

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique



Université A-MIRA de Bejaia

Faculté des sciences exactes

Département Informatique



*Mémoire de MASTER Professionnel
En informatique
Option
Administration et sécurité des réseaux*

Thème :

*configuration des équipements réseau en vue
de partage des ressources informatiques*

Encadré par :

✚ TOUAZI Djoudi

Présenté par :

✚ AMARI Chérif

✚ HAMMADI Oussama

Devant le jury composé de :

Président : SALHI Nadir

Examinatrice : BENMAMAR Ferroudja

Promotion 2011/2012

Remerciements

Nous tenons à remercier DIEU, le tout puissant, de nous avoir donné la volonté et le courage pour réaliser ce modeste travail.

Un très grand merci à notre encadrant de mémoire, TOUZI DJOUDI, pour la qualité de sa collaboration, ses précieux conseils, son aide constante et pour la façon efficace et amicale avec laquelle il a suivi ce travail. Pendant les nombreuses heures passées, on a beaucoup appris à son contact.

Nous remercions l'ensemble des membres du jury

Un grand merci à tous ceux qui ont contribué dans la réalisation de ce travail.

Enfin nous adressons nos plus sincères remerciements à nos parents nos proches et nos amis.

Dédicaces

**Je dédie ce modeste travail reflétant mon effort
consenti durant le cursus universitaire à :**

**A ma très chère mère qui est pour mon corps
mieux qu'un cœur et que dieu la protège ;**

A la mémoire de mon père ;

A mes frères et sœurs ;

A toute ma grande famille AMARI;

A mon copain de chambre (B.AMAR) ;

A mes collègues;

Et à tous mes amis ;

A tous que j'aime.

Sans oublier : Bizou,yaya,nada,dano,jojo

A. Chérif

**Je dédie ce modeste travail reflétant mon effort
consenti durant le cursus universitaire à :**

**A ma très chère mère qui est pour mon corps
mieux qu'un cœur et que dieu la protège ;**

**A mon cher père qui à sacrifié son temps pour
nous ;**

A mes sœurs ;

A toute ma grande famille HAMMADI;

A mes collègues ;

Et à tous mes amis ;

A tous que j'aime.

H.Oussama

Table des matières

Liste des tableaux

Table des figures

Introduction générale1

Chapitre 1 : Etat de l'art sur les réseaux informatique

1.1 Introduction2

1.2 Historique des réseaux.....2

1.3 Que signifie le terme réseau2

1.4 Intérêt des réseaux3

1.5 Différents types de réseaux3

1.5.1 Topologie des réseaux.....3

1.5.2 Typologie des réseaux5

1.6 Différents types d'administration des réseaux6

1.7 Les différents architecteurs des réseaux6

1.7.1 Le modèle de référence OSI6

1.7.1.1. Définition du modèle OSI7

1.7.1.2. Principe du modèle OSI7

1.7.1.3. Les différentes fonctions de chaque couche8

1.7.2. Modèle TCP/IP11

1.7.2.1 Les différentes fonctions de chaque couche11

1.7.3. Similitudes et différences entre le modèle OSI et TCP/IP11

1.8 Sécurité des réseaux informatiques.....12

1.8.1 Les attaques réseaux12

1.8.1.1 Faiblesses des protocoles :.....13

1.8.1.2 Faiblesses d'authentification :.....	13
1.8.1.3 Faiblesses d'implémentation :.....	13
1.8.1.4 Faiblesses de configuration :.....	13
1.8.2 Analyse des risques et objectifs de la sécurité.....	13
1.8.3 Principes génériques d'une politique de sécurité réseau.....	14
1.8.4 Typologie des politiques de sécurité réseau.....	15
1.8.5 Proposition de stratégies de sécurité réseau	15
1.9 Conclusion.....	17

Chapitre 2 : Concepts fondamentaux de partage des ressources

PARTIE THEORIQUE

2.1 Introduction	18
2.2 Définition des termes	18
2.2.1. Ressource informatiques	18
2.2.2 Définition de matériel informatique	18
2.3 Eléments de réseaux	19
2.3.1. Serveurs	19
2.3.2 Clients	19
2.3.3 Liaisons	19
2.3.4 Données partagées	19
2.3.5 Imprimantes et autres périphériques partagés	20
2.3.6 Protocoles de communication	20
2.3.7 Équipements d'interconnexion	20
2.4 Les types de réseau	22
2.4.1 Réseau avec infrastructure	22
2.4.1.1 Réseaux sans fil avec infrastructure	22
2.4.2 Réseaux sans infrastructure (Le mode Ad-Hoc)	23
2.4.2.1 Réseaux sans fils et sans infrastructure.....	23

2.5 Type d'imprimante réseau	24
2.6 Conclusion	26

PARTIE PRATIQUE

2.7 Partager une connexion ADSL, dossiers ou imprimantes sous Windows 7	27
2.7.1 Partager une connexion ADSL, dossiers et imprimantes dans un réseau de type Infrastructure	27
2.7.1.1 Création d'un groupe résidentiel	29
2.7.1.2 Les opérations effectuées sur les autres ordinateurs:.....	30
2.7.1.3 Mettre en partage des dossiers publics ou personnels :.....	31
2.7.1.4 Accéder aux dossiers partagés :.....	33
2.7.1.5 Mettre en partage une imprimante :.....	33
2.7.1.5.1 Accéder à l'imprimante partagée :.....	35
2.7.2 Partager une connexion ADSL, dossiers et imprimantes dans un réseau de type sans Infrastructure	36
2.8 Conclusion	38

Chapitre 3 : Serveur d'impression CUPS

PARTIE THEORIQUE

3.1 Introduction	39
3.2 Présentation de CUPS	39
3.3 Principe de fonctionnement de CUPS	40
3.4 Avantage CUPS	41
3.5 Les différentes situations d'une architecture de partage d'imprimante	41
3.5.1 Situation 1 : l'imprimante est connectée directement à l'ordinateur.....	41
3.5.2 Situation 2 : L'imprimante est accessible via un réseau.....	42
3.6 Présentation de Samba	44

3.7 Les fonctionnalités de samba	44
3.8 Architecture de Samba	45
3.9 Conclusion	45

PARTIE PRATIQUE

3.10 Introduction	46
3.11 Etape de configuration du serveur d'impression CUPS	46
3.12 Configuration du mot de passe pour l'administration CUPS	48
3.13 Création du certificat et de la clef SSL pour CUPS	48
3.14 Configuration de Samba pour les clients Windows	49
3.15 Attribution des adresses IP pour les imprimantes réseau	50
3.16 Connexion et administration du serveur CUPS	51
3.16.1 Interface d'administration Web.....	51
3.16.2 Interface d'administration à travers le gestionnaire d'impression	55
3.17 Fiche descriptive du serveur	59
3.18 Conclusion	63
Conclusion générale	64

LISTE DES TABLEAUX

TABLE 1.1 - Différence entre les typologies réseaux	4
TABLE 3.1 - Fiche descriptive du serveur.....	58

TABLE DES FIGURES

FIGURE 1.1 - Topologie en bus.....	3
FIGURE 1.2 - Topologie en anneau	4
FIGURE 1.3 - Topologie en étoile.....	4
FIGURE 1.4 - Topologie maillée	4
FIGURE 1.5 - Modèle OSI.....	7
FIGURE 1.6 - Principe du modèle OSI.....	8
FIGURE 1.7 - Les faiblesses exploitées par les attaques réseau	12
FIGURE 2.1 - Réseaux avec infrastructure.....	22
FIGURE 2.2 - Réseaux sans fil avec infrastructure.....	22
FIGURE 2.3 - Echange en mode infrastructure	23
FIGURE 2.4 - Echange en mode Ad-hoc	23
FIGURE 2.5 - Réseaux sans fil et sans infrastructure	24
FIGURE 2.6 - Serveur d'impression.....	24
FIGURE 2.7 - Imprimantes partagées	25
FIGURE 2.8 - Imprimante Peer-to-Peer.....	25
FIGURE 2.9 - Connexion au réseau local	27
FIGURE 2.10 - Fenêtre de partage de connexion	28
FIGURE 2.11 - Fenêtre pour l'ouverture de centre de partage	28
FIGURE 2.12 - Fenêtre de partage de fichiers et d'imprimantes.....	28
FIGURE 2.13 - Fenêtre de partage de dossiers publics	29
FIGURE 2.14 - Fenêtre pour accéder au groupe résidentiel	29
FIGURE 2.15 - Fenêtre pour la modification de mot de passe de groupe résidentiel	30
FIGURE 2.16 - Fenêtre pour joindre le groupe résidentiel.....	30
FIGURE 2.17 - Fenêtre pour la confirmation de mot de passe de groupe résidentiel	31
FIGURE 2.18 - partager un dossier.....	32

FIGURE 2.19 - Fenêtre de choix d'utilisateur.....	32
FIGURE 2.20 - Fenêtre pour accéder aux dossiers partagés.....	33
FIGURE 2.21 - Partager une imprimante.....	34
FIGURE 2.22 - Les propriétés de l'imprimante.....	34
FIGURE 2.23 - Fenêtre de choix d'une imprimante	35
FIGURE 2.24 - Fenêtre d'ajout d'une imprimante.....	36
FIGURE 2.25 - Fenêtre de configuration d'un réseau Ad-hoc	37
FIGURE 2.26 - Fenêtre de configuration d'authentification d'un réseau Ad-hoc	37
FIGURE 2.27 - Fenêtre d'identification d'un réseau Ad-hoc	38
FIGURE 3.1 - Le schéma fonctionnel de CUPS	40
FIGURE 3.2 - L'imprimante connectée directement à l'ordinateur	41
FIGURE 3.3 - L'imprimante est accessible via un réseau	42
FIGURE 3.4 - L'imprimante raccordée à un boîtier	43
FIGURE 3.5 - L'imprimante communiquée à un ordinateur.....	44
FIGURE 3.6 - Interface d'administration Web	51
FIGURE 3.7 - Ajouter une imprimante	52
FIGURE 3.8 - choix de l'interface	52
FIGURE 3.9 - choix de la connexion	53
FIGURE 3.10 - Fiche d' descriptive d'imprimante	53
FIGURE 3.11 - Le choix de pilotes	54
FIGURE 3.12 - Choix des modèles d'imprimante	54
FIGURE 3.13 - Les paramètres par default	55
FIGURE 3.14 - Le gestionnaire d'impression	55
FIGURE 3.15 - Choix de périphérique	56
FIGURE 3.16 - Choix de pilote	56
FIGURE 3.17 - Description d'imprimante	57
FIGURE 3.18 - Paramètres de l'imprimante	57
FIGURE 3.19 - Comportements de l'imprimante	58
FIGURE 3.20 - Contrôle des accès de l'imprimante relié au réseau	58

Introduction générale

Introduction Générale

L'évolution technologique a conduit à la possibilité de construire des systèmes Informatiques de plus en plus sophistiqués et de moins en moins encombrants. Pour permettre d'équiper le maximum de points d'utilisation, et de fournir pour tout employé d'une entreprise, d'une administration, et donc d'un établissement d'enseignement, l'outil indispensable améliorant son efficacité et par suite sa productivité.

Les réseaux informatique permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types, d'ordinateurs que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simple terminaux graphique. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche, etc....) et des particuliers (messagerie, loisirs, services d'informations par minitel et internet ...).

Chaque fabricant d'imprimantes va rajouter ses propres options, et définir ses propres codes pour activer des fonctions spécifiques, une fois dépassée la fonction d'impression proprement dite, pas mal d'autres informations doivent être transmises, chacune codée de façon différente. D'où une profusion de pilotes, chacun adapté à un modèle ou à une famille de modèles d'imprimantes. La tâche des administrateurs devient complexe : à chaque nouvelle imprimante, il faut configurer tous les postes des utilisateurs susceptibles de s'en servir. De plus, il faut être capable de limiter les impressions, de les compter, voire de les facturer. Le recours aux serveurs d'impression devient indispensable.

Les fabricants de photocopieurs vont même plus loin : leurs serveurs d'impression sont capables de stocker toutes les impressions, puis c'est l'utilisateur, devant un photocopieur quelconque, qui déclenche l'impression. L'utilisateur n'a plus à savoir vers quelle imprimante il envoie son fichier, c'est devant la machine qu'il rappelle son impression en attente dans le serveur.

Le présent mémoire est composé de trois chapitres. Dans le premier nous illustrons en générale les réseaux informatique, en tenant compte de leurs caractéristiques physiques et logiques, ensuite nous présentons les différents attaques réseaux et les moyens qui permettent de leurs faire face. Dans le deuxième chapitre nous introduisons dans la première partie les concepts fondamentaux de partage des ressources et l'interconnexion des équipements, ensuite la réalisation pratique du partage des ressources. Dans le troisième chapitre nous élaborons la mise en place d'un serveur d'impression CUPS.

Chapitre 1

Etats de l'art

1.1 Introduction

Dans ce chapitre nous allons présenter des généralités sur les réseaux informatiques et leurs caractéristiques ; nous présentons également quelques concepts et modèles les plus utilisés.

1.2 Historique des réseaux

Peu après la seconde guerre mondiale, nous sommes à l'aube de la micro-informatique ; seules les grandes entreprises pouvaient se doter de matériel informatique. Le seul moyen d'échanger des données de station à station était " la disquette ". Pour un même département, cela ne pausait guerre de problèmes. Cependant, la chose devenait plus compliquée lorsqu'il s'agissait d'un bureau situé à un autre étage, ou dans un autre bâtiment.

