Figure 10.15
Boîte de dialogue Propriétés de Ethernet

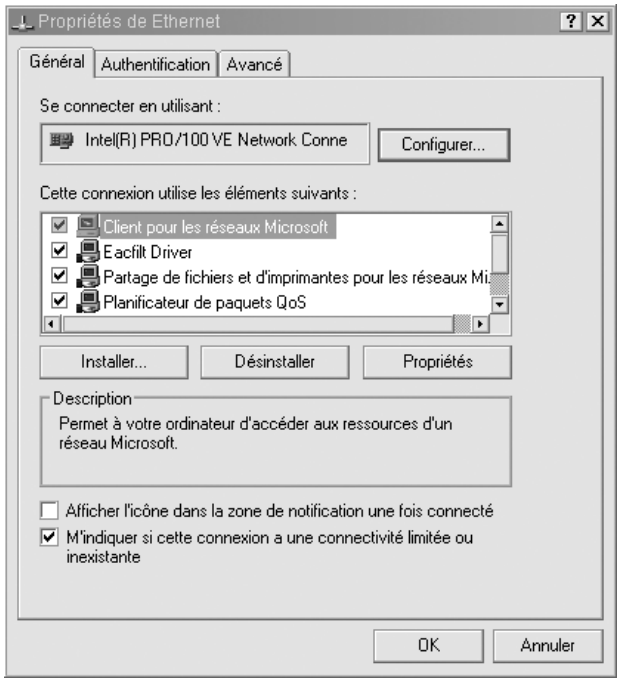
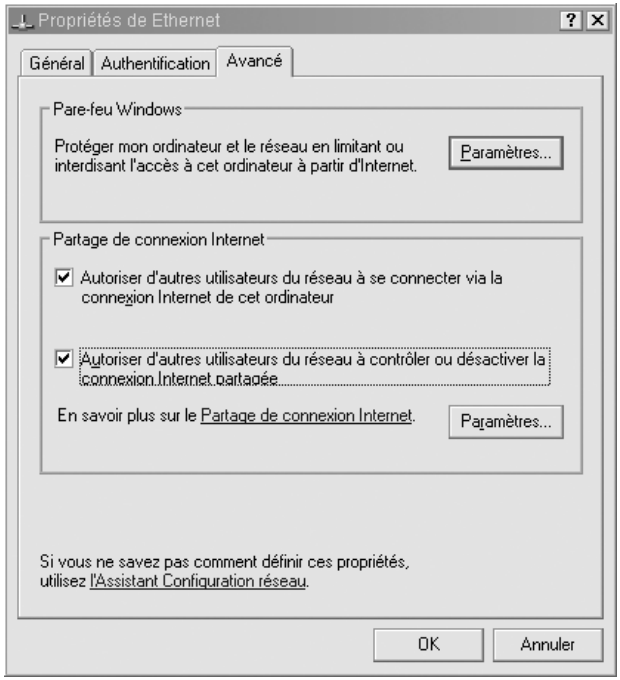


