

- 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.

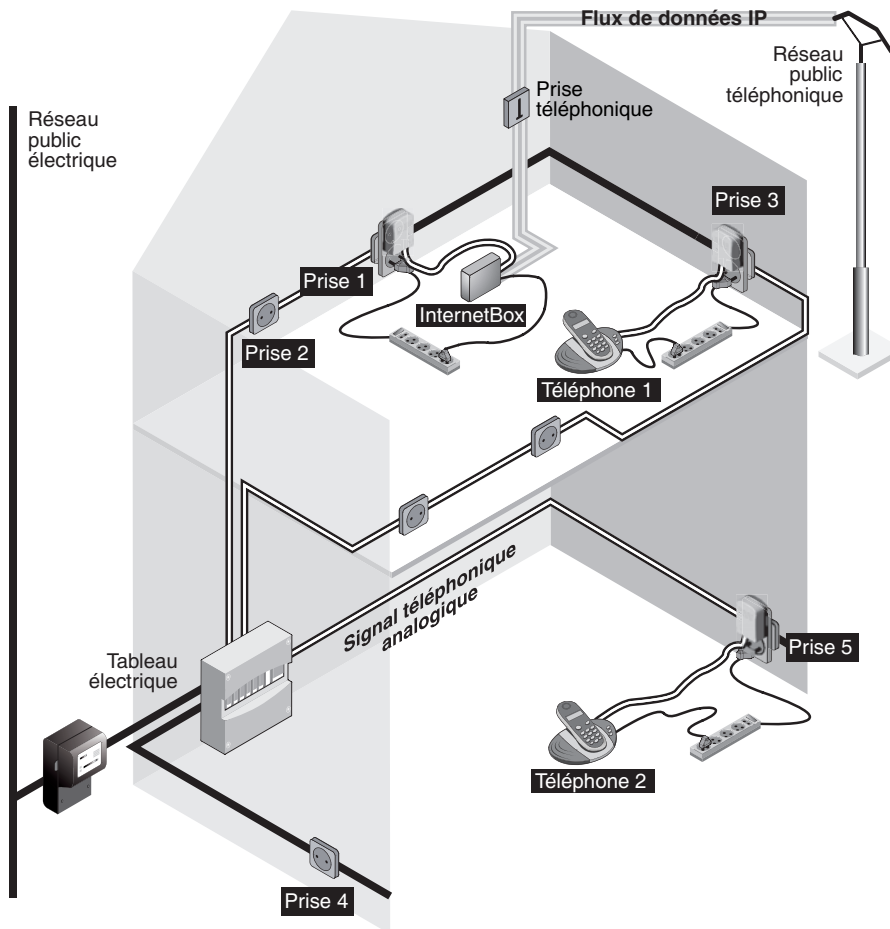


Figure 10.7

*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.