Les réseaux modernes sont apparus au cours des années 1960 à la faveur d'une technologie totalement nouvelle permettant de transporter de l'information d'une machine à une autre. Ces machines étaient des ordinateurs de première génération.

Les réseaux de téléphonie existaient quant à eux depuis longtemps. Ils utilisaient la technologie dite de commutation de circuits et le support de lignes physiques reliant l'ensemble des téléphones par le biais de commutateurs. Lors d'une communication, ces lignes physiques ne pouvaient être utilisées que par les deux utilisateurs en contact. Le signal qui y transitait était de type analogique.

La première révolution des réseaux a été apportée par la technologie numérique des codecs (codeur-décodeur), qui permettaient de transformer les signaux analogiques en signaux numériques, c'est-à-dire une suite de 0 et de 1. Le fait de traduire tout type d'information sous forme de 0 et de 1 permettait d'unifier les réseaux. Dans cette génération, la commutation de circuits était toujours fortement utilisée. [1]

1.3 Que signifie le terme réseau

Un réseau en général est le résultat de la connexion de plusieurs machines entre elles, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations.

Le terme réseau en fonction de son contexte peut désigner plusieurs choses. Il peut désigner l'ensemble des machines, ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés, ce qui 'est le cas lorsque l'on parle d'Internet. Le terme réseau peut également être utilisé pour décrire la façon dont les machines d'un site sont interconnectées. [2]

1.4 Intérêt des réseaux

Un ordinateur est une machine permettant de manipuler des données. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre-eux afin de pouvoir échanger des informations.

☞ Un réseau informatique peut servir plusieurs buts distincts

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.).
- La communication entre personnes (courrier électronique, discussion en direct, etc.).
- La communication entre processus (entre des ordinateurs industriels par exemple).
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau).
- Le jeu vidéo multi-joueurs...

Les réseaux permettent aussi de standardiser les applications, pour qualifier les outils permettant à plusieurs personnes de travailler en réseau. Par exemple la messagerie électronique et les agendas de groupe permettent de communiquer plus efficacement et plus rapidement.

☞ Voici un aperçu des avantages qu'offrent de tels systèmes

- Diminution des coûts grâce aux partages des données et des périphériques,
- Standardisation des applications.
- Accès aux données en temps utile.
- Communication et organisation plus efficace.

Aujourd'hui, avec internet, on assiste à une unification des réseaux. Ainsi, les intérêts de la mise en place d'un réseau sont multiples, que ce soit pour une entreprise ou un particulier.

1.5 Différents types de réseaux

1.5.1 Topologie des réseaux

Décrit la manière dont les équipements réseau sont connectés entre eux. C'est aussi une représentation d'un réseau

- ✚ **La topologie en bus** : Topologie réseau dans laquelle des nœuds multiples accèdent à un même bus partage. Cette topologie est l'organisation la plus simple d'un réseau. Elle est extrêmement vulnérable étant donné que si un des nœuds est défectueux, cela entraînera un partitionnement du réseau.

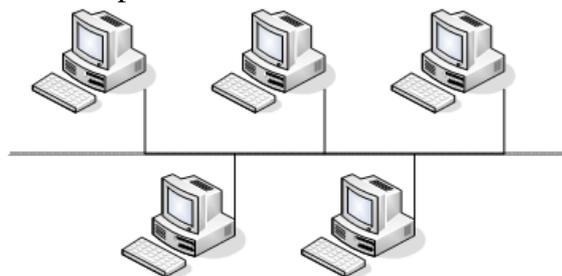


FIGURE 1.1 – Topologie en bus

- ✚ **La topologie en anneau :** Dans cette configuration, le support relie toutes les stations, de manière à former un circuit en boucle. L'information circule dans une seule direction, le long de support de transmission.les réseaux en anneaux utilisent des techniques de jeton, par lesquelles seule le coupleur qui possède le jeton à le droit de transmettre.

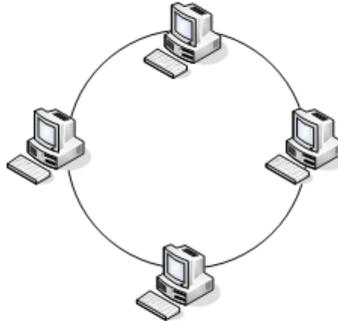


FIGURE 1.2 – Topologie en anneau

- ✚ **La topologie en étoile :** Dans cette topologie, chaque équipement est relié à un nœud central. Les performances d'un réseau en étoile dépendent principalement du nœud central. Ce type de réseau est relativement efficace et économique, Dont la pluparts des réseaux fonctionnent sur ce principe.

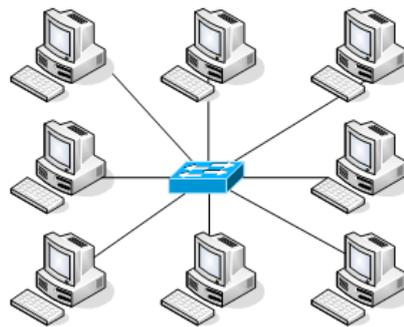


FIGURE 1.3 – Topologie en étoile

- ✚ **La topologie complète (maillée) :** Cette topologie consiste à relier chaque point l'un à l'autre. Elle n'est pas utilisée en pratique. C'est la topologie la plus sûr mais elle est très couteuse.

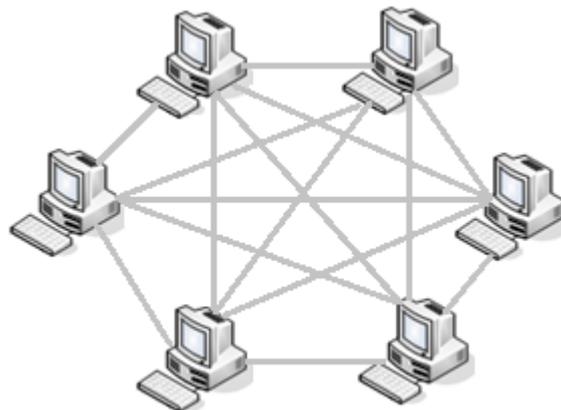


FIGURE 1.4 – Topologie maillée

1.5.2 Typologie des réseaux

✚ Les réseaux locaux (LAN : local area network)

Un LAN est un groupe d'ordinateurs connectés partageant une infrastructure de communication commune et des ressources dans une petite zone géographique comme votre domicile, par exemple. Les LAN peuvent s'articuler autour d'un serveur central qui contrôle toute l'activité ou bien du Peer-to-Peer où chaque machine gère ses propres ressources. Le standard de connexion le plus répandu est appelé Ethernet, de tels réseaux offrant en général une bande passante comprise entre 10Mbit/s et 100Mbit/s. [3]

✚ Les réseaux métropolitains (MAN : métropolitain area network)

Un réseau métropolitain MAN interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local. La bande passante peut être de quelque centaine de Kbit/s à quelques Mbit/s. [3]

✚ Les réseaux étendus (WAN : wide area network)

Les WAN connectent les systèmes sur une large zone géographique le réseau internet est par exemple, un WAN qui s'étend sur l'ensemble du globe et fonctionne comme une autoroute informatique véhiculant les données d'un LAN à l'autre. En règle générale, les utilisateurs de réseaux domestiques n'ont aucune espèce de contrôle sur les réseaux WAN est sur leurs périphériques. [3]

Il existe trois autres types de réseaux

- Les TAN (Tiny Area Network) identiques aux LAN mais moins étendus (2 à 3 machines),
- Les CAN (Campus Area Network) identiques au MAN (avec une bande passante maximale entre tous les LAN du réseau) ;
- Les SAN (Storage Area Network) identifiées au WAN mais ils permettent de transférer des données de haut débit sur une distance de 100 KM.

✚ Différence entre eux

	DISTANCE	TAUX DE PERTE	DEBIT
LAN	Inférieur à 1Km	N'est pas important	Entre 10Mbit/s et 100Mbit/s
MAN	Entre 1Km et 10Km	Moyen	De centaines de Kbit/s à quelque Mbit/s
WAN	Supérieur à 10KM	élevé	De quelque Kbit/s à quelque Mbit/s

TABLE 1.1- Différence entre les typologies réseaux

1.6 Différents types d'administration des réseaux

a - Point à Point (Peer-to-Peer ou P2P)

Les réseaux Point-à-Point permettent à des ordinateurs sur un réseau de partager leurs données et ressources. Chaque ordinateur sur un réseau de Point-à-Point stocke ses propres informations et ressources. Il n'y a aucun ordinateur central qui commande ou contrôle le réseau. Toutes les machines sur le réseau ont les mêmes droits. Si l'on considère l'un de ses postes est un serveur, c'est pour le but de partager les ressources, si non elle consomme les ressources d'autres postes.

b - Client / Serveur (Server based)

Il y a au moins un serveur central qui s'occupe de la sauvegarde de données, du partage de périphériques et de l'installation des services, etc.

Toutes les machines qui sont connectées au réseau sont contrôlées par ce serveur. Les serveurs effectuent la plupart des traitements et des tâches. La plupart des réseaux Client/serveur ont un (des) administrateur(s) de réseau pour prendre soin des tâches administratives quotidiennement.

1.7 Les différents architecteurs des réseaux

Le transport des données d'une extrémité à une autre d'un réseau nécessite un support physique ou hertzien de communication.

Pour que les données arrivent correctement au destinataire, avec la qualité de service, ou QoS (Quality of Service), exigée, il faut en outre une architecture logicielle chargée du contrôle des paquets dans le réseau.

Les trois grandes architectures suivantes s'épilouent actuellement le marché mondial des réseaux :

- ✚ l'architecture OSI (Open Systems Interconnection), ou interconnexion de systèmes ouverts, provenant de la normalisation de l'ISO (International Standardization Organization) ;
- ✚ l'architecture TCP/IP utilisée dans le réseau Internet ;
- ✚ l'architecture introduite par l'UIT (Union internationale des télécommunications) pour l'environnement ATM (Asynchronous Transfer Mode).

1.7.1 Le modèle de référence OSI

Cette architecture est introduite par l'ISO il y a plus de vingt ans et qui constitue toujours le modèle de référence pour décrire les éléments nécessaires à la réalisation d'une architecture réseau.

1.7.1.1. Définition du modèle OSI

Les concepts architecturaux utilisés pour décrire le modèle de référence à sept couches proposé par l'ISO sont décrits dans la norme ISO (7498). [1]

La figure suivante illustre cette architecture.

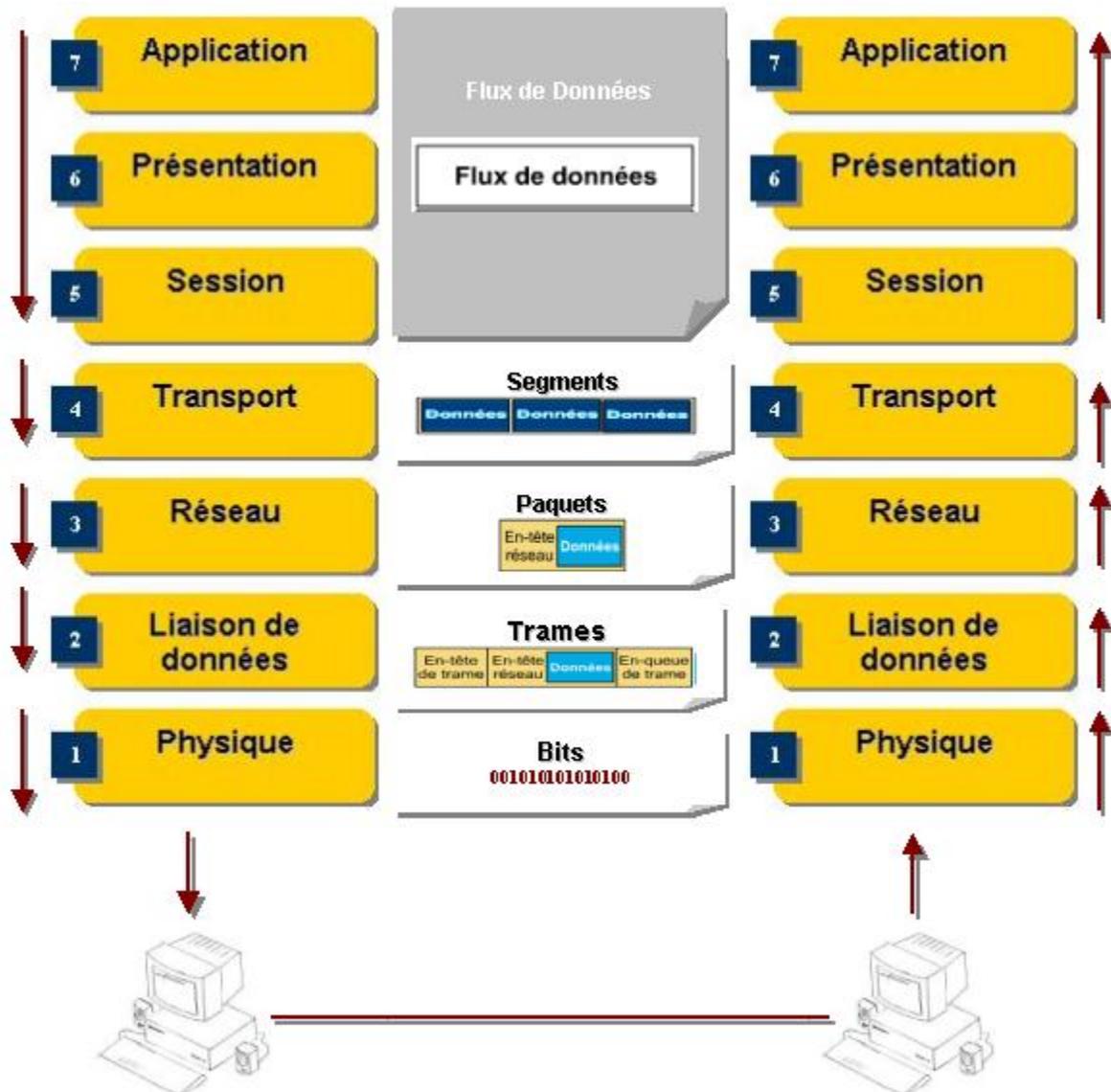


FIGURE 1.5 – Modèle OSI

1.7.1.2. Principe du modèle OSI

Les communications entre 2 machines utilisent des protocoles différents structurés en couche. Chaque couche fournit des services pour la couche au-dessus.