Figure 10.16
Paramètres de configuration avancés de la connexion



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).*

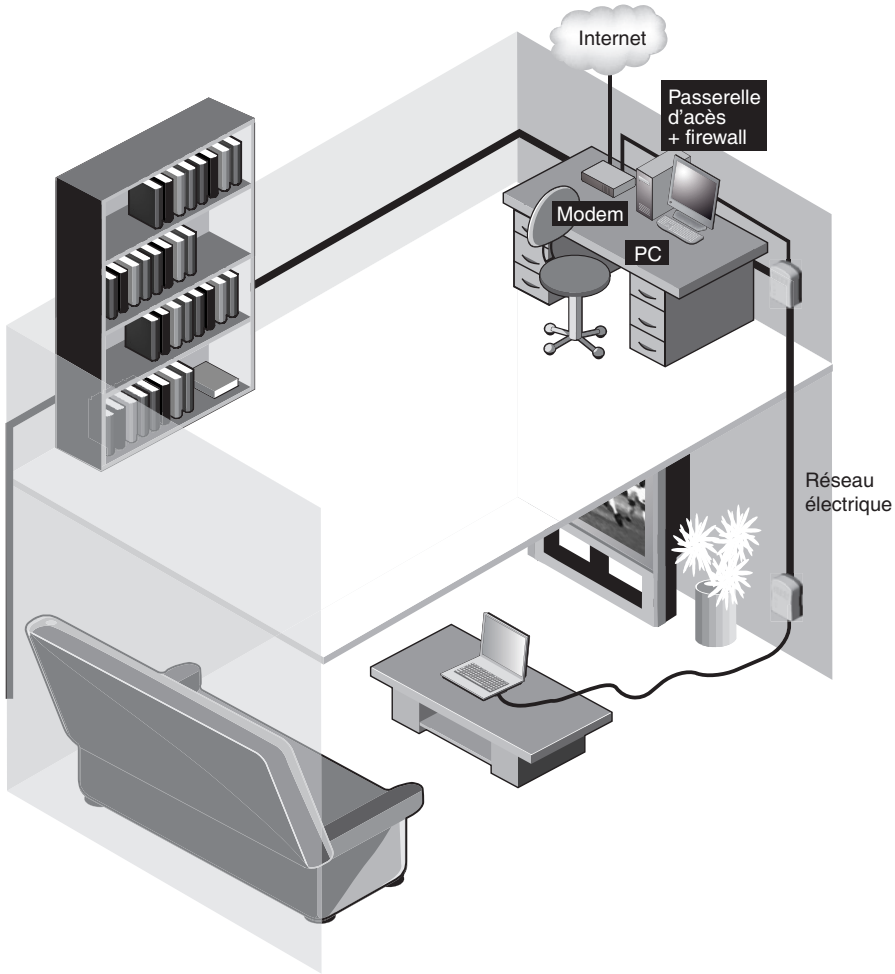


Figure 10.17
Réseau CPL avec passerelle d'accès sécurisée par firewall

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.

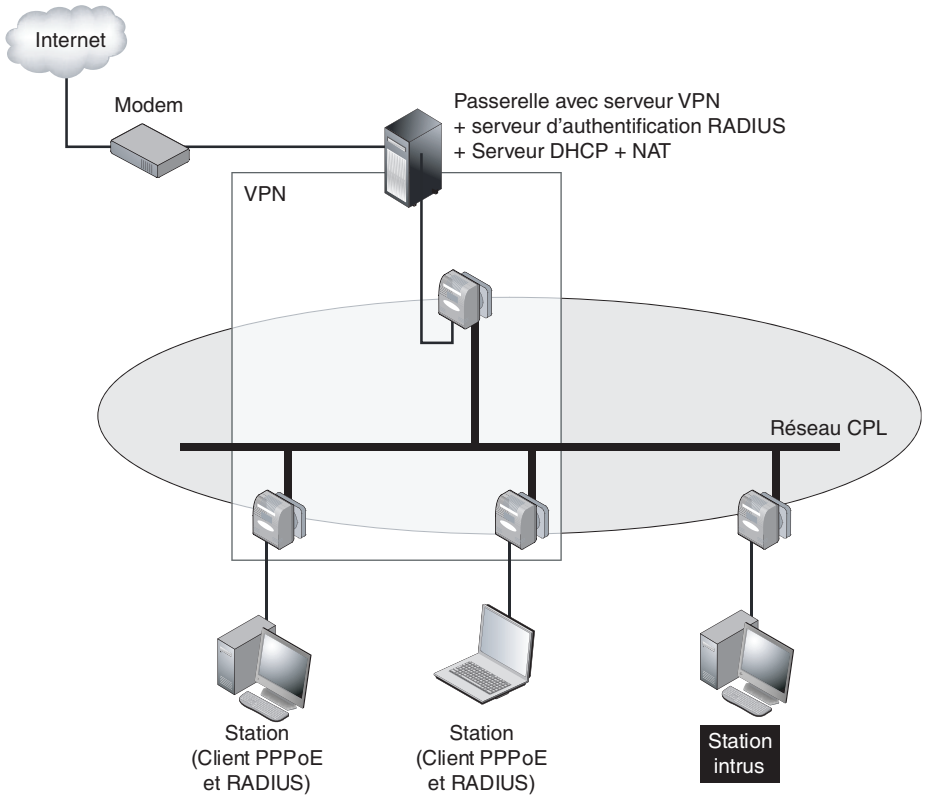


Figure 10.18

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.

