11. Nous laissons de côté la configuration du réseau CPL, qui est identique à celle du réseau HomePlug Turbo indiquée au chapitre 9.

Figure 13.5
Produits hybrides CPL/Wi-Fi NetPlug Turbo de Thesys

Pour configurer ce réseau hybride, il est nécessaire d'accéder aux paramètres de l'équipement Wi-Fi. Ces paramètres se configurent *via* une interface HTTP au niveau de l'équipement Wi-Fi, comme illustré à la figure 13.6.

Figure 13.6
Configuration des équipements CPL/Wi-Fi

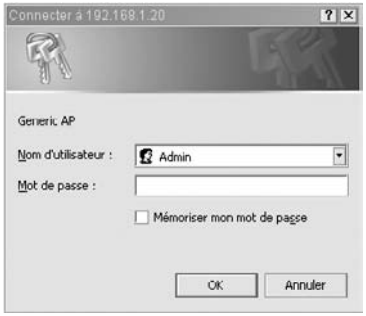


La station de configuration du réseau a l'adresse IP 192.168.1.30 sur la figure, et l'équipement CPL/Wi-Fi à configurer l'adresse par défaut 192.168.1.20. Il suffit de connecter la station de supervision en Ethernet à l'équipement CPL et d'ouvrir un explorateur Internet à l'adresse 192.168.1.20.

La fenêtre illustrée à la figure 13.7 s'affiche alors. Le nom d'utilisateur par défaut est **Admin** et le mot de passe vide.

Figure 13.7

Connexion à l'équipement CPL faisant office de point d'accès Wi-Fi



Après connexion, la page HTML illustrée à la figure 13.8 s'affiche, avec les paramètres par défaut du point d'accès Wi-Fi. Il est alors nécessaire de configurer la sécurité de ce point d'accès.

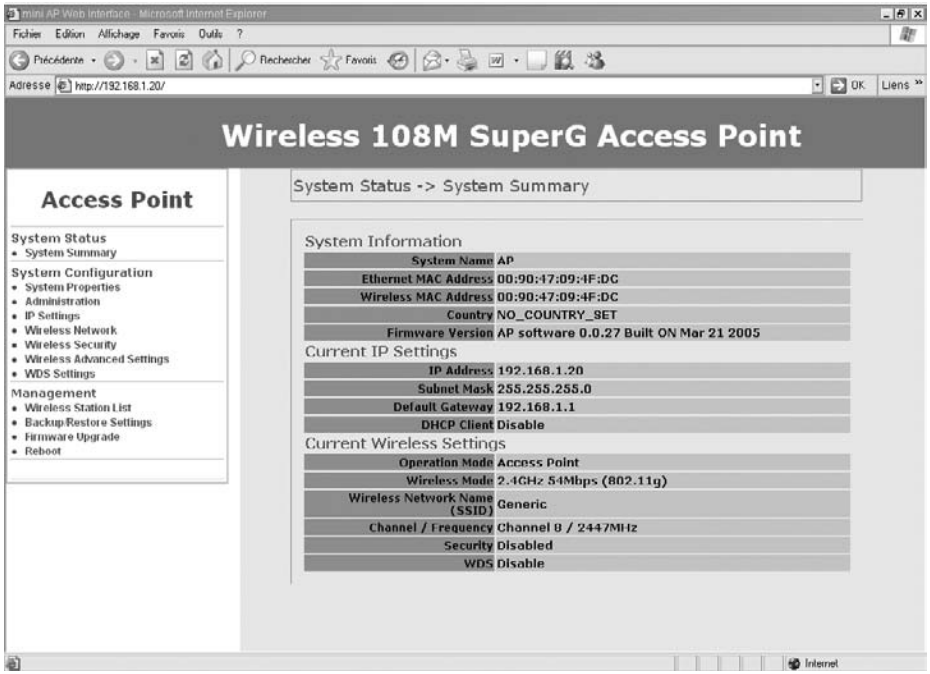


Figure 13.8

Paramètres par défaut du point d'accès Wi-Fi

Dans le sous-menu System Properties du menu System Configuration, il est important de configurer le nom de l'équipement, la région d'utilisation et le mode 802.11 utilisé. Ici, l'équipement servant de point d'accès, nous choisissons le mode Access Point, comme illustré à la figure 13.9.