Chaque couche est responsable d'un aspect particulier de communication.

Quand des données sont transférées sur un réseau, elles doivent passer par chaque couche de modèle OSI.

Lorsque les données traversent chaque couche, l'information est ajoutée aux données.

Quand les données atteignent la destination, elles doivent encore passer par les couches de modèle OSI, et l'information additionnelle est enlevée à chaque couche.

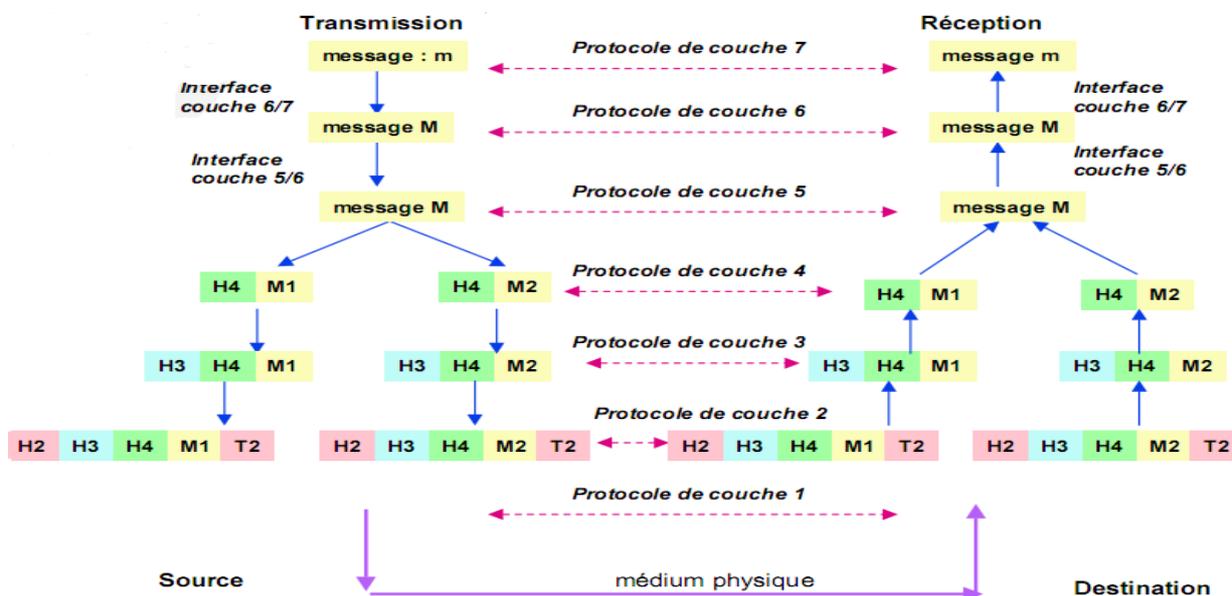


FIGURE 1.6 – Principe du modèle OSI

1.7.1.3. Les différentes fonctions de chaque couche

a - Couche physique

La couche PHYSIQUE (PHYSICAL LAYER) transmet des flux de bits bruts sur le support de communication. La couche PHYSIQUE est en relation directe avec la carte réseau.

Les fonctions de la couche PHYSIQUE

- La gestion du branchement au support.
- Le branchement du câble à la carte réseau.
- La définition du nombre de broches du connecteur.
- La fonction de chacune des broches du connecteur.
- La gestion des signaux, électriques, optiques, mécaniques.
- L'encodage et la synchronisation du flux de bits.
- La durée de chaque bit, les caractéristiques de l'impulsion électrique ou optique.
- La méthode d'accès des bits sur le support de communication.
- L'envoi des trames sur le réseau.

b - Couche liaison de données

La couche LIAISON (DATA LINK LAYER) gère le transfert des trames. Une trame (souvent synonyme de paquet) est une structure logique et organisée dans laquelle sont placées les données. La structure d'une trame (d'un paquet) est toujours la même. La trame est constituée de plusieurs éléments et dans un ordre précis.

Les fonctions de la couche LIAISON

- La préparation des trames pour la couche PHYSIQUE :
- La fabrication des trames en fonction de la méthode d'accès au réseau.
- La division des messages en trames de bits bruts ou leur regroupement.
- Le contrôle CRC des erreurs dans la transmission d'un paquet.
- L'envoi et la réception d'un accusé de réception pour chaque trame, sinon la trame est réexpédiée.

c - Couche réseau

La couche RESEAU (NETWORK LAYER) se charge de l'adressage des messages. La couche RESEAU fournit un schéma d'adressage. La couche RESEAU traduit les adresses logiques (les adresses IP) en adresses physiques (les adresses MAC des cartes réseaux).

Les fonctions de la couche RESEAU

- La traduction des adresses et des noms logiques en adresses physiques.
- Le routage des messages en fonction de leur priorité et de l'état du réseau.
- La gestion du trafic sur le réseau.
- La commutation de paquets.
- Le contrôle de l'encombrement des messages sur le réseau.
- Le découpage ou le réassemblage des messages en fonction de la capacité de carte réseau (et de celle de son correspondant).

d - Couche transport

La couche TRANSPORT (TRANSPORT LAYER) s'assure que les paquets ont été reçus dans l'ordre, sans erreurs, sans pertes, ni duplication. La couche TRANSPORT gère l'empaquetage et le réassemblage des paquets ainsi que le contrôle et la correction des erreurs.

Les fonctions de la couche TRANSPORT

- La division des messages longs en plusieurs paquets.
- Le contrôle de la taille des paquets.
- Le regroupement des messages courts en un seul paquet.
- Le rassemblement des paquets en un seul message.
- L'extraction et la reconstitution du message d'origine.
- L'envoi et la réception d'un accusé de réception.
- Le contrôle du flux et la correction des erreurs dans la reconstitution des paquets.

e - Couche session

La couche SESSION (SESSION LAYER) gère la connexion entre deux ordinateurs du réseau.

Les fonctions de la couche SESSION

- L'ouverture et la fermeture d'une connexion (d'une session).
- La reconnaissance des noms.
- La synchronisation des tâches utilisateur à l'aide de points de contrôle.
- Le contrôle du dialogue entre les processus communicants (qui transmet, à qui, à quel moment, pour combien de temps, ...).

f - Couche présentation

La couche PRESENTATION (PRESENTATION LAYER) détermine le format utilisé pour l'échange des données entre ordinateurs du réseau.

Les fonctions de la couche PRESENTATION

- La conversion du format issu de la couche APPLICATION en un format Standard.
- La conversion des protocoles.
- La traduction et l'encodage des données.
- La conversion du jeu de caractères.
- L'exécution des commandes graphiques.
- La compression ou la décompression des données.

Un utilitaire appelé « redirecteur » (REDIRECTOR) opère sur la couche PRESENTATION et permet de rediriger les opérations d'Entrée/Sortie vers les ressources d'un serveur. La couche PRESENTATION permet par exemple d'afficher des données UNIX sur un écran MS-DOS.

g - Couche application

La couche APPLICATION (APPLICATION LAYER) joue le rôle d'une interface d'accès des applications au réseau. La couche APPLICATION concerne les applications réseaux qui tournent sur un poste (TELNET, FTP,...), et correspond à l'interface de l'utilisateur.

Les fonctions de la couche APPLICATION

- La gestion des applications réseaux.
- Utilitaires de transfert de fichiers.
- Logiciels d'accès aux bases de données.
- Messagerie électronique.
- L'accès au réseau.
- Le contrôle du flux et la correction des erreurs.

1.7.2. Modèle TCP/IP

Dans les années 1970, le département de la Défense américain, ou DOD (Département Of Défense), décide, devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, de définir sa propre architecture.

Cette architecture, dite TCP/IP, est à la source du réseau Internet. Elle est aussi adoptée par de nombreux réseaux privés, appelés intranet. Les deux principaux protocoles définis dans cette architecture sont les suivants :

- IP (Internet Protocol), de niveau réseau, qui assure un service sans connexion.
- TCP (Transmission Control Protocol), de niveau transport, qui fournit un service fiable avec connexion. TCP/IP définit une architecture en couches qui inclut également, sans qu'elle soit définie explicitement, une interface d'accès au réseau.

TCP/IP ne suit pas directement le modèle OSI parce que la normalisation OSI lui est postérieure. Cependant cette famille de protocole suit également un schéma en couche :

1.7.2.1 Les différentes fonctions de chaque couche

a - Couche Hôte _ Réseau

Ensemble des routines d'accès au média, cette couche correspond à la couche physique et liaison de donnée de modèle OSI.

b - Couche Internet

Définie les datagrammes et leur routage, Elle correspond à la couche réseau de modèle OSI.

c - Couche Transport

Assure le transfert d'un site à un autre, Elle correspond à la couche transport et session de modèle OSI.

d - Couche Application

Applications utilisées sur le réseau, Cette couche correspond aux deux couches : session Présentation et application de modèle OSI.

1.7.3. Similitudes et différences entre le modèle OSI et TCP/IP

Les modèles OSI et TCP/IP présentent un grand nombre de similitudes:

-  Tous deux comportent des couches.
-  Tous deux comportent une couche application, bien que chacune fournisse des services différents.
-  Tous deux comportent des couches réseau et transport comparables.
-  Tous deux s'appuient sur un réseau à commutation de paquets, et non sur un réseau à commutation de circuits.

Ils présentent également quelques différences:

- ✚ TCP/IP intègre les couches application, présentation et session du modèle OSI dans sa couche application.
- ✚ TCP/IP regroupe les couches physiques et liaison de données du modèle OSI dans sa couche d'accès au réseau.
- ✚ TCP/IP semble plus simple, car il comporte moins de couches.
- ✚ Lorsque la couche transport du protocole TCP/IP utilise le protocole UDP, la transmission des paquets n'est pas fiable tandis qu'elle est toujours fiable avec la couche transport du modèle OSI.

1.8 Sécurité des réseaux informatiques

Avec la généralisation d'Internet et des moyens de communication modernes, une nouvelle forme d'insécurité s'est répandue, elle s'appuie sur l'utilisation de codes informatiques pour perturber ou pénétrer les réseaux et les ordinateurs.

Les problématiques de sécurité sont de plus en plus nombreuses et les attaques liées à l'ouverture des réseaux informatique sont de plus en plus fréquentes.

1.8.1 Les attaques réseaux

Les attaques réseaux sont très nombreuses, elles touchent généralement les trois composantes suivantes d'un système : la couche réseau, en charge de connecter le système au réseau, le système d'exploitation, en charge d'offrir un noyau de fonction au système, et la couche applicative, en charge d'offrir des services spécifiques. [4]

L'objectif est de présenter les faiblesses les plus couramment exploitées par les attaques et les mécanismes de ces attaques. La figure suivante illustre ces faiblesses :

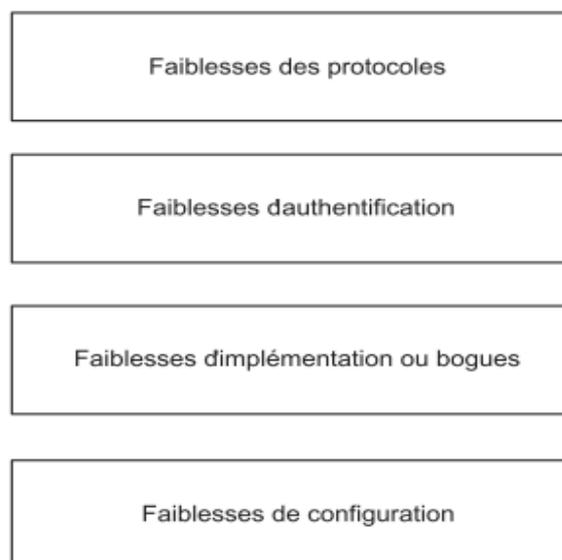


FIGURE 1.7 – Les faiblesses exploitées par les attaques réseau

1.8.1.1 Faiblesses des protocoles :

Les protocoles réseau n'ont pas été conçus pour tenir compte des problèmes de sécurité. Le protocole IP, par exemple, ne comporte pas de couche sécurité. La plupart des protocoles utilisés dans un réseau, tels SNMP (Simple Network Management Protocol) pour l'administration et la supervision des réseaux, n'implémentent pas de véritable couche de sécurité et s'exposent à diverses attaques, tels que : les attaques par fragmentation, déni de service, etc.

