02

La transmission des données

Le chapitre précédent a permis de comprendre la façon dont les éléments autour des réseaux se sont développés du point de vue de la théorie ainsi que de la normalisation. Ces principes sont maintenant clairs, mais, votre réseau n'est toujours pas construit. La transmission des données (couche 1 de l'OSI) s'effectue sur des supports soit physiques (câbles, fibres), soit moins matériel comme le sans fil. Ce chapitre vous les présente ainsi qu'une technologie émergente : le CPL (courant porteur en ligne).

1. Les câblages

Les câbles sont les premiers types de supports utilisés pour la transmission des informations. Une estimation de 2004 estime qu'il existe 925 Millions de prises réseaux de part le monde. Les données peuvent êtres transmises au moyen de courant électrique alternatif mais aussi de lumière comme c'est le cas dans les fibres optiques. La réalisation d'un plan de câblage est la première étape. En effet, il est utile de définir les distances maximales entre les points les plus éloignés, les débits voulus, le protocole réseau mis en place, ainsi que la topologie utilisée. Ces éléments entrent en considération, comme nous allons le voir, dans le choix du bon type de câblage. Le plan réalisé, les choix effectués, il faut alors certainement poser des goulottes ou des rails afin de créer le chemin de câbles dans la salle ou le bâtiment.

1.1 Normalisation et appellation

Afin de permettre aux différents matériels de communiquer ensemble il a été nécessaire d'unifier ces câbles. C'est le travail de l'IEEE. La dénomination des câbles provient de leurs travaux. Cette dénomination est basée sur les principales caractéristiques des câbles :

- l'atténuation du signal ;
- la bande passante (fréquence maximale du signal en Hertz) ;
- le débit maximum possible exprimé en Mbits/s ;

- le taux d'erreur (le support selon sa qualité est lui-même source d'erreur) ;
- la facilité à être connecté au matériel.

L'IEEE utilise le débit, le type du canal ainsi que la longueur ou le type du support dans la construction du nom.

- **Le débit en Mbits/s (10, 100, 1000 …)**

Attention

Un amalgame est souvent fait entre la fréquence en Mhertz et le débit en Mbit/s proposé par le câble. Pour certain type de câble (coaxiaux), il y a correspondance mais pour les autres ce n'est pas souvent le cas. Par exemple, les paires torsadées 1000BaseT permettent d'atteindre 1000Mbit/s mais grâce à un artifice qui permet d'utiliser les 4 paires avec un débit pour chacune de 250Mbit/s. Le câble n'a pas une fréquence de 1000Mhertz mais de 80Mhertz.

- **Le type de canal de communication utilisé**

  Bande de base (ou Base Band).Il ne peut passer sur le support qu'un seul signal. Le canal n'est donc utilisé que par un équipement à la fois. On peut le comparer avec le téléphone standard où une seule personne peut parler à la fois.

  Bande large (ou Broad Band). Le support est découpé virtuellement en plusieurs canaux. Plus d'une machine peut transmettre ses données à la fois. On peut le comparer avec la télévision, qui, sur un même câble reçoit plusieurs chaînes. Ce câble normalisé par le 802.14, était utilisé pour la communication ethernet par modem câble ou sur des réseaux CATV (Community Antenna TeleVision).

- **La longueur maximale d'un segment en centaines de mètres ou le type du support**

Nous obtenons alors des câbles 10BASE2, 10BASE5, 10BROAD36, 100BASE-T, 100BASE-F...

Par exemple, le câble dont l'appellation est 10BASE2 indique que la Bande de base est de 10MHz sur une distance maximale de 200 mètres.

A noter

Ethernet définit par le 802.3 s'appuie sur la méthode d'accès CSMA/CD. Tous les câbles qui vont êtres étudiés découlent de cette norme.

D'autres organismes ont aussi pris part à cette normalisation l'ISO, les groupements américains EIA (Electronic Industries Alliance : http://www.eia.org/) crée en 1924 et TIA (Telecommunications Industry Association : http://www.tiaonline.org). Ces deux derniers travaillent en étroite collaboration du fait de leur histoire croisée. Le TIA a été créé en 1988 suite à la fusion de l'USTSA (United States Telecommunications Suppliers Association) et de la branche télécommunication de l'EIA, l'ITTG (Information and Telecommunications Technologies Group). Pour ces raisons,on trouve des standards nommés EIA/TIA..

Malgré cette recherche d'homogénéisation, il existe des différences entre les USA et le reste du monde.

Pour bien comprendre, certaines notions utilisées dans la chaîne de câblage, doivent êtres vues et comprises.

Définition

Un canal de câblage est le chemin qui sépare les matériels qui communiquent. Le chemin entre le commutateur et le poste de travail représente un canal de câblage.

Définition

Une catégorie définit dans le standard américain EIA/TIA 568B, les performances d'un canal, d'un câble ou d'un connecteur.

Une catégorie définit dans la norme internationale ISO IS11803 et EN 50173 les performances du câble et du connecteur. Tandis que pour le canal, on parle de classe de performance.

Ces termes seront étudiés plus en profondeur dans la partie portant sur les câbles torsadés.

1.2 Les câbles coaxiaux

Ces câbles sont dépassés mais, sont intéressants à connaître car ils sont à l'origine du câblage.
Il existe deux types de câbles coaxiaux :

- Le 10Base2 connu sous l'appellation Ethernet Fin
- Le 10Base5 connu sous l'appellation Ethernet gros

Ces deux câbles ont des points communs

- La topologie utilisée avec ce type de câble est celle du bus.
- La vitesse de transmission sur les câbles coaxiaux est limitée à 10Mégabits par seconde
- La bande passante est de 10Mhertz
- Le terminateur est un bouchon qui possède une impédance de 50 Ohms
- Au maximum 5 segments peuvent être mis bout à bout au moyen de 4 répéteurs ou concentrateurs
- Sur ces 5 segments, 3 sont des segments porteurs et 2 sont des segments de liaison
- Ils utilisent des connecteurs de type N (rond à vis)

Définition

Un segment porteur est une portion de câble sur laquelle des équipements peuvent être connectés.
Un segment de liaison est une portion de câble sur laquelle on ne peut connecter d'équipements. Il n'est utile que pour allonger la distance entre deux entités.

Nous allons étudier maintenant les contraintes sur ces deux câbles.

Câble 10BASE2 ou Ethernet fin

Ce câble est aussi appelé thin Ethernet.
Le câble contient en son centre un fil en cuivre. Ce conducteur est entouré d'un diélectrique servant d'isolant, d'un blindage composé de tresses le protégeant des perturbations extérieures et enfin d'une gaine en PVC, comme le montre la Figure 2.1.

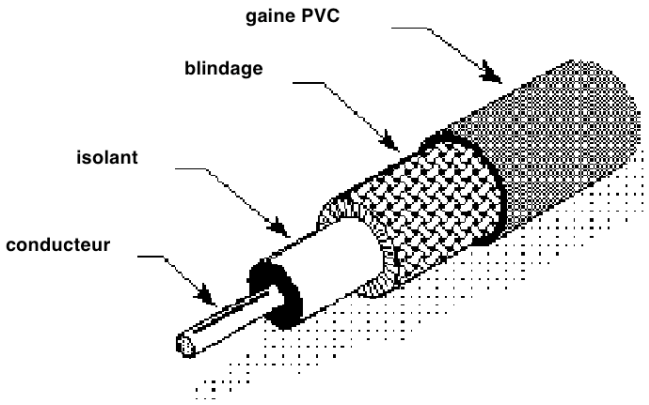


Figure 2.1,
Structure du câble Ethernet fin.

L'impédance des bouchons qui terminent le câble doit être de 50 Ohms.

Définition

L'impédance est la mesure de la résistance pour les courants alternatifs. L'unité de mesure est l'Ohm.

La vitesse de transmission des informations est de 10 Mbit/s. La longueur maximale d'un segment est de 185 mètres. On peut mettre bout à bout 5 segments, soit une couverture maximale de 5 × 185 = 925 mètres.

Définition

Sur les cinq segments, seuls trois peuvent être "porteurs", c'est-à-dire contenir des matériels. On parle de la règle des 5,4,3 : 5 segments, 4 répéteurs ou concentrateurs pour les lier et 3 segments porteurs.Sur un segment peuvent êtres connectés, au moyen de transceivers, souvent directement intégré à la carte réseau du matériel, un maximum de 30 postes. L'espacement entre chaque poste doit être au minimum de 0,5 mètre. Le diamètre du câble est de 5 millimètres. Ce câble pourra donc permettre au maximum la connnexion de 90 équipements (3 segments porteurs contenant 30 postes chacun).

Comme le montre les figures 2.2, 2.3 et 2.4, la connexion sur le câble se fait grâce aux connecteurs de type BNC (Bayonet Neil-Concelman). Ils ont une impédance de 50 ohms. Les connexions à la carte réseau de l'équipement, se font au moyen de prises BNC en T. Ces connecteurs sont simples à positionner sur la carte réseau. Par contre les prises en T nécessitent plus de travail. En effet pour les insérer sur le câble il faut tout d'abord le sectionner pour sertir deux prises BNC à chaque extrémité des ces deux sections pour ensuite y installer cette prise en T qui viendra se connecter sur la carte réseau de l'équipement.

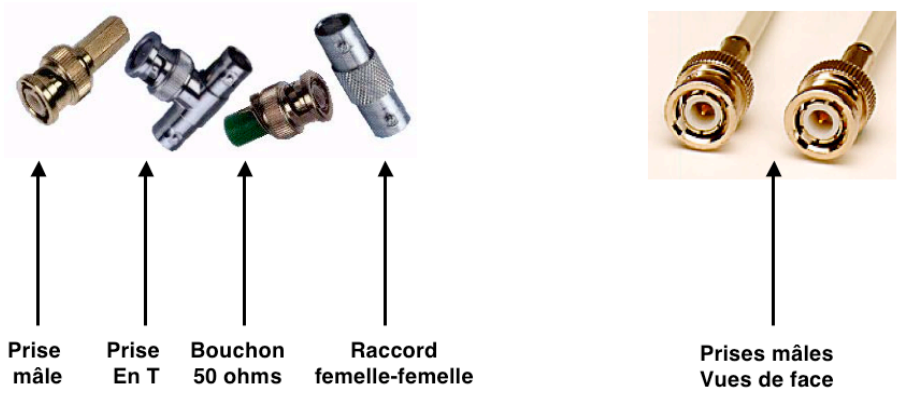


Figure 2.2,

Différents types de prises associées au 10BASE2.

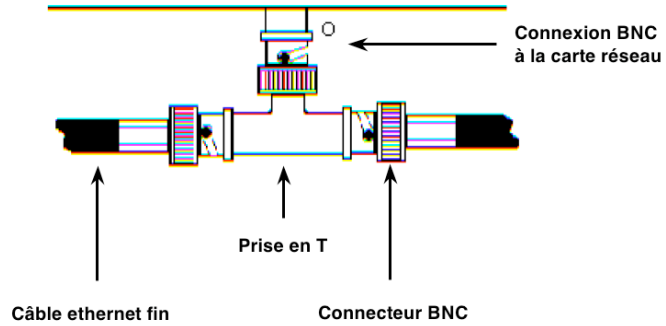


Figure 2.3,

Deux câbles 10BASE2 raccordés par une prise BNC en T.

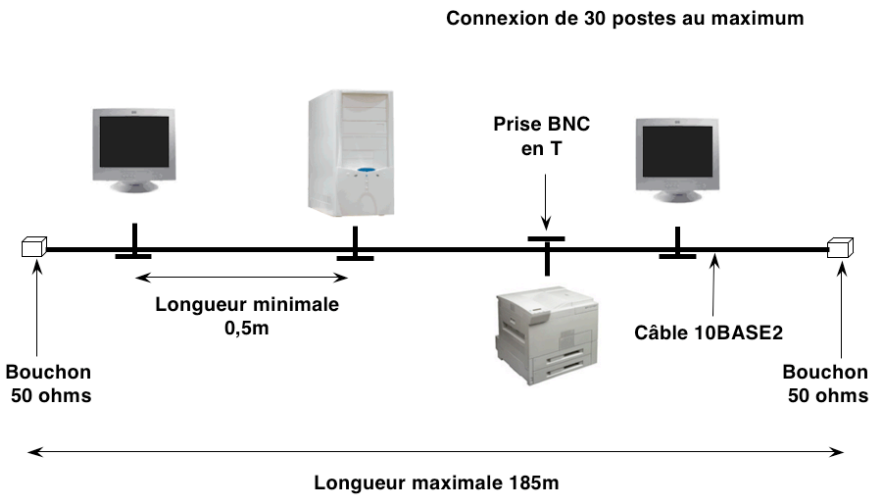


Figure 2.4,

Contraintes sur un segment 10BASE2.

Câble 10BASE5 ou Ethernet gros

Ce type de câble est aussi appelé Thick Ethernet. Sa structure est expliquée avec la Figure 2.5.

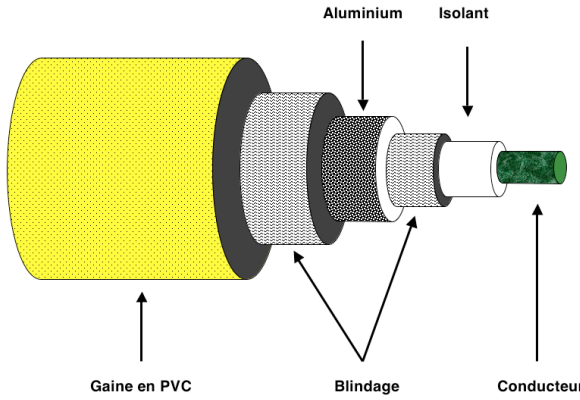


Figure 2.5,

Structure du câble Ethernet gros.

L'impédance du câble à ses extrémités est de 50 ohms. Il est donc nécessaire d'utiliser des bouchons d'impédance 50 Ohms comme terminateur de câble.

La vitesse de transmission sur un câble 10Base5 est de10 Mbit/s.

La longueur maximale d'un segment est de 500 mètres.

Attention

Vous ne pouvez pas utiliser des longueurs aléatoires de câbles.

En effet, la fréquence oblige à découper son câble selon certaines règles. Les longueurs doivent être des multiples de 23,4m. Si vous avez besoin de 100 mètres de câbles vous devez sectionner le câble le plus proche d'une longueur multiple de 23,4 mètres soit 117 mètres (5 x 23,4 m).

On peut mettre bout à bout cinq segments soit une couverture maximale de 5x500=2500 mètres.

Attention

La règle des 5,4,3 est aussi applicable au câble 10Base5..Sur un segment, 100 postes au maximum peuvent être connectés. L'espacement entre chaque poste doit être un multiple de 2,5 mètres (voir figure 2.7). Une marque noire sur le câble permet de se repérer. Le câble a pour diamètre dix millimètres. Ce câble pourra donc permettre au maximum la connnexion de 300 équipements (3 segments porteurs contenant chacun 100 postes).

La connexion sur le câble se fait au moyen d'un transceiver différent de celui utilisé avec le 10BASE2. En effet, la fixation se fait au moyen d'une prise vampire (voir figure 2.6 et figure 2.8). Une partie de cette prise se retrouve au contact avec le blindage pendant qu'une aiguille est enfoncée dans le câble pour être mise en contact avec le conducteur.

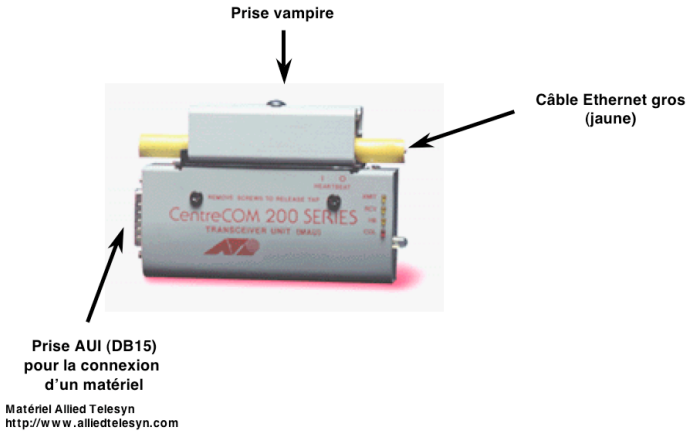


Figure 2.6,

Transceiver pour le raccordement d'un matériel sur un câble 10BASE5.

Le transceiver est connecté sur le câble mais, il faut encore y connecter un équipement. Cette manipulation ne peut se faire directement car le câble 10Base5 est très rigide, lourd et il y a un risque fort de détérioration de la connectique sur la carte réseau de l'équipement. Cette manipulation peut malgré tout se fait au moyen d'un câble Drop. La distance maximale de ce câble est de 50 mètres s'il est rond et quelques centimètres s'il est plat. Ce câble plus souple est connecté à la prise vampire (transceiver) pour être ensuite connecté à la carte réseau de l'équipement. La connectique utilisée est la prise DB15 (15 broches) aussi appelée prise AUI (Attachment Unit Interface). Le câble 10Base5 est très contraignant mais permet d'atteindre des distances raisonnables (2,5km) pour une utilisation dans un LAN. Pour cette raison, il est encore utilisé mais essentiellement pour réaliser des liaisons point à point qui permet de relier des ensembles de structures éloignés plutôt que des équipement dans un même ensemble.

Attention

Une prise AUI contient des alimentations électriques dans ses broches. Pour cette raison, vous ne pouvez utiliser un transceiver pour passer de la technologie AUI à une autre. Vous devrez alors connecter utiliser un répéteur.

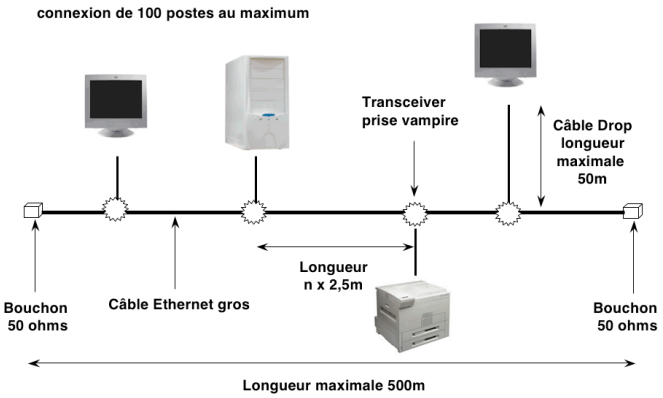


Figure 2.7,

Contraintes sur un segment 10BASE5.

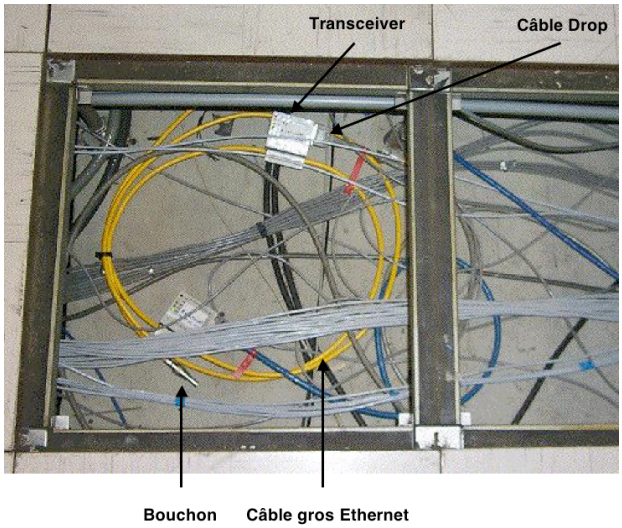


Figure 2.8,

Câble 10Base5 avec prise vampire dans un faux-plancher.

Tableau 2.1 Récapitulatif des contraintes sur les câbles coaxiaux

Câble	Max. segment	Nb. Postes max./Segment	Dist. Min. inter-poste	Connecteur	Segments Porteurs	Max. segment	Débit Max.
10Base2	185 m	30	0,5 m	BNC	3	5	10Mbits/s
10Base5	500 m	100	2,5 m	AUI/DB15	3	5	10Mbits/s

1.3 Les câbles torsadés

Il n'est pas toujours simple de s'y retrouver. En effet, il existe la norme de l'ISO/IEC 11801 dont découle la norme Européenne EN 50173 et les standards EIA/TIA 568-B1 et EIA/TIA 568-B2 qui propose les recommandations TSB36, TSB40 et TSB53. TSB signifie Technical System Bulletin.

- Le TSB36 porte sur le câble torsadé dont la puissance est de 100 Ohms en UTP (Cable Specifications for Unshielded Twisted Pair Cables)
- Le TSB40 porte sur le connecteur RJ45 à Contact AutoDénudant (CAD) (Transmission Specifications for Unshielded Twisted-Pair Connecting Hardware)
- Le TSB53 porte sur les câbles blindés 150 Ohms et connecteur hermaphrodite (Cable Specifications for Shielded Twisted Pair Cables)

Le sujet de l'ISO11801 est « Generic cabling for customer premises » tandis que le sujet de l'EIA/TIA 568 est « Commercial Building Telecommunications Cabling Standard ».

Il y a quelques petites différences que les tableaux 2.2 indiquent.

Il est à noter que l'EIA a produit un bulletin, le TSB67, qui spécifie les mesures obligatoires à effectuer pour la certification des installations en paire torsadées ainsi que les caractéristiques des appareils permettant ces mesures. Ces mesures sont aussi mentionnées dans la norme ISO11801. Une partie est reprise dans les tableaux 2.2.