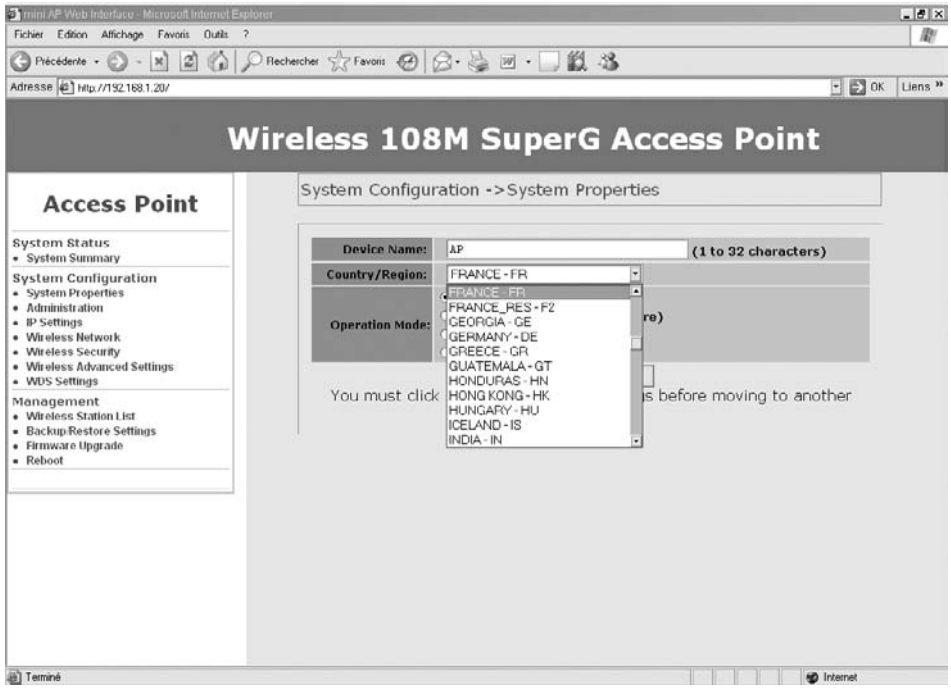


Figure 13.9

Configuration des propriétés du point d'accès Wi-Fi

Dans le sous-menu Administration du menu System Configuration, il est important de changer le nom d'utilisateur et le mot de passe d'accès à l'interface administrateur de l'équipement afin d'éviter que d'autres personnes connectées au réseau CPL n'atteignent la configuration du réseau Wi-Fi, comme illustré à la figure 13.10.

Le sous-menu IP Settings permet de changer l'adresse IP du point d'accès Wi-Fi en fonction du plan d'adressage mis en place au niveau du réseau LAN. Nous conservons ici la configuration par défaut illustrée à la figure 13.11.

L'étape suivante de la configuration concerne les paramètres propres au réseau Wi-Fi et à sa sécurité. Nous devons d'abord choisir un SSID, c'est-à-dire un nom de réseau Wi-Fi, afin que les clients qui désirent se connecter le reconnaissent. Nous choisissons ici **Les réseaux CPL.** Nous devons ensuite choisir un mode de fonctionnement de l'interface radio, ici « 802.11 Super G dynamic », qui offre des débits théoriques pouvant aller jusqu'à 108 Mbit/s, comme illustré à la figure 13.12.