1.8.1.2 Faiblesses d'authentification :

Les versions actuelles des protocoles IP ou ICMP ne disposent pas de mécanisme d'authentification, c'est pour quoi elles subissent des attaques s'appuyant sur ces faiblesses, comme les attaques : ARP, man-in-the-middle, spoofing...etc

1.8.1.3 Faiblesses d'implémentation :

Le développement des logiciels et des protocoles réseaux se base souvent sur l'aspect fonctionnel sans tenir compte de la sécurité ce qui entraine de grandes faiblesses. Parmi les attaques qui exploitent ce genre de faiblesse on trouve : Attaque sur les bogues des piles TCP/IP

1.8.1.4 Faiblesses de configuration :

Une mauvaise configuration des équipements réseaux, pare-feu, routeur, etc., est souvent exploitée pour mener des attaques. Les erreurs de configuration peuvent être de plusieurs natures, incluant l'erreur humaine, par conséquent les équipements réseau ne doivent être accèdes ou configurés que par des acteurs autorisés.

1.8.2 Analyse des risques et objectifs de la sécurité

La détermination des éléments critiques d'une entreprise est une tâche délicate et qui est prête à la discussion, chaque service ou département se considérant souvent comme un secteur clé. Un bon moyen pour y parvenir consiste à mener avec les responsables de l'entreprise une analyse des risques. Une telle analyse consiste tout d'abord à identifier les ressources ou les biens vitaux de l'entreprise. Ces derniers peuvent être de plusieurs ordres :

- ✓ matériel (ordinateurs, équipements réseau, etc.) ;
- ✓ données (bases de données, sauvegardes, etc.) ;
- ✓ logiciels (sources des programmes, applications spécifiques, etc.) ;
- ✓ personnes (salariés, personnel en régie, etc.).

Une fois les éléments critiques et les objectifs de sécurité identifiés, il convient, pour chacune des ressources vitales, d'associer les trois éléments suivants, qui visent à définir l'analyse de risques proprement dite, telle que définie par l'ISO comme la combinaison de la probabilité d'un événement et de ses conséquences :

- ✚ **Menace.** La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant, qu'il soit interne ou externe. La probabilité qu'un événement exploite une faiblesse de sécurité est généralement évaluée par des études statistiques, même si ces dernières sont difficiles à réaliser.
- ✚ **Vulnérabilité.** Il s'agit d'une faiblesse de sécurité qui peut être de nature logique, physique, etc. Une vulnérabilité peut découler, par exemple, d'une erreur d'implémentation dans le développement d'une application, erreur susceptible d'être exploitée pour nuire à l'application (pénétration, refus de service, etc.). Elle peut également provenir d'une mauvaise configuration, etc.
- ✚ **Conséquence.** Il s'agit de l'impact (perte financière, dommages sur l'image de marque, etc.) sur l'entreprise de l'exploitation d'une faiblesse de sécurité

1.8.3 Principes génériques d'une politique de sécurité réseau

La politique de sécurité réseau vise à satisfaire les critères suivants :

- ✚ **Identification.** Information permettant d'indiquer qui vous prétendez être. Une identification élémentaire est le nom d'utilisateur que l'on saisit dans un système informatique. Une identification plus évoluée peut être fournie par un relevé d'empreinte digitale, une analyse faciale ou rétinienne, etc.
- ✚ **Authentification.** Information permettant de valider l'identité pour vérifier que vous êtes celui que vous prétendez être. Une authentification élémentaire est le mot de passe que vous entrez dans le système informatique. Une authentification forte combine une chose que vous possédez et une chose que vous connaissez (numéro de carte bancaire et code personnel, par exemple).
- ✚ **Autorisation.** Information permettant de déterminer quelles sont les ressources de l'entreprise auxquelles l'utilisateur identifié et autorisé a accès, ainsi que les actions autorisées sur ces ressources. Cela couvre toutes les ressources de l'entreprise.
- ✚ **Confidentialité.** Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données.
- ✚ **Intégrité.** Ensemble des mécanismes garantissant qu'une information n'a pas été modifiée.
- ✚ **Disponibilité.** Ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles, que ces dernières concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc.
- ✚ **Non-répudiation.** Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.
- ✚ **Traçabilité.** Ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure. [4]

1.8.4 Typologie des politiques de sécurité réseau

Une politique de sécurité peut être trop permissive ou au contraire trop restrictive. Dans le premier cas, elle risque de présenter une faiblesse de sécurité par son côté laxiste. Dans le second, elle peut devenir inapplicable du fait de règles trop strictes. Toute déviation de la politique de sécurité fait l'objet d'une revue spécifique afin de corriger la faiblesse de sécurité engendrée et les exceptions associées. Une politique de sécurité réseau couvre les éléments suivants :

- ✚ **Sécurité de l'infrastructure.** Couvre la sécurité logique et physique des équipements et des connexions réseau, qu'elles soient internes ou fournies par les FAI.
- ✚ **Sécurité des accès.** Couvre la sécurité logique des accès locaux et distants aux ressources partagés entre les entreprises, ainsi que la gestion des utilisateurs et de leurs droits d'accès au système d'information de l'entreprise.
- ✚ **Sécurité du réseau intranet face à Internet ou aux tierces parties.** Couvre la sécurité logique des accès aux ressources de l'entreprise (extranet) et l'accès aux ressources extérieures (Internet). [6]

1.8.5 Proposition de stratégies de sécurité réseau

Nous commençons par définir un périmètre autour de réseau d'entreprise (intranet) face au réseau internet. Nous définissons également des périmètres de sécurité pour chacun des sous réseau inclus dans le réseau.

- ✚ **Stratégie des périmètres de sécurité :** Nous définissons également des périmètres de sécurité pour chacun des sous-réseaux inclus dans le réseau intranet, Notre objectif est de compartimenter le réseau et de créer une imbrication des périmètres de sécurité afin de rendre plus difficile une pénétration éventuelle.
- ✚ **Stratégie des goulets d'étranglement :** Les contrôles d'accès définissent ce qu'il est autorisé de faire pour entrer dans un périmètre de sécurité du réseau. Nous partons du postulat que « **tout ce qui n'est pas autorisé est interdit** ». Les contrôles d'accès définissent par ailleurs les conditions à respecter pour avoir le droit d'entrer dans le périmètre de sécurité.
- ✚ **Stratégie de moindre privilège :** « *Un utilisateur ne dispose que des privilèges dont il a besoin.* » De nos jours, un utilisateur au sein de l'entreprise est toujours relié au réseau interne, lequel héberge les stations de travail des utilisateurs, mais également les serveurs locaux, de fichiers et d'impression, par exemple, ou globaux, associés à l'activité de l'entreprise, offrant également un accès à Internet. L'application stricte de cette stratégie, dans laquelle un utilisateur dispose du droit d'accès à un système spécifique et à aucun autre, est généralement difficile à réaliser de manière globale.
- ✚ **Stratégie de confidentialité des flux réseau :** Tout message qui doit être émis à l'extérieur ou vers d'autres réseaux doit être protégé. Pour y parvenir, le message doit être chiffré au moyen d'une table alphabétique de substitution uniquement connue de l'émetteur et du récepteur.

- ✚ **Stratégie Antivirus :** Tout document numérique ou tout autre vecteur de propagation de virus fait l'objet d'un contrôle avant de pénétrer dans un périmètre de sécurité.

Les virus peuvent entrer et se propager dans l'entreprise par de multiples vecteurs tels que les suivants :

- ✓ Média amovible (disquette, CD-ROM, DVD-ROM, clé USB, etc.) ;
- ✓ Courrier électronique ;
- ✓ Navigateur Internet (utilisation d'une application hostile en langage Java ou autre) ;
- ✓ Accès distant au réseau de l'entreprise (utilisateur itinérant) ;
- ✓ Téléchargement de fichier infecté.

Les logiciels antivirus peuvent être placés en plusieurs endroits, tels que les suivants :

- ✓ Points d'interconnexion entre le réseau intranet et Internet ;
- ✓ Autres points d'interconnexion (accès distant, etc.) ;
- ✓ Relais de messagerie interne ;
- ✓ Stations de travail ;
- ✓ Serveurs de fichiers et d'impressions ;
- ✓ Serveur, quelque soit leurs fonctions.

- ✚ **Stratégie de participation universelle :** Des campagnes d'information et de sensibilisation à la sécurité sont lancées afin de faire comprendre les risques que font peser sur l'entreprise les menaces extérieures.

Une campagne d'information et de sensibilisation de la sécurité vise à inciter les employés à :

- ✓ Verrouiller leur station de travail lorsqu'ils ne l'utilisent pas.
- ✓ Ne laisser entrer aucune personne qui ne possède pas de badge de l'entreprise, et signaler toute personne qui ne possède pas de badge de l'entreprise aux services de sécurité.
- ✓ Ne pas installer de logiciel sur leur station de travail.
- ✓ Ne pas s'échanger de fichiers par d'autres moyens que ceux en place.
- ✓ Utiliser un mot de passe non trivial.
- ✓ Ne pas inscrire leur mot de passe sur un papier collé sur leur écran ou leur bureau.
- ✓ Ne pas laisser les fenêtres ouvertes lorsqu'elles débouchent sur un toit.
- ✓ Ne pas bloquer en position ouverte les portes qui doivent rester fermées (salle machine, etc.).

- ✚ **Stratégie de contrôle régulier**

La stratégie de contrôle régulier consiste à simuler des tentatives de pénétration surprises afin de vérifier le bon fonctionnement des mécanismes de sécurité.

L'application de la politique de sécurité est validée par un contrôle de sécurité régulier.

1.9 Conclusion

Dans ce chapitre nous nous sommes intéressés aux réseaux informatique, à la communication au sein de ces réseaux et aux modèles et standards de communication les plus utilisés. Nous avons aussi vu les différents types de réseaux et les différentes politiques de la sécurité utilisés.

Chapitre 2

Concepts fondamentaux de partage des ressources

PARTIE 1
THEORIQUE

2.1 Introduction

Dans ce chapitre nous allons aborder dans la partie théorique les concepts fondamentaux de partage des ressources ainsi que les équipements d'interconnexion nécessaires et leurs caractéristiques, ensuite on passera au partage des ressources sur les équipements pratiquement dans la deuxième partie.

2.2 Définition des termes

2.2.1. Ressource informatiques

Les moyens informatiques locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par un établissement.

- **Ressource internet :** Une ressource Internet est un élément d'intérêt pour un internaute et qui est disponible dans un des sites Internet du réseau. Une ressource Internet peut être un système de recherche (Gopher, Web), un navigateur Web, une base de données accessible par FTP, ou même un correspondant lors d'une session de dialogue en direct. [1]
- **Autres types de ressources**
 - Un temps du processeur
 - Une mémoire vive et virtuelle
 - Un espace du disque dur
 - Un périphérique externe

2.2.2 Définition de matériel informatique

Le matériel informatique est l'ensemble des composants formant la partie matérielle (physique) d'un ordinateur, contrairement au logiciel qui concerne les composants logiques (intangibles). Toutefois, le concept est entendu d'une manière plus ample et est utilisé pour désigner tous les composants physiques d'une technologie.

Dans le cas de l'informatique et des ordinateurs personnels, le terme matériel désigne non seulement les composants physiques internes (disque dure, carte mère, microprocesseur, circuits, câbles, etc.), mais aussi les périphériques (scanners, imprimantes).

Le matériel informatique peut être soit basique (les dispositifs nécessaires pour faire marcher l'ordinateur) soit complémentaire (pour réaliser des fonctions spécifiques).

Concernant les types de matériel informatique, nous retiendrons les dispositifs d'entrée (ceux qui permettent de saisir des informations dans le système, comme le clavier et la souris, les dispositifs de sortie (ceux qui montrent à l'utilisateur le résultat de tout un ensemble d'opérations réalisées dans l'ordinateur. Exemple: écran, imprimante), les dispositifs d'entrée et de sortie (modem, cartes réseau, mémoires USB), l'unité centrale de traitement ou CPU (les composants qui interprètent les instructions et qui traitent les données) et la mémoire vive ou RAM (qui est utilisée pour stocker provisoirement l'information). [5]

2.3 Eléments de réseaux

Un réseau informatique est caractérisé par un aspect matériel : le matériel réseau (des câbles, des ordinateurs, des ressources...), c'est-à-dire les éléments physique qui composent le réseau, et un aspect logiciel : les protocoles de communication. Notons que chaque type de réseau nécessite un matériel spécial ainsi que des protocoles bien déterminés. [6]

2.3.1. Serveurs

Les serveurs sont des ordinateurs puissants qui fournissent des ressources partagées aux utilisateurs. Ils disposent d'une carte réseau, d'un ou plusieurs processeurs, d'une mémoire vive importante, de plusieurs disques durs et des composants logiciels de communication. Ils sont sécurisés par une alimentation régulée par un onduleur et des composants redondants (alimentation, disques durs). Un serveur assume un seul ou plusieurs des tâches suivantes :

- ✚ Serveur de fichiers : stockage des données des utilisateurs.
- ✚ Serveurs d'impression : stocke les files d'attente, gère les quotas des utilisateurs.
- ✚ Serveurs d'authentification : gère les connexions des utilisateurs.

2.3.2 Clients

Tout type d'ordinateur ou de terminal, quel que soit son système d'exploitation (Windows, linux, MacIntosh), muni d'une carte réseau et des composants logiciels de communication. Les clients accèdent aux ressources partagées fournies par un serveur de réseau.