Tableau 2.2 Comparatif entre les normes ISO-11801 et EIA/TIA-568-B

ISO/CEI 11801				
Classes	Largeur de Bande (MHz)	Altération (db)	NEXT (db)	ELFEXT (db)
D	100	24	30,1	17,4

E	250	35,9	33,1	15,3
F	600	54,6	51,2	31,3

EIA/TIA 568-B.1 et 568-B.2*				
Catégorie	Largeur de Bande (MHz)	Altération (db)	NEXT (db)	ELFEXT (db)
5	100	21,6	27,1	17,0
5e	100	24	30,1	17,4
6*	250	35,9	33,1	15,3
7	Pas de standard			

Tableau 2.3 Equivalence entre les normes ISO-11801 et EIA/TIA-568-B

ISO/CEI 11801	EIA/TIA 568
Classe D	Catégorie 5/5e
Classe E	Catégorie 6

Définition

Altération : c'est la dégradation du signal su une distance de 100m.

Définition

NEXT (Near End Cross-Talk) appelé aussi paradiaphonie. C'est une fuite d'énergie entre deux câbles, due à des interférence magnétiques (diaphonie) dans le cas d'un couplage de 2 émetteurs. Cette mesure s'effectue à l'extrémité où le signal est envoyé.

Définition

ELFext (Equal Level Far End CrossTalk). Cela représente les interférence qu'il peut y avoir entre deux pairs de câbles adjacentes. Cette mesure à lieu à l'extrémité opposée d'où le signal est envoyé.

D'autres mesures sont utilisées comme l'ACR (Attenuation to Cross-talk Ratio) qui permet de faire le rapport entre le signal et les interférences induites par la diaphonie que l'on peut aussi obtenir en effectuant la différence entre NEXT et l'Altération. Plus ce rapport est élevé meilleures sont les performances du câble.

On ne parle pas des classes A,B et C ou des catégories 1,2 ou 3 car elle correspondent à des technologies en câble torsadée dépassées.

Aujourd'hui, la catégorie réellement utilisée est la catégorie 6. La catégorie 7 n'est pas utilisée aux Etats Unis et peu en Europe. En 2002 elle représentait 1% du marché. A noter que les connecteurs ne sont pas les mêmes qu'en catégorie 6 car ils sont limités à 250Mhz.

L'impédance des câbles définis dans la norme ISO 11801 sont de 100, 120 ou 150 ohms tandis que dans les spécifications EIA/TIA elles sont de 100 et 150 ohms. Le câble 120 ohms possède un meilleur rapport qualité/prix que le 150 ohms et des performances accrues par rapport au 100 ohms.

Le tableau 2.4 propose une vue globale par classes des fréquences et des technologies mises en œuvre pour les câbles torsadés.

Classe	Fréquence	Utilisation
A	100 Khz	Téléphonie
B	1 MHz	Numéris

C	16 MHz	10 Base T
D	100 MHz	100/1000 Base T
E	250 MHz	1000 Base Tx
F	600 MHz	GigaBits

Tableau 2.4 Caractéristiques par classe de câbles

Actuellement, la majeure partie du câblage s'effectue en classe D ou E à savoir en catégorie 5 ou 5e.

Les paires torsadées sont constituées de 4 paires de fils en cuivre. Chacune de ces paires est torsadée selon un pas de torsade différent, diminuant ainsi les problèmes de diaphonie et paradiaphonie. Chacune possède un couple de couleur afin de les distinguer lors du câblage. Il y a les couples Vert/Vert-blanc, Orange/Orange-blanc, Bleu/Bleu-Blanc et Marron/Marron-blanc.

Il existe quatres types de câbles torsadés.

- UTP (Unshielded Twisted Pair) : paire torsadée non blindée (la plus courante)
- FTP (Foiled Twisted Pair) : paire torsadée possédant une feuille d'aluminium autour des paires (perturbations divisées par 10)
- STP (Shielded Twisted Pair) : paire torsadée possédant une tresse métallique autour des paires. Ce câble est plutôt utilisé dans des réseaux token ring (perturbations divisées par 100)
- SSTP (Shielded Shielded Twisted Pair) : paire torsadée possédant une feuille métallique autour de chaque paire de fils ainsi qu'une tresse autour des 4 paires.

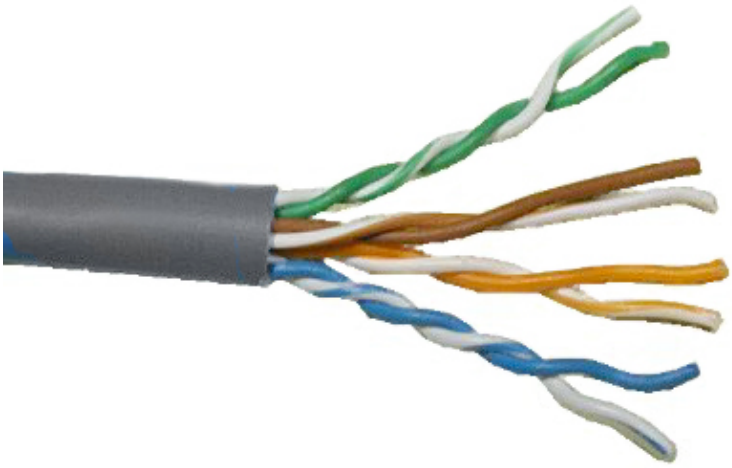


Figure 2.9,

Câble torsadé.

Les câbles blindés sont utilisés dans le cas où il y a des interférences électriques dans l'environnement du câblage. Le SSTP est préconisé dans le cas de liaison très haut débit pour éviter les interférences entre les paires.

La prise qui est associée à ce câble est une prise RJ45 qui signifie Registered Jack 45 où 45 correspond au brochage (voir figure 2.10).

Remarque

Pour qu'un câblage soit considéré comme blindé, il est nécessaire non seulement que le câble lui-même le soit (FTP ou STP) mais aussi le connecteur RJ45.

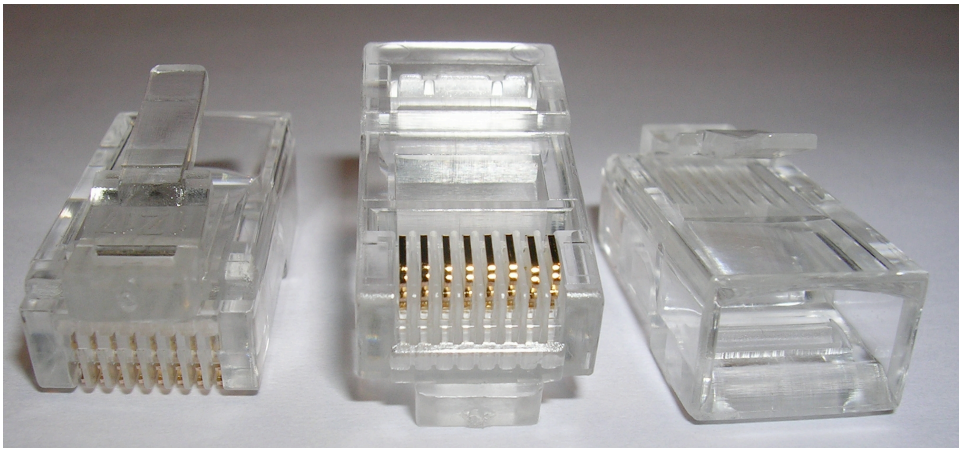


Figure 2.10,

Différentes vues d'une prise RJ45.

Cette prise propose 8 emplacements pour y glisser les 8 fils en cuivre. Lors de la création d'un câble, il est nécessaire de posséder une prise à sertir (figure 2.11) qui permet de mettre en contact les pinôches (pin en anglais) de la prise (partie métallique cuivrée) et la partie cuivre de chaque fils du câble par écrasement.

Figure 2.11,

Prise à sertir.

Au sein de la spécification 568, il existe deux standards, le 568A et le 568B qui concerne les câbles UTP et la façon dont doit être réalisée la terminaison (mise en place de la prise RJ45). La différence se situe dans l'utilisation et le positionnement des couleurs des paires dans la prise RJ45. La norme EIA/TIA-568B est utilisée pour une question de compatibilité avec des installations de câblage utilisant la norme AT&T 258A. Cette dernière devenant de moins en moins utilisée, la norme EIA/TIA-568A est donc privilégiée pour la mise en place des terminaisons.

Lorsque vous effectuez le câblage de la prise RJ45, il est important de positioner les couleurs selon un ordre défini par la norme utilisée (voir figure 2.13). Dans tous les cas, vous devez tenir la prise RJ45 avec l'ergot vers le bas et l'arrière de la prise vers vous. La pinôche 1 se situe alors à votre gauche et la pinôche 8 sur votre droit (voir figure 2.12).

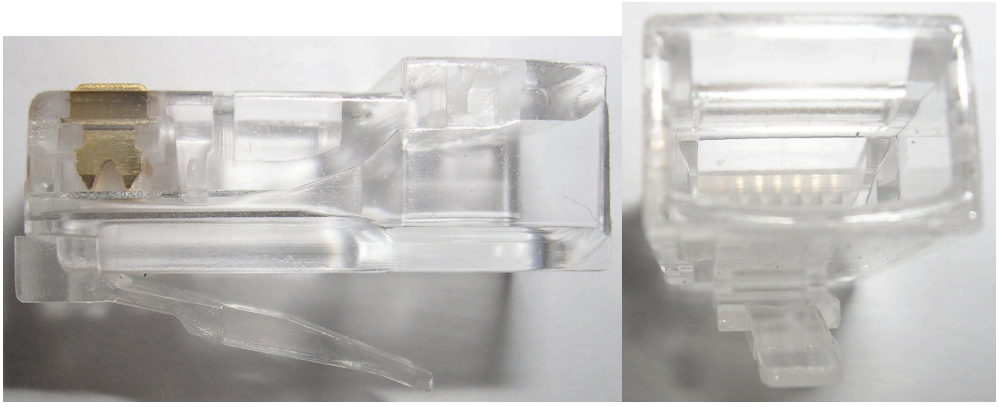


Figure 2.12,
Position de la prise RJ45 pour le câblage.

568 A	
Numéro de Pin	Couleurs
1- T3	Blanc/Vert
2 - R3	Vert
3 - T2	Blanc/Orange
4 - R1	Bleu
5 - T1	Blanc/Bleu
6 - R2	Orange
7 - T4	Blanc/Marron
8 - R4	Marron

568 B	
Numéro de Pin	Couleurs
1- T3	Blanc/Orange
2 - R3	Orange
3 - T2	Blanc/Vert
4 - R1	Bleu
5 - T1	Blanc/Bleu
6 - R2	Vert
7 - T4	Blanc/Marron
8 - R4	Marron

Tableau 2.5 Câblage de la terminaison RJ45 en 568A et 568B

Les limites des connexions baseT (10BaseT, 100BaseTx) sont de 100 mètres par segments.

La norme 802.3 définit les débits de 10 Mbits/s sur du 10BaseT, tandis que la norme 802.3u (1995 mise à jour en 1998) définit des débits de 100Mbits/s sur du 100BaseTx UTP catégorie 5 ou STP.

Ce câble est appelé Fast-Ethernet. Seules les paires [1-2] et [3-6] sont utilisées. Les fils 1 et 2 pour la transmission (TD+ et TD-) tandis que les fils 3 et 6 pour la réception (RD+ et RD-).

Remarque

TD signifie Transmit Data. Les fils sur une paire sont polarisés. L'un permet d'envoyer le signal positif tandis que l'autre le signal négatif.

Il n'est alors possible d'utiliser que 2 segments mis bout à bout et relayer par un répéteur ou un matériel qui possède cette fonction.

La topologie utilisée avec les câbles BaseT est la topologie étoile avec au centre de cette étoile un concentrateur (hub) ou un commutateur (switch).

Il existe aussi le câble 100BaseT4 qui utilise les 4 paires en UTP catégorie 3,4 ou 5. Une paire pour la transmission, une pour la réception et deux pour les transmissions bi-directionnelles.

Deux types de câbles sont utilisés en fonction des matériels à connecter.

- Le câble droit (tableau 2.5) pour lequel, les couleurs au niveau des deux prises RJ45 sont les mêmes pour chacune des pinôches des deux côtés du câble.
- Le câble croisé (tableau 2.6) pour lequel les couleurs sont « croisées ». Ceci est dans le cas où vous reliez deux matériels identiques (PC-PC, hub-hub …). La seule exception est le lien entre un PC et un routeur qui nécessite là aussi un câble croisé. N'oubliez pas que la pinôche 1 se situe à gauche et que l'ergot se situe en bas, l'arrière de la prise vers vous (voir figure 2.12).

A noter

Certains matériels, comme les commutateurs, proposent des ports MDI/MDI-X (Medium-Dependent Interface) qui permettent de définir automatiquement si il est nécessaire de croiser ou non le câble. Vous pouvez alors utiliser indistinctement un câble croisé ou un câble droit.

1ère prise RJ45	couleurs
1➢ RD+	Blanc/Vert
2➢ RD-	Vert
3➢ TD+	Blanc/Orange
4	Bleu
5	Blanc/Bleu
6➢ TD-	Orange
7	Blanc/Marron
8	Marron

2ème prise RJ45	couleurs
1➢ RD+	Blanc/Orange
2➢ RD-	Orange
3➢ TD+	Blanc/Vert
4	Blan/Marron
5	Marron
6➢ TD-	Vert
7	Bleu
8	Blanc/Bleu

TD = Transmit Data (paire 1-2 pour la réception)

RD = Received Data (paire 3-6 pour l'émission)

Tableau 2.6 Câble 100BaseTx croisé selon la norme 568A

Les câbles BaseT, du fait de l'utilisation de 2 paires, peuvent permettre de transmettre l'information en Full-Duplex. Ce qui signifie qu'une paire est dédiée à l'émission du signal et que dans le même temps l'autre paire est dédiée à sa réception. Ce système n'est possible que si les cartes réseaux de vos matériels le permettent. Les débits sont alors « doublés » 100Mbits/s dans un sens et 100Mbits/s dans l'autre simultanément soit 200Mbits/s. Dans ce contexte, un autre avantage est qu'il n'y a pas de collision les signaux ne pouvant se « rencontrer ».

Dans le cas où la transmission ne se fait que dans un sens à la fois, on parle de half-duplex.

A noter

Certains matériels, comme les commutateurs, proposent des ports auto-sensing qui permettent d'adapter automatiquement la vitesse de transmission au type de la carte et à sa configuration.

Au delà des débits de 100Mbits/s, il existe les débits 1000Mbits/s.

- 1000 Base-T définit par le standard IEEE802.3ab. Il ne peut y avoir qu'un seul segment de 100 mètres. La norme 1000BaseT du 802.3ab a été créée permettant de normaliser les hauts débits sur du câble torsadé de catégorie 5 UTP. Le comité est le 802.3ab qui la ratifiée en juin 1999 sous le nom 1000 Base T. Un réseau 1000 Base T peut atteindre 100 mètres au maximum (un seul segment possible). Les signaux passent par les quatre paires (deux paires pour le 100 Base Tx). Le taux d'erreur (Bit Error Rate) en 1000 Base T est de : 10 puissance -10 soit moins d'un bit erroné sur dix milliards transmis ce qui est identique au BER du Fast Ethernet (100 Base T). La transmission des données sur le 1000 Base T est bidirectionnelle contrairement au Base T qui est unidirectionnelle. La transmission et la réception se font sur la même paire. Ceci est possible grâce

à des dispositifs hybrides positionnés aux extrémités des câbles et qui évitent les mélanges des signaux en émission et en réception.

- Giga-Bit ethernet standardisé par l'IEEE en juin 1998 sous l'appellation 802.3z. Cette norme, décrit les fibres optiques (SX, LX) mais aussi le câble torsadé 1000BaseCX blindé d'impédance 150 ohms. Un segment a une longueur maximale de 25 mètres. Pour cette raison, ce type de câblage est essentiellement utilisé en rocade pour des liaisons entre matériels réseaux ou dans une baie de brassage.

A noter

Les ports Giga Bits sur les matériels tels les commutateurs de marque cisco sont appelés port GBIC (GigaBits Interface Converter).

1.4 Les supports optiques

Le matériel associé à ces câbles sont encore très chers comme les émetteurs/récepteur, les testeurs. De plus, le câblage est complexe à effectuer et il est nécessaire de posséder des outils particuliers assez coûteux. C'est pourquoi ils sont le plus souvent utilisés pour des liaisons point à point. Les fibres optiques sont aussi utilisés dans des connexions hauts débits vers des disques durs (Fiber Channel) avec des technologies de type SAN (Storage Area Network).

Les fibres optiques sont composées de trois éléments principaux.

- Le coeur en silice où passe les ondes.
- La gaine optique qui permet de conserver les ondes dans le coeur en jouant sur l'indice de réfraction.
- La protection.

Les fibres sont souvent appelées brins. Dans un même câble, les brins sont regroupés par multiples de 2, 6 ou 12.

Le principe est de faire pénétrer des rayons lumineux dans le cœur avec des indices de réfractions différents (voir figure 2.13). Ces rayons sont générés par trois type de sources possibles :

- LED (Light Emitting Diode) émet sur des longueurs d'ondes de 850nm (nano mètres) ou 1300nm sur des fibres multimodes.
- Laser utilisé avec des fibres monomodes ou multimodes très précis qui permet d'atteindre de hauts débits en émettant sur des longueurs d'ondes de 1310nm ou 1550nm.
- VCSEL (Vertical Cavity Surface Emitting Laser) qui émet sur une longueur d'onde de 850nm sur des fibres multimodes. Ce système est de plus moins coûteux que les autres systèmes d'émission.

La fibre optique est caractérisée par sa bande passante en Mégahertz ainsi que l'atténuation du signal en décibels par kilomètre. Un affaiblissement de 3db correspond à une perte d'environ 50% du signal. Cet affaiblissement dépend du type de fibre utilisé (diffusion et absorption des matériaux) (voir tableau 2.7).

Fibre (Diamètre du cœur)	Affaiblissement à 850nm par km	Affaiblissement à 1300nm par km
Multimode 62,5µ	3,5 db	1,5 db
Multimode 50µ	2,7 db	1 db

Tableau 2.7 Affaiblissement du signal en fonction de la fibre et de la longueur d'onde d'émission

note

Pourquoi mesurer l'atténuation d'une fibre optique en décibel alors que nous parlons de lumière et non de son ?

Le décibel (dixième de Bell) est une mesure apparue avec l'invention du téléphone par Alexander Graham Bell (1847-1922).

Les rapports entre deux éléments s'expriment en pourcentage, mais historiquement tout peut aussi s'exprimer en décibels, que ce soit des signaux électriques, optiques, thermiques, taille, poids.

Si dans une fibre optique, vous injectez, un Watt au moyen d'un laser et qu'en sortie vous en récupérez 0,5 Watt, le coefficient sera :

(Puissance en sortie)/ (Puissance en entrée): 0,5 / 1 = 0,5 soit 50/100 soit 50 % de perte. La fibre est de très mauvaise qualité.Le décibel permet d'obtenir une échelle logarithmique de ces coefficients et donc des courbes de rapport.

La « formule » de calcul du rapport en décibel est : -10 Log coefficient.

Le logarithme n'est pas népérien (base e) mais en base 10.

Dans notre cas de fibre optique nous obtiendrons :

-10 Log 0,5 = -10 x -0,3 = 3

La perte en décibel est : 3db.

Vous pouvez tout exprimer avec ce rapport de décibel.

Un rapport de taille entre deux individus, l'un A fait 1,88 mètre, l'autre B 1,58 mètre.

Le coefficient est de 0,84 (1,58 / 1,88) soit un rapport de 84%.

L'individu B est 0,76db (-10 Log 0,84) plus petit que l'individu A ....

Deux sortes de fibres existent (Voir figure 2.13) :

- Les fibres multimodes

  Ce type de fibre regroupe les fibres à saut d'indice et à gradient d'indice.

  Le cœur de ces fibres est grand par rapport à la longueur d'onde du signal optique émit. Cinquante à deux cents microns mètres pour le cœur et de l'ordre d'un micron pour le signal. Cette fibre permet donc de propager plusieurs centaines de signaux (phase différente).

  La bande passante peut varier de 200 à 1500 Mégahertz par kilomètre.

  Il existe deux fibres dont le mode de propagation est différent :

  Les fibres à saut d'indice. L'indice de réfraction change brusquement lorsque l'on passe du centre de la fibre à sa périphérie.

  Les fibres à gradient d'indice. L'indice de réfraction diminue selon une loi précise, du cœur vers la périphérie. Les ondes passant par le centre sont les moins rapides mais comme elles parcourent moins de chemin elles arrivent en même temps que celles qui sont en périphérie.

- Les fibres monomodes

  Le cœur est proche de la longueur d'onde du signal. Il ne peut donc y avoir qu'un seul mode de propagation suivant l'axe de la fibre. Il n'y a donc pas de dispersions des temps de propagation. La bande passante et presque infinie> 10Gigahertz par kilomètre.

  Cette fibre est de meilleure qualité que la fibre multimode.

A noter

Alcatel a réussi à transmettre des données à une vitesse de 10TBits/s (10.000 Gbits/s). De plus, Alcatel a réussi a transmettre des données sur une distance de 7300Kms à la vitesse de 3Tbits/s.

Les ondes sont créées par des diodes au laser ayant une grande puissance d'émission.