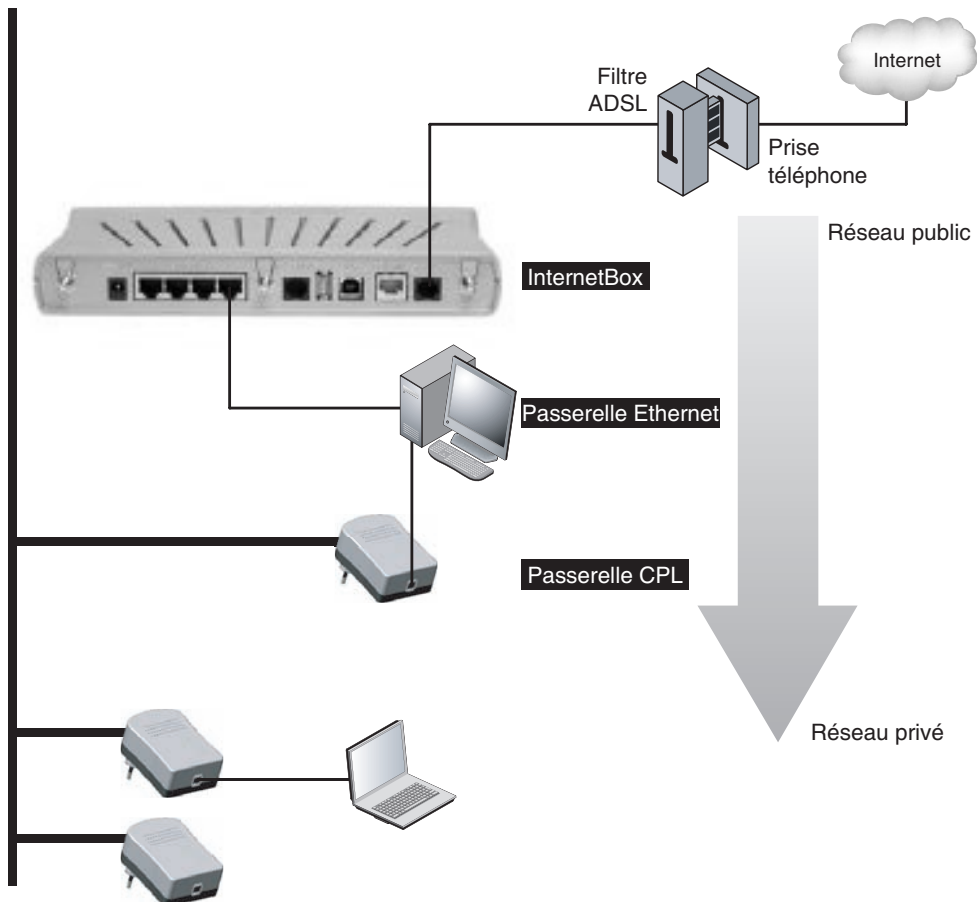
**Tableau 10.3 Niveaux de priorité des trafics de données pour la passerelle CPL**

Priorité pour le trafic de données	Priorité HomePlug 1.0 et Turbo
0	CA0 <span style="float: right;">Priorité basse</span>
1	
2	CA1
3	