2.3.3 Liaisons

Les liaisons s'effectue à l'aide de câble (liaison filaire exemple paire torsade, fibre optique, câble coaxial, ...) ou sans câble (radio, infra-rouge).

Pour relier un ordinateur a un réseau, il faut aussi disposer d'une carte réseau. Elle comporte à son extrémité un connecteur (port) qui permet d'insérer un câble du réseau. Une carte réseau est une interface qui permet de connecter un ordinateur au support de transmission utilisé par le réseau. Elle contrôle le flux d'information qui circule entre l'ordinateur et le réseau.

2.3.4 Données partagées

Ce sont des fichiers accessibles sur les serveurs du réseau. Les données des utilisateurs ne sont plus stockées sur un disque dur local mais sur des espaces de stockage hébergés par des serveurs (disque dur,CD-Rom) ou archivées sur des supports amovibles (bandes, CD-RW, DVD-RW).

2.3.5 Imprimantes et autres périphériques partagés

Les imprimantes sont des autres ressources (en outre de données partagées) fournies par des serveurs. Dans un souci de diminution des coûts, certains périphériques ne sont plus rattachés à l'ordinateur mais partagés pour plusieurs postes. C'est le cas des imprimantes, des tours de CD-Rom,...

2.3.6 Protocoles de communication

Les protocoles de communication sont des spécifications qui permettent à plusieurs machines de communiquer. Dans un environnement hétérogène aussi bien matériel avec des composants de technologies différentes que logicielles (système d'exploitation, logiciels), les normes de communication sont standardisées afin de faciliter l'échange des flux d'information. Les plus utilisés aujourd'hui : DNS, DHCP, SMTP, POP, HTTP, FTP, sont bâtis autour de TCP/IP : Transfert Composant Protocol / Internet Protocol.

2.3.7 Équipements d'interconnexion

L'interconnexion de réseaux peut être locale: les réseaux sont sur le même site géographique. Dans ce cas, un équipement standard (exp. répéteur, routeur) suffit à réaliser physiquement la liaison. L'interconnexion peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (exp. modems).

- **Modem** : Les modems (modulateur/démodulateur) permettent aux ordinateurs d'échanger des données par l'intermédiaire des réseaux téléphoniques. Le modem émetteur a pour rôle de convertir les données de l'ordinateur (données numérique) pour les rendre transmissibles à travers la ligne téléphonique (signaux analogiques). Le modem récepteur a pour rôle de convertir les signaux analogiques qu'il reçoit de la ligne téléphonique en information exploitable pour l'ordinateur (signaux numériques).
- **Répéteur** : Un des problèmes les plus gênants lors de la construction d'un réseau est la limitation en terme de distance qui est introduite par les médiums de communication. En effet, plus un câble est long, plus l'atténuation du signal qui circule sur ce câble va être grande. Un des moyens de pallier cet inconvénient est l'utilisation de la fibre optique qui subit une atténuation moindre. La solution réside dans un appareil se nommant « répéteur ». Un répéteur a pour rôle de faire suivre les signaux transmis sur un réseau en empêchant toute perte de signal. Parmi ses caractéristiques on peut citer :
 - ✓ Amplification et régénération du signal d'origine pour lui permettre de voyager sur de plus longues distances dans le média.
 - ✓ Possibilité de changer de média (passer d'un câble coaxial à une paire torsadée). Il constitue ainsi un prolongement du réseau existant.

- **Pont** : Un pont est un appareil qui permet aux ordinateurs d'un réseau d'échanger des informations :
 - ✓ Création d'inter réseaux : Les ponts servent à relier les réseaux isolés pour leur permettre de fonctionner ensemble sous la forme d'un même grand réseau. Subdivision d'un réseau existant : il est également possible de subdiviser un réseau surchargé en parties plus petites. Cette subdivision permet de réduire le volume des informations qui doivent circuler dans chaque partie du réseau.
 - ✓ Filtrage : les ponts déterminent si les informations à transmettre doivent rester au sein du même réseau ou s'il faut les faire passer de l'autre côté du pont. Lorsque l'ordinateur de destination fait partie du réseau situé de l'autre partie du pont, le pont fait suivre les informations à ce réseau.

Les ponts améliorent ainsi les performances des réseaux qu'ils séparent en ne faisant suivre les informations à un réseau donné que lorsque c'est nécessaire.

- **Concentrateur (hub) et commutateur (Switch)** : Un hub ou un Switch est un système de connexion centralisé où se rejoignent tous les câbles. Les réseaux modernes utilisent presque tous ce type d'équipement. Il possède généralement 4, 8, 16 ou 32 ports. Pour connecter un ordinateur au réseau, il suffit de connecter un câble qui part de la carte réseau à une prise murale qui est connectée au hub ou Switch. Le hub constitue un « répéteur multiport » car tout signal reçu sur un port est répété (diffusé) sur tous les autres ports. Un message émis par un ordinateur est reçu par tous les autres ordinateurs, mais seul la destination tient compte du message en faisant une copie. Les autres ordinateurs ignorent le message. Un Switch constitue un « pont multiport » car il filtre le trafic pour l'acheminer uniquement vers son destinataire.
- **Passerelle** : Une passerelle est une interface qui permet de relier des réseaux de types différents. Ainsi, il est possible d'utiliser une passerelle pour transférer des informations entre un réseau de Macintosh et un réseau PC. Lorsque le réseau ne parvient pas à reconnaître la destination des informations, il transmet ses informations à une passerelle par défaut.
- **Routeur** : Un routeur permet de relier différents réseaux les uns aux autres. Il a pour rôle de diriger les informations dans la direction appropriée. Les informations peuvent souvent emprunter plusieurs chemins. Beaucoup de routeurs permettent de brancher directement un ordinateur pour entrer ses informations. Les routeurs réalisent une cartographie des réseaux et ils les subdivisent en segments. Chaque segment reçoit une adresse qui lui est propre. L'adresse du segment du réseau et celle de l'ordinateur destination aident le routeur à calculer le meilleur chemin pour acheminer les données.

2.4 Les types de réseau

Le type de réseau dépendra du matériel dont vous disposez.

2.4.1 Réseau avec infrastructure

Un ou plusieurs ordinateurs reliés à un modem routeur ADSL (ou un modem ADSL Ethernet relié à un routeur).

Le mode Infrastructure mène à l'échange de données, au jeu en réseau, mais aussi au partage de connexion Internet et/ou d'une imprimante sur plusieurs ordinateurs. [7]

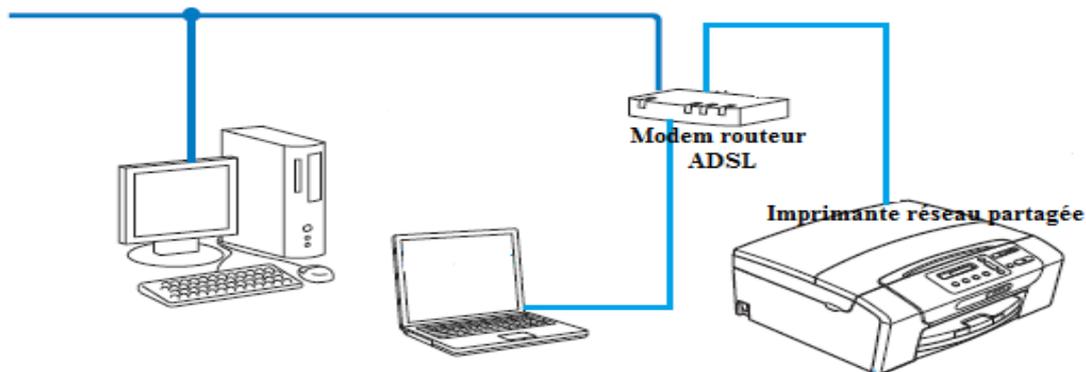


FIGURE 2.1- Réseaux avec infrastructure

2.4.1.1 Réseaux sans fil avec infrastructure

Ce type de réseau est composé des sites (hôte) fixes formant des réseaux filaire et des sites mobiles.

En général les sites fixes, appelés stations de bases, sont munis d'une interface de communication sans fil avec les sites mobiles qui se trouvent dans sa zone géographique. Par contre les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire. Quand l'imprimante sans fil se trouve sur ce type de réseau, il reçoit toutes les tâches d'impression via un point d'accès.

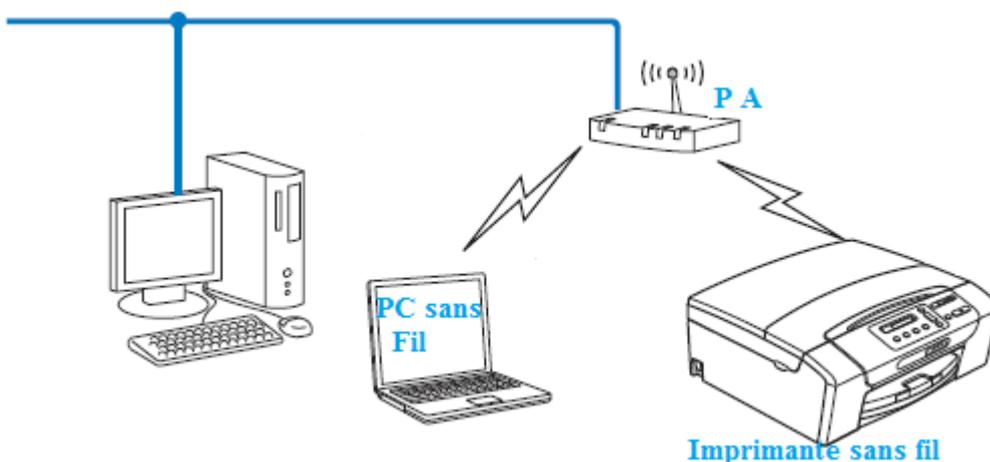


FIGURE 2.2 – Réseaux sans fil avec infrastructure

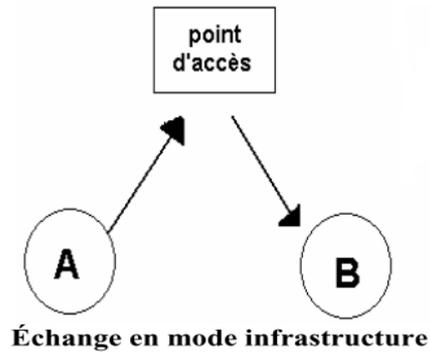


FIGURE 2.3 – Echange en mode infrastructure

2.4.2 Réseaux sans infrastructure (Le mode Ad-Hoc)

Ad hoc (aussi appelé Peer to Peer ou ordinateur à ordinateur), dans lequel les ordinateurs sont directement connectés les uns aux autres, par câble ou par CPL (Courant Porteur en Ligne), une technologie qui utilise l'installation électrique existante de votre habitation pour transporter en tout confort des données numériques (audio, vidéo, Internet, fichiers) au sein d'un réseau personnel sécurisé sans aucun routeur. Le mode Ad hoc mène à l'échange de données ou au jeu en réseau entre deux ordinateurs.

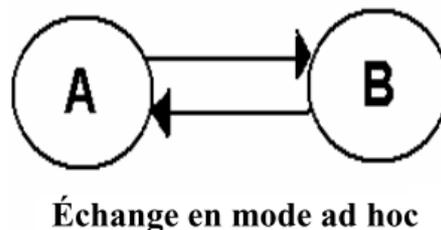


FIGURE 2.4 – Echange en mode Ad-hoc

2.4.2.1 Réseaux sans fils et sans infrastructure

Ce type de réseau n'a pas de point d'accès central. Les clients sans fil communiquent directement entre eux. Si une imprimante sans fil se trouve sur ce type de réseau, elle reçoit directement toutes les tâches d'impression de l'ordinateur qui envoie les données d'impression.

Un réseau ad hoc mobile, appelé généralement MANET (Mobile Ad hoc NETWORK), est un réseau composé de nœuds mobiles dont le seul moyen de communication est l'utilisation des interfaces sans fil ayant aucune infrastructure ou administration centralisée. Les nœuds, ayant le même rôle qu'un routeur dans les réseaux fixes, peuvent se déplacer aléatoirement, s'auto-organiser arbitrairement et d'une manière parfois imprévisible. Les MANets sont généralement déployés dans des scénarios de secours (incendies, tremblement de terre etc.), opérations temporaires ou tout simplement s'il n'y a pas de ressources pour établir un réseau avec infrastructure. A cause de l'absence d'infrastructure, l'installation de ces types de réseaux s'avère facile.

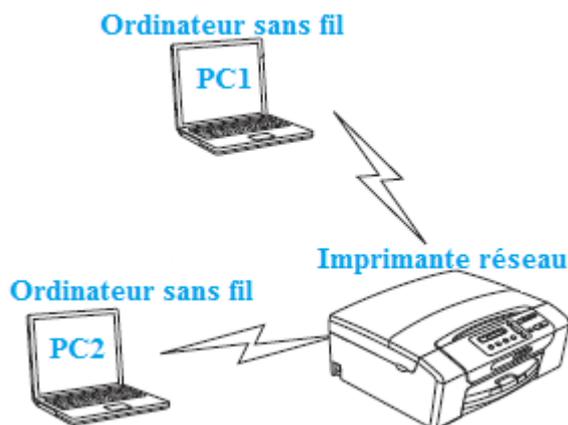


FIGURE 2.5 – Réseaux sans fil et sans infrastructure

2.5 Type d'imprimante réseau

- a- Imprimante partage en réseau (Serveur d'impression) :** Dans un environnement partagé en réseau, chaque ordinateur envoie les données via un ordinateur contrôlé de façon centrale. Ce type d'ordinateur est souvent appelé un « SERVEUR » ou un « SERVEUR D'IMPRESSION ». son rôle consiste à contrôler toutes les tâches d'impression.