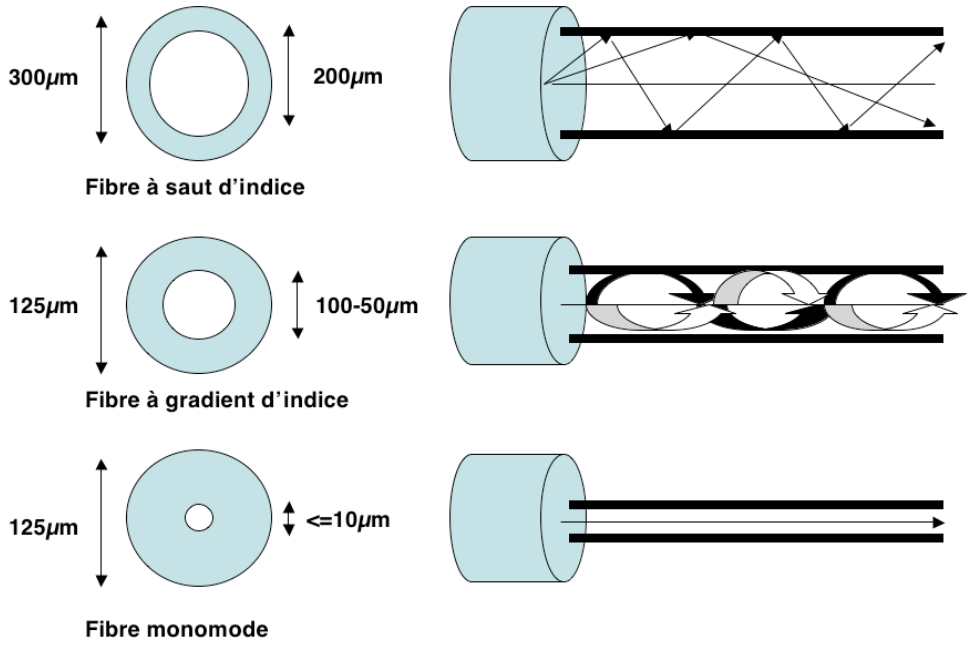


Figure 2.13,

Parcours du signal optique pour les différents modes.

Plus l'atténuation est faible, plus le signal pourra parcourir un chemin important.

La fibre monomode est celle qui permettra un cheminement maximal.

La propagation du signal dans une fibre optique est unidirectionnelle. Il faut donc deux brins, un pour l'émission et un pour la réception.

La longueur maximale d'un segment peut atteindre deux mille mètres avec une fibre multimode et vingt kilomètres avec une fibre monomode voir plus avec des fibres G652/G653/G655 ou G692 (2000km). Le taux d'erreur sur de la fibre optique (BER) est de 10^-12.

Le nombre de postes reliés dépend de la nature du matériel actif utilisé.

Les connexions se font au moyen de prises ST (rond), MIC, SC (carré) ou MT-RJ (proche de la connectique RJ45).

Il existe plusieurs types de câbles dont l'utilisation et les contraintes sont différentes.

Nous n'entrerons pas dans les détails mais il existe des fibres 10BASE-FL (Fiber Link), 10BASE-FB (Fiber Backbone), BASE-FP (Fiber Passive), BASE-VG (Voice Grade, méthode d'accès différente de CSMA/CD) pour le transport de la voix ou de la vidéo Mais les plus utilisées sont les 100BaseFX, 1000BaseSX, 1000BaseLX ainsi que les 1000BaseLH.

- Le 100BaseFX est normalisé, comme le 100BaseTX, sous l'appellation 802.3u appelée aussi Fast Ethernet. De ce fait, le 100BaseFX utilise le protocole CSMA/CD. La fibre est de type multimode possédant une longueur d'onde de 1330 nm. Un segment peut atteindre de 400 mètres à 2km.
- 1000BaseSX est normalisé en 802.3z. Le S signifie Short et désigne des fibres « courtes distances ». Les longueurs d'ondes sont de 850nm.
- 1000BaseLX est normalisé en 802.3z. Le L signifie Longue et désigne des fibres « longues distances ». Les longueurs d'ondes vont de 1310nm (multimode) à 1550 nm (monomode).
- 1000BaseLH (Long Haul) est une fibre longue portée (Long Haul) de type multimode (50 µm-550m) ou monomode (LHA<=70km ou LHB<=150km).

A Noter

Les appellations différent selon les constructeurs Cisco et Foundry. En effet, un 1000BaseLX chez Foundry se retrouve en 1000BaseLH chez Cisco. Un 1000BaseLH chez Foundry se retrouve en 1000BaseZX chez Cisco.

Il existe aussi une normalisation 802.3ae qui correspond aux débits de 10GBits/s qui a été ratifiée en Juin 2002. On y retrouve des câbles 10GBaseSR, 10GBaseSW, 10GBaseLR, 10GBaseLW, 10GBaseER, 10GBaseEW et 10GBaseLX4 (1310nm). Les câbles S correspondent à une longueur d'onde de 850nm sur de la multimode, les L à 1310nm et les E à 1550nm sur de la monomode. Les lettres déterminent le type de codage utilisé pour la transmission des données ainsi que les types d'utilisation des fibres. La lettre R désigne une utilisation sur fibre noire (fibre louée et connectée par le locataire) tandis que la lettre W désigne une utilisation du standard américain SONET (Synchronous Optical NETwork).

Le tableau 2.8 propose un récapitulatif.

	Longueur d'onde Nanomètre (nm)	Type de fibre diamètre en microns (µm)	Bande passante en Mégahertz par kilomètre	Distance maximale atteignable
1000BaseSX	850	62,5	160	220m
	850	62,5	200	275m
	850	50	400	500m
	850	50	500	550m
1000BaseLX	1310	62,5	500	550m
	1310	50	400	550m
	1310	50	500	550m
	1550	9/10	1000	5km (Cisco 10km)
1000BaseLHA/ZX	1550	9/10	-	70km
1000BaseLHA/ZX	1550	8	-	150km
10GBaseSR/SW	850	50	-	300m
10GBaseLX4	1310	50	-	300m
10GBaseLX4	1310	9/10	-	10km
10GBaseLR/LW	1310	9/10	-	10km
10GBaseER/EW	1550	9/10	-	40km

Tableau 2.8 Spécification des câbles optiques

Rappel

La fréquence et la longueur d'ondes sont liées. La fréquence définit le nombre de fois où le signal est à sa valeur maximale (ou minimale) sur une période d'une seconde. La longueur d'onde définit la distance entre deux valeurs identiques successives d'une même onde. L'unité est le nanomètre (10-9 mètre). Plus la longueur d'onde est petite, plus la fréquence est grande.

L'émission des signaux au sein des fibres a évolué depuis les années 1990. Utilisant précédemment le multiplexage temporelle TDM (Time Division Multiplexing) basée sur une émission de la lumière à intervalles de temps différents sur une même longueur d'onde (agrégation de signaux), les signaux sont alors émis avec la modulation WDM (Wavelength Division Multiplexing) qui corrrespond à un multiplexage de longueurs d'ondes (recommandation ITU-T G692 « Optical interfaces for multichannel systems with optical amplifiers ») (voir figure 2.14). De ce système découlent d'autres modulations possibles qui permettent des débits de plus en plus importants.

- WDM (Wavelength Division Multiplexing) : émission de plusieurs signaux à la même vitesse de modulation mais avec une longueur d'onde différente. Chaque longueur d'onde est séparée de 1,6nm (200GHz) ou 0,8nm (100GHz) dans la fenêtre de 1530 à 1565 nm.
- DWDM (Dense Wavelength Division Multiplexing) : on parle d'émission dense à partir du moment où l'espacement entre deux longueurs d'onde est égal à 100GHz (0,8nm), 50GHz (0,4nm

soit 80 canaux) ou 25Ghz (0,2nm soit 160 canaux). Les fréquences des ondes qui passent dans la fibre sont très proches. Ce système est essentiellement utilisé dans les transmissions longue distance (MAN). Le débit par longueur d'onde est de 10Gbits/s (0,8nm) à 40Gbits/s (0,2nm).

- U-DWDM (Ultra - Dense Wavelength Division Multiplexing) : on parle d'émission ultra dense du fait que l'espacement entre les longueurs d'onde est de 10GHz (0,08nm). Les débits par longueur d'onde étant là aussi de 10Gbits/s, le débit maximal qui peut être obtenu est de l'ordre de 4000Gbits/s soit 4TBits/s.
- CWDM (Coarse Wavelength Division Multiplexing) : ce multiplexage optique est moins onéreux que les solutions précédentes du fait de l'utilisation de lasers non régulés en température. Les émissions se font dans la fenêtre 1270-1610 avec des espacements de 20nm et des distances maximales de 40km à 80km. La recommandation qui s'y rapporte est ITU-T G695 créée en 2003. Le débit par longueur d'onde est de 1,25Gbits/s à 2,5Gbits/s pour 8 à 16 canaux.

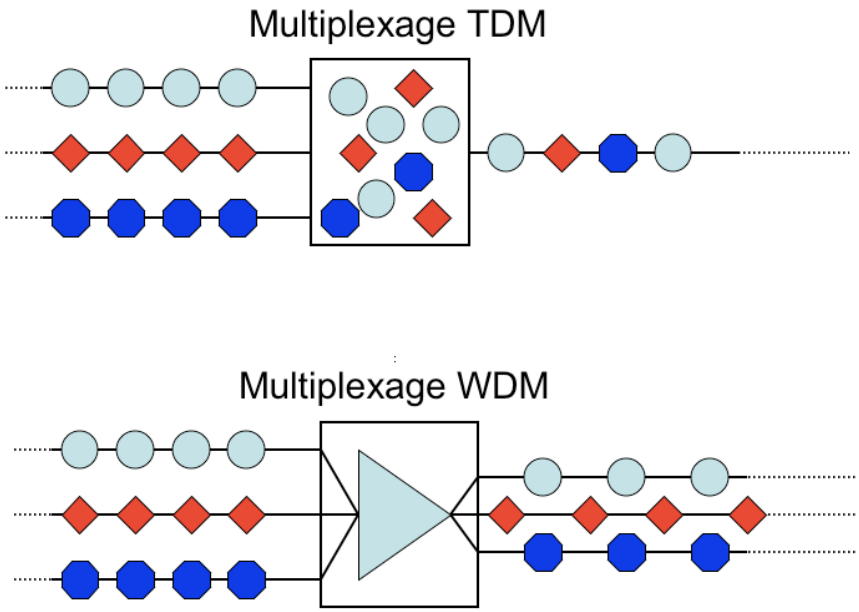


Figure 2.14,

Différence entre le multiplexage temporel (TDM) et le multiplexage de longueur d'onde (WDM).

Un câble optique apporte des avantages comme le débit accru sur ce support ou l'accroissement de la sécurité. Il est en effet très difficile « d'écouter » le trafic d'une fibre, le piratage est donc peu probable. Le raccordement à un câble cuivre au moyen de répéteurs ou d'autres matériels est simple. De plus, le câble est insensible aux perturbations magnétiques et il est très léger.

La liaison entre les segments se fait avec des amplificateurs de type EDFA (Erbium-Doped Fiber Amplifier).

A noter

En 2004, Alcatel a réussi à transmettre sur une distance de 100km des données sur 256 canaux ayant chacun un débits de 40Gbits/s soit un total de 10TBits/s en utilisant des amplificateurs Erbium/Raman.

Cette firme a aussi réussi à transmettre des données sur 7300km à 3TBits/s sur 300 canaux chacun à 10Gbits/s.

De plus, France Telecom associé à Deutsche Telekom et Alcatel a testé (expérimentation TOPRATE) sur une installation existante (430 km) en fibre monomode ITU-T G652 de délivrer par canal un débit de 170 Gbits/s sur 8 canaux. Pour se rendre compte de ce que cela représente, vous pouvez transférer 4 DVD en une seconde.

2. Le sans fil

Aujourd'hui il n'est plus question que de mobilité, de bureau de travail nomade …. C'est la grande mode, que ce soit dans les entreprises, les universités ou chez les particuliers, tout le monde doit avoir sa solution Wi-FI (Wireless Fidelity). Le sans-fil, englobe un certain nombre de normes. L'étendue de ses utilisations va du WWAN au WPAN. Les normes les plus connues sont le 802.11 et ses déclinaisons pour les WLAN et le Bluetooth pour le WPAN.

Mais, la technologie sans-fil n'est pas si récente que cela. En effet, le premier réseau sans-fil commercial date de 1982 aux USA. Plus près de nous, en 1986, France Telecom lance Radiocom. En 1992, les premiers réseaux GSM (Global System for Mobile communications) qui fait passer le sans-fil de l'analogique au numérique arrivent en France (GSM, UMTS (Universal Mobile Telecommunication System), GPRS (General Packet Radio Service) …). Aujourd'hui des solutions sans-fil sont testées dans des cafés, dans les gares SNCF ainsi dans les TGV, les hôtels ...

2.1 Normalisation du WLAN

Les normes pour le WLAN 802.11

Les normes 802 découlent du travail de l'IEEE. Aujourd'hui, la mode est au sans-fil dans les réseaux locaux ou chez les particuliers. Apple a lancé très rapidement son produit AirPort, solution Wi-Fi à la portée de tous, ses concurrents (Cisco, 3COM …) ne sont pas en reste et proposent aussi leurs solutions.

Rien de plus simple à priori que d'installer un point d'accès, quelques cartes PCMCIA et le tour est joué.

Nous verrons dans la partie sécurité que d'autres éléments peuvent entrer en jeu et faire déchanter les non-initiés.

La norme 802.11b

La première norme 802.11 est arrivée en 1997, avec au début un débit normalisé de 2Mbits/s loin des solutions filaires de l'époque. En 1998 arrive la norme 802.11b, la plus utilisée actuellement, qui autorise un débit théorique de 11Mbits/s (6Mits/s en débit pratique).

Certains constructeurs proposent un débit de 22Mbits/s (« double rate ») sur cette norme. Cela engendre une non compatibilité avec les autres matériels à 11Mbits/s.

C'est cette norme que l'on connaît sous le nom Wi-Fi, marque déposée par WECA (Wireless Ethernet Compatibility Alliance) avec le tiret qui devient ensuite Wi-Fi aliance.

C'est un regroupement des principales entreprises informatiques.
http://www.weca.net

La norme est soit disant « indépendante » des constructeurs mais elle doit être certifiée par le WECA pour pouvoir se développer ...

Elle propose un débit correct et une portée sans obstacle de 300m. De plus du fait de la libération des bandes hertziennes utilisées il n'est pas nécessaire de faire une déclaration auprès des autorités gouvernementales pour son utilisation dans des locaux fermés avec une puissance maximale de 100mW. L'émission se fait en séquence directe (longueur d'onde constante).

Le codage des ondes est réalisé grâce à la modulation DSSS (Direct Sequence Spread Spectrum). Le problème de ce codage est qu'il y a de nombreuses pertes de données dues notamment aux obstacles.

En effet, le terme Direct indique que seul un canal est utilisé pour l'émission des signaux. Si ces derniers rencontrent un obstacle, il n'y a pas de moyen de correction, il y aura une erreur. Ces pertes engendrent un grand nombre de messages de correction d'erreur chargeant d'autant la bande passante d'où le faible débit.

La méthode de détection des pertes est proche de ce que l'on trouve sur la norme 802.3 (topologie Bus). En effet, la détection se fait grâce à la méthode CSMA/CA (Carrier Sense Multiple Acces/Collision Avoidance) tandis que sur la topologie bus on parle de CSMA/CD (Carrier Sense Multiple Acces/Collision Detection). Le fonctionnement de ces deux technologies est donc très proche. Pour le sans-fil, le principe est de dire que le paquet est perdu à partir du moment où la réponse du récepteur

indiquant que ce paquet est bien arrivé n'est pas reçu par l'émetteur dans un laps de temps borné et définit.

Le débit dépend aussi de la méthode utilisée pour réaliser la modulation de fréquences (modulation de phase). La modulation DSSS peut être obtenue en utilisant 3 méthodes (rotation de phase pour chaque bit) :

Méthode	Débit Max. Mbits/s	Signification
DBPSK	1	Differential Binary Phase Shift Keying
DQPSK	2	Differential Quadrature Phase Shift Keying
CCK	5,5 et 11	Complementary Code Keying

Tableau 2.9 Les différentes méthodes utilisées dans la modulation DSSS

Remarque

La puissance d'émission dépend en fait de la puissance de l'antenne.

C'est pour cela que l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes), anciennement ART (Association de Régulation des Télécommunications) prend une autre mesure en compte qu'elle appelle PIRE (Puissance Isotrope Rayonnée Equivalente). Certaines antennes proposent une puissance de 30mW mais qui correspond en fait à une puissance de 100mW PIRE.

C'est cette puissance PIRE qui est prise en compte..

La norme 802.11b fonctionne dans la bande des 2,4GHZ à 11Mbits/s sur une distance maximale de 300 mètres. Toutes ces mesures sont théoriques. La pratique renvoie des performances bien moindres.

Cette bande est divisée en 14 canaux chacun séparé de 5MHZ comme le montre le tableau 2.10. Les cartes sans fil scrutent ces bandes afin de déterminer s'il existe des points d'accès et en cas de multiples points d'accès elles se calent sur celle qui propose le signal le plus fort.

Canal	1	2	3	4	5	6	7
Fréquence GHZ	2,412	2,417	2,422	2,427	2,432	2,437	2,442

Canal	8	9	10	11	12	13	14
Fréquence GHZ	2,447	2,452	2,457	2,462	2,467	2,472	2,477

Tableau 2.10 Fréquences des canaux utilisés dans la norme 802.11b

Les puissances PIRE autorisées sont les suivantes (sur la bande des 2,4GHZ).

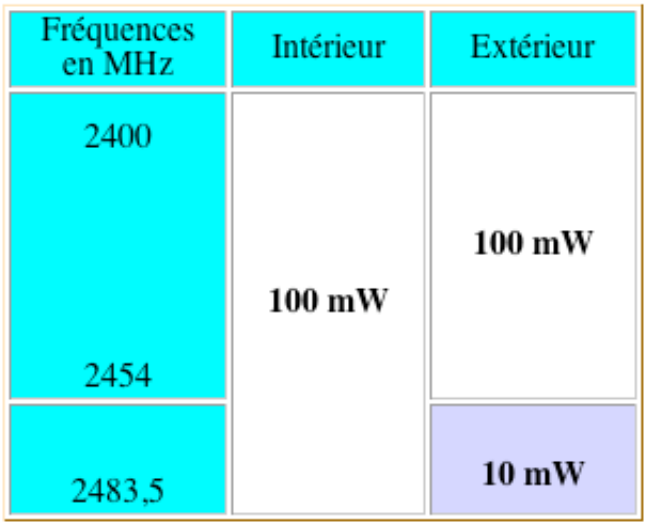


Figure 2.15,

Les puissances PIRE autorisées dans la bande des 2,4Ghz

Les conditions d'utilisation en France des installations radioélectriques sont régies par l'arrêté du 23 Décembre 2002 faisant suite à la décision n° 02-1008 (http://www.arcep.fr/textes/avis/index-02-1008.htm).

Voir aussi l'additif de Juillet 2003 (http://www.arcep.fr/communiques/communiques/2003/index-c220703.htm).

Lors d'une installation sans fil, la valeur des bandes passantes et le réglage des points d'accès sont très importants. En effet, avec une bande passante de 11Mbits/s et suivant le théorème de Shannon, le spectre d'émission peut atteindre 22MHZ. Ceci implique que si vous possédez deux bornes dont les émissions peuvent se situer dans les mêmes zones géographiques, vous aurez des interférences ce que l'on appelle overlapping. Il faut donc régler les canaux de telle sorte que ceux qui se trouvent proches soient séparés au minimum de 22MHZ.

Pour trois bornes, vous pouvez ainsi utiliser les canaux 1, 6 et 11.

Il faut aussi prendre en compte dans ce cas, le roaming qui correspond au temps de latence pour que votre communication s'effectue lors d'un passage d'une borne à une autre. Plus ce temps de latence est grand moins la qualité de votre réseau sera bon.

Vous pouvez utiliser deux modes d'accès :

- Le mode Had'Hoc. Chaque carte peut se connecter à toutes les autres cartes
- Le mode infrastructure (le plus utilisé). On installe une borne (point d'accès) et les cartes s'y connectent.

Remarque

L'inconvénient majeur de cette norme est sa faible sécurisation. De plus, si vous mettez le peu de sécurité possible via le module d'encryptage WEP (Wireless Encryption Privacy), le débit théorique de 11Mbits/s tombe à … moins de 2Mbits/s (c'est du non commuté).

La norme 802.11g

Cette norme a suplanté la norme 802.11b. Elle a été adoptée en Juin 2003 par l'IEEE. On la retrouve aussi sous l'appellation Wireless-G.

Cette norme permet d'atteindre des débits théoriques de l'ordre de 54Mbits/s. Ceci grâce à l'utilisation du codage OFDM (Orthogonal Frequency Division Multiplexing) plus performant que celui de la norme 802.11b. L'émission des données se fait sur plusieurs fréquences à la fois. Il suffit alors que le signal

d'une des fréquences atteigne le récepteur pour que la communication soit valide. L'une des limites du 802.11b est donc « supprimée ».