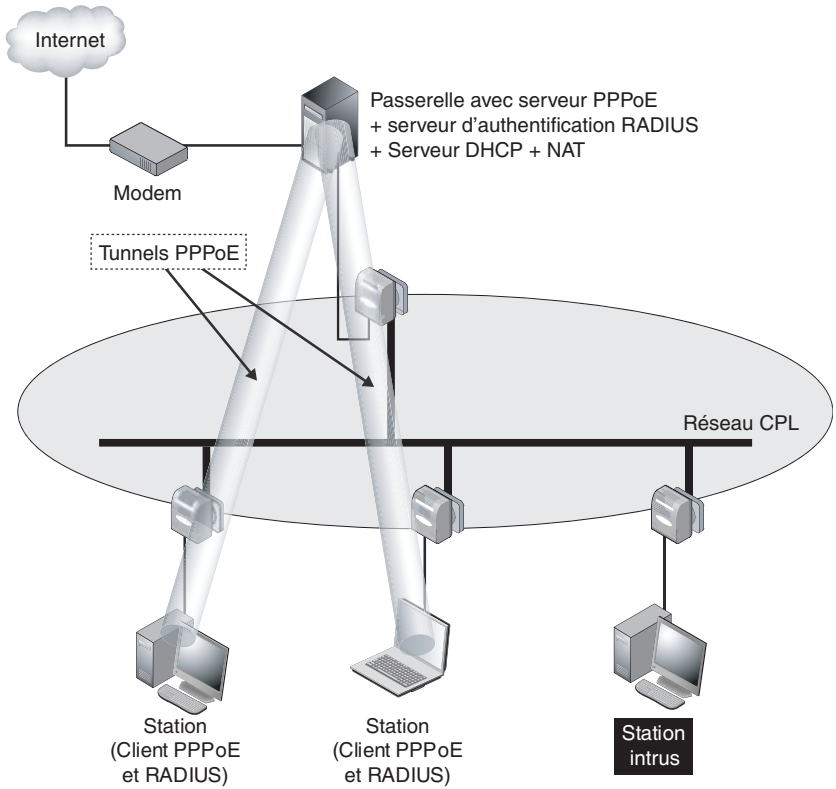


Figure 10.19

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

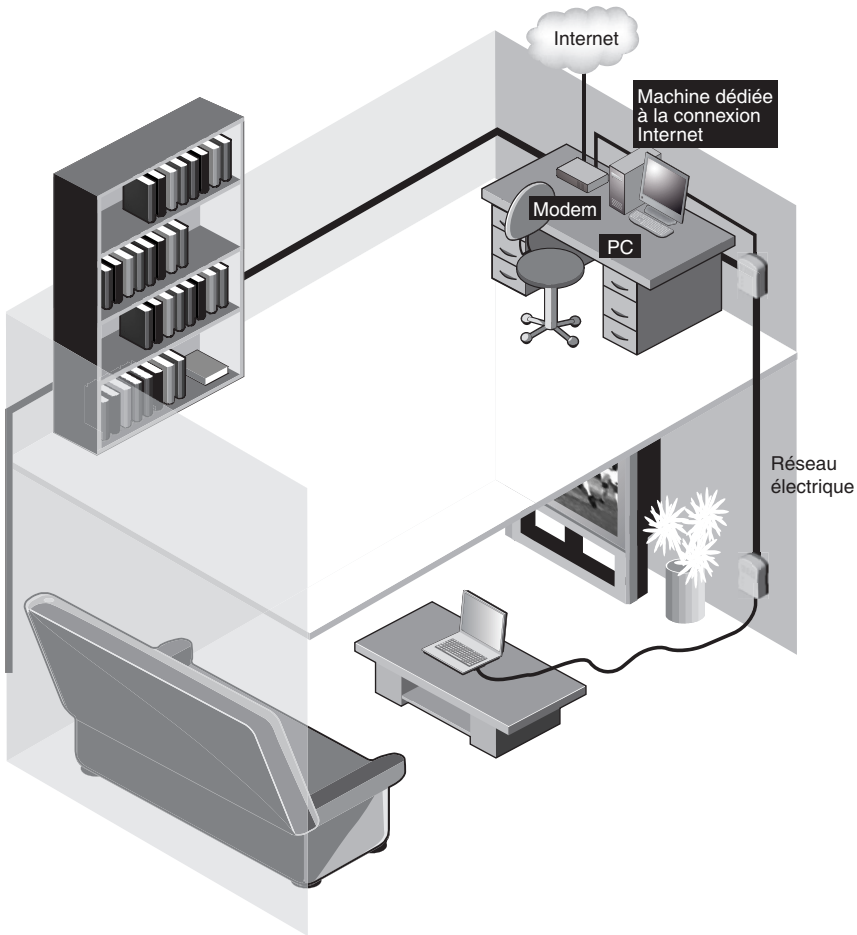
Dans un réseau CPL, toute connexion Internet peut être utilisée : modem 56 K, RNIS, câble, ADSL, ADSL2+, satellite ou FTTH (Fiber to the Home). Étant donné que la vitesse de transmission d'un réseau CPL est comprise entre 1 et 14 Mbit/s pour HomePlug 1.0, 1 à 85 Mbit/s pour HomePlug Turbo et 1 à 200 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.