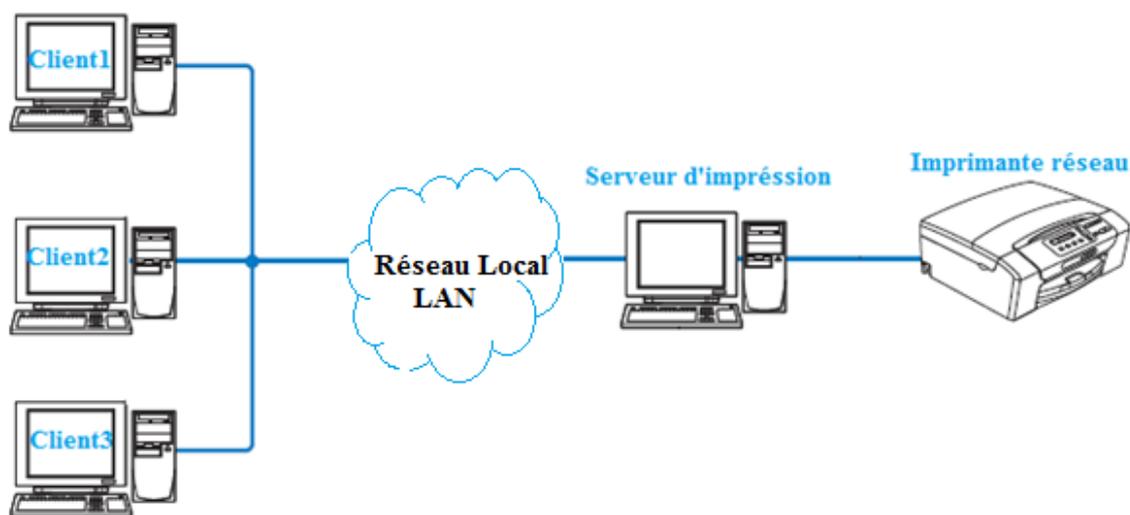


FIGURE 2.6 – Serveur d'impression

Il existe deux types de partage d'imprimante réseau selon l'architecture du réseau.

- b- L'imprimante partagée :** (on peut voir l'imprimante par le voisinage réseau) par le biais d'une file d'attente, ou nom de partage

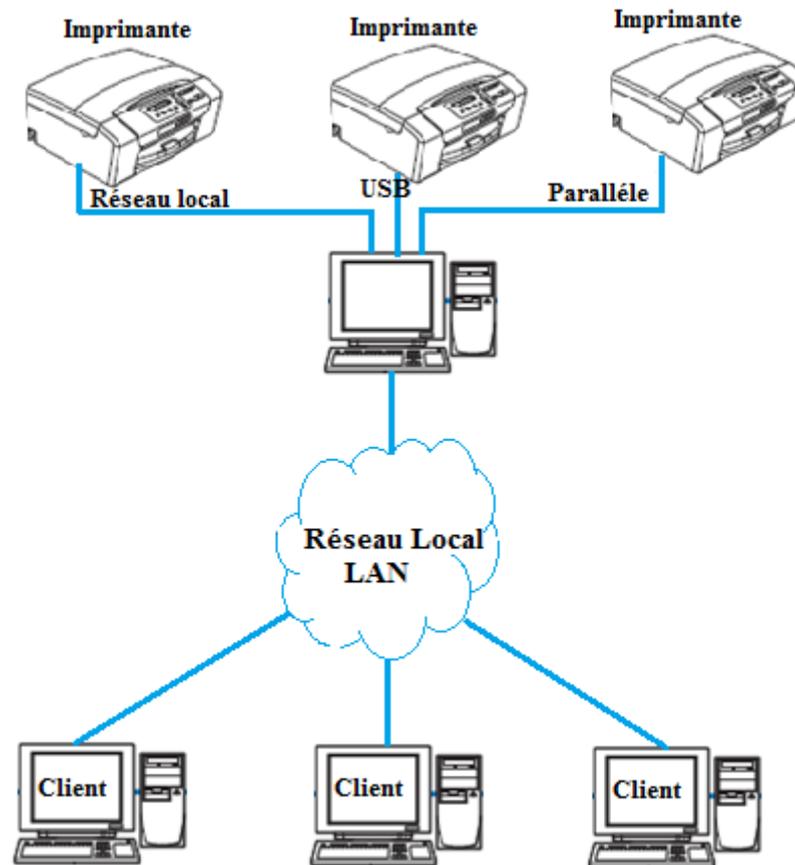


FIGURE 2.7 – Imprimantes partagées

c- L'imprimante dans un réseau Peer-to-Peer : Dans un environnement Peer-to-Peer, chaque ordinateur échange directement les données avec chaque appareil. Il n'y a pas de serveur central contrôlant l'accès aux fichiers ou le partage des imprimantes.

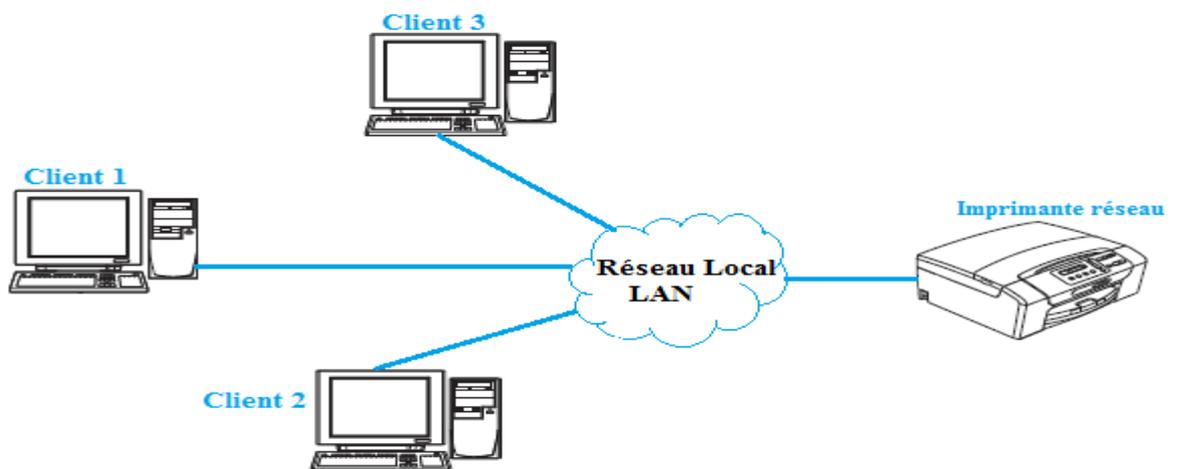


FIGURE 2.8 – Imprimante Peer-to-Peer

- ✚ Sur un réseau plus petit comprenant 2 ou 3 ordinateurs, nous recommandons la méthode d'impression Peer to Peer car elle est plus facile à configurer que la méthode d'impression partagée en réseau.
- ✚ Chaque ordinateur doit utiliser le protocole TCP/IP.
- ✚ Il faut configurer une adresse IP appropriée pour l'imprimante et les ordinateurs.
- ✚ Si vous utilisez un routeur (switch, hub ...), il faut configurer l'adresse de la passerelle sur les ordinateurs et sur l'imprimante réseau.

2.6 Conclusion

Dans cette première partie nous avons vu ce qu'étaient le partage et les équipements nécessaire pour un bon fonctionnement de ceux-ci. Au sein d'un réseau ne se limite pas au simple fait de transmettre et de partager des données mais il y'a de nombreux mécanismes qui entre en jeu.

PARTIE 2
PRACTIQUE

2.7 Partager une connexion ADSL, dossiers ou imprimantes sous Windows 7

Pour créer un réseau d'ordinateurs, partager des données, une imprimante ou une connexion ADSL entre des ordinateurs équipés de **Windows 7**, il n'est pas indispensable que les ordinateurs appartiennent au même **groupe résidentiel**. En revanche, si vous effectuez le partage entre **Windows 7** et un système d'exploitation antérieur, veillez à bien définir le même groupe résidentiel sur tous vos ordinateurs.

Avant d'effectuer la procédure de partage, assurez-vous d'avoir les droits administrateur.

2.7.1 Partager une connexion ADSL, dossiers et imprimantes dans un réseau de type Infrastructure

Si vous disposez d'un modem routeur ou d'un routeur connecté à un modem et d'un ou plusieurs ordinateurs, votre réseau sera par défaut en mode Infrastructure. Dans ce mode, les ordinateurs sont connectés à votre point d'accès, votre modem routeur ou votre routeur connecté à un modem. Le mode Infrastructure est idéal pour échanger des données, jouer en réseau, mais aussi pour partager une connexion Internet et/ou une imprimante sur plusieurs ordinateurs.

Les étapes à suivre sont :

- Accédez au Centre Réseau et partage. Pour ce faire, sélectionnez le menu Démarrer/Panneau de configuration.
- Cliquez sur la rubrique Réseau Internet, puis Centre Réseau et partage. Dans la fenêtre Centre Réseau et partage, cliquez sur le lien Connexion au réseau local, comme elle est illustré dans la figure 2.9.

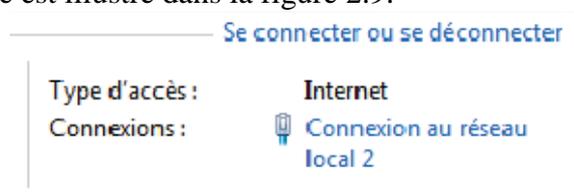


FIGURE 2.9 - Connexion au réseau local

- Dans la fenêtre État de Connexion au réseau local, cliquez sur Propriétés.
- Dans l'onglet Propriétés de Connexion au réseau local, sélectionnez Protocole Internet version 4 (TCP/IPv4).
- Cliquez sur Propriété.
- Dans la fenêtre Propriétés de Protocole Internet version 4 (TCP/IPv4), sélectionnez Obtenir une adresse IP automatiquement et Obtenir les adresses des serveurs DNS automatiquement.
- Cliquez sur OK pour valider.
- Dans la fenêtre partage cocher les deux cases, puis cliquer sur OK pour valider

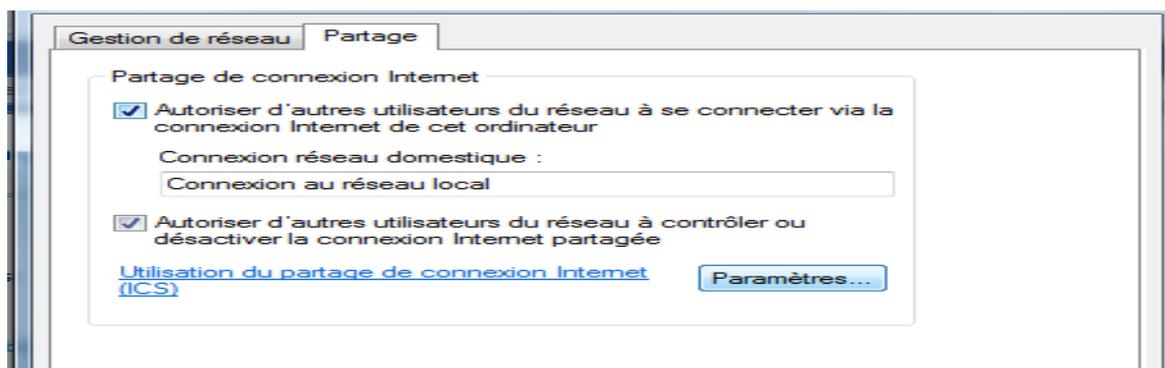


FIGURE 2.10 – Fenêtre de partage de connexion

Avant de mettre en partage vos dossiers, votre imprimante ou votre connexion, vous devez activer le partage depuis le Centre Réseau et partage.

- Pour ouvrir le Centre Réseau et partage, cliquez sur l'icône de réseau dans la Barre des tâches Windows, puis sur le lien Ouvrir le Centre Réseau et partage.

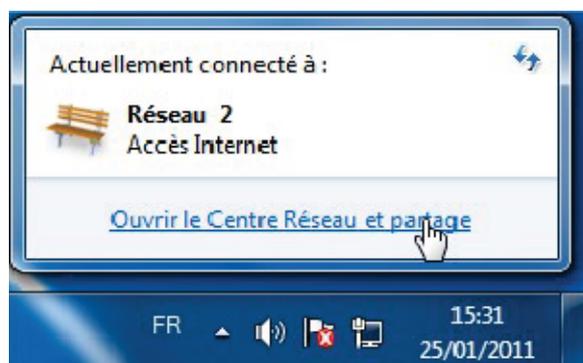


FIGURE 2.11 – Fenêtre pour l'ouverture de centre de partage

- Pour activer le partage d'imprimante, vous devez avoir préalablement installé une imprimante.
 - ✓ Cliquez sur le lien Modifier les paramètres de partage avancés.
 - ✓ Dans la zone Partage de fichiers et d'imprimantes, sélectionnez Activer le partage de fichiers et d'imprimantes.