L'avantage de cette norme hormis son débit est le fait qu'elle utilise les mêmes fréquences que la norme 802.11b (bande des 2,4Ghz). De ce fait la majorité des cartes construites aujourd'hui, propose une compatibilité avec la norme 802.11b. Mais attention la compatibilité sur des cartes Wi-Fi (802.11b) a 11Mbits/s ne permet bien évidemment pas un débit de 54Mbits/s.

Remarque

Il ne faut pas attendre de miracle de cette norme même si sur le papier elle paraît mieux, elle conserve malgré tout les défauts de la 802.11b, à savoir, une transmission des informations de manière « non commutée » ce qui pose à nouveau des problèmes de sécurité et de partage de bande passante.

Tout comme le 802.11b, le débit chute dès que vous mettez en œuvre les sécurités. Les débits sont alors plus près des 20Mbits/s ce qui malgré tout est de toutes les façons mieux que la norme 802.11b.

Résultat, tous les constructeurs s'engouffrent dans ce nouveau marché prometteur, tel Apple avec sa borne AirPort Extreme (ventes multipliées par 2 par rapport à la borne 802.11b pourtant déjà un succès) ou 3Com avec sa gamme complète Wireless Lan. Cisco a passé la vitesse supérieure en signant un partenariat avec Intersil (leader dans les semi-conducteurs) dès 2002 ainsi qu'en rachetant en 2003 l'entreprise Linksys (Performante sur le marché des PME/PMI et des particuliers) pour 500Millions de Dollars. L'offre de Cisco orientée entreprise avec les solutions AirConnect s'étoffe donc avec l'arrivée dans son périmètre de Linksys.

Cet engouement rend les produits 802.11g attractifs au niveau du coût puisque entre du 802.11b ou du 802.11g (compatible 802.11b rappelons le) il n'y a que très peu d 'écart.

Mais, attention, tout n'est pas rose dans le monde du 802.11g. En effet, du fait de la modulation utilisée (multifréquence OFDM), seules 3 bandes de fréquence ne se chevauchent pas. Il n'est donc pas possible d'installer plus de 3 réseaux sans-fil dans une zone commune de couverture sous peine de génération de grosses interférences.

Autre bémol, le débit au-delà d'une certaine distance décroît très brutalement à la différence du 802.11b qui a une baisse progressive de son débit. Ceci aboutit à des performances plus modestes que ce qui est annoncé et relativise la puissance du 802.11g (Voir tableau 2.11).

En théorie

Débit Max.	Indoor	Outdoor
54 Mbits/s	27 m	76 m
48 Mbits/s	29 m	--
36 Mbits/s	30 m	--
24 Mbits/s	42 m	--
18 Mbits/s	54 m	183 m
12 Mbits/s	64 m	--
9 Mbits/s	76 m	--
6 Mbits/s	91 m	396 m

En pratique

Distance entre l'AP et le Client	Débit effectif constaté (indoor)
0 à 20 mètres	35 Mbits/s
20 à 50 mètres	11 Mbits/s
50 à 200 mètres	5 Mbits/s et 0 Mbits/s

Tableau 2.11 différence entre les données théoriques et pratiques d'une borne en 802.11g

Tout comme pour le 802.11b, la méthode utilisée pour moduler la fréquence (OFDM) diffère pour obtenir les différents débits comme le montre le tableau 2.12:

Méthode	Débit Max.	Signification
BPSK	6 à 9 Mbit/s	Binary Phase Shift Keying
QPSK	12 à 18 Mbits/s	Quaternary Phase Shift Keying
16-QAM	26 à 36 Mbits/s	quadrature amplitude modulation (16 états 4 bits donc 2^4)
64-QAM	48 à 54 Mbits/s	quadrature amplitude modulation (64 états 6 bits donc 2^6)

Tableau 2.12 Les différentes méthodes utilisées dans la modulation OFDM

Attention

Il ne faut pas oublier que ce débit est partagé par tous les postes connectés et utilisant la borne ce qui relativise encore plus ces débits. Plus il y a de connectés moins le débit effectif est grand par utilisateur.

Remarque

Certains constructeurs proposaient dès Mai 2003, alors que la norme 802.11g n'était pas encore officialisée, des équipements compatibles 802.11b et 802.11g à 100Mbits/s tel « Wireless Turbo » de US Robotics. Ce dernier indique malgré tout qu'en mettant les « sécurités » au maximum (WEP 256 bits) le débit passe à … 20Mbits/s.

Attention

Autre point à ne pas négliger, le nombre de connexions maximales sans-fil autorisé sur une borne. En effet, ce nombre n'est pas infini. La limite haute sur un AP est de l'ordre de 250 mais est souvent plus proche de 128 utilisateurs simultanés. Les ponts (lien entre le réseau filaire et le sans-fil) ou les routeurs proposent un certain nombre de connexion sans-fil et un certain nombre de connexion filaire sur ces matériels. Ce qui est mis en avant est souvent le nombre total et rarement le détail qu'il faut chercher dans la documentation du produit. Exemple :

« Haut débit à 54 Mbps, plus partage sécurisé de l'accès Internet pour 128 utilisateurs sans fil (jusqu'à 253 max.) dans un rayon de 100 mètres ; compatibilité ascendante avec les produits 11b »

Il est bien indiqué 128 sans-fil mais à la première lecture on peut supposer que les *253 max.* sont aussi sans-fil. Il n'en est rien. La phrase est tournée différemment dans la documentation détaillée (« *conçu pour 253 utilisateurs maximum (dont 128 sans fil) »,*) plus clair non ?

Attention

Quelle que soit la norme 802.11, le simple fait d'activer une carte sans-fil sur un portable, diminue énormément l'autonomie de ce dernier (De 30 à 40%). Pensez donc à désactiver la carte si celle-ci n'est pas utilisée.

2.2 Normalisation du WPAN

Les normes du WPAN Bluetooth et 802.15.1

Le sans fils « personnel » explose avec l'arrivée notamment des PDA (Personal Digital Assistant) et les liaisons sans-fil proposées avec l'ordinateur (souris, clavier, téléphone …). On parle alors de WPAN (Wireless Personal Area Network). Il existe de nos jours une seule grande « norme » : Bluetooth.

Les autres normes comme Homerf ont été balayées par le poids des sociétés intégrés dans le groupe de travail Bluetooth.

Le nom Bluetooth n'est pas un acronyme, mais une « plaisanterie » ou plutôt un clin d'œil à l'histoire scandinave. En effet un certain Harald Blaatand (910-986) surnommée Bluetooth (Harald la dent bleue) à unifié le Danemark et la Norvège.

Le constructeur Ericson en 1994 travaille à l'unification des technologies sans-fil, il choisit alors ce nom. Ericson est rejoint par d'autres grands constructeurs tels IBM, Intel, Nokia au début de « sa croisade » au sein d'un groupe Bluetooth SIG (Bluetooth Special Interest Group).

Aujourd'hui plus de 2400 constructeurs ont rejoint ce groupe dont 3Com, Apple et Microsoft.

Les matériels basés sur cette norme sont aujourd'hui très nombreux voir incontournables, Ericson estimait en 2002 que 100 millions de matériels utilisaient des puces de cette norme.

La première norme, Bluetooth 1.0A date de 1999. Une révision en norme Bluetooth 1.1 a eu lieu en 2001 sans pour le moment améliorer le débit. Les futures normes sont prévues pour proposer un débit de 2 à 10 Mbits/s théoriques sur 100 mètres maximums. La norme 802.15.1 de l'IEEE date elle de Juin 2002 et est compatible avec la spécification Bluetooth V1.1.

Actuellement, d'un point de vue technique, Bluetooth propose de faibles débits (1Mbits/s théorique), un rayon d'action de 10 à 30 mètres, une consommation d'énergie faible permettant ainsi d'obtenir des matériels très petits.

Il utilise la bande de fréquence des 2,4 Ghz (2,400 Ghz à 2,4835 Ghz).

Il permet de gérer, au maximum 8 matériels Bluetooth sur une même connexion. Il utilise la norme DECT (Digital European Cordless Telecommunications) hérité des téléphones sans-fil (dont Ericson est l'un des leaders). La norme DECT permet de faire transiter la voix en mode numérique d'un téléphone sans-fil vers sa base.

Le site de référence est http://www.bluetooth.com/.

L'émetteur et le récepteur peuvent changer de canal d'émission et de réception sans perte de connexion de manière automatique pour éviter les engorgements de la bande passante (1600 fois par secondes).

C'est le maître qui décide de ce saut. Il y a donc un ensemble de processus de contrôle de connexion assez important qui prenne une partie non négligeable de la bande passante d'où des débits plutôt orientés vers les 800kbit/s.

Les matériels sont organisés en tous petits réseaux appelés des ***piconets***. Chaque piconet possède un maître et au maximum 7 esclaves. Plusieurs piconets peuvent communiquer entre eux cela forme alors un ***scatternet***. Un matériel esclave dans un piconet peut devenir maître d'un autre piconet adjacent. Au maximum un scatternet peut être constitué de 10 piconets ceci représente donc 72 matériels.

Bluetooth est une norme qui propose une sécurité intéressante à la différence de la norme 802.11b. Elle est héritée de celle des téléphones sans-fil. En effet, les matériels Bluetooth comme les téléphones portables possèdent une adresse physique unique, un code d'authentification à 4 chiffres et un dispositif de cryptage sur une clé aléatoire à 128 bits. Ces éléments en mode sécurisé entrent en compte lors des communications.

La faiblesse qui devrait être bientôt supprimée vient de ce code à 4 chiffres trop faible et du au fait que les matériels Bluetooth sont dépourvus de prise secteur. Ils fonctionnent sur batterie. Une des attaque est le DOS (Deny Of Service) avec une sollicitation importante du matériel maître qui « s'essoufle » et donc ne répond plus.

HomeRF

HomeRF qui signifie Home Radio Frequency est basée sur la norme 802.11b et DECT (Digital European Cordless Telecommunications). Nous avons évoqué précédemment la norme 802.11b, nul besoin d'y revenir. L'alliance des deux est la norme HomeRF.

Le groupe de travail se nomme Home Radio Frequency Working Group. Il est composé initialement par IBM, HP, Intel, Compaq et Microsoft.

La première norme sort en 1998. Elle propose théorique de 10Mbits/s sur une distance de 50 à 100 métres. Le débit pratique est plus proche des 3 à 4 Mbits/s.

La bande passante utilisée par la norme HomeRF 1.2 est 2,4Ghz.

La topologie utilisée est soit une topologie Client/ Serveur (Partage de ressource) ou point à point pour des échanges entre deux postes (ce que ne propose pas la norme 802.11b en mode de base : mode infrastructure).

2.3 La sécurité du sans fil

Le Wi-Fi est un vrai défis et une vraie révolution. Le développement de ces outils à été plus rapide que l'apparition des normes, il en découle de sérieux problèmes de base. Nul jour sans un article de presse sur la faiblesse de la sécurité du Wi-Fi. La sécurité autour de Bluetooth est moins problématique du fait de sa faible portée et des mécanismes hérités des téléphones portables.

Nous allons donc nous focaliser sur la sécurité autour du Wi-Fi (norme 802.11b et 802.11g).

Principes de base

Rappelons le principe de base du 802.11 qui est celui de permettre à tous les matériels désirant se connecter à une borne (Point d'Accès) de scanner tous les canaux disponibles pour ensuite tomber sur l'AP désiré. Avec ce système, il est donc impossible de « masquer » l'existence d'un AP. il suffit de se promener avec son portable ou son PDA pour découvrir le plus simplement du monde l'existence dans un lieu d'un AP même en cachant le SSID (Service Set IDentifier).

Les ondes ne sont pas « directionnelles », elles vont partout où leur puissance le permet. Il est donc « facile » de capter le signal d'un AP même si vous n'êtes pas invités. Il suffit que ce matériel possède un sniffer pour capter les paquets de données.

Pour utiliser un AP, il faut s'y associer. Pour cela il faut trouver le canal utilisé et connaître le numéro d'identification de cet AP (SSID).

Récupération des informations importantes

Le premier point est automatiquement fait par la carte sans-fil, l'AP émettant régulièrement des trames (Beacon Frames) pour s'annoncer.

Pour le second point, il faut savoir que le SSID est contenu dans les trames émises et ce en clair. Il suffit de sniffer ces trames pour obtenir le SSID de l'AP à laquelle on veut se connecter. Ceci peut même être fait avec un simple PDA ou des outils comme airtraf, WiFiScanner sous linux, APScanner sous Mac, linkferret (sniffer basique) sous windows par exemple (Voir le site de hacker http://www.wlanhacker.de/dietools.html) ou ethereal-XTRA (http://www.ethereal.com sur toutes plateformes).

Un outils commercial mais utilisable en test est assez intéressant EtherDetect (http://www.effectech.com).

Attention

Si vous récupérez des logiciels sur des sites de hacker ou des sites de faible confiance, ces logiciels peuvent être des piéges et peuvent aider à vous faire pirater donc MEFIANCE !

Le rapport basique suivant est fourni par le logiciel Wireless Scanner, mais c'est le point de départ aux attaques. Ce type de logiciel permet de déterminer le niveau de vulnérabilité de l'AP. 0 représentant une borne « sûre » (cryptage …).

MAC Address	SSID	Signal	Channel	Vulns	Probable Vendor
00:02:2D:77:77:77	Hacme	45	6	2	Lucent ORiNOCO
00:04:5A:CC:BB:AA	linksys	54	6	4	Linksys
00:05:5D:78:9A:BC	GoISS!	105	6	0	D-Link
00:06:1D:88:88:88	Andy	42	10	3	Lucent ORiNOCO
00:07:0E:66:77:88	Leslie	54	4	2	Cisco Aironet
00:20:D8:AA:AA:AA	Internetx	50	9	2	Baystack
00:30:AB:55:55:55	secure1	72	6	2	Netgear
00:40:96:EE:EE:EE	400	36	3	2	Cisco Aironet
00:80:C6:99:99:99		60	2	0	SOHOware NetBlaster II
00:90:D1:BB:BB:BB		60	11	1	SMC
00:A0:0F:33:33:33		36	8	1	Symbol
00:A0:F8:66:66:66	Bob_in_Marketi	42	3	3	Symbol

Figure 2.16,

Exemple du résultat du scan avec Wireless Scanner

Il est nécessaire de s'associer à l'AP ce qui peut impliquer d'être vite découvert.

Il est malgré tout possible de sniffer le réseau sans-fil sans s'associer à l'AP. Pour cela il faut utiliser le mode monitor ou debug ou RFMON (appellation CISCO). Dans ce cas, la carte remonte toutes les trames 802.11 brutes.

Attention

Pour pouvoir utiliser un sniffer et récupérer les trames (niveau 2) vous devez basculer votre carte réseau en mode promiscuous afin de permettre a ces informations de remonter aux couches supérieures. Sans ce basculement, votre sniffer ne récupérera pas grand chose d'intéressant. Certaines cartes, notamment celles en 802.11g bloquent cette possibilité.

- Le WarDriving ou Trébucher sans Fil

Il existe actuellement un certain nombre d'outils logiciels et humains pour trouver les points d'accès. Un site très intéressant permet de montrer et de cartographier les points d'accès. Même si c'est aux USA, il est possible de faire de même en France et c'est édifiant (http://www.worldwidewardrive.org/ ou http://www.wardriving.com/). Selon leurs statistiques 88000 AP ont été trouvées et 67% n'ont pas activé le cryptage WEP, 27% possède le SSID par défaut et 24% cumule (SSID par défaut sans activer le WEP).

Cette cartographie est généralement réalisée avec des outils tels NetStumbler (pour l'écoute GPS) et StumbVerter (pour la cartographie) sous windows, kismet sous linux (http://www.kismetwireless.net/) ou macstumbler sous macintosh (http://homepage.mac.com/macstumbler/).

Il fleurit en ce moment des associations dont le but est intéressant mais très dangereux. Elles mettent en place des réseaux associatifs d'utilisateurs qui ouvrent leur AP pour permettre une utilisation « libre » des réseaux sans-fil.

Attention à ne pas faire n'importe quoi et mettre une politique de sécurité en place sinon cela risque de poser de gros problèmes en cas de piratage via une des structures à disposition.

La ville de Nantes fait partie des pionnières (http://www.nantes-wireless.org/) et met en place ces sécurités comme me l'a signalé l'un des initiateurs du projet.

« Notre but n'est pas de créer un réseau communautaire sans sécurité, mais de construire (un) des réseaux communautaires de la taille d'un quartier, d'une rue et tout ça avec un minimum de sécurité (openVPN sécurité, FreeRadius ..). »

Ces points d'accès libres sont appelés Hotspots (en rapport avec le surf sur les grandes vagues).

Il existe là aussi des sites qui référencent ces zones « libres » (http://www.journaldunet.com/dossiers/wifi/annuairewifi.shtml).

Vous trouverez un exemple de carte intéractive de Paris, fournissant les informations nécessaires pour se connecter aux bornes détectées en cliquant simplement sur les numéros indiquées sur la carte (http://www.paris-sansfil.fr/).

- WarChalking ou CraieFiti

Il existe aussi d'autres méthodes pour détecter les AP et leurs états : regarder les trottoirs. En effet une nouvelle mode est lancée, qui existait déjà au niveau artistique mais qui est mise au service (ou le contraire) du WiFi : le warchalkink en Français le craiefiti. Des dessins à la craie sont mis aux endroits où des AP ont été découvertes avec en prime l'état voir des renseignements plus complets sur cet AP. Les codes sont proposés dans l'image ci-dessous.

Il y a trois états définis ouvert, fermé et Wep actif.

Quelques photos (http://craiefiti.free.fr):

Attention

Si vous utilisez une borne dont vous n'avez pas la gestion qui dit que celui qui la gère n'épie pas vos communications (mél, banque, navigation …). Il suffit de posséder un sniffer ou simplement de loguer ce qui passe par la borne et le tour est joué. Regardez un peu les forums de discussions sur le sans fil « j'utilise la connexion sans fil de mon voisin, c'est super ». Il ne faut pas voir le mal partout mais certaines bornes peuvent être ouvertes volontairement, pensez-y.

Le cryptage WEP

Afin « d'augmenter » la sécurité, l'idée du cryptage des communications paraît une bonne solution. WEP (Wired Equivalent Privacy) propose cette solution. Ce système permet d'intégrer une clé de cryptage basée sur l'algorithme RC4 jusqu'à 128 bits, sur l'AP et sur les clients. Cette clé a le défaut d'être le plus souvent statique et donc en cas de changement, la modification doit se faire sur tous les matériels utilisant le réseau sans-fil.

Le principal problème du WEP est qu'il est basé sur un algorithme de chiffrage le RSA (inventé en 1977 par Rivest-Shamir-Adleman).

Cet algorithme est public depuis 1994 et des mathématiciens (Fluhrer, Mantin et Shamir) ont montré qu'il y avait des failles dans cet algorithme.

En effet, sur une clé de 64 bits (ou 128 bits), 24 servent pour l'initialisation et les 40 (ou 104) autres servent pour le chiffrement. De plus la partie qui sert au chiffrement est statique et peut être « facilement » découverte si le vecteur d'initialisation n'est pas correctement généré (mode pseudo aléatoire, compteurs …) ou simplement en récupérant les en-têtes des paquets IP.

Attention

Pour crypter les données, et afin d'éviter que le cryptage se fasse sur une même base (la clé Wep), le protocole ajoute un élément aléatoire pour le codage. Le vecteur d'initialisation (Initialization Vector ou IV) comme le monre la figure 2.18. Problème, le client ne possède pas ce vecteur, il faut donc lui envoyer. Ceci se fait, en clair, dans le paquet de données transmis. Ce vecteur change à chaque envoi.

Hélas, le vecteur d'initialisation du protocole WEP est un champ de 24 bits (sur les clés de 64 bits et 128 Bits). Une si petite taille entraîne la réutilisation du même vecteur au bout d'un certain temps. Un point d'accès surchargé, qui envoie constamment des paquets de 1500 octets à 54Mbps par exemple, épuisera l'espace d'initialisation (IV) après (1500*8/(54*10^6))*2^24 = 3728 secondes, ou 1 heure.

Il est alors possible d'effectuer des comparaisons entre les paquets codés pour en déduire la clé.

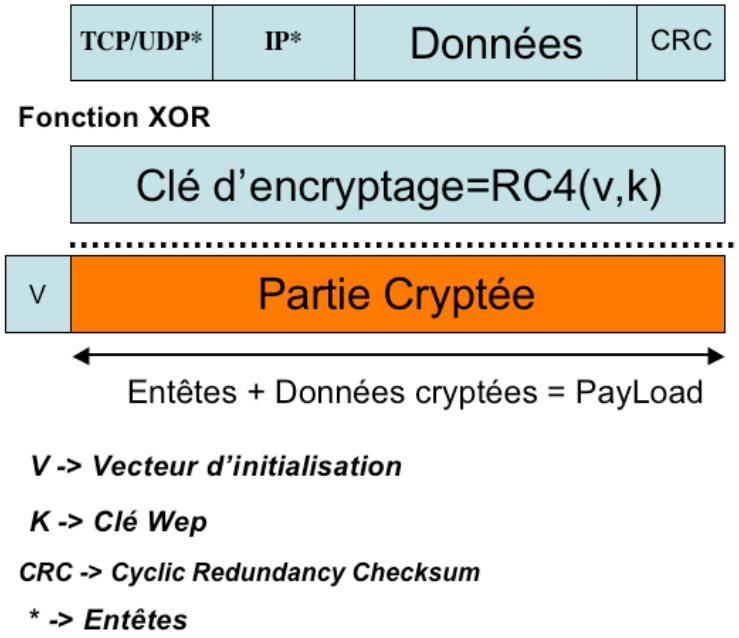


Figure 2.17,

Fonctionnement du cryptage Wep.