**Tableau 10.3 Niveaux de priorité des trafics de données pour la passerelle CPL (suite)**

Priorité pour le trafic 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](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.

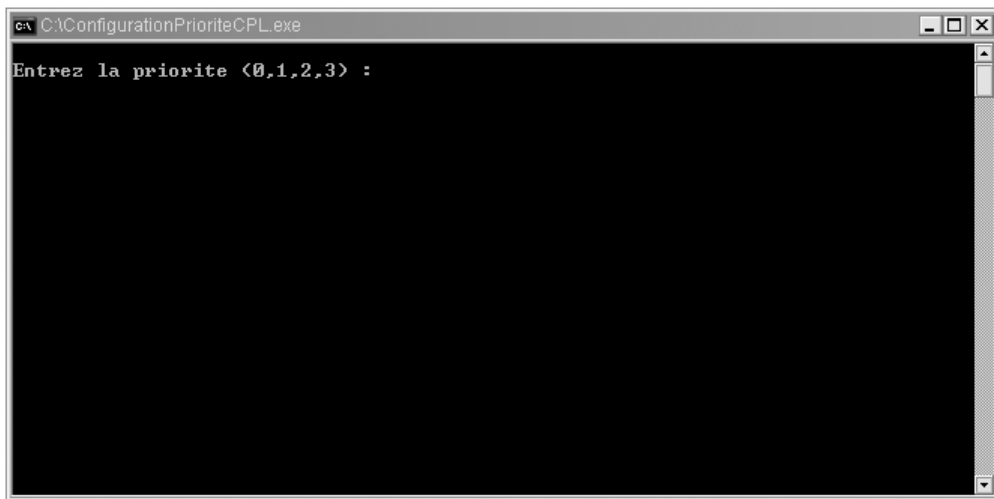
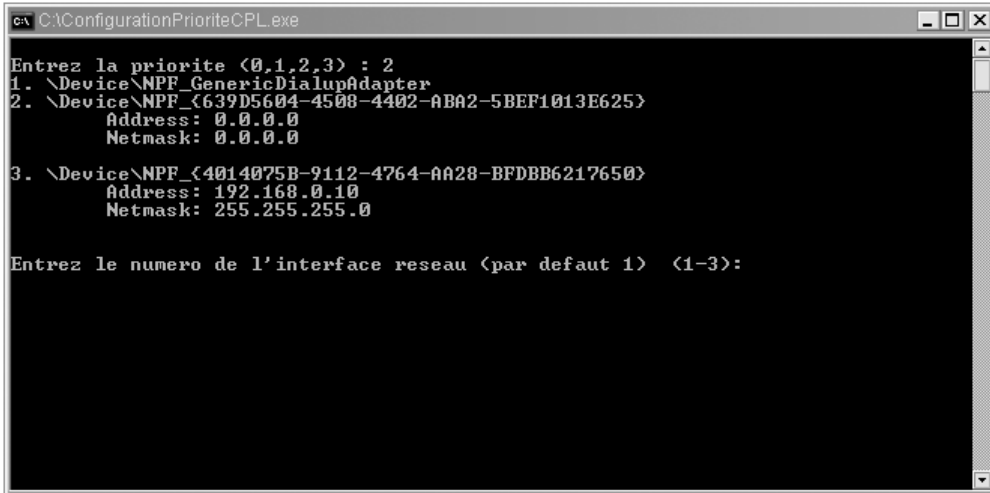