Partage de fichiers et d'imprimantes

Lorsque le partage de fichiers et d'imprimantes est activé, toute personne sur le réseau peut accéder aux fichiers et aux imprimantes que vous avez partagés à partir de cet ordinateur.

- Activer le partage de fichiers et d'imprimantes
- Désactiver le partage de fichiers et d'imprimantes

FIGURE 2.12 – Fenêtre de partage de fichiers et d'imprimantes

Un dossier public est un dossier que d'autres utilisateurs de cet ordinateur ou du même réseau peuvent partager.

- Dans la zone Partage de dossiers publics, sélectionnez Activer le partage afin que toute personne avec un accès réseau puisse lire et écrire des fichiers dans les dossiers Public (le contenu de ces dossiers ne contiendra aucune limitation en termes de consultation, d'écriture ou autre).

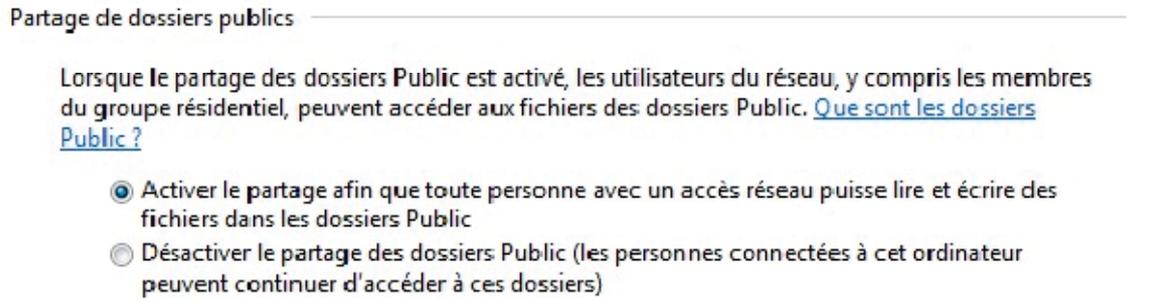


FIGURE 2.13 – Fenêtre de partage de dossiers publics

- Cliquez ensuite sur le bouton Enregistrer les modifications avant d'activer le partage des fichiers multimédias.

2.7.1.1 Création d'un groupe résidentiel

- Accédez au groupe résidentiel. Pour ce faire, sélectionnez le menu Démarrer/Panneau de configuration /Réseau et Internet.

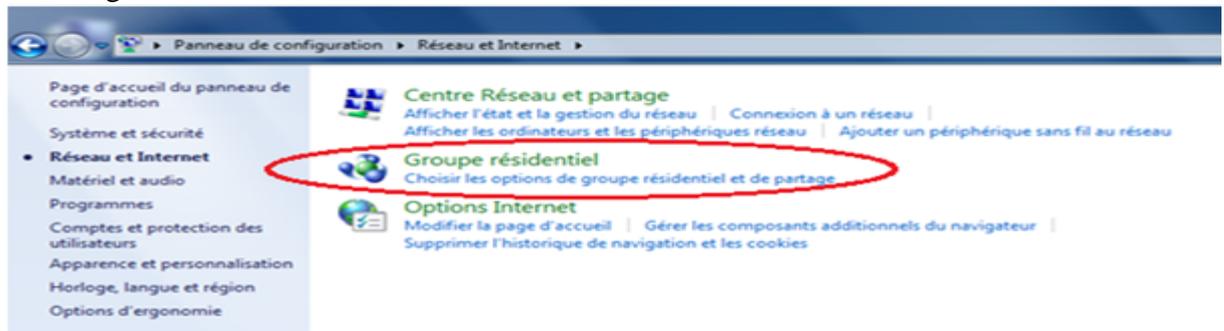
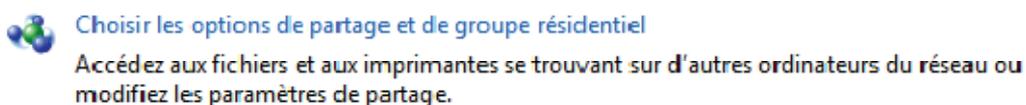


FIGURE 2.14 – Fenêtre pour accéder au groupe résidentiel

- Créer un groupe résidentiel
- Activer le partage des fichiers multimédias :
 - ✓ Cette option permet d'activer le partage de votre musique, vos vidéos et vos images ou imprimantes.
 - ✓ Dans le Centre Réseau et partage, cliquez sur la rubrique Choisir les options de partage et de groupe résidentiel.



- ✓ Dans la zone Partage des bibliothèques et des imprimantes, cochez Images, Musique et Vidéos et imprimantes.



- ✓ Cliquez sur le bouton Enregistrer les modifications.
- Modification de mot de passe du groupe résidentiel :
 - ✓ Dans la zone modifier les paramètres du groupe résidentiel, cliquer sur modifier le mot de passe.
 - ✓ Introduisez votre nouveau mot de passe et cliquez sur suivant.

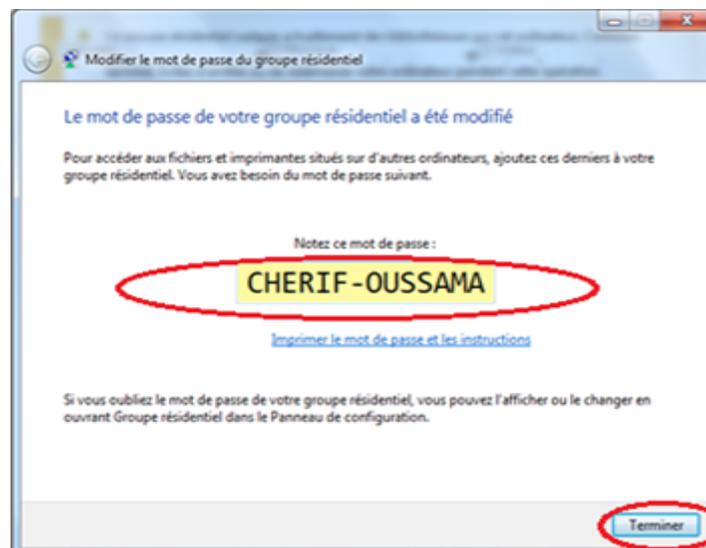


FIGURE 2.15 – Fenêtre pour la modification de mot de passe de groupe résidentiel

2.7.1.2 Les opérations effectuées sur les autres ordinateurs:

- Cliquez sur joindre le groupe résidentiel.



FIGURE 2.16 – Fenêtre pour joindre le groupe résidentiel

- Pour introduire le nouveau mot de passe dans les autres clients.

Modifier les paramètres du groupe résidentiel

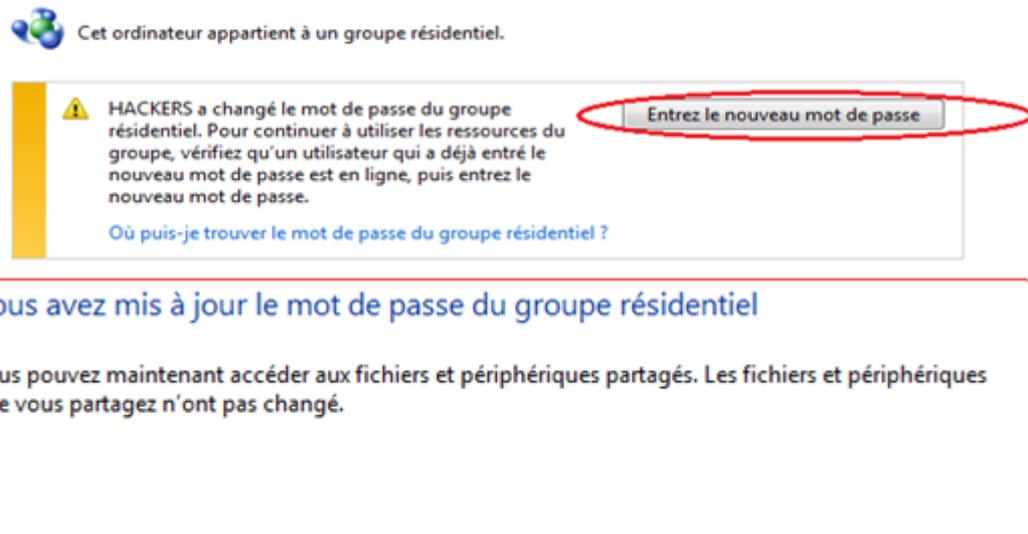


FIGURE 2.17 – Fenêtre pour la confirmation de mot de passe de groupe résidentiel

2.7.1.3 Mettre en partage des dossiers publics ou personnels :

Sous Windows 7, il existe deux types de dossiers : les dossiers personnels ou locaux et les dossiers publics. Un dossier personnel est un dossier appartenant à un utilisateur spécifique créé sur l'ordinateur, alors qu'un dossier public est un dossier que tout autre utilisateur de cet ordinateur ou du même réseau peut partager. Par essence, un dossier public est partagé, donc disponible pour tous en lecture (niveau d'autorisation minimum). Pour partager des dossiers personnels (votre dossier d'images personnelles, par exemple), il sera nécessaire de choisir les personnes qui auront accès à leur contenu et de définir le niveau d'autorisation, comme indiqué dans la procédure ci-après.

- Sélectionnez le dossier que vous souhaitez partager, sans l'ouvrir.
- Cliquez à l'aide du bouton droit de la souris sur le dossier. Sélectionnez partager avec.(voir la figure 2.18)

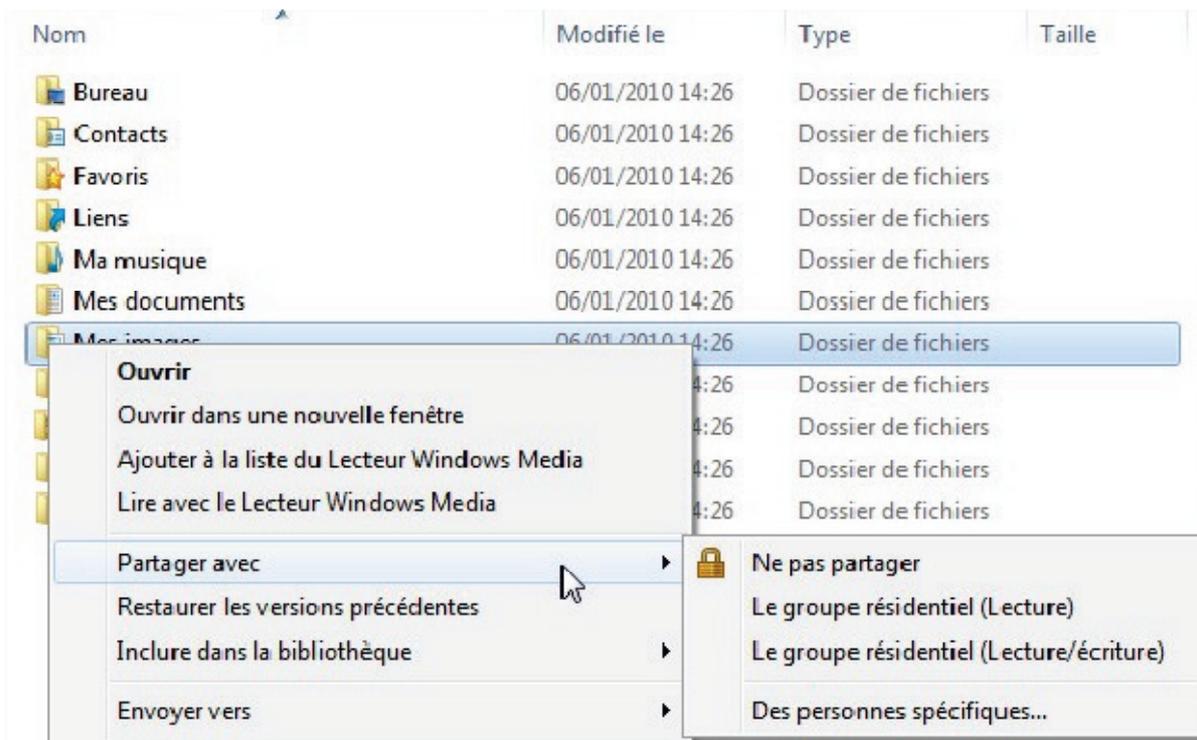


FIGURE 2.18 – partager un dossier

- Vous pouvez partager ce dossier avec Le groupe résidentiel (Lecture), Le groupe résidentiel (Lecture/écriture) ou Des personnes spécifiques. Le groupe résidentiel correspond aux ordinateurs qui font partie du groupe Réseau domestique.
- Si vous activez le partage avec des personnes spécifiques, sélectionnez les utilisateurs qui auront accès à ce dossier.