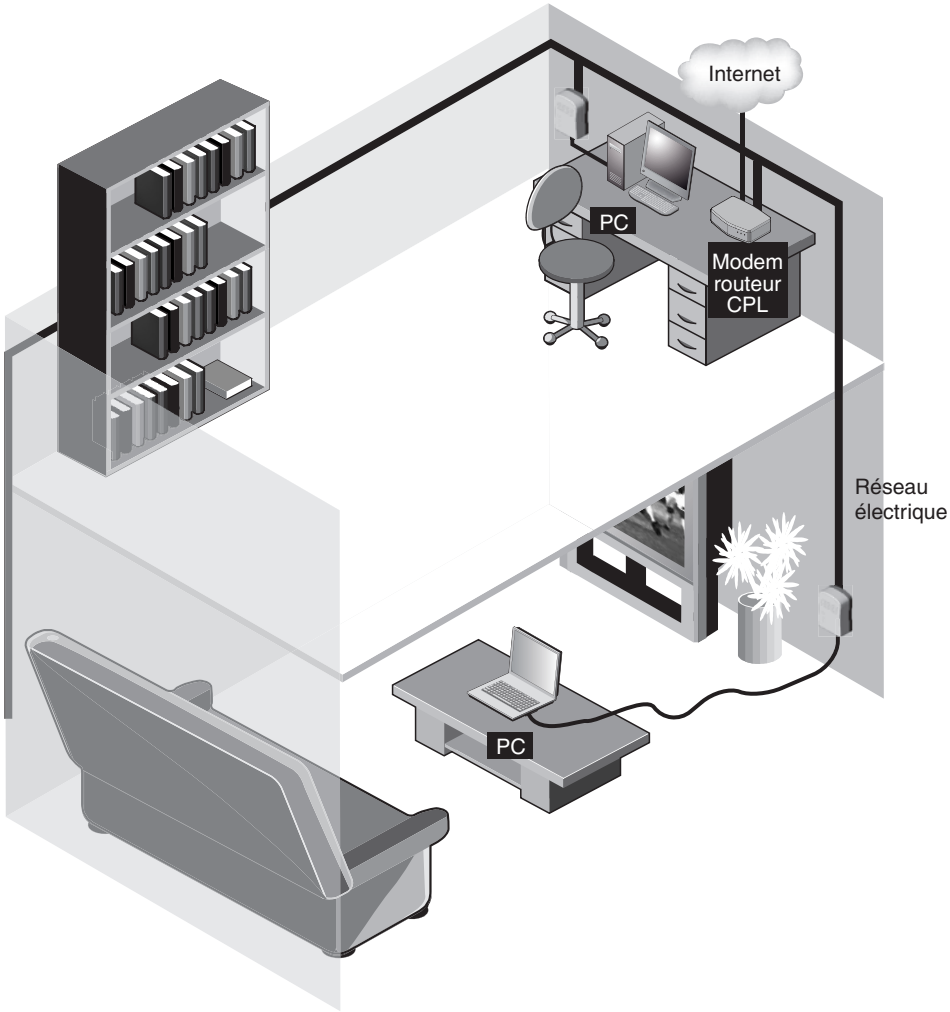


Figure 10.21

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

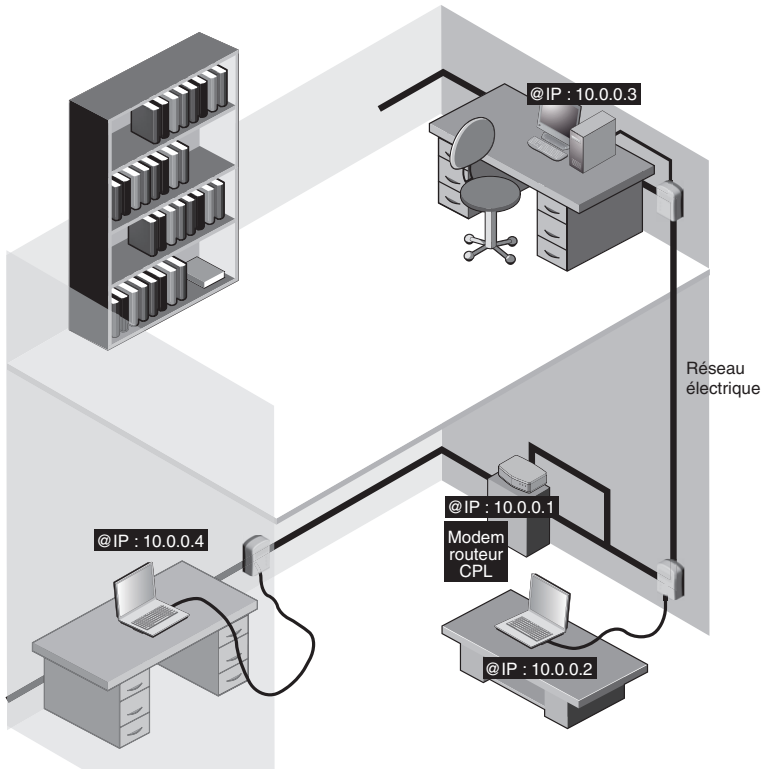
Pour partager une connexion Internet, deux protocoles sont utilisés, le NAT (Network Address Translation) et DHCP (Dynamic Host Configuration Protocol) :