Figure 10.9

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.



```
C:\ConfigurationPrioriteCPL.exe
Entrez la priorite <0,1,2,3> : 2
1. \Device\NPF_GenericDialupAdapter
2. \Device\NPF_{639D5604-4508-4402-ABA2-5BEF1013E625}
   Address: 0.0.0.0
   Netmask: 0.0.0.0
3. \Device\NPF_{4014075B-9112-4764-AA28-BFDBB6217650}
   Address: 192.168.0.10
   Netmask: 255.255.255.0
Entrez le numero de l'interface reseau <par default 1> <1-3>:
```

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](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).

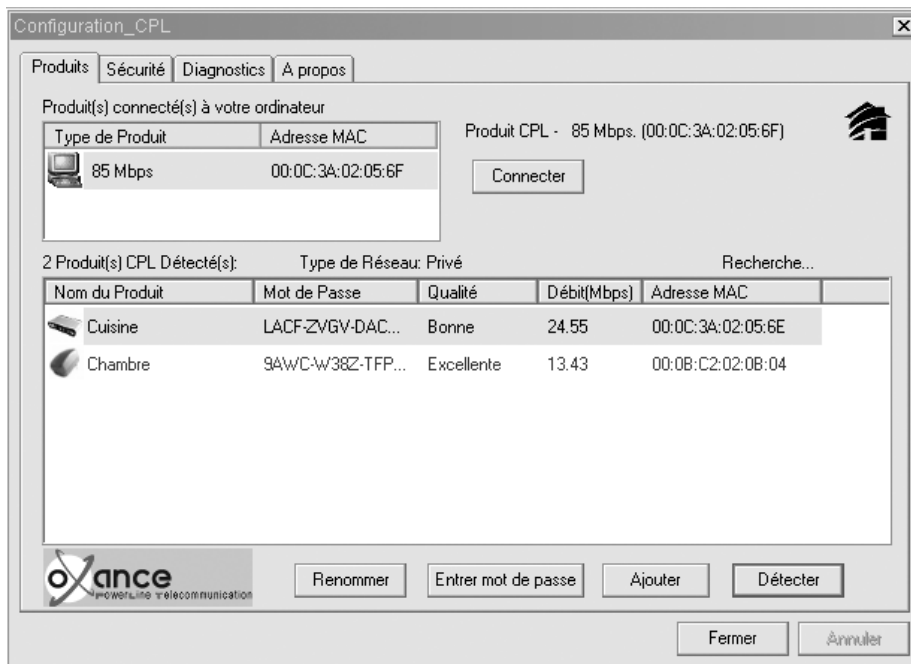
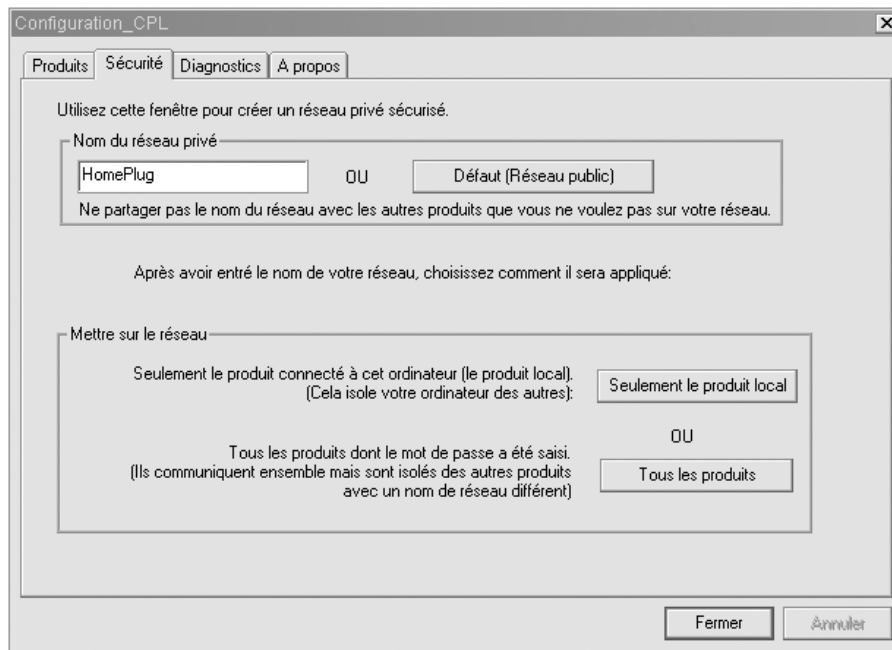