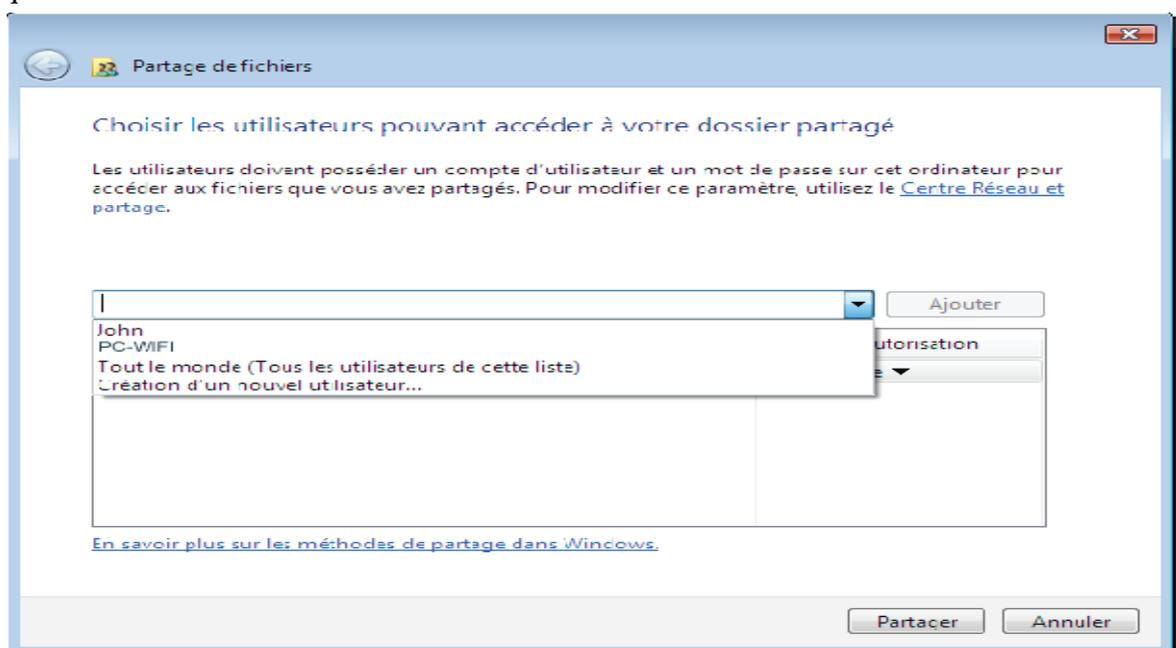


FIGURE 2.19 – Fenêtre de choix d'utilisateur

- Dans la fenêtre Partage de fichiers, sélectionnez le ou les utilisateurs qui pourront accéder à ce dossier, puis cliquez sur Ajouter.

- Vous pouvez donner accès à tous les utilisateurs sans restriction (option Tout le monde) ou sélectionner des utilisateurs spécifiques préalablement créés sur votre PC. Vous pouvez également créer de nouveaux utilisateurs en cliquant dans la liste déroulante sur Création d'un nouvel utilisateur...
- Choisissez le Niveau d'autorisation souhaité en cliquant sur la ligne de l'utilisateur : Lecture (autorisation d'affichage uniquement), Lecture/écriture (autorisation d'affichage, d'ajout et de suppression) ou Propriétaire (autorisation d'affichage, de modification, d'ajout et de suppression).
- Cliquez sur le bouton Partager. Notez bien que le chemin indiqué, permettra d'accéder au dossier partagé sur le réseau depuis un autre ordinateur.

2.7.1.4 Accéder aux dossiers partagés :

- Dans l'Explorateur de fichiers, accessible dans Démarrer/Ordinateur, double-cliquez sur Réseau.
- Vous accédez à la liste des ordinateurs du même réseau. Servez-vous du chemin indiqué par Windows lors de la création du partage.
- Double-cliquez sur l'ordinateur qui partage les dossiers auxquels vous souhaitez accéder.
- Si un mot de passe a été défini, saisissez votre nom d'utilisateur et votre mot de passe.

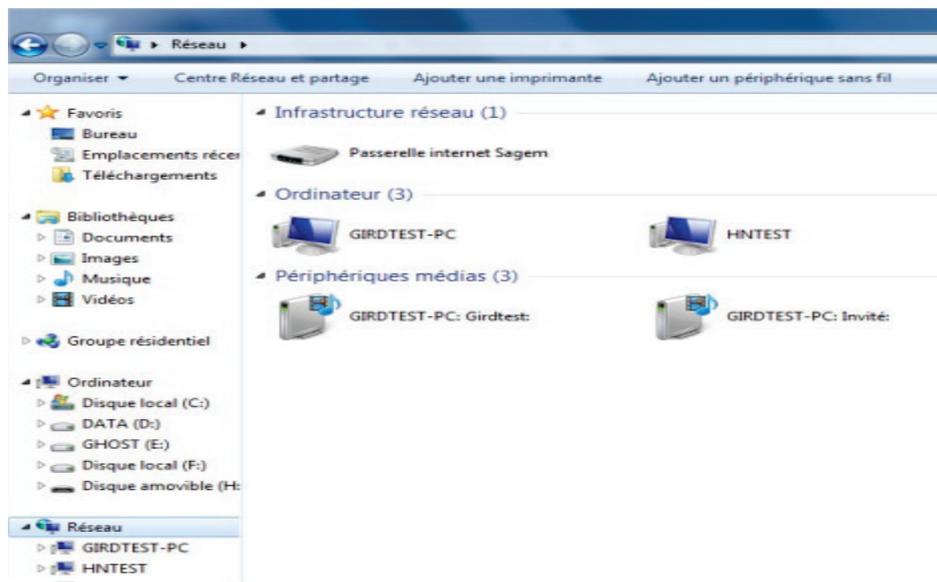


FIGURE 2.20 – Fenêtre pour accéder aux dossiers partagés

Tous les dossiers partagés apparaissent. Selon votre niveau d'autorisation, vous pouvez afficher, modifier, ajouter et/ou supprimer les dossiers et fichiers partagés.

2.7.1.5 Mettre en partage une imprimante :

Il est possible de mettre une imprimante en réseau et d'en faire profiter tous les ordinateurs de la maison connectés en réseau.

- Pour accéder à une imprimante en réseau, le partage de celle-ci doit être préalablement activé dans le Centre Réseau et partage. Ensuite l'imprimante doit être mise en partage sur l'ordinateur sur lequel elle est branchée et installée.

Sur l'ordinateur connecté à l'imprimante :

- Cliquez sur Démarrer/Périphériques et imprimantes.
- La liste des imprimantes installées s'affiche.

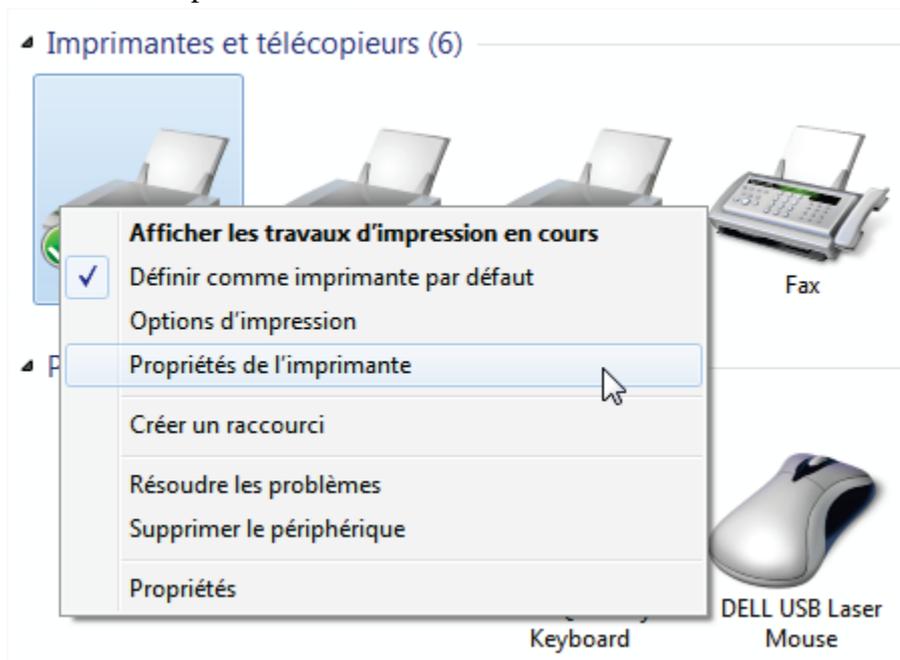


FIGURE 2.21 – Partager une imprimante

- Cliquez avec le bouton droit de la souris sur l'imprimante et sélectionnez Propriétés de l'imprimante.

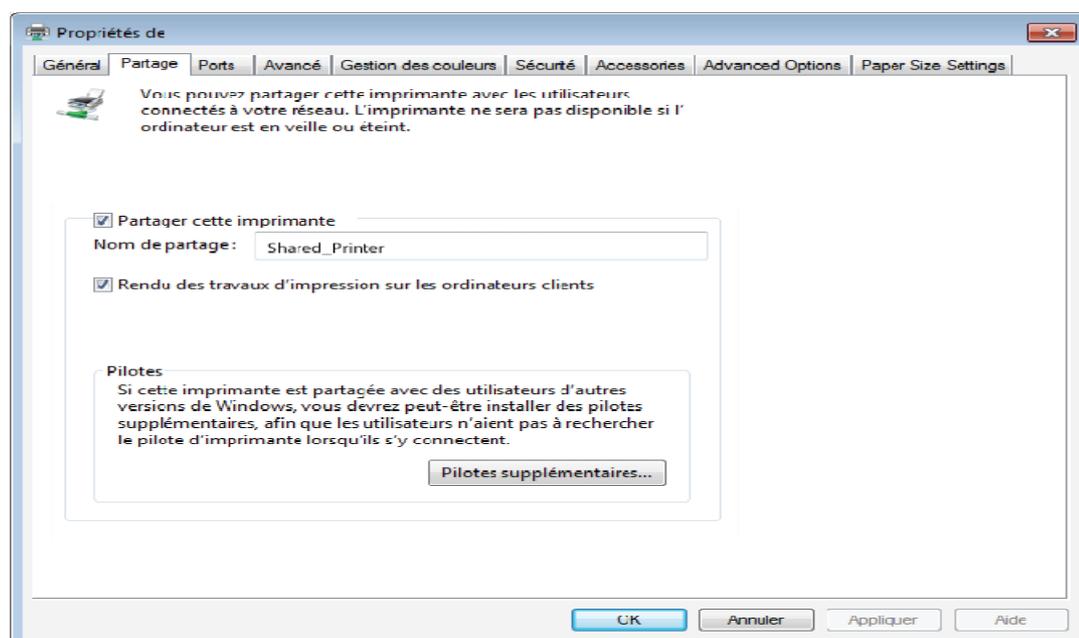


FIGURE 2.22 – Les propriétés de l'imprimante

- Dans la fenêtre Propriétés de [nom imprimante], sélectionnez l'onglet Partage.
- Cochez la case Partager cette imprimante.
- Choisissez le nom de l'imprimante qui sera affiché sur le réseau dans Nom du partage.
- Cliquez sur Appliquer, puis sur OK.

2.7.1.5.1 Accéder à l'imprimante partagée :

Sur les ordinateurs qui vont utiliser l'imprimante partagée :

- Cliquez sur Démarrer/Périphériques et imprimantes.
- Cliquez sur le bouton Ajouter une imprimante.

Ajouter une imprimante

L'assistant Ajouter une imprimante s'affiche.

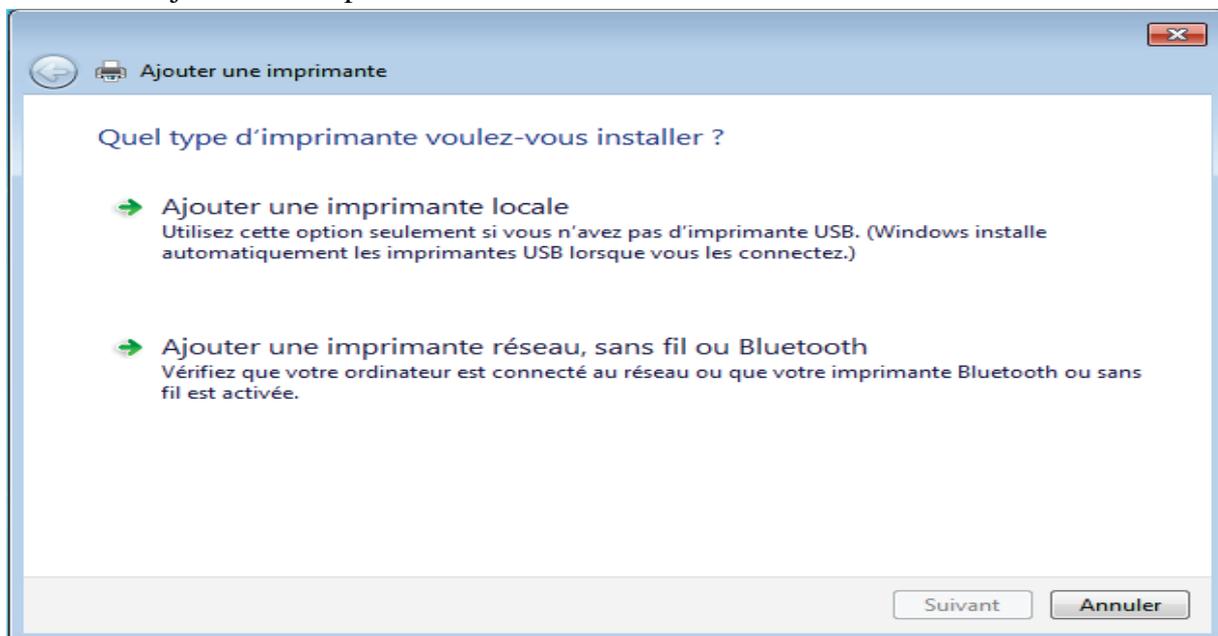


FIGURE 2.23 – Fenêtre de choix d'une imprimante

- Cliquez sur Ajouter une imprimante réseau, sans fil ou Bluetooth.