- 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

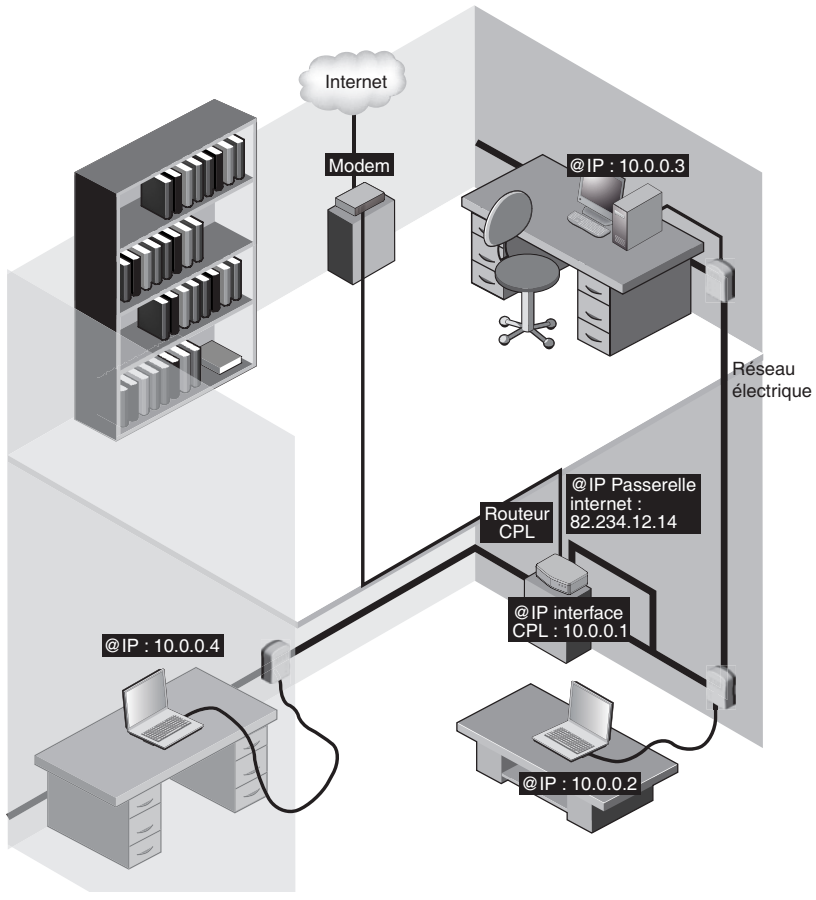
Les adresses DNS sont données par le fournisseur d'accès Internet, sauf dans le cas où un DNS local est présent dans le réseau domestique.