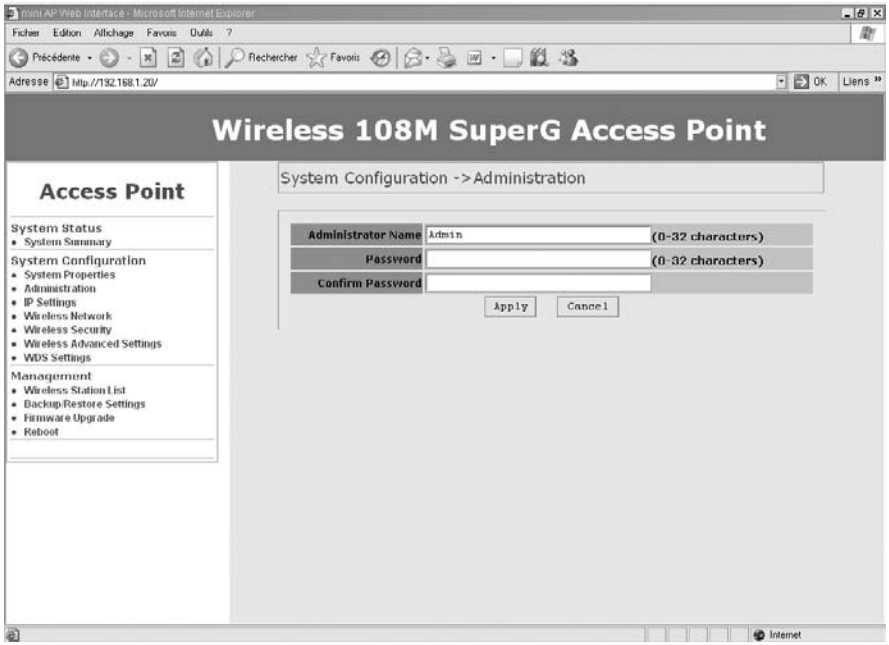


Figure 13.10

Configuration du compte administrateur du point d'accès Wi-Fi

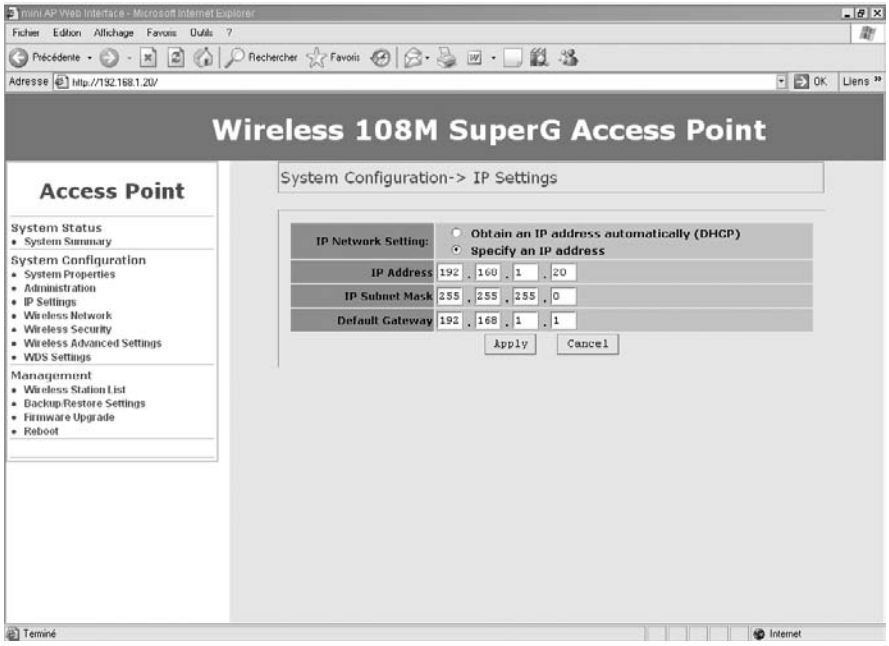


Figure 13.11

Configuration de l'adresse IP du point d'accès Wi-Fi

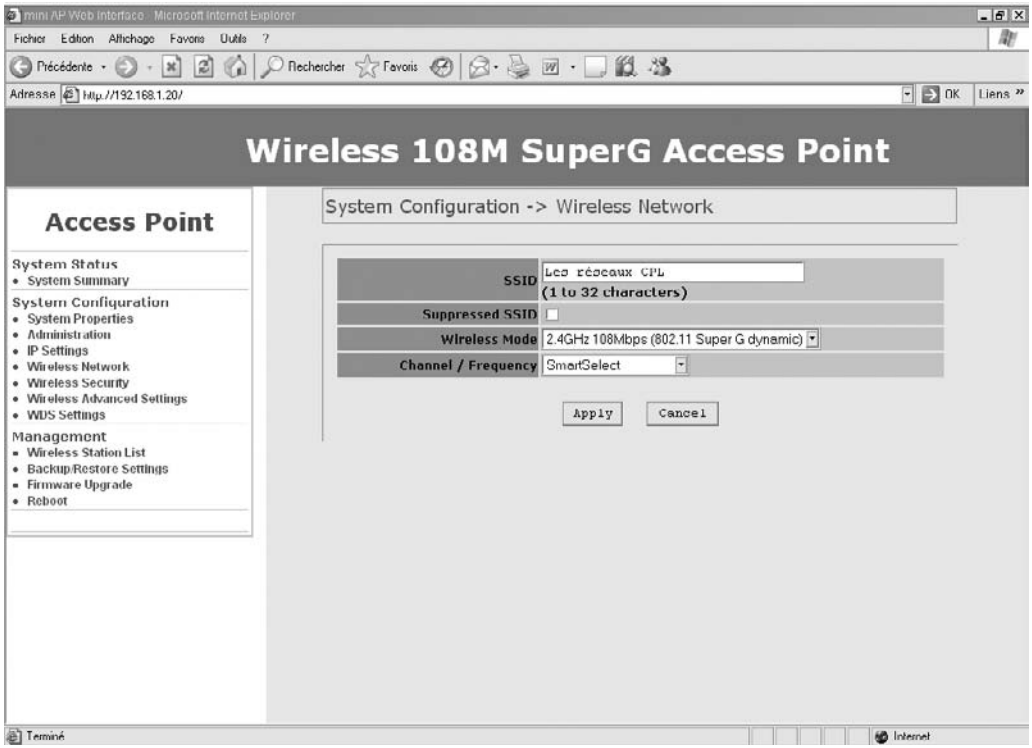


Figure 13.12

Configuration du SSID et du mode IEEE 802.11

Il est alors possible de sélectionner un canal (de 1 à 11) dans la bande des 2,4 GHz ou de choisir le mode SmartSelect, qui effectue un choix dynamique du meilleur canal en fonction de l'encombrement, du nombre de clients, etc.