Malgré le chiffrage, il existe donc des trous de sécurité. Certaines trames passent en clair lors d'échanges, il est donc possible à partir de ces trames et d'un outils tel airsnort (http://airsnort.shmoo.com/) et wepcrack (http://wepcrack.sourceforge.net/), de déduire la clé Wep.

Attention

Le chiffrage se fait pour les communications sans fil donc entre les clients et la borne, mais pas entre la borne et la connexion filaire au réseau d'entreprise. Cette partie peut être un point faible dans votre architecture.

Pire, lors de la phase d'authentification entre le client et l'AP, ce dernier envoie un texte en clair au client qui crypte cette chaîne avec sa clé et renvoie ce cryptage. Si le cryptage est conforme, l'AP accepte la communication et l'association du client. Connaissant le texte en clair et son cryptage, il est alors possible d'en déduire la clé.

Il est aussi possible de récupérer la communication après l'AP au niveau de la partie filaire. A ce niveau, les communications ne sont plus cryptées.

Il est tout de même à noter que ces méthodes ne sont pas à la portée de n'importe qui. Malgré tout, beaucoup d'utilisateurs de solution sans-fil ne mettent pas en place le cryptage rendant le travail du pirate plus simple.

Pour apporter un peu plus de sécurité à votre réseau sans-fil :

- Mettre le réseau sans-fil dans une DMZ (DeMilitary Zone)
- Affecter une adresse IP fixe à l'AP mais aussi aux autres matériels
- Mettre l'AP à un endroit impossible à atteindre physiquement
- Modifiez le SSID par défaut
- Désactivez la diffusion du SSID (SSID Broadcasts)
- Modifiez le mot de passe par défaut du compte administrateur
- Activez le filtrage des adresses MAC (MAC Address Filtering)
- Modifiez régulièrement le SSID

- Activez le cryptage WEP 128 bits
- Modifiez les clés de cryptage WEP régulièrement.

Bien évidemment tout ceci n'est pas des plus simples car certaines informations doivent, dans le même temps, être modifiées sur les clients (SSID, Clé WEP) ce qui rend ces recommandations difficiles à suivre, mais la sécurité est à ce prix.

Remarque

Le filtrage des adresses MAC n'est pas une sécurité, car il existe un certain nombre d'outils permettant de faire du « spoofing » d'adresse MAC tels etherspoof (Macintosh) ou smac (windows) pour ne citer qu'eux.

A noter

Le site http://www.security-labs.org/ propose un certain nombre de documents sur la sécurité.

Il existe des solutions basées sur la norme 802.1x qui permettent une génération de clés dynamiques plus sûres mais plus complexes à mettre en œuvre car nécessitant un serveur d'authentification.

La norme 802.1x pour une meilleure sécurité

Il existe malgré tout des possibilités de sécuriser votre réseau sans-fil. Ces possibilités sont plus complexes à mettre en œuvre et sont donc plus orientées entreprises que particuliers. La norme 802.1x, dont le draft 8 date du 3 Décembre 2003, propose une sécurisation plus forte.

La norme 802.11 s'appuie sur la norme 802.1x pour la partie authentification. Trois entités entrent en jeu :

- Le poste à authentifier (client)
- Le Point d'Accès (borne, routeurs, pont …)
- Le serveur d'authentification

Le client doit être authentifié avant de pouvoir utiliser réellement le réseau (voir figure 2.18). Pendant la phase d'authentification, seuls les échanges portant sur cette authentification sont relayés par l'AP en direction du serveur d'authentification.

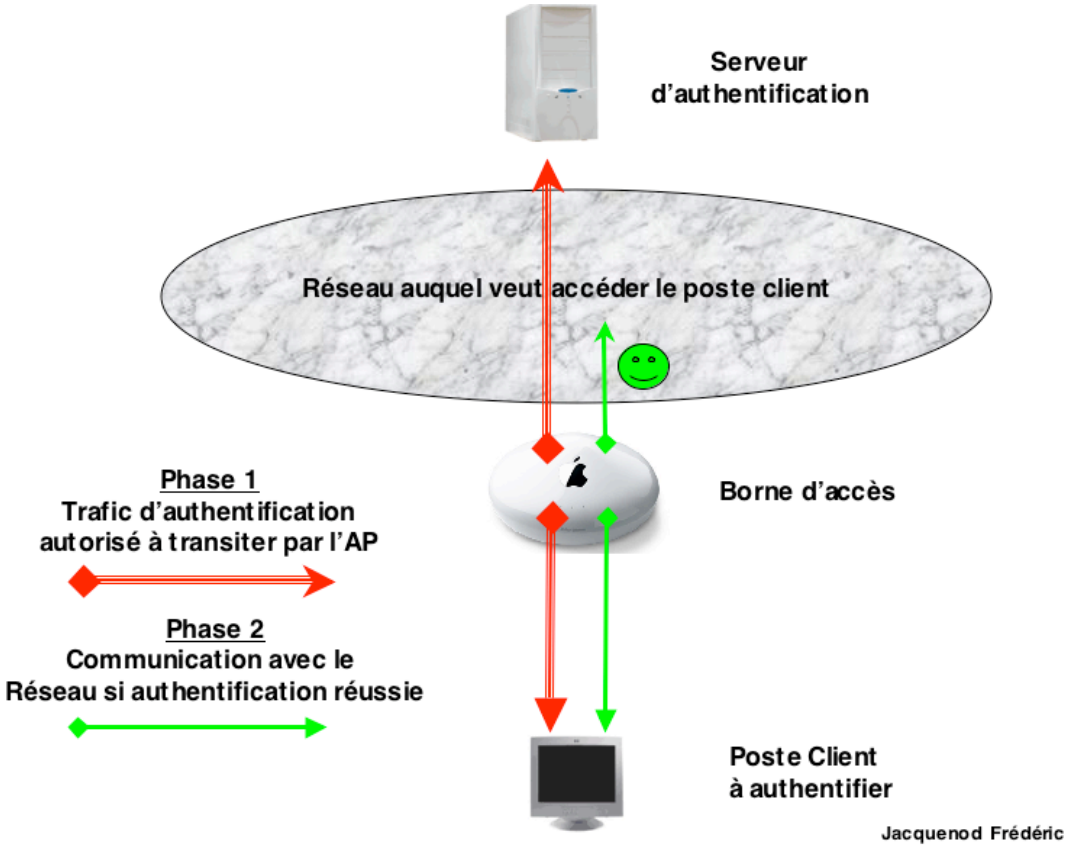


Figure 2.18,

Schéma des échanges lors de l'utilisation d'une sécurisation en 802.1x.

La norme 802.1x se base sur le protocole d'authentification EAP (Extensible Authentication Protocol). EAP est un standard de l'IETF (Internet Engineering Task Force). La spécification se trouve dans le RFC (Request For Comment) 3748. EAP a été défini pour la communication via modem en utilisant le protocole PPP (Point to Point Protocol).

Il y a deux phases définies par le protocole EAP:

- La demande d'authentification entre l'AP et le client (login, mot de passe, certificat, biométrie …) appelée aussi EAPOL (EAP Over Lan)
- La transmission de ces informations entre l'AP et le serveur d'authentification (souvent un serveur RADIUS (Remote Authentication Dial In User Service)) appelée aussi EAPOR (EAP Over Radius)

Bien sûr préalablement à la partie authentification, le client doit s'associer à l'AP.

Le protocole EAP est complété par d'autres outils de gestion de l'authentification, il en résulte un choix à faire lors du montage de son réseau et de la partie authentification.

- EAP-TLS : EAP + Transport Layer Protocol basé sur les clés publiques PKI (Public-key infrastructure) appelées aussi certificats. Les clés WEP sont générées de manière automatique.
- EAP-TTLS (Tunneled et EAP-PEAP (Protect EAP)) assez proche de EAP-TLS à la différence près qu'un tunnel (VPN Virtual Private Network) est utilisé en plus du système de PKI. Ce système augmente la sécurité via un nouveau chiffrement de la communication. Les clés WEP sont générées de manière automatique.

- EAP-MD5 (EAP-Message Digest 5) C'est le plus simple à mettre en œuvre car seul le couple login-mot de passe est demandé. Par contre rien n'est chiffré. De plus les clés WEP ne sont pas dynamiques.
- EAP-LEAP (EAP-LightWeight EAP) Cette association est propriétaire CISCO mais il est possible d'utiliser en plus une des méthodes précédentes. Les clés WEP sont générées de manière automatique.

La nocivité des ondes

Là aussi, il est nécessaire de relativiser cette notion. Non pas qu'il n'y ait aucun problème. Les ondes dégagent de l'énergie et nous sommes entourés de ces ondes (télévision, téléphone portable, sans-fil, lumière …). Tout va dépendre de la puissance de ces ondes.

Les cartes sans-fil ont généralement une puissance de 30mW.

Technologie	Puissance
Sans-Fil	30mW
Borne Sans-Fil	< 100mW
Téléphone GSM	600mW
GSM (Global System for Mobile)	< 2 W
Antenne GSM	20 à 50 W
Four à micro-ondes	1kW
Emetteur de la tour Eiffel	6 MW

Tableau 2.13 Valeurs d'émission des ondes en fonction de différentes sources

Rappel

Le champ magnétique décroît selon la formule 1/r^2. r étant le rayon ou la distance en mètres.

Etant donné ces chiffres, il faudrait pour obtenir la puissance équivalente à un téléphone GSM positionné près de son oreille environ une dizaine de portables munis d'une carte sans-fil sur la tête ou 1000 portables sur les genoux ou mieux, 100.000 dans une salle …

3. Le Courant Porteur en Ligne (CPL)

Le CPL (Courant Porteur en Ligne) appelé aussi PLC (Power Line Communication) ou BPL (Broadband over Power Line) est une technologie qui commence à faire parler d'elle. Pour s'en convaincre il suffit de regarder le nombre d'articles qui sortent sur ce sujet depuis 2003 (Le monde informatique, 01Net, réseaux&telecoms, New York Times …).

Mais que se cache t'il derrière cette « nouvelle » technologie ?

Le contenu qui suit est axé essentiellement sur le CPL coté Hautes Fréquences à des fins de communication réseaux et non Basses Fréquences utilisée dans la domotique.

3.1 Définition, normalisation et historique

Le CPL est une technologie assez récente dans le cadre d'une utilisation pour des réseaux informatiques. Malgré tout son déploiement est déjà en cours dans quel cadre s'effectue t'il ? Quelles sont les technologies mises en œuvre ?

Définition

Le CPL est une technique qui permet d'utiliser les lignes électriques basse et moyenne tension (220 volts ou 380 Volts), pour y faire passer des ondes courtes à hautes fréquences sur la bande des 1,6 MHz à 30 MHz au moyen d'un couplage avec les signaux électriques (50Hz en France).

Normalisation

En Mars 2000, une alliance est passée entre une dizaine de grands groupes industriels notamment ceux représentant les producteurs d'électricité. Se retrouvent des entreprises telles EDF, Amperion, France Telecom, Belkin Corporation, IBEC, Motorola, Sony, ST&T, Netgear …

Le nom de cette association est HomePlug Power Alliance. Ils sont actuellement plus de 70. Le site internet se situe à l'adresse http://www.homeplug.org.

De cette alliance née une spécification le HomePlug 1.0 en Juin 2001. Tout comme pour le WiFi, ce sont les industriels qui « imposent » leurs spécifications. Il est à noter qu'il n'y a toujours pas à ce jour de norme associée au CPL même si un groupe de travail (P1901) de l'IEEE prévoit de produire un certain nombre de nomes sur le CPL pour fin 2006. Par contre la plupart des produits commercialisés respectent les spécifications du HomePlug.

La spécification actuelle est la HomePlug 1.01.

Il existe d'autres spécifications proposées par cette alliance.

- HomePlug AV (Audio Visual) propose des débits de 50 à 200 Mbits/s. Cette spécification a été approuvée le 18 Août 2005 et doit permettre le passage de vidéo (télévision Haute Définition), de la voix sur IP (VoIP) avec une meilleure sécurisation (basée sur une clé AES 128 bits) et une gestion de la qualité de service.
- HomePlug BPL (Broadband PowerLine) qui spécifie (prévu pour fin 2006) la mise en place de la liaison entre le client (Home) et le gestionnaire (fournisseur du courant).
- HomePlug CC (Command and Control) qui doit spécifier l'utilisation du courant comme moyen de contrôle d'applications domotiques (lumière, climatisation, sécurité …).

Historique

Cette technologie existe depuis les années 1980 comme méthode de transport des informations à bas débits pour des applications de domotique notamment pour piloter à distance des appareils électriques (radiateurs, lumière …). D'ailleurs, EDF (Electricité De France) l'utilise à cette époque pour effectuer ses maintenances à distance. Les plus répandues, qui fonctionnent toujours sont connues sous les appellations X10, Lonworks et CEBus. LonWorks (Local operating networks) a été mis au point par la société Echelon à travers un protocole réseau LonTalk proche d'IP. CEBus (Consumer Electronics Bus) est un standard de communication développé par l'EIA (Electronics Industry Association) et le CEMA (Consumer Electronics Manufacturers Association) et approuvé en 1992. Ce standard est ouvert et par conséquent tout le monde peut l'utiliser.

La limitation du débit n'a pas permis leurs utilisations pour des applications informatiques plus gourmandes.

- En 1998, création de Power Line Telecom Forum (PLTF) qui devient ensuite UPLC, la branche pour le développement du CPL (PLC en anglais), de l'UTC (United Telecom Council) en Amériques du Nord.
- En 1999, Nor-Web, filiale de Nortel tente une percée avec cette technologie. Cela se solde par un échec. Le directeur de Nor-Web, Tim Watkins explique alors à un journal Suisse, la CyberGazette la raison de cet échec. « *L'expérimentation a été un succès technique, meilleur que ce à quoi nous nous attendions, mais l'étude de marché n'a pas convaincu le groupe de l'existence d'un marché suffisant pour le développement de cette technologie, … Les compagnies d'électricité n'ont pas montré un enthousiasme suffisant pour investir dans les modifications de leurs réseaux nécessaires à l'aboutissement d'une proposition rapide.* ».
- En Mars 2000, une alliance est passée entre une dizaine de grands groupes industriels notamment ceux représentant les producteurs d'électricité. Se retrouvent des entreprises telles EDF,

Amperion, France Telecom, Belkin Corporation, IBEC, Motorola, Sony, ST&T, Netgear … Le nom de cette association est HomePlug Power Alliance. Ils sont actuellement plus de 70.

- De cette alliance née une spécification le HomePlug 1.0 en Juin 2001. Tout comme pour le WiFi, ce sont les industriels qui « imposent » leurs spécifications. Il est à noter qu'il n'y a toujours pas à ce jour de norme associée au CPL. Par contre la plupart des produits commercialisés respectent les spécifications du HomePlug. La spécification actuelle est la HomePlug 1.01. La spécification HomePlug AV (50 à 200 Mbits/s) a été approuvée le 18 Août 2005 et doit permettre le passage de vidéo (télévision Haute Définition), de la voix sur IP (VoIP) avec en plus une meilleure sécurisation et une gestion de la qualité de service.
- Création de l'association PLCForum en 2000. Cette association a pour but de promouvoir le CPL en Europe (http://www.plcforum.com).
- Création de l'association PLCA le 5 Décembre 2001 pour la promotion du CPL en Amérique du Nord. Tout comme le PLC forum, ce sont les grands industriels qui sont à la tête de ce groupe (http://www.plca.net).
- De nombreux tests ont été effectués en vraie grandeur ou sont en cours de réalisation. Les précurseurs sont les Suisses avec un test en 2001 à Fribourg sous le contrôle de l'OFCOM (Office Fédéral de la COMmunication). Un guide est produit en Février 2003 suite aux différentes expérimentations et aux 4400 mesures sur 236 points concernant les perturbations engendrées par les PLC. De très nombreuses voix s'élèvent alors contre l'utilisation du CPL. Certains, comme Jacques Mézan de Malartic, parlent même « *de cancer des ondes courtes* ».
- En Europe une organisation milite pour le développement du CPL : le PUA (Plc Utilities Alliance). On y retrouve là aussi de grands industriels Européens de l'électricité (EDF, Endesa, Enel, Iberdrola …). Ce groupe est plus orienté marketing que technologies.
- Le PUA a lancé un test de grande envergure à Saragosse en 2002 portant sur plus de 300 immeubles, 20.000 maisons. 140 transformateurs ont été installés et configurés par 25 personnes en 5 mois. DS2 est le nom de la puce qui est installée au cœur des transformateurs. Actuellement plus de 2000 utilisateurs s'en servent. Chaque transformateur peut gérer de 1 à 133 utilisateurs. Selon l'étude, 4 personnes sur 5 sont très satisfaites du PLC (attention aux chiffres, le but du PUA est un but commercial). Ce test se base sur la technologie de l'espagnol DS2 (Design of Systems on Silicon qui se situe à Valence http://www.ds2.es).
- L'IEEE étudie une autre technologie qui permet de faire passer du courant électrique sur des câbles ethernet (150 watts maxi). Cette technologie est en cours de normalisation sous l'appellation 802.3af. Elle est soutenue notamment pas Cisco, mais a comme contrainte de devoir conserver pour les appareils purement électriques le réseau électrique habituel. Il faut se doter d'un PSE (Power Source Equipement) qui est un petit module qui permet d'alimenter en courant (à partir d'une connexion au câble via la carte réseau) les appareils tels, les caméras, les disques et autres périphériques … Le site http://www.poweroverethernet.com/ propose un certain nombre de documents techniques sur les produits issus de cette gamme.
- En France, EDF, n'est pas autorisé à faire un travail de fournisseur réseau de manière directe. Il a donc créé une filiale Edev CPL en Mai 2003.
- 1er Janvier 2004, la commission Européenne lance le projet Opera (Open PLC European Research Alliance) sur 4 ans et un budget de 20 Millions d'Euros (9M de la part de la CEE) dans le but de proposer une norme d'ici la fin de l'année 2004 puis d'effectuer des tests.
- Le 13 Janvier 2004, HomePlug Powerline Alliance annonce l'arrivée de trois nouveaux membres et non des moindres : Comcast, DS2 et EarthLink. HomePlug Alliance comprend désormais plus de 50 membres. Le président de DS2 Jorge Blasco le dit clairement, le CPL est une opportunité commerciale unique : « *Powerline Networking and Powerline Access (BPL) have already demonstrated their strength in the marketplace. Powerline Access is a very promising market. We are delighted to see that the HomePlug Alliance is focused on a synergistic development of both market segments.* ».
- En Avril 2004 G.W.Bush président des états-unis autorise l'utilisation du CPL (BPL) « *Power lines were for electricity; power lines can be used for broadband technology. So the technical standards need to be changed to encourage that.*».
- Octobre 2004, les constructeurs Legrand, ST Micro et LEA mettent sur le marché une prise électrique avec module CPL intégré dénommé le « smartplug ». Ce produit a reçu le soutien du projet Européen Eureka (http://www.eureka.be). Ce produit répond à la norme NFC 15-100 (obligatoire depuis le 1er juin 2003 dans les constructions neuves).

- Au CeBIT d'Hanovre en Mars 2004, la société Française SpidCom (http://www.spidcom.com/), créée en Septembre 2002, filiale de ELSYS Design, effectue une démonstration de sa puce SPC200, basée sur la technologie FLIP (FLexIble Powerline) développée en partenariat avec EDF, qui permet un débit de 168Mbits/s (224Mbits/s théoriques et 100Mbits/s pratiques) sur courant électrique.
- Après une période de tests, l'ARCEP le 20 avril 2005 (http://www.arcep.fr/communiques/communiques/2005/c05-19.htm) autorise les opérateurs à déployer du CPL suite aussi à une recommandation de la commission européenne en date du 12 Avril 2005.

« Paris, le 20 avril 2005

L'Autorité de régulation des télécommunications lève le statut transitoire qui était jusqu'à présent appliqué aux réseaux filaires basés sur la technologie des Courants Porteurs en Ligne (CPL).

L'Autorité vient de réaliser un bilan des expérimentations des réseaux filaires basés sur la technologie des Courants Porteurs en Ligne. L'analyse des divers rapports a permis à l'Autorité de s'assurer que les exploitants de réseaux filaires basés sur cette technologie peuvent faire face aux obligations liées à l'autorisation de réseau ouvert au public. … ».

3.2 Caractéristiques techniques

Cette partie présente au-delà de l'aspect normalisation et historique les éléments et choix techniques qui sont faits permettant au CPL d'être utilisé.

Les fréquences

Cette technologie utilise l'infrastructure électrique existante en couplant ses signaux au courant alternatif comme le montre la figure 2.19.