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.

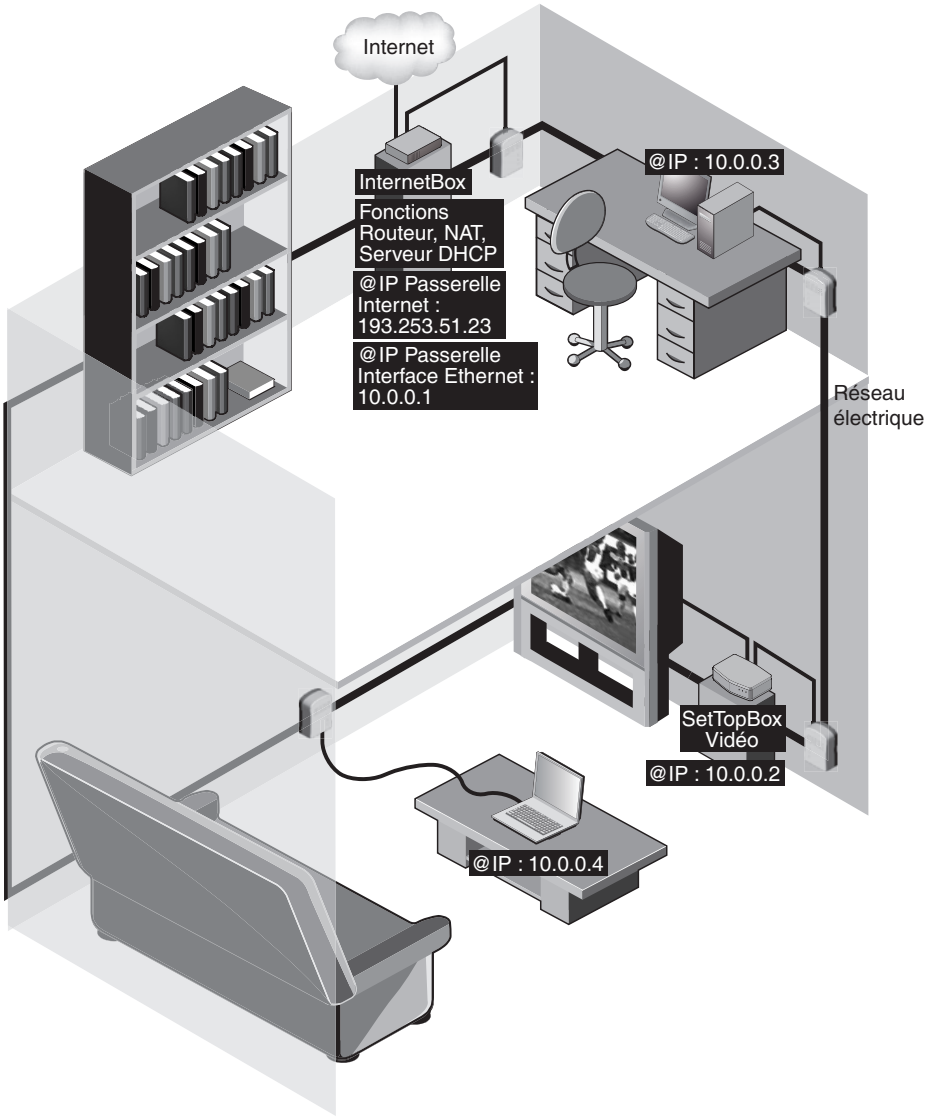


Figure 10.24

Architecture d'un réseau CPL domestique avec passerelle d'accès à Internet dédiée