Figure 10.11

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.

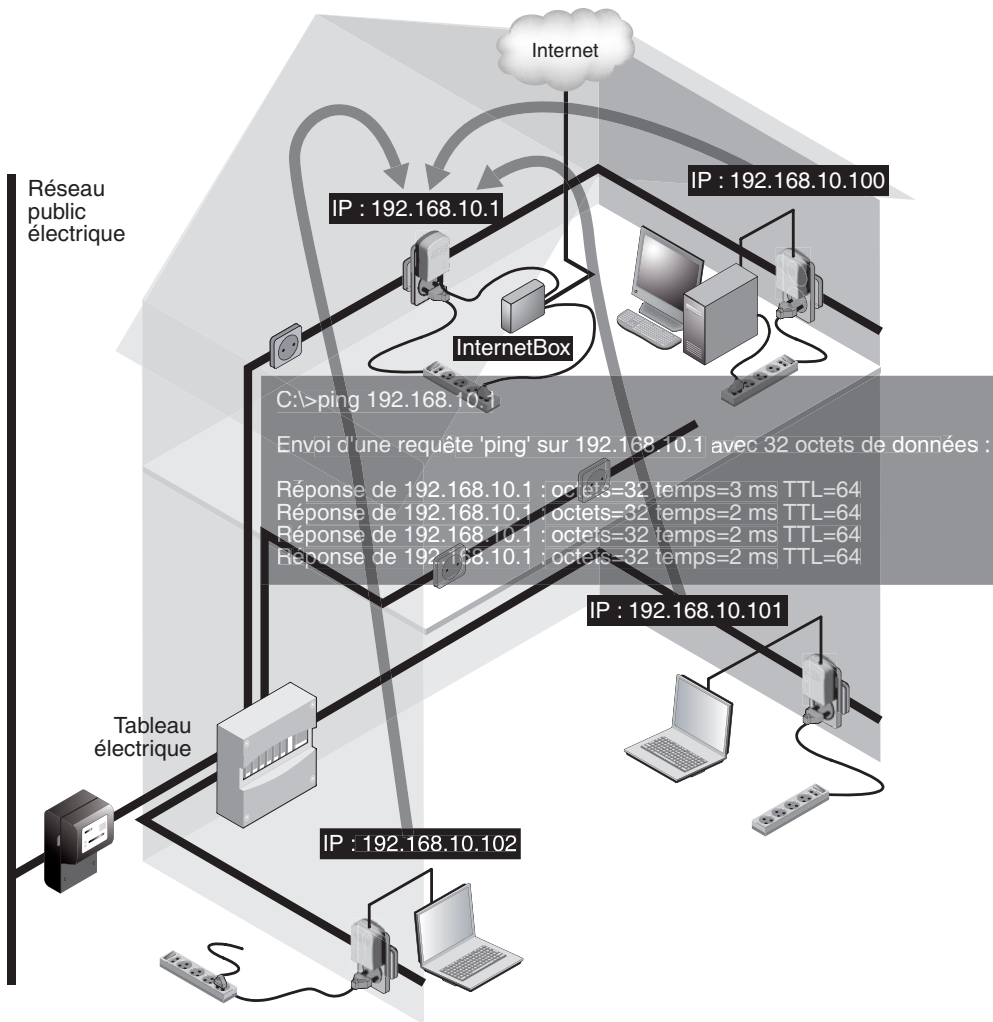


Figure 10.13

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'Internet-Box 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.

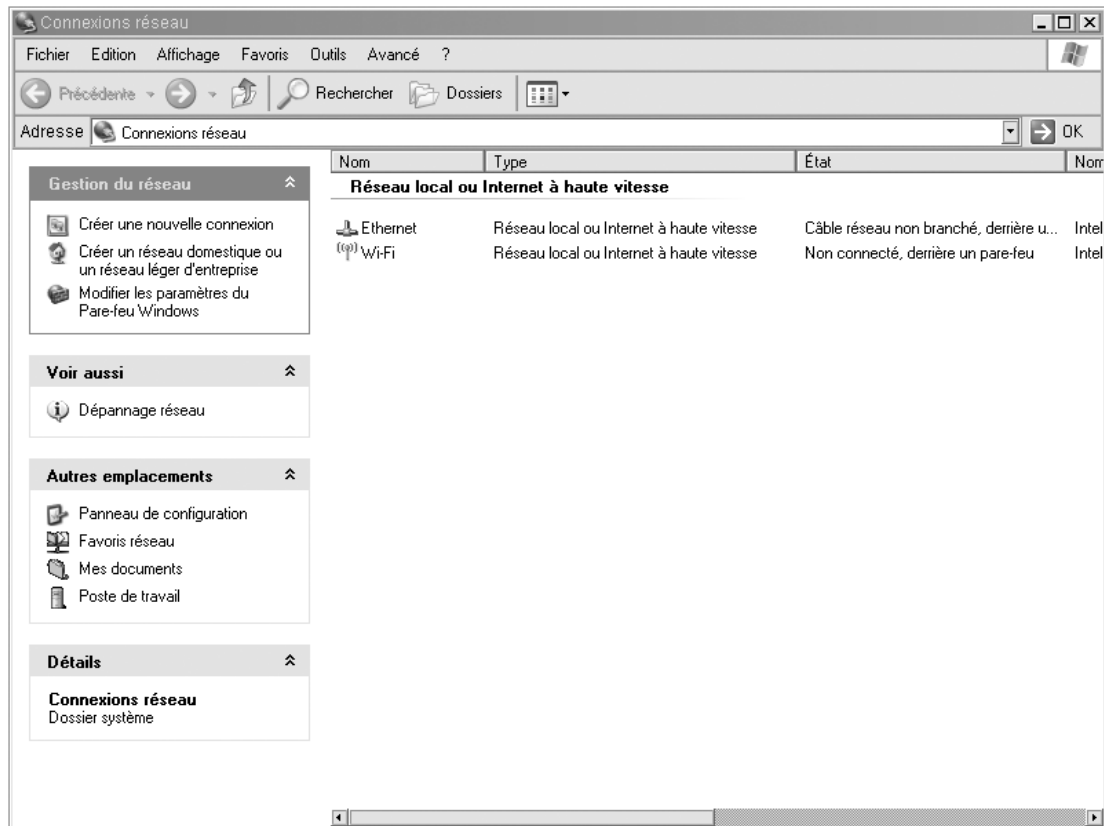


Figure 10.14

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).