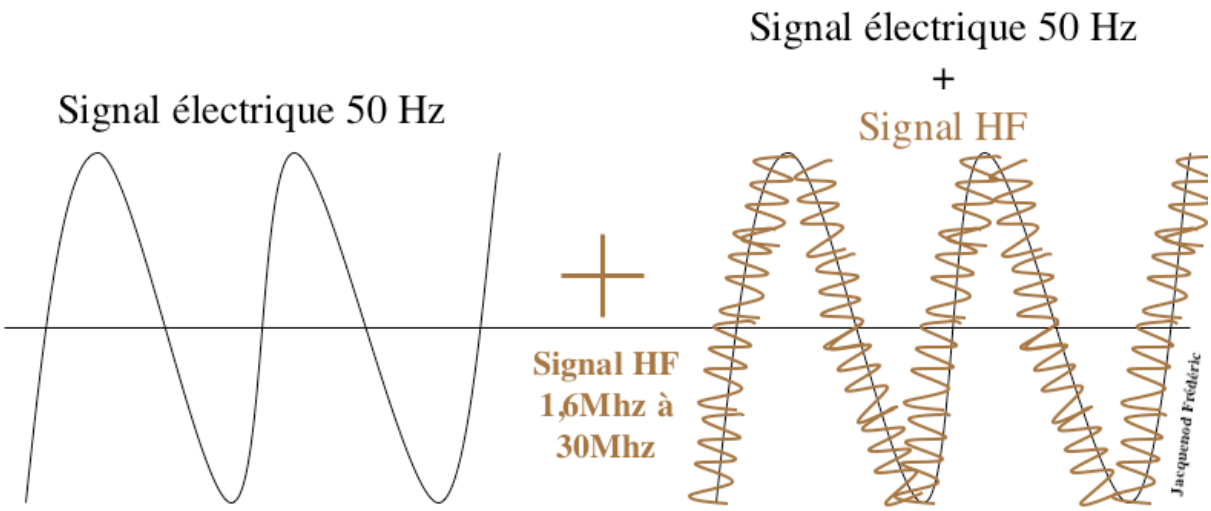


Figure 2.19,

Couplage des signaux électriques.

Les adaptateurs CPL récupèrent le signal et suppriment les fréquences basses (le courant) pour isoler les fréquences hautes (données informatiques). Les fréquences utilisées vont de 1,6 MHz à 30 Mhz soit des fréquences sur un bande large (Hautes Fréquences) mais en ondes courtes.

Les débits et les limites

Les débits moyens actuels sont situés aux alentours de 14Mbits/s en « indoor » partagés par tous les postes reliés à la même ligne électrique. Le CPL fonctionne comme une topologie Bus.

L'évolution de la vitesse de transmission est rapide.

En effet en 1998, le débit était de 0,4Mbit/s, en 2001 le débit proposé était de 2 Mbits/s théoriques alors qu'aujourd'hui il est proche de 200Mbits/s.

Attention

Les chiffres avancés sont à scinder en deux parties. Les débits en « indoor » (dans la maison, en aval du compteur électrique) sont situés actuellement entre 14Mbits/s et 45Mbits/s théoriques.

Les débits en « outdoor » (entre le compteur et le transformateur général du quartier) sont situés entre 14 Mbits/s et 224 Mbits/s théoriques.

Ces débits sont modulés en fonction de plusieurs critères :

- La distance entre la prise électrique et le transformateur
- Le nombre d'utilisateurs connectés
- Si vous êtes en « indoor » ou en « outdoor »
- Le nombre de répéteurs installés entre le transformateur et la prise
- La charge du circuit électrique (plus il y a de matériels consommant de l'électricité plus le débit diminue, halogène, fours, multiprises …)
- Le type de matériel utilisé

Attention

Les valeurs indiquées sont souvent celles obtenues au niveau du câble électrique et non à la sortie de la prise (plusieurs utilisateurs, répéteurs, appareils électrique branchés …). De plus, la valeur en sortie de prise (2 à 10Mbits/s) sera partagée par tous les matériels connectés à la prise si vous y branchez un concentrateur. Comme pour le WiFi, l'utilisation du cryptage diminue aussi le débit effectif.

- Les liaisons sont au maximum de 800 mètres en « outdoor » c'est à dire entre votre compteur et le transformateur général (station électrique) de votre quartier (boucle locale). Les fréquences utilisées vont de 1,5Mhz à 30Mhz pour le transport de l'information. Entre 100 et 250 points d'accès « indoor » peuvent être gérés.
- La spécification HomePlug 1.01 indique 15 points d'accès maximum par réseau logique. Certains constructeurs comme Oxance avec sa gamme PLA proposent jusqu'à 250 points d'accès par réseau logique.
- Les liaisons en « indoor » peuvent allées jusqu'à 200-300 mètres. Les fréquences utilisées vont de 1,5Mhz à 30Mhz.
- Pour éviter des perturbations entre le réseau « outdoor » et celui « indoor », les fréquences utilisées peuvent être différentes. Certaines spécifications préconisent d'utiliser en « outdoor » les bandes de fréquences 1,5 MHz à 10 MHZ et en « indoor » 10 MHz à 30 MHz. Lorsque l'on voit les spécifications des produits vendus, on s'aperçoit qu'ils utilisent plus généralement en « indoor » les bandes 4 MHz à 21 MHz.
- Le nombre d'utilisateurs en « indoor » varie selon le débit, le matériel utilisé, le nombre de porteuses (modulation de fréquences, multiples spectres ayant une fréquence différente) autorisées. Le Celektron à 14Mbits/s permet d'utiliser 84 porteuses sur le circuit électrique.
- La spécification HomePlug 1.01 propose un cryptage DES 56 bits jusqu'à la carte réseau connectée à la prise.

Attention

Une fois sorti de la prise, il n'y a plus de cryptage sur le câble ethernet ou sur le câble usb (Universal Serial Bus) qui relie la carte réseau à la prise.

- Les liaisons ne peuvent se poursuivre en amont du compteur électrique.
- Le CPL ne fonctionne que si dans une infrastructure électrique monophasée.

Pour palier à certaines de ces limites, il est mis en place des solutions de Qualités de Services (Qos).

Les méthodes de transport des signaux

Ces débits sont possibles grâce à l'utilisation, comme pour le sans-fil de la modulation OFDM (Orthogonal Frequency Division Multiplexing). Le principe est de répartir un débit important sur une série de sous-porteuses modulées à bas-débits. Ces sous-porteuses sont en fait des modulations de fréquences orthogonales (Même espace entre chacune d'elles). On retrouve ce principe dans les liaisons sans-fil 802.11a et 802.11g.

La méthode d'accès est celle de la topologie bus sous la forme dérivée CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) et non celle dérivée de la topologie bus 802.3 CSMA/CD (Carrier Sense Multiple Access / Collision Detection). La technique a été mise au point par Intellon, constructeurs notamment de puces pour le CPL (http://www.intellon.com) sous la marque PowerPacket (http://www.oxance.com/french/technologie.html). On retrouve cela aussi dans la transmission des ondes pour la télévision terrestre sans fil ainsi que dans la norme 802.11a (appelé aussi Wifi5 qui permet des hauts débits grâce à l'utilisation de 8 canaux dans la bande des 5GHz).

A ce système, s'ajoutent deux autres mécanismes.

- Le virtual Carrier Sense qui permet de réduire les collisions de paquets. La station qui veut émettre envoie d'abord un petit paquet de contrôle (RTS : Request To Send) vers le destinataire. Ce dernier répond avec un paquet CTS (Clear To Send) si le support est libre. La topologie est celle du bus, tous les postes vont recevoir le RTS ou le CTS. Dès qu'ils l'ont, ils mettent en place un timer qui les empêchera d'émettre pendant la durée estimée de communication indiquée dans le RTS ou le CTS. Cette durée se nomme DIFS (Distributed Inter Frame Space).
- L'envoi par le récepteur d'un accusé de réception (Positif ACKnowledge) sans lequel l'émetteur ne transmet pas la suite. Si il ne le reçoit pas il émet à nouveau le paquet au bout d'un certain temps. Le principe est basé sur le théorème de Backoff exponentiel qui permet en cas de collision détectée de modifier sur les stations le nombre maximum (n) de manière exponentielle. Un nombre x est alors tiré aléatoirement entre 0 et n. Ce nombre permet d'accéder au support au bout de x durées de temps. Il y a alors beaucoup moins de chance que plusieurs stations aient le même nombre et par conséquent cherche à communiquer en même temps provoquant alors une collision. Ce nombre correspond au nombre de slot (intervalle) qu'il doit attendre avant de pouvoir émettre. Un slot possède une durée déterminée par le Slot Time.

Déploiement

Il n'est pas nécessaire d'installer de pilotes sur les PC, les matériels PLC sont « autonomes » (adaptateurs, hub). Par contre, il est bien sûr nécessaire de configurer la carte réseau des PC (et matériel réseau PCL routeur …) comme pour tout raccordement à un réseau.

La mise en place du CPL se fait à deux niveaux :

- Un niveau appelé « outdoor » (extérieur) qui correspond à la partie qui se situe en amont du compteur électrique. On parle souvent de mise en place d'une boucle locale ou dernier kilomètre (last mile). Cette boucle relie les différentes habitations ou lieux où l'on veut mettre en place une solution CPL. Cette partie est gérée par le fournisseur d'accès.
- Un niveau appelé « indoor » (intérieur) qui correspond à l'habitation ou le lieu dans lequel le CPL est utilisé. Cet endroit se situe en aval du compteur électrique. C'est l'utilisateur qui le met en place, sauf si un appareil doit être installé sur le compteur électrique. Par contre, les adaptateurs installés sur les prises, les ponts, le routeur … sont à la charge de l'utilisateur final.

La partie qui permet de faire passer le flux informatique en amont du point d'entrée global, à savoir le transformateur ou la station électrique pour le quartier, ne peut se faire en CPL. En effet, cette partie est une partie Haute Tension, le CPL ne fonctionne que sur basse ou moyenne tension. Les expériences mises en place et testées comme celle de La Haye-du-Puits (voir figure 2.20), a nécessité la pose de fibre optique le long des câbles hautes tensions, reliant ainsi le transformateur global du quartier à l'internet via une liaison fibre optique classique. Le choix de la fibre est dû à la distance plus grande qui peut être parcourue avec cette technologie mais aussi au fait que les rayons lumineux qui transitent par la fibre optique, ne sont pas perturbés par les ondes électromagnétiques (parasites) engendrés par le courant.

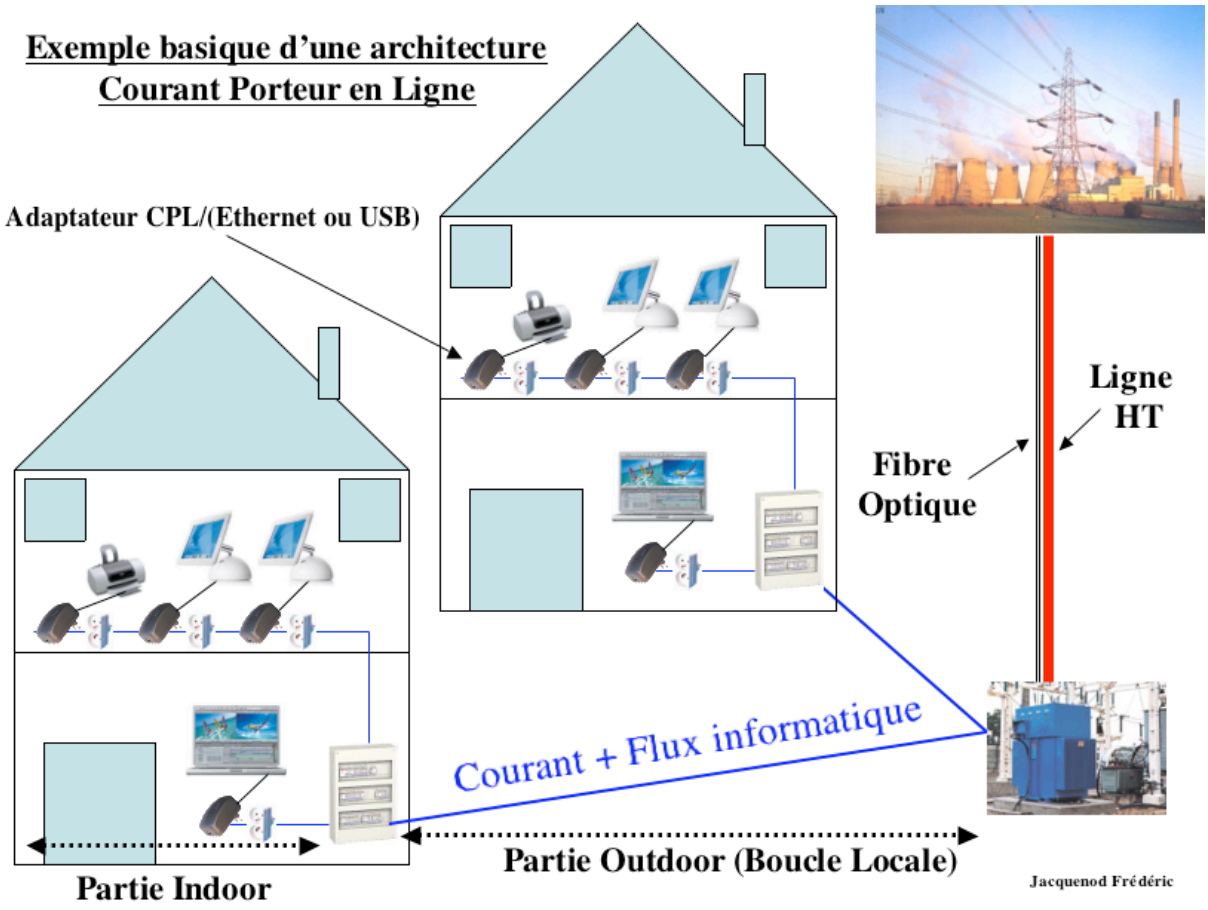


Figure 2.20,

Architecture standard d'une installation CPL.

Il existe un grand nombre de possibilités pour le déploiement. Tout va dépendre de ce que vous désirez faire et de ce que vous avez comme technologie de raccordement à l'internet (si vous en avez une).

En effet, rien n'oblige d'avoir une liaison Fibre Optique vers le Point d'accès à internet fourni par votre fournisseur (POP : Point of Presence), vous pouvez avoir une liaison téléphonique ou pas de liaison du tout (connexion en local).

Vous possédez l'ADSL et vous disposez déjà d'un modem-routeur ADSL. Dans ce cas, branchez le modem-routeur sur un adaptateur CPL (coupleur CPL) que vous branchez à son tour dans une prise électrique.

Vous possédez un réseau Ethernet connecté (ou non) à l'internet, et vous voulez lui associer un réseau CPL pour l'agrandir de façon simple. Dans ce cas utilisez un pont Ethernet/CPL que vous branchez d'un côté sur la partie Ethernet (port d'un switch, d'un hub …) et de l'autre sur une prise électrique. Si la partie Ethernet possède une connexion à l'internet via un routeur par exemple, votre réseau CPL y aura aussi accès.

Vous pouvez aussi connecter un switch ou hub « normal » sur un adaptateur CPL connecté à une prise électrique pour multiplier le nombre d'accès possibles. Attention malgré tout, aux limitations aussi bien concernant le nombre d'utilisateurs que de matériels connectés.

Il existe aussi des possibilités récentes de coupler votre réseau CPL avec un réseau sans-fil. Vous connectez le point d'accès sans-fil/Cpl à la prise électrique. Les matériels sans-fil vont communiquer avec la borne qui leurs permet ensuite de communiquer avec ceux connectés au réseau CPL (voir figure 2.21).

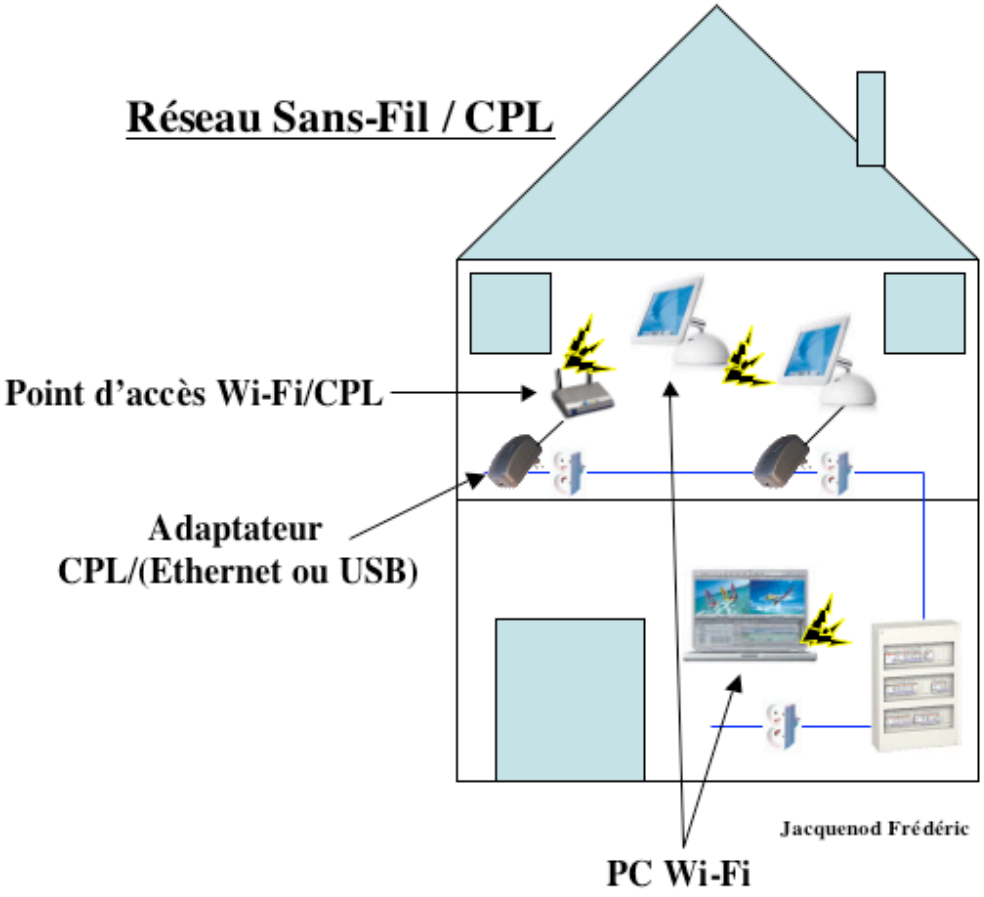


Figure 2.21,
Association d'une technologie sans fil et cpl.

3.3 Avantages et inconvénients de la technologie CPL

Si l'on regarde les articles qui parlent du CPL, tout paraît simple et idyllique. Le CPL c'est l'avenir et il faut déployer cette technologie au plus vite. L'ARCEP indique d'ailleurs dans son communiqué du 20 avril 2005 : « L'Autorité considère donc que les contraintes qui avaient justifié le statut expérimental retenu lors de l'instruction de la première demande de réseau CPL ne sont plus pertinentes aujourd'hui. »

Malgré tout des voix se sont élevées contre la mise en place de cette technologie. Quelles en sont les raisons ?

Les avantages

L'un des premier avantage est le fait que le CPL fonctionne sur un support existant dans la majeure partie des lieux notamment au sein des habitations, bureaux … Nul besoin de re-câbler les espaces qui ont besoin de l'informatique en réseau. Toute personne ayant l'électricité potentiellement peut avoir accès au réseau informatique. Il est donc possible de désenclaver des zones qui ne peuvent êtres reliées par des technologies type ADSL voir même des pays en voie de développement.

De plus, les CPL peuvent êtres utilisés en parallèle à d'autres technologies. En effet, il existe un certain nombre de passerelles vers des technologies comme l'ADSL, le câble, le satellite … Le coût de mise en place du CPL est comparable à la mise en place de technologies comme le sans fil.

Les champs d'applications sont importants. Ils vont de la domotique en passant par la vidéo (TVHD, télésurveillance…), la voix et bien sûr le transport des données. Les distances de couverture proposées par le CPL sont équivalentes aux technologies câbles et sans fil.

Le CPL propose de base une sécurisation des données sur le support électrique au moyen de codage type DES 56 bits (voir AES (Advanced Encryption Standard) 128 Bits chez certains fournisseurs comme Oxance). De plus, Le CPL est une technique plus sûre car il est plus difficile d'écouter un câble électrique que de capter une onde hertzienne (sans fil).

L'utilisation du CSMA/CA plus d'autres techniques vues dans les parties précédentes permettent, malgré la bande partagée par tous, d'éviter un trop grand nombre de collisions.

Les inconvénients

Souvent les avantages sont aussi des inconvénients et cela se confirme avec le CPL.

La technologie utilisée (CSMA/CA) découle du travail du groupe 802.3 concernant la topologie bus. Par conséquent, le débit même élevé en « indoor », est partagé par tous les matériels connectés à une même ligne électrique. Plus vous avez de matériels informatiques utilisant le support électrique, moins votre débit sera important. Ce problème se retrouve en « outdoor », où le point d'accès global (pour un immeuble, pour la boucle locale …) est aussi partagé par tous les utilisateurs connectés. Pour ces raisons, les débits effectifs sur du 45Mbits/s sont plus proches des 2 à 5 Mbits/s. L'installation est simple si elle est basique. Mais dès que vous vous lancez dans la configuration des outils avancés, des connaissances réseaux sont nécessaires comme avec toutes technologies réseau que ce soient du WiFi, du câble …

La sécurisation proposée est faible. 56 Bits ne représentent que 7 octets. Le sans-fil même avec des cryptages plus importants (128 voir 256 bits) est une solution réputée peu sécurisée alors le CPL …

La sécurisation via le cryptage ne se fait qu'à l'intérieur du réseau électrique (prolongement possible dans de rares cas). Une fois le signal sortie de la prise via l'adaptateur, il n'y a plus de cryptage. Il est donc possible de récupérer les données en clair. Rappelez-vous que la topologie est une topologie Bus, donc chaque matériel connecté à la prise (à travers un hub par exemple ou une borne sans-fil) récupère ces données qu'elles soient pour lui ou non. Le tri se fait alors au niveau des couches physiques de la carte réseau en étudiant les en-têtes ethernet des paquets. Il est donc possible au moyen d'un « sniffer » de récupérer ces paquets non cryptés.