Choix du mode IEEE 802.11

Lorsque le réseau est configuré en mode « 802.11 Super G dynamic », il est important de vérifier que tous les clients 802.11 qui se connectent au réseau supportent ce mode. Si ce n'est pas le cas, il est préférable de choisir les modes 802.11b ou 802.11g, qui sont supportés par la plupart des terminaux Wi-Fi actuels.

Une fois le mode réseau 802.11 configuré, nous pouvons passer au paramétrage de la sécurité du réseau Wi-Fi, qui constitue un des points de faiblesses des réseaux Wi-Fi.

Dans la mesure où le réseau CPL est sécurisé et physiquement difficile d'accès, il est possible de maintenir un bon niveau de sécurité pour l'ensemble du réseau hybride. Dans notre exemple, le sous-menu Wireless Security du menu System Configuration nous

permet de choisir le mode WPA-PSK avec cryptage de la clé de type AES (il faut toutefois que ce mode soit supporté par les cartes Wi-Fi clientes, ce qui est généralement le cas des cartes récentes) en indiquant la phrase de cryptage (ici **Les1Réseaux2CPL3,** comme illustré à la figure 13.13).

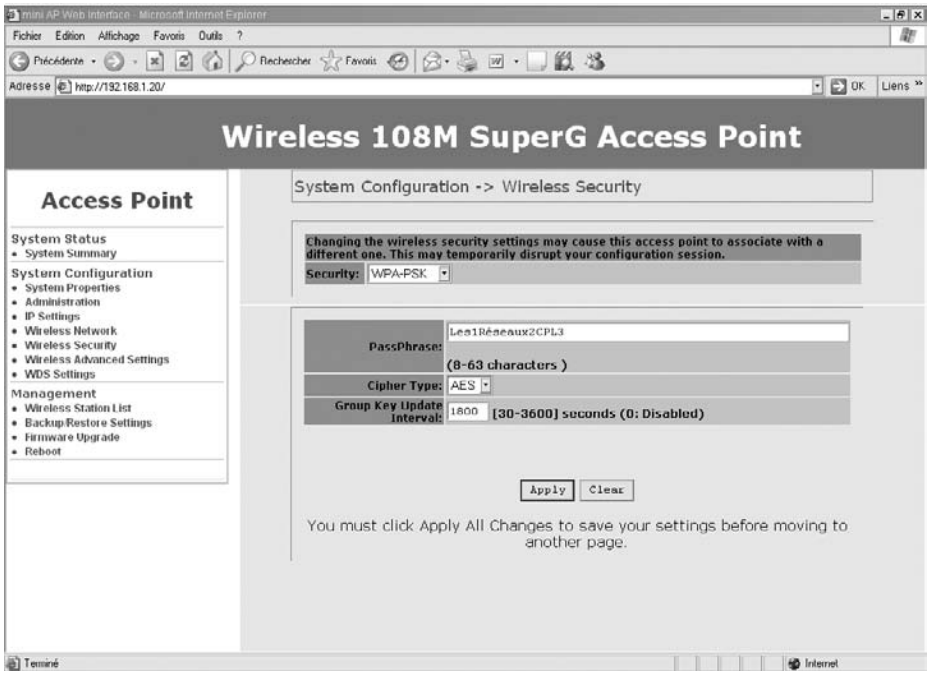


Figure 13.13
Configuration de la sécurité du réseau Wi-Fi

La configuration globale du réseau Wi-Fi est terminée.

Il est possible de vérifier l'ensemble des paramètres de configuration dans le sous-menu System Summary du menu System Status. La figure 13.14 illustre l'ensemble des paramètres que nous venons de configurer.

Cet exemple de configuration montre qu'une architecture de réseau hybride CPL/Wi-Fi comportant des équipements intégrés permet de déployer facilement et rapidement un réseau aux performances optimales utilisant le réseau électrique comme dorsale Ethernet et les équipements CPL/Wi-Fi sur prise électrique comme réseau de desserte avec une couverture radio complète.

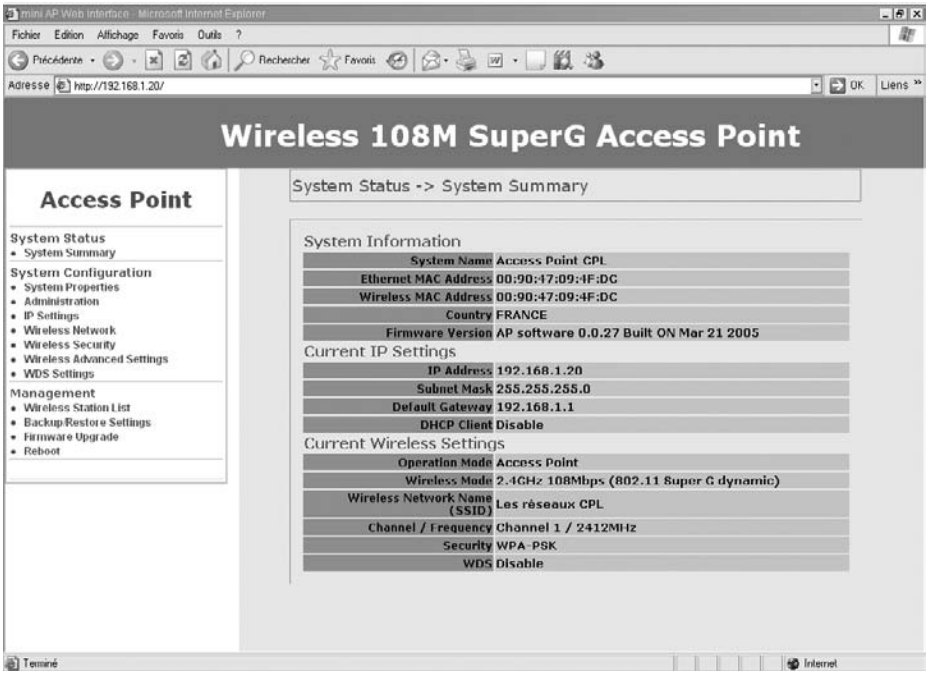


Figure 13.14
Récapitulatif des paramètres du réseau Wi-Fi

La cohabitation entre CPL et Wi-Fi est ainsi à la fois logique et naturelle pour offrir la mobilité dans un contexte domestique aussi bien que professionnel.

CPL et Ethernet filaire

La cohabitation entre CPL et réseau filaire (câble Ethernet, fibre optique, câble TV, câble téléphonique, etc.) ne génère pas de perturbation puisque les bandes de fréquences utilisées par ces technologies sont toutes situées hors des bandes de fréquences des CPL.

Seule la technologie de desserte VDSL, qui permettra d'atteindre des débits de plusieurs dizaines de mégabits par seconde sur les câbles téléphoniques en cuivre, utilisera la bande de fréquences des 138 kHz à 12 MHz et sera donc susceptible de souffrir d'interférences potentielles puisque les technologies CPL occupent la bande des 2-30 MHz, émettant un bruit électromagnétique autour des câbles électriques qui peut atteindre 70-80 dBµV (en valeur dite « quasi peak »).

La figure 13.15 illustre les différentes bandes VDSL et la place des bandes CPL dans cet espace fréquentiel.

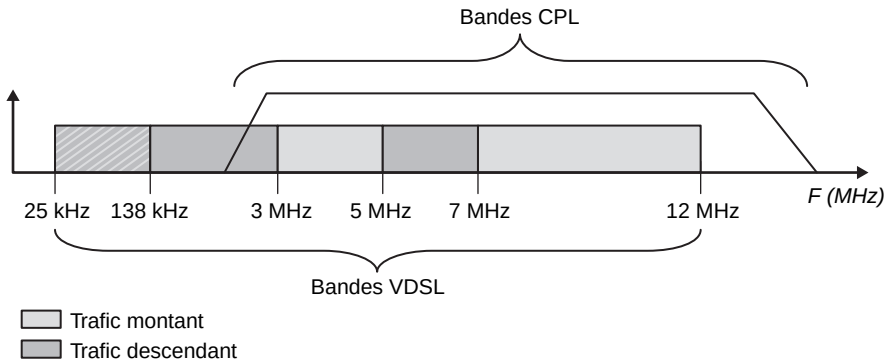


Figure 13.15

Interférences potentielles entre les bandes VDSL et CPL

Dans le domaine des réseaux locaux, la cohabitation entre technologies CPL et filaires ne pose pas de problème, si bien que les technologies filaires sont fréquemment utilisées comme dorsales pour les réseaux locaux CPL.

Avantages et inconvénients des technologies réseau

Afin de dresser une comparaison entre les technologies CPL et les autres technologies réseau, le tableau 13.2 récapitule les principaux avantages et inconvénients de chacune ces technologies.