Les limitations qu'elles soient au niveau des distances, du nombre des utilisateurs connectés à un point d'accès, ou sur les adaptateurs, les débits … du fait de l'absence de norme ne sont pas clair et dépendent d'un grand nombre de critères difficiles à évaluer. Les débits et les distances dépendent des matériels utilisés, du nombre de connexions, des distances, des parasitages du réseau électrique … Par exemple, les lignes électriques sont soumises à de fortes variations de performance dès que des matériels « gourmands » électriquement y sont connectés. Même avec des appareils ménagers de moindre importance le débit chute invariablement (démarrage du réfrigérateur, allumage d'un néon …).

Mais, le principal sujet de préoccupation est le parasitage des ondes courtes aux alentours des réseaux CPL mis en place. Deux visions s'affrontent, d'un côté les industriels et de l'autre les radioamateurs.

Les câbles électriques ont été développés pour y faire transiter des ondes courtes à basses fréquences (50 Hz ou 60 Hz). De fait, les protections (« blindages ») sont « efficaces » pour ce type d'ondes, et évitent les parasitages des alentours par le flux de courant.

Par contre, rien n'a été prévu pour empêcher les parasitages des ondes courtes à hautes fréquences (celles du CPL 1,5Mhz à 30Mhz), le câble électrique n'est pas prévu pour cela.

Il faut savoir que ces ondes courtes à hautes fréquences sont utilisées par les radios amateurs. C'est le seul système qui permet de communiquer « directement » sans passer par des satellites, des lignes téléphoniques et ceci juste en positionnant des antennes.

Ces longueurs d'ondes sont très utilisées par les services de sécurité comme la croix-rouge, les militaires, les pompiers, la police … Mais aussi dans les pays en voix de développement.

Le problème vient que dans les zones où se situent des déploiements de CPL, les parasitages sont tels qu'il est alors impossible d'utiliser ces ondes courtes par les radios amateurs.

Le site des radioamateurs http://plc.radioamateur.ch se fait l'écho de ces protestations.

Le site de l'OFCOM (Office Fédéral de la COMmunication suisse) :

http://www.ofcom.ch/fr/funk/elektromagnetisch/plc_freiburg/index.html évoque aussi ce problème.

« En 2002, un réseau PLC a été installé dans la ville suisse de Fribourg. L'Office fédéral de la communication a mené une campagne de mesure de grande envergure sur ce site, dans le but de montrer

dans quelle mesure le pouvoir perturbateur PLC affecterait la qualité de la réception radio dans la bande des ondes courtes, compte-tenu du bruit radioélectrique déjà existant en milieu urbain et rural.

Les résultats montrent que l'augmentation du niveau de bruit en milieu urbain reste modeste pour les fréquences inférieures à 10MHz. Alors que les fréquences supérieures peuvent êtres sensiblement affectées. Les mesures, effectuées sur le domaine public, montre que l'intensité du rayonnement parasite du réseau PLC installé à Fribourg excède la limite des dispositions allemandes NB30 à toutes les fréquences mesurée entre 2.4 et 25.4 MHz. »

Rappel

Il faut savoir qu'il existe des normes de parasitage. Certaines valeurs ne doivent pas êtres dépassées. On parle de norme NB30. Cette norme Allemande spécifie le taux de perturbations maximales autorisés engendré par le CPL. Certains trouvent cette norme déjà peu contraignante par rapport à d'autres par exemple celle anglaise.

On parle Champs Electro-Magnétiques (CEM) pour les ondes basses fréquences et de rayonnements électro-magnétiques pour les ondes hautes fréquences.

A noter

Jacques Mézan de Malartic, qui fait partie du groupe CEM (Compatibilité ElectroMagnétique) de l'union Française des Radioamateurs, a publié un article en décembre 2003 intitulé « Les CPL ou le cancer des ondes courtes ». Ce document est consultable sur le site http://plc.radioamateur.ch.

D'un autre coté, il est possible de lire sur le site du gouvernement Français à l'adresse

http://www.haut-debit.gouv.fr/pourquoi-comment/cpl.html

« Elle [*La technologie des courants porteurs*] consiste à séparer les signaux à basse fréquence (courant alternatif) et les ondes de haute fréquence sur lesquelles transitent les données numériques. Grâce à cette superposition, le fonctionnement des équipements électriques n'est pas perturbé. »

De même, sur le site PLC-J (PLC pour le Japon) à l'adresse : http://www.plc-j.org/en/faq.html il est indiqué dans la FAQ (foire aux Questions) :

« Q06.Is there a possibility for PLC to interfere with radio communication and telecommunication even after the voltage leakage prevention measure is applied?

A06.We will make sure that our measure will prevent interference over the radio communication and telecommunication. »

Problèmes et exercices

Les exercices de ce chapitre ont pour but de vous faire manipuler les concepts associés au câblage dans son ensemble. Vous allez être confronté à des problèmes qui se retrouvent au sein des entreprises pour des ingénieurs réseaux. Comment mettre en place un réseau ? Quelles sont les meilleures solutions à déployer ? Que proposer pour améliorer une solution déjà existante ?

A la fin de ce chapitre et de ces exercices, vous serez capables d'analyser et proposer des solutions concernant les topologies et la connectivité (câble, sans fil, connectiques …).

Les éléments de câblage

La normalisation dans l'appellation des câbles, la bonne connaissance des connecteurs, des règles de câblage sont des points très importants qu'il est nécessaire de maîtriser. En effet, ces éléments sont la base de départ du câblage car ils définissent souvent la capacité des solutions mises en place et les technologies associées qui en découlent.

2.1 Dénomination des câbles

Énoncé

a. Selon la normalisation associée à la dénomination des câbles, quel serait le nom du câble coaxial qui possède les caractéristiques suivantes ?

- Débit maximal 200Mbits/s
- Fréquence 50 MHertz
- Bande passante de base
- Longueur maximale d'un réseau 1500 mètres.

b. Dans quelle topologie pourrait il être utilisé ?

c. Sachant que le nombre maximum de postes sur ce réseau avec ce câble est de 330, que pouvez en déduire du nombre maximum connectable sur un segment ?

d. Si ce câble était un câble torsadé quel serait son nom ?

Solution

a. C'est L'IEEE qui a déterminé la façon dont les câbles se nomment. Il prend en compte le débit (Mbits/s), le type de bande ainsi que la longueur maximale d'un segment (centaine de mètres). Les câbles coaxiaux suivent la règle des 5,4,3 à savoir 5 segments, 4 répéteurs et 3 segments porteurs.

Par conséquent, le réseau s'étendant au maximum sur 1500m cela implique qu'un segment a une longueur de 1500/5 soit 300 mètres.

Ce câble, si il existait, se nommerait 200Base3.

b. La topologie associée aux câbles coaxiaux est la topologie Bus qui découle des la norme 802.3.

c. La règle 5,4,3 indique que 3 segments au maximum sont des segments porteurs des 2 autres sont des segments de liaison. Il est donc possible de connecter 110 matériels réseau par segment (330/3).

d. 200BaseTx

2.2 Les connectiques

L'exercice suivant permet de vérifier que les connaissances de bases sont bien assimilées. Notamment en ce qui concerne la partie câblage, base de la mise en place d'un réseau.

Énoncé

a. Voici un tableau de correspondance. Vous devez associer chacun des éléments entre eux. A un élément de la colonne de gauche ne correspond qu'un élément de la colonne de droite. Justifiez brièvement la motivation de vos choix.

802.11g	Ethernet Fin
BNC	DB15
RJ45	OFDM
MTRJ45	1000BaseCx
AUI	1000BaseLx

b. Vous devez relier 2 bâtiments espacés de plus de 600 mètres, quelles solutions préconisez-vous ?

Solution

a.

802.11g	OFDM
BNC	Ethernet Fin
RJ45	1000BaseCx
MTRJ45	1000BaseLx

AUI	DB15

La technologie sans fil 802.11g utilise la modulation OFDM.

Le connecteur BNC est associé au câble coaxial ethernet fin appelé aussi 10Base2.

Le connecteur RJ45 est lui associé aux câbles paires torsadées. Le seul qui soit de ce type est le 1000BaseCx.

Le connecteur MTRJ45 est un des connecteurs associés aux technologies fibre optique. Le câble 1000BaseLx en est un.

Le connecteur AUI associé au câble coaxial ethernet gros, est aussi appelé DB15.

b. Dans toutes technologies proposées une liaison optique basée sur un fibre monomode est envisageable. Si des problèmes techniques empêchent de tirer ce câble (autorisation des services de l'équipement pour traverser un espace public …), il peut être envisagé l'utilisation d'une ligne spécialisée (LS) fournie par un provider (France Telecom, Tele2 …). Une dernière solution serait l'utilisation des ondes à travers les technologies comme le laser ou le sans fil type winmax.

2.3 Cas simple

L'exercice suivant correspond à un cas très simple de mise en réseau de deux PC.

Énoncé

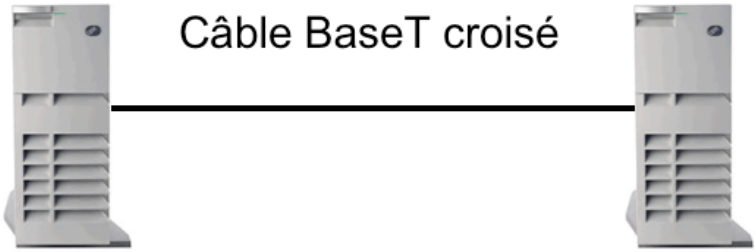
a. Vous désirez transférer un gros volume de données 1 Giga octets entre deux PC récents, un sous windows et un PC sous système apple OSX. Comment pouvez vous effectuer ce transfert ?

b. Que vous apporterait une communication full duplex au lieu de half duplex en terme de débit et de temps de transfert du fichier de 1Go ?

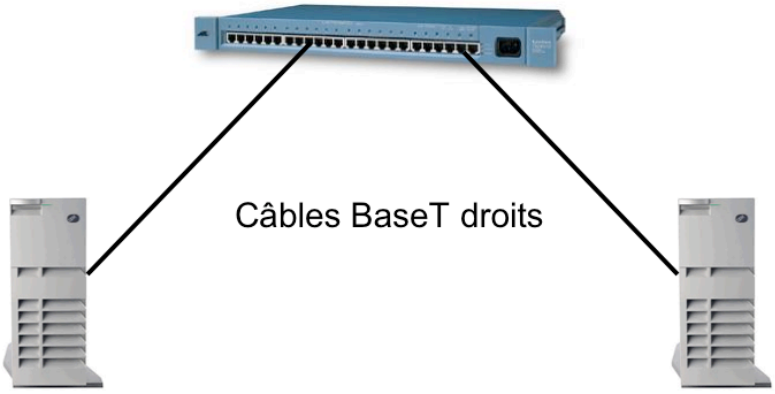
Solution

a. Plusieurs possibilités sont envisageables.

- La plus simple est de brancher entre chaque PC via la carte ethernet (carte réseau) un câble torsadé de type 100BaseTx croisé. Il est aussi nécessaire de modifier les configurations réseaux de chacun des postes afin que les deux matériels se retrouvent dans le même domaine d'adressage (voir chapitre suivant).



- La deuxième solution est de se procurer un hub (concentrateur) ou un switch (commutateur) et de brancher vos deux PC à ce matériel réseau via deux câbles BaseT droits. Dans ce cas aussi il est nécessaire que les deux PC soient dans le même réseau.



b. Dans le cas d'une communication en 100Mbits/s, le débit serait en quelque sorte doublé atteignant ainsi 200Mbits/s. Dans le cas d'une liaison half-duplex, le fichier de 1Go est transféré en environ 80 secondes. En effet, 1 octet représente 8 bits. Par conséquent, une liaison 100Mbits/s est équivalente à une liaison 12,5 Octets/s. 1000 octets / 12,5 représente un délai de 80 secondes (1 minute 20s). Si la liaison est de 200 Mbits/s le délai est divisé par 2 ce qui représente un délai de 40 secondes pour transférer notre fichier. Attention, dans ce calcul ne sont pas comptées les trames et les données ajoutées (entêtes, contrôle).

2.4 Evolution d'un réseau

L'exercice suivant vous permet de comprendre un cas souvent rencontré, celui de la migration des réseaux afin de faire évoluer une solution en une autre plus performante et adaptée aux nouveaux besoins.

Énoncé

a.Voici une phrase tirez d'une discussion entre deux ingénieurs dans laquelle certains mots sont manquants. Retrouvez les, en fonction du contexte, en justifiant vos choix.

« Mon entreprise possède encore une topologie …. avec un câblage coaxial fin en …. et des connecteurs de type …. Le directeur m'a chargé de basculer cette vieille topologie en une topologie …. afin de résoudre les problèmes de flux et de proposer un débit de 100Mbits/s garantit par connexion.

Les matériels centraux seront deux …. que je vais relier avec un câble 100BaseTx …. car il ne possède pas de port de type …. Les postes à connecter sont éloignés de moins de …. mètres je vais donc pouvoir utiliser un seul segment. Les cartes réseaux que je désire acheter, vont me permettre de doubler le débit en utilisant le mode …. »

b. Si l'entreprise possédait un câblage en catégorie 4 que proposeriez vous pour améliorer les choses et selon vous quels éléments devraient évoluer ?

Solution

a. « Mon entreprise possède encore une topologie bus avec un câblage coaxial fin en 10Base2 et des connecteurs de type BNC. Le directeur m'a chargé de basculer cette vieille topologie en une topologie étoile afin de résoudre les problèmes de flux et de proposer un débit de 100Mbits/s garantit par connexion.

Les matériels centraux seront deux switchs que je vais relier avec un câble 100BaseTx croisé car il ne possède pas de port de type MDI/MDIX. Les postes à connecter sont éloignés de moins de 100 mètres je vais donc pouvoir utiliser un seul segment. Les cartes réseaux que je désire acheter vont me permettre de doubler le débit en utilisant le mode full-duplex »

Le câble coaxial fin est une autre appellation du câble 10Base2 que l'on trouve dans la topologie bus. Le connecteur associé est le BNC. Pour proposer une solution ayant un débit de 100Mbits/s avec des éléments centraux, il ne peut s'agir que de la topologie étoile. Les deux matériels proposant un débit garantit sont donc des switchs. Pour relier deux matériels de même type, si ceux-ci ne possèdent pas de port MDI/MDIX, il faut utiliser un câble croisé. Les ports MDI/MDIX permettent de croiser le signal de manière automatique si le câble est droit au lieu d'être croisé. Pour des câbles 100BaseTx, la longueur maximale d'un segment est de 100 mètres. Pour doubler la vitesse il faut passer de half-duplex à full-duplex.

b. Si le câblage est en catégorie 4 cela signifie que c'est une topologie étoile ce qui est déjà bien. Par contre les débits sont limités à 10Mbits/s. Il faut donc recâbler en catégorie 5e ou 6 et faire évoluer les autres matériels (interconnexion) mais aussi certainement les cartes réseaux des PC pour qu'ils puissent fonctionner en 100Mbits/s.

Mise en place de solution réseau

Le choix d'une solution réseau passe d'abord par le choix de la topologie et des composants associés. Il est nécessaire de se poser les bonnes questions, de bien connaître l'environnement et les besoins, en un mot produire un bon cahier des charges. Les exercices suivants proposent de réfléchir sur ces points importants pour bien démarrer dans la conception réseau.

2.3 Topologie

Cet exercice propose une réflexion gobale sur une mise en place à partir d'un cas concret.

Énoncé

Vous êtes chargés de la mise en place d'une infrastructure réseau à l'échelle d'une salle de formation. Cette salle doit comprendre 20 postes et une imprimante, le tout doit pouvoir communiquer ensemble.

La connectique vers le réseau gobal est gérée à travers un routeur déjà en place.

Quelles sont les principales questions à poser et à vous poser avant de proposer des solutions ?

Indiquée la topologie et les câbles que vous choisiriez.

Solution

La connectique vers le réseau de l'entreprise est déjà présente. Il faut donc se focaliser sur la mise en place de la salle. En fonction des réponses aux questions, des choix seront possibles et d'autres non.

- L'environnement de travail

  Il est important de déterminer les possibilités de mise en place d'un câblage. Il est possible que la salle prévue soit dans un environnement protégé et qu'il soit impossible d'y faire des trous pour y passer des câbles et y poser des goulottes. Ces problématiques se retrouvent dans des endroits comme des bibliothèques, des salles des monuments historiques … Dans ce cas, une solution sans fil ou CPL s'imposera. Vous pouvez aussi être dans un cas où toutes perturbations électromagnétiques est interdites (hôpitaux) et donc le sans fil ou CPL seront là proscrits.

- Les besoins

  Les questions autour des besoins sont très importantes. En effet vous ne proposerez pas les même technologies si les utilisateurs doivent faire passer sur le réseau de la vidéo ou si ils sont simplement là pour faire de la bureautique ou accéder à l'internet. Il faut donc calibrer le câblage en fonction des besoins présents mais aussi futurs. Dans 5 ans est-ce que la technologie choisie sera encore à jour ou du moins pourra t'elle évoluer.

En fonction des contraintes liées aux questions précédentes une topologie en étoile avec du câbles 100BaseT catégorie 5e/6 qui permet une évolution en Giga Bit paraît une bonne solution et un bon compromis avec les besoin présents et futurs généralement exprimés.

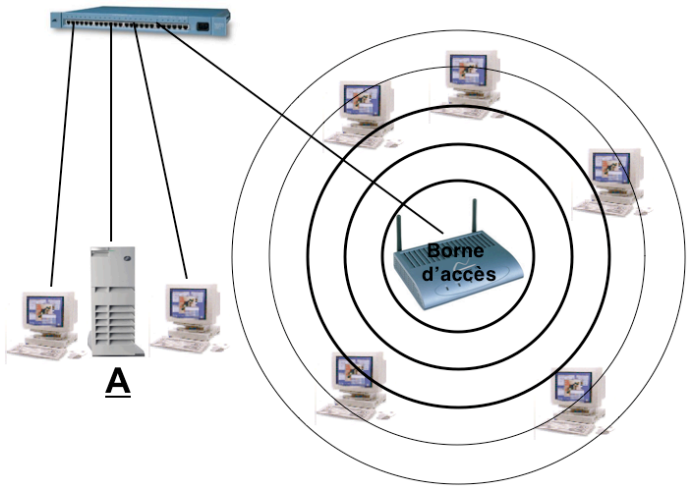
Une autre solution est le sans fil qui permettra un moindre débit mais une souplesse notamment pour les intervenants possédant un portable.

2.4 Topologie

A partir d'un cas existant, vous devez analyser ce qui existe et proposer des solutions pour l'améliorer.

Énoncé

Voici la topologie d'un réseau.



Le matériel d'interconnexion est un concentrateur.

Les utilisateurs (postes banalisés) s'authentifient au moyen du serveur d'authentification **A** connecté au concentrateur via un service de NIS (Network Information Service) ou ldap (Lightweight Directory Access Protocol). Le réseau sans-fil est protégé au moyen d'une clé Wep 64 bits.

a. Dans quelle catégorie de réseau pouvez-vous classifier cet ensemble ?

b. Quelles topologies sont présentes ?

c. Indiquez les points faibles de cette structure en termes de débits et de sécurité en justifiant vos réponses.

d. Que pourriez-vous proposer pour améliorer ce dispositif ?

Solution

a. L'organisation est celle d'un petit ensemble. En effet, étant donné les technologies misent en œuvre les distances entre les différents postes sont assez faibles. Les éléments présents dans cette topologie permettent de dire que ce réseau est de type réseau local LAN avec une partie réseau sans-fil WLAN.

b. On retrouve deux parties dans cette infrastructure :

- La première partie est filaire. Y sont connectés notamment le serveur d'authentification ainsi que la borne sans-fil. C'est une topologie étoile. On peut supposer que c'est 100BaseTx. L'utilisation d'un concentrateur implique que cette partie filaire se comporte comme si c'était une topologie Bus.
- La deuxième partie est sans-fil. La topologie est particulière car c'est une organisation en étoile mais avec un fonctionnement en bus (Tout le monde communique avec tout le monde). La technologie utilisée est le CSMA/CA. On peut supposer que c'est du 802.11g.

c. Les points faibles sont nombreux du fait des éléments mis en place.