Tableau 13.2 Comparaison des différentes technologies réseau

Technologie réseau	Coût	Inconvénient	Avantage
Câble Ethernet (CAT5 100baseT)	Élevé	– Passage de câbles – Coût du câble	– QoS garantie – Sécurité accrue (contrôle des accès aux prises RJ-45, filtrage) – Débit garanti – Alimentation par PoE
Wi-Fi (IEEE 802.11g)	Moyen	– Étude de couverture radio – Implémentation du cryptage WPA et AES – Besoin de serveur RADIUS – QoS non garantie	– Évolutivité du réseau – Mobilité et handover – ToIP sur Wi-Fi – Réseau hybride avec dorsale filaire

Tableau 13.2 Comparaison des différentes technologies réseau *(suite)*

Câble TV	Élevé si passage de câbles	– Passage de câbles – Média potentiellement partagé nécessitant une authentification	– Possibilité d'utiliser des câbles existants – QoS garantie – Difficulté d'accès au média physique
Fibre optique (fibre plastique)	Élevé	– Passage de câbles – Coût des équipements actifs	– Très haut débit – Immunité aux bruits – Idéal pour dorsale filaire – Difficulté d'accès au média physique
CPL HomePlug Turbo	Moyen	– Nécessite une étude d'ingénierie du site et du réseau électrique – Nécessite une bonne connaissance du réseau électrique – Difficulté d'accès de certains emplacements des équipements – Nécessite une bonne connaissance des risques électriques	– Débit utile élevé – Facilité de configuration – Évolutivité du réseau – Possibilité de réseau temporaire – Sécurité du média – Plusieurs VLAN sur le même réseau électrique
CPL HomePlug AV			– Débit utile pour applications vidéo HD – QoS garantie – Cohabitation avec autres équipements HomePlug 1.0 et Turbo – Respect des immunités électromagnétiques – Réseaux hybrides CPL/Wi-Fi
Câble téléphonique	Élevé si passage de câbles	– Câble téléphonique public appartenant à France Télécom	– Utilisation des câbles existants – Débit élevé et garanti – QoS garantie – Sécurité du média physique

Certaines d'entre elles ont connu un fort développement parce qu'elles répondaient à des besoins en apportant des fonctionnalités que n'offraient pas les autres (prix, facilité de déploiement, évolutivité, sécurité, etc.).

Optimisation des architectures réseau

La multiplication des technologies réseau disponibles actuellement rend légitime de rechercher le meilleur de chacune d'elles afin de construire une architecture réseau optimale.

Pour cela, il est important d'analyser le cahier des charges du réseau à mettre en place et de dresser la liste des caractéristiques les plus importantes du bâtiment à équiper.

L'étude d'ingénierie du réseau vise à identifier notamment les caractéristiques suivantes :

- structure des bâtiments (taille des pièces, possibilité de passage de câbles, matériaux des murs pour la transmission radio, etc.) ;
- réseaux existants (réseaux téléphoniques privés reliant plusieurs bâtiments d'un site, réseaux câble TV, etc.) ;
- cartographie du réseau électrique et position du tableau électrique ;
- performances réseau attendues pour les applications (temps de transit, latence, jitte, etc.) ;
- besoins d'évolutivité, de déménagement, réseaux temporaires, réseaux de tests, etc. ;
- groupes d'utilisateurs et besoins des réseaux logiques spécifiques ;
- facilités de déploiement, de configuration et de supervision globale du réseau.

Ces caractéristiques sont essentielles à préciser pour construire une architecture réseau à la fois performante et stable dans le temps.

De la même manière que nous avons établi un tableau comparatif des avantages et inconvénients des différentes technologies réseau, nous détaillons au tableau 13.3 les conditions d'utilisation optimale de chacune de ces technologies.

Tableau 13.3 Conditions d'utilisation optimale des technologies réseau

Technologie réseau	Condition d'utilisation optimale
Câble Ethernet	– Passage de câbles facile (colonnes montantes, autres travaux prévus, alimentation par PoE, etc.) – Architecture réseau optimale (étoile, anneau, branches, etc.)
Wi-Fi	– Couverture radio performante – Bonne gestion du *handover* entre cellules – Bonne gestion de la sécurité
Câble TV	– Passage de câbles facile – Accès au média existant facile
Fibre optique	– Passage de câbles facile – Équipements actifs optimisant le multiplexage – Bon choix du mode optique et des longueurs d'onde
CPL	– Bonne connaissance du réseau électrique – Réseau hybride avec dorsale filaire
Câble téléphonique	– Possibilité de placer les équipements à proximité du PABX – Disponibilité de liens point-à-point

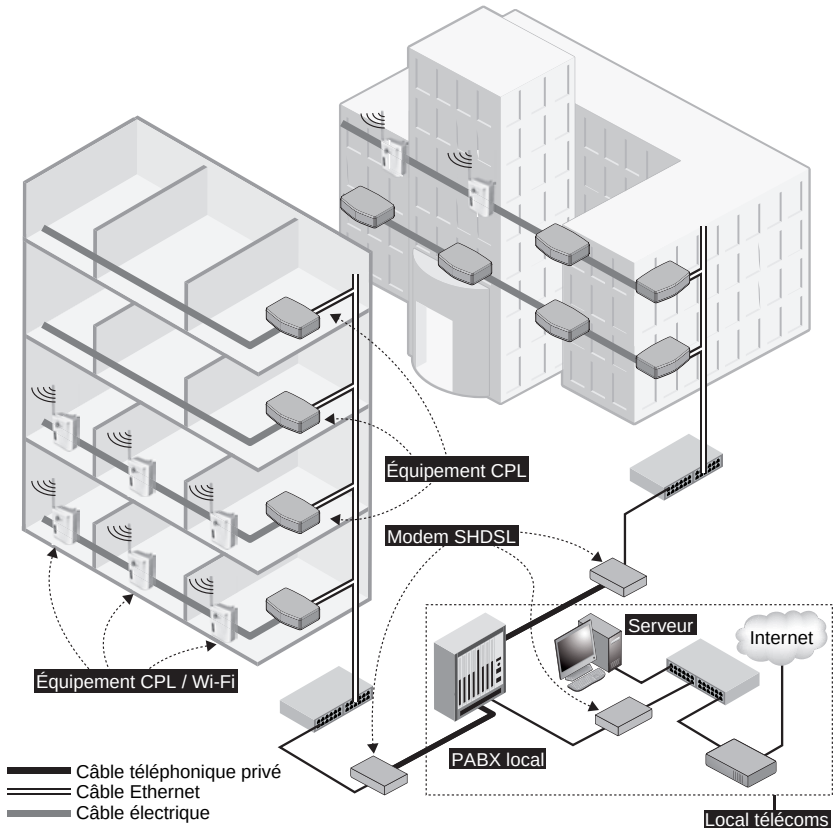
Exemple d'architecture optimisée

Nous allons prendre l'exemple du réseau informatique d'une installation comportant deux bâtiments disposant déjà de lignes téléphoniques privées partant d'un PABX local pour relier les deux bâtiments.

Ces bâtiments comportant plusieurs étages, nous désirons implémenter la mobilité des utilisateurs dans chaque pièce et entre les deux bâtiments. Nous supposons que les colonnes montantes sont accessibles et permettent de passer des câbles supplémentaires et d'installer les équipements réseau facilement.

Une bonne connaissance du réseau électrique de chacun des étages et si possible de l'ensemble du bâtiment est nécessaire à la mise en place des équipements CPL.

Figure 13.16
Exemple d'architecture hybride optimisée



Pour répondre à ces besoins et à ce cahier des charges, l'architecture hybride illustrée à la figure 13.16 est composée des éléments suivants :

- liens IP entre le local télécoms et les bâtiments à l'aide de modems SHDSL sur les câbles téléphoniques en paires torsadées ;

- dorsale Ethernet le long des colonnes montantes pour alimenter chaque étage en connexion IP ;
- réseau CPL d'étage, avec un équipement passerelle par étage connecté à la dorsale Ethernet ;
- équipement hybride CPL/Wi-Fi sur prise dans chaque pièce afin d'assurer une couverture Wi-Fi complète ;
- clients connectés au réseau soit par le biais de cartes IEEE 802.11, soit grâce à des équipements CPL raccordés aux « passerelles » CPL d'étage.

Cette architecture n'est qu'un exemple de réseau hybride. Elle offre cependant une utilisation optimale des contraintes du lieu d'installation du réseau. Chacune de ces contraintes peut se transformer en avantage pour peu que nous choisissions la technologie réseau adaptée.

CPL/Wi-Fi, un couple parfait ?

Comme indiqué à maintes reprises dans cet ouvrage, il existe de nombreuses similitudes entre les technologies CPL et Wi-Fi, hormis le support de communication, que ce soit au niveau des débits proposés, des fonctionnalités ou même des coûts des équipements. Il était donc assez logique de voir ces deux technologies se rapprocher afin de permettre d'utiliser le réseau électrique comme dorsale Ethernet et les interfaces Wi-Fi pour connecter les clients du réseau local.

De plus en plus de fabricants proposent des équipements couplant les deux technologies. Le développement des tout derniers standards va bientôt amener sur le marché des équipements couplant HomePlug AV et IEEE 802.11 Super G dynamic afin d'offrir de meilleurs débits et la diffusion des flux vidéo HD.

La figure 13.17 illustre l'échange de trames entre un équipement CPL et un équipement Wi-Fi, avec, en dessous, un exemple d'équipement hybride CPL/Wi-Fi. Les fabricants travaillent actuellement à l'optimisation des connexions entre interfaces CPL et radio afin d'éviter les phases d'encapsulation et de désencapsulation des trames.

Annexe

Références

Sites Web

Organismes de standardisation

IEEE

http://www.ieee.org

http:// grouper.ieee.org/groups/1901/ pour le groupe de travail lié aux CPL

ETSI

http://www.etsi.org

IETF

http://www.ietf.org

Cenélec

http://www.cenelec.org

CEI, et plus particulièrement CISPR 22

http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=dirdet.p&progdb=db1&committee=CI&css_color=purple&number=CIS/I

Technologies CPL

HomePlug

http://www.homeplug.org

DS2

http://www.ds2.es

Spidcom

http://www.spidcom.com

Sites portails sur les CPL

CPL-France

http://www.cpl-france.org

CPL News

http://www.cpl-news.com

Powerline communications.net

http://powerlinecommunications.net

PUA

http://pua-plc.com

PLC Forum

http://www.plcforum.org

CEPCA Alliance

http://www.cepca.org

Réglementation

Texte officiel sur les CPL

http://www.telecom.gouv.fr/telecom/cpl.pdf

ARCEP

http:// www.art-telecom.fr/communiques/communiques/2005/c05-19.htm

Produits

http://www.aceex.com

http://www.acer.com

http://www.amigo.com.tw/

http://artimi.com/

http://asokausa.com/

http://www.atlantisland.it/

http://bewan.com

http://www.billion-france.com/

http://cometlabs.com/

http://www.courantmultimedia.fr

http://www.connectland.net/

http://www.corinex.com

http://www.defidev.com/

http://www.devolo.com

http://www.dynamode.co.uk/

http://www.edimax.com/

http://eichhoff.de

http://www.gigafast.com

http://www.ilevo.com

http://www.jaht.com/

http://www.leacom.fr

http://www.linksys.com

http://www.Main.net-plc.com/

http://global.mitsubishielectric.com/bu/plc/

http://www.msi-computer.fr/

http://netgear.com/

http://www.niroda.com/

http://www.olitec.fr/

http://www.ovislink.fr

http://www.oxance.com

http://www.packardbell.fr

http://peabird.com

http://phonex.com

http://www.powernetsys.com

http://www.powertec.com.au

http://www.sagem.com

http://www.schneider-electric.fr

http://siemens.com

http://smc.com

http://www.stt.com.tw

www.sei.co.jp

http://www.telkonet.com

http://www.omenex.com

http://www.xeline.com

http://www.xnet.com.tw

http://www.yakumo.de

http://www.zyxel.fr

Produits CPL bas débit

http://www.siconnect.com

http://www.itrancomm.com

http://www.arianecontrols.com

Livres et articles

Le premier livre sur les CPL en anglais, très technique et complet sur les premières technologies CPL :

DOSTERT (KLAUS), *Powerline communications*, Prentice Hall, 2000

Un livre complet sur les technologies CPL pour les réseaux de desserte :

HRASNICA (H.), HAIDINE (A.), LEHNERT (R.), *Broadband Powerline Communications: Network Design*, 2004, Wiley

Un mémoire de thèse majeur sur les modélisations de réseau électrique dans les bandes utilisées par les technologies CPL :

ISSA (F.), « Analyse et modélisation du réseau électrique Basse Tension aux fréquences courants porteurs de la gamme [1-30MHz] », Université Paris XI, 2002

Un livre de référence en anglais sur la technologie HomePlug 1.0 rédigé par des chercheurs de l'Université de Floride :

LEE (M. K.), NEWMAN (R. E.), LATCHMAN (H. A.), KATAR (S.), YONGE (L.), *HomePlug 1.0 Powerline Communication LANs– Protocol Description and Performance Results*, version 5.4, 2000, Wiley

Un article complet sur les technologies CPL en anglais :

PAVLIDOU (F.-N.), LATCHMAN (H. A.), HAN VINCK (A. J.), NEWMAN (R. E.), *"Powerline communications and applications", International Journal of Communication Systems*, 2003, Wiley

Un mémoire de thèse important sur les notions de rayonnement électromagnétique des technologies CPL :

RAZAFFERSON (R.), « Analyse du rayonnement et des couplages électromagnétiques provoqués par des signaux hautes fréquences interférant avec des câbles d'énergie basse tension », Université de Lille I, 2002

Index

D