- En terme de débit la partie sans fil et filaire, à travers la borne et le concentrateur, proposent des points durs de ralentissement. En effet, la borne partage son débit avec tous les matériels connectés en sans fil ainsi qu'avec les matériels connectés à travers le concentrateur. Plus il y aura de postes de travail connectés, moins il y aura de débit effectif pour chacun. Tout cet ensemble fonctionne comme une topologie bus (émulation d'un bus). On y retrouve donc aussi la problématique des collisions qui vont se répercuter dans tout le réseau local (filaire et sans fil).
- Sur la partie sans fil, la sécurisation proposée est assez faible du fait de l'utilisation d'une clé wep de 64 bit. Rappelez-vous que le cryptage en Wep 64 bits ne représente que 40 bits réels du fait de l'utilisation de 24 bits pour le vecteur d'initialisation. La clé représente seulement un mot de 5 caractères (5 * 8 bits). Cette clé peut être cassée sans trop de difficultés. De plus, les communications ne sont cryptées au moyen de la clé Wep que pour la partie sans fil. Par conséquent, le lien entre la borne et le concentrateur et tout ce qui est connecté au concentrateur n'utilise plus de cryptage, les communications passent en clair.
- Sur la partie filaire, le concentrateur est le principal élément faible. En effet, son fonctionnent s'assimile à celui de la topologie bus en envoyant systématiquement toutes les trames sur tous les ports sans distinction (flooding). De ce fait, en prenant en compte le positionnement du serveur d'authentification, qui y est connecté, du passage en clair des communications (utilisation des protocoles sans cryptage NIS ou LDAP), les logins et mots de passe peuvent êtres interceptés par n'importe quel utilisateur ayant installés un simple sniffer sur un des postes de la partie filaire.

d. Les solutions sont assez nombreuses et peuvent agir par palier.

Si l'infrastructure doit être conservée telle quelle, les deux éléments à mettre en place en urgence et qui n'agiront que sur la sécurité sont :

- un renforcement de la sécurisation sur la partie sans fil en montant à 128 bits la clé wep. Ce changement nécessite de modifier la configuration sans fil de tous les postes de la partie sans fil pour y insérer la nouvelle clé. Un filtrage des adresses Mac peut être envisagé à condition que le parc à gérer ne soit pas trop grand et que les postes soient toujours les mêmes.
- Mettre en place une authentification utilisant des communications cryptées sur la partie filaire. L'utilisation de ldaps en lieu et place des NIS ou du ldap de base est une première solution. Ldaps est un protocole utilisant des clés de cryptage privées et publiques à travers la mise en place d'une liaison ssl (Secure Sockets Layer).

Dans le cas où, l'infrastructure peut être modifiée et qu'une refonte de ce réseau peut être envisagée, plusieurs points sont à modifier.

- Sur la partie sans fil, l'abandon du cryptage via une clé wep en faveur d'un cryptage plus resistant est préconisé. Le mieux est l'utilisation d'une solution basée sur un serveur radius mais de manière

plus simple, la mise en place d'une clé WPA est déjà un progrès sensible. Attention, tous les matériels ne le supportent pas (borne et postes).

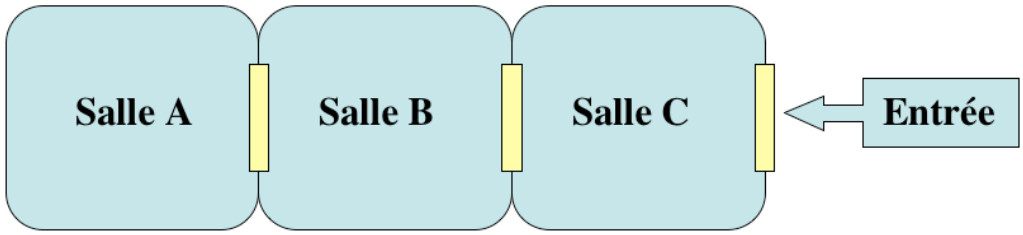
- Sur la partie filaire, le changement du concentrateur par un commutateur augmentera sensiblement les débits. En effet, le serveur d'authentification très sollicité aura une liaison 100Mbits voir Giga/Bits dédiée lui proposant ainsi un débit garantit. Ce changement de matériel augmentera la sécurité sur la partie filaire du fait de la commutation gérée par ce matériel. Seul le port sur lequel se situe le matériel destinataire recevra les données. Malgré tout, il est nécessaire de sécuriser les communications pour éviter un passage en clair des données. On retrouve la mise en place d'une solution de cryptage des données à travers un ldaps par exemple ou d'ipsec (IP security protocol) en mode transport ou tunnel.

2.5 Les interférences dans la mise en place d'une solution sans fil

Cet exercice vous permet de vous familiariser avec une des technologies émergeantes qu'est le sans fil et notamment sur les problématiques de perturbations.

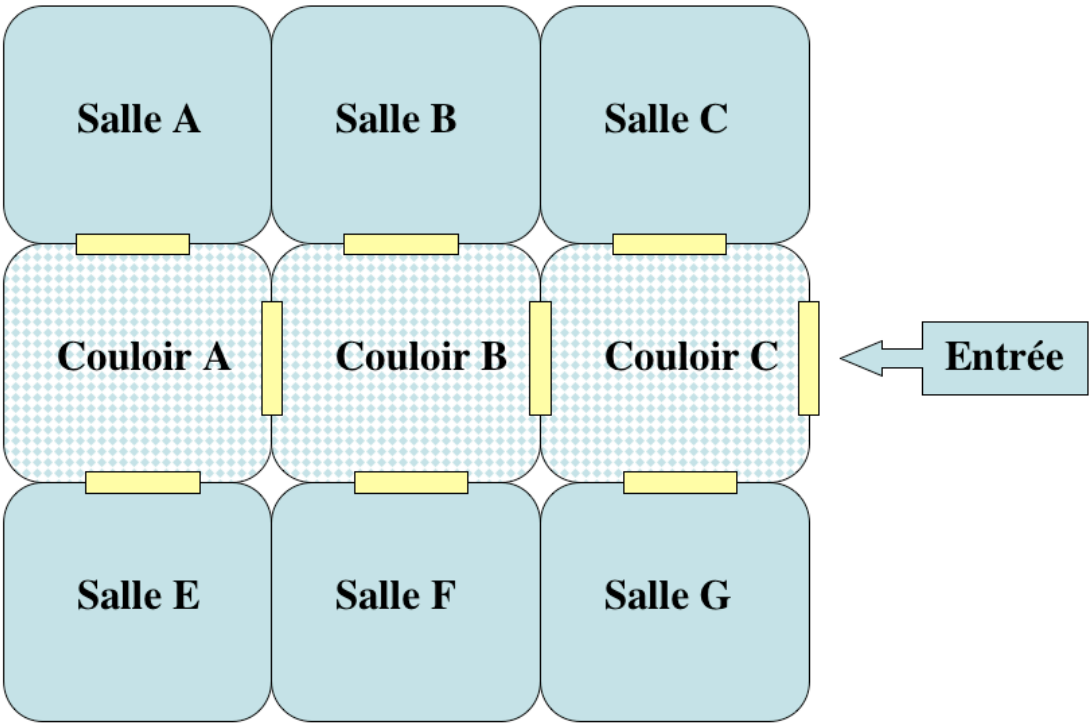
Énoncé

a. Vous devez mettre en place une solution de bornes sans fil dans 3 salles. Ces salles se situent l'une à la suite de l'autre et sont séparées chacune par un mur qui n'est que peu perméable aux ondes. On supposera que vous ne deviez vous soucier que des bornes sans fil, le reste de la connectique entre les bornes et le réseau sera étudié plus tard.



Que proposez vous comme solution et à quel problème devez-vous faire particulièrement attention ?

b. Vous devez maintenant faire évoluer cette solution en proposant une connexion pour 9 espaces réparties de la façon suivante. Les couloirs doivent aussi être utilisable comme zone de connexion. On supposera que les murs ne laissent passer que les ondes qui leurs sont adjacentes. Par exemple, la salle A est ainsi perturbée par les ondes de la salle B et du couloir A mais pas par celles de la salle C, de la salle E ou du couloir B.



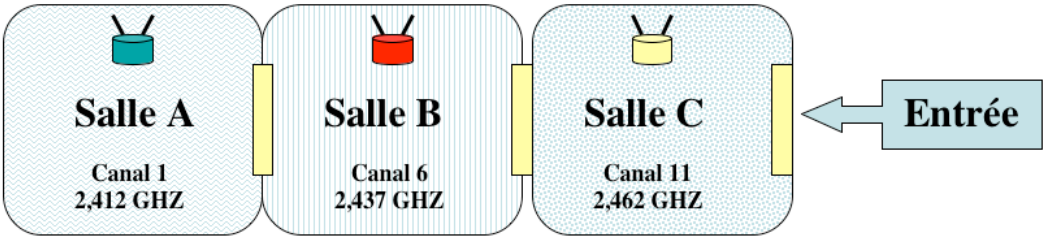
Faites un schéma en indiquant le canal et la fréquence choisie pour chacune des bornes.

Solution

a. La problématique lorsque plusieurs bornes sont installées les unes près des autres est celui des perturbations des bornes les unes par rapport aux autres. Comme l'indique le théorème de Shannon, il est alors nécessaire d'utiliser des fréquences qui ne se recoupent pas et donc séparées de 22MHz minimum. Habituellement, les fréquences utilisées sont celles des canaux 1, 6 et 11 mais d'autres espacés de la même manière peuvent aussi être utilisées. Il est possible aussi de régler la puissance des bornes pour éviter qu'elles n'émettent de manière trop forte et ainsi « confiner » ces ondes à l'intérieur d'un espace défini.

Canal	1	2	3	4	5	6	7
Fréquence GHZ	2,412	2,417	2,422	2,427	2,432	2,437	2,442

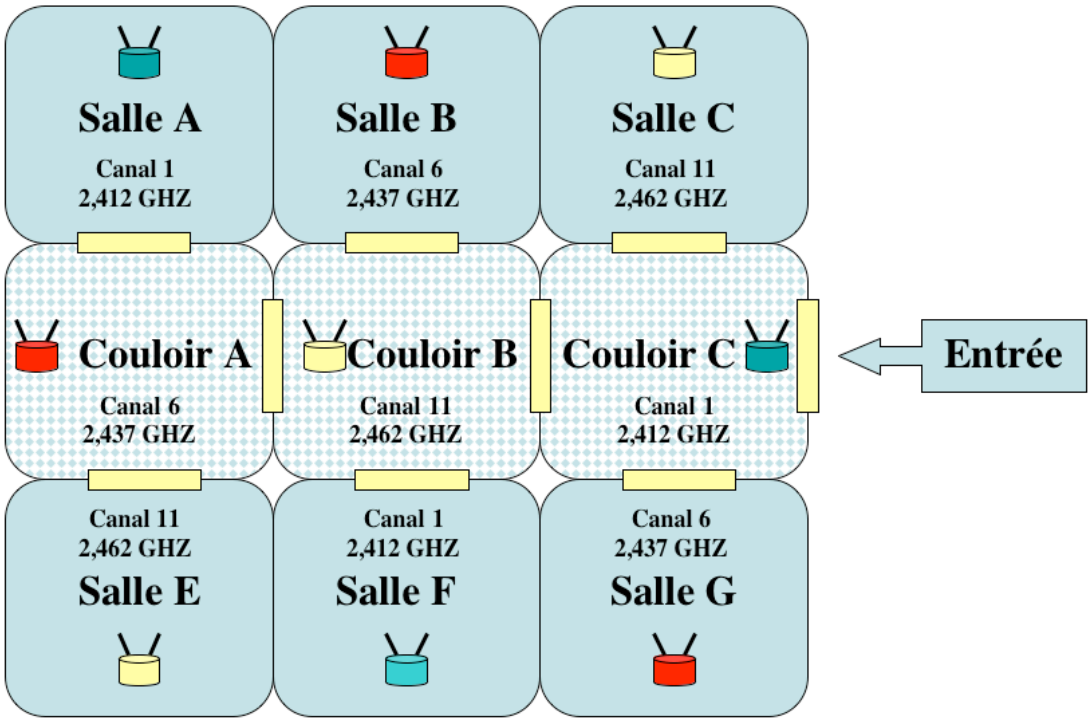
Canal	8	9	10	11	12	13	14
Fréquence GHZ	2,447	2,452	2,457	2,462	2,467	2,472	2,477



b. Le schéma de mise en place est plus complexe. On suppose que les bornes sont réglées de telle sorte que seules les salles adjacentes se perturbent.

Canal	1	2	3	4	5	6	7
Fréquence GHZ	2,412	2,417	2,422	2,427	2,432	2,437	2,442

Canal	8	9	10	11	12	13	14
Fréquence GHZ	2,447	2,452	2,457	2,462	2,467	2,472	2,477



2.6 Sécurisation du sans fil

La mise en place de solutions sans fil nécessite une bonne connaissance des problématiques liées à la sécurité des transmissions. Les questions suivantes vous permettent de les revoir pour des cas auxquels vous serez ou avez déjà été confrontés.

Énoncé

a. Vous venez d'acquérir une borne sans fil à votre domicile que vous désirez la connecter à votre connexion internet (câble, adsl, téléphone …). Quelles précautions devez-vous prendre ?

b. Vous utilisez votre connexion dans votre cuisine au moyen de votre portable mais malheureusement lorsque vous faîtes fonctionner certains matériels vous avez des problèmes de connexion. Quel matériel peut les provoquer et pour quelle raison ?

c. Dans votre chambre vous détectez très bien votre borne mais aussi un certain nombre d'autres bornes aux alentours. Certaines sont protégées par des clés de cryptage mais une ne l'est pas et peu être utilisée en « toute liberté ». Si vous le faîtes quels risques peut il y avoir ? Si vous décidez malgré tout de le faire que devez-vous prendre comme protection ?

d. Votre voisin a détecté votre borne et vous demande de pouvoir l'utiliser et en échange de partager la facture de votre fournisseur d'accès. Vous avez confiance en lui et acceptez. Comment faire pour que seuls ses ordinateurs puissent utiliser votre borne ?

Solution

a. Les ondes ne s'arrêtent pas aux limites de votre appartement, il suffit pour s'en rendre compte d'activer votre carte sans fil et vous découvrirez certainement autour de chez vous de nombreuses bornes. Par conséquent le minimum à faire est la mise en place de clé WEP (128 bits) ou WAP ainsi qu'un filtrage des adresses MAC pour ne permettre qu'à vos ordinateurs « en théorie » de s'associer à votre borne. Vous pouvez aussi empêcher la diffusion du SSID (l'identifiant de la borne). Ne laissez pas les réglages par défaut, ceux-ci sont connus de tous, il suffit d'effectuer une petite recherche sur internet ou sur le site du constructeur de votre borne. N'oubliez pas non plus de vérifier régulièrement les traces d'accès à votre borne, celles-ci sont souvent étonnantes et très instructives.

b. Un matériel qui perturbe les ondes hertziennes du sans fil (2,4Ghz) sont celles des micro-ondes qui peuvent émettre sur la même fréquence. En effet, les micros-ondes sont réglés sur des bandes allant de 1GHz (bande L) à 100GHz (bande W). Si votre micro-onde utilise la bande L celle-ci est réglée pour utiliser la bande de fréquences allant de 2GHz à 4GHZ donc la même que celle utilisée pour le sans fil. Par conséquence, votre micro-onde peut perturber les communications.

c. Vous ne pouvez utiliser une borne qui n'est pas la votre du point de vue légale, même si cette borne est ouverte. Si malgré tout vous décidez de le faire, soyez vigilent car il existe des bornes pièges appelées vulgairement « pièges à cons » ou plus techniquement honeypot ou pot de miel. Ces noms indiquent bien ce qu'elles représentent à savoir des points de passage des communications scannées au moyen d'outils d'analyse réseau (sniffer). Certaines personnes « libèrent » l'accès à leur borne pour simplement vous espionner. Par conséquent la règle principale est de ne jamais utiliser une borne de ce type pour effectuer des actions sensibles, telle la connexion à sa banque, à un compte nécessitant d'entrer un identifiant et/ou un mot de passe. Ne l'utiliser que pour de la navigation en masquant votre adresse MAC ou au moins en ne divulguant pas des informations permettant de vous retrouver (nom de votre ordinateur ...). Sinon, vous pouvez « vous protéger » en utilisant des connexions cryptées de bout en bout via les protocoles « sslisés » (utilisent le cryptage ssl) comme : https, ldaps, pops, imaps ... En effet, même si la communication est interceptée, celle-ci ne sera pas décryptable donc les données ne seront pas utilisables.

d. De même que précédemment, vous devez avoir toute confiance en la personne avec qui vous partagez votre connexion car c'est vous qui possédez l'abonnement et donc vous qui serez responsable de tout ce qui passe par cette connexion. Vous pouvez alors effectuer un filtrage des adresses mac, affecter une clé de cryptage wep ou wpa que vous lui communiquerez. Pensez à la changer de temps à autre et vérifier là aussi ce qui transite par votre borne en regardant les traces.

2.7 Autre technologie sans fil

Il existe des technologies autres que le 802.11 qui prennent de plus en plus de place notamment avec l'avènement des réseau de téléphonies 3G ainsi que la mise à disposition de périphériques utilisant des technologies telle le bluetooth. Cet exercice permet d'évaluer les possibilités de mise en réseau de ces matériels.

Énoncé

a. Quel est le nombre maximum de matériels qu'il est possible d'associer si vous utilisez la technologie bluetooth ?

Solution

a. Avec cette technologie, il est possible d'associer les matériels dans un petit réseau appelé piconet. Chaque piconet peut compter 8 matériels dont un est nécessairement le maître. 10 piconets au maximum peuvent êtres associés et former un scatternet. Sur les 10 piconets, qui représentent séparément 80 matériels, 8 matériels sont en même temps maîtres et esclaves et font donc partis de deux réseaux à la fois. Par conséquent, on peut associer 72 matériels au maximum (8 * 10) – 8 = 72.

2.8 Utilisation du CPL

Le CPL se développe de plus en plus et de manière rapide malgré les problèmes inhérents à toute nouvelle technologie. Ces exercices permettent de préciser et de réfléchir à la mise en place de cette méthode de communication.

Énoncé

Vous avez mis en place une solution CPL dans votre maison de deux étages vous permettant de connecter en réseau vos ordinateurs dont un portable.

a. Lorsque vous connectez votre portable à la prise cpl/usb dans votre cuisine, vous avez parfois des coupures de connexions. Quelle en est la raison et comment l'éviter ?

b. Vous désirez connecter vos ordinateurs à l'internet. Quelles sont les possibilités ?

c. Votre voisin désire profiter de votre connexion à l'internet et vous demande si il peut utiliser lui aussi son réseau électrique et par conséquent, habitant à coté de chez vous, passer par votre connexion internet. Que lui répondez-vous ?

d. Quelle solution pourriez-vous alors mettre en œuvre ?

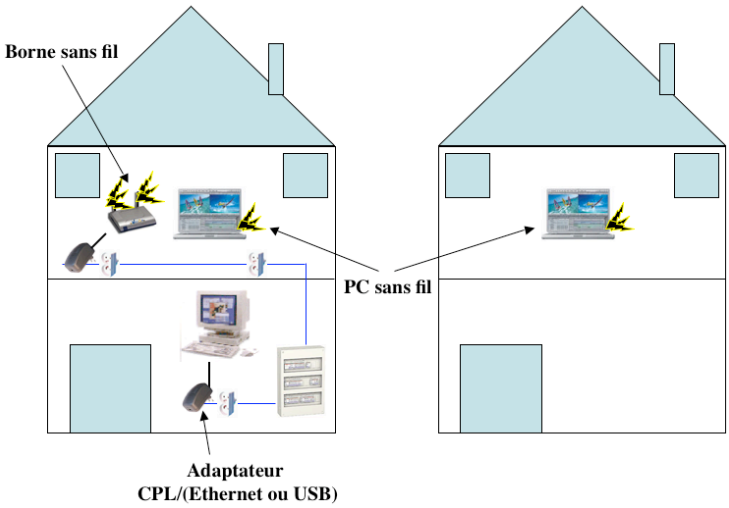
Solution

a. L'utilisation du CPL passe par le système électrique de votre maison ou appartement. Le système électrique qui se situe dans votre cuisine est utilisé par d'autres appareils comme le micro-onde, four mais aussi le réfrigérateur. Ces éléments demandent une grosse puissance et dès qu'ils démarrent, engendrent des distorsions du courant et perturbent par conséquent le signal qui transite sur le signal électrique d'où les problèmes de connexions lors de leurs utilisations. Pour éviter ce problème il faut connecter votre CPL sur une prise électrique qui ne se situe pas sur le circuit électrique des appareils pré-cites.

b. Pour connecter votre réseau interne à l'internet vous êtes obligés de passer par un fournisseur d'accès. Pour cela toutes les possibilités habituelles sont disponibles. Vous pouvez utiliser un matériel cpl/adsl, cpl/modem, cpl/ethernet … Si vous faîtes partie d'une zone de déploiement massive du cpl, il est possible que l'offre de connexion soit proposée par l'entreprise proposant le cpl à travers une connexion globale. Dans ce cas ce sera cette entreprise qui sera aussi votre fournisseur d'accès.

c. Le signal généré par les modules cpl ne peut dépasser votre propre compteur électrique. Par conséquent votre voisin ne pourra en aucun cas « coupler » son réseau cpl au votre. Ceci est une limitation forte mais aussi une sécurité. En effet, le cpl utilisant une topologie bus, les communications ne sont pas orientées seulement vers le destinataire mais passent par le circuit électrique et arrivent au niveau de chaque prise. Votre voisin ne pourra pas récupérer vos communications. Par contre n'importe qui branchant un module cpl sur une prise pourra y connecter un ordinateur et « sniffer » les paquets.

d. Pour le partage de la communication, la seule possibilité est de mettre en place une borne sans fil couplée à votre cpl. Votre voisin pourra alors utiliser votre borne sans fil et ainsi se connecter par ce biais à votre réseau et par prolongement à l'internet. Vous pouvez utiliser un module cpl associé à une borne sans fil ou directement un module cpl/sans fil.


Borne sans fil
PC sans fil
Adaptateur
CPL/(Ethernet ou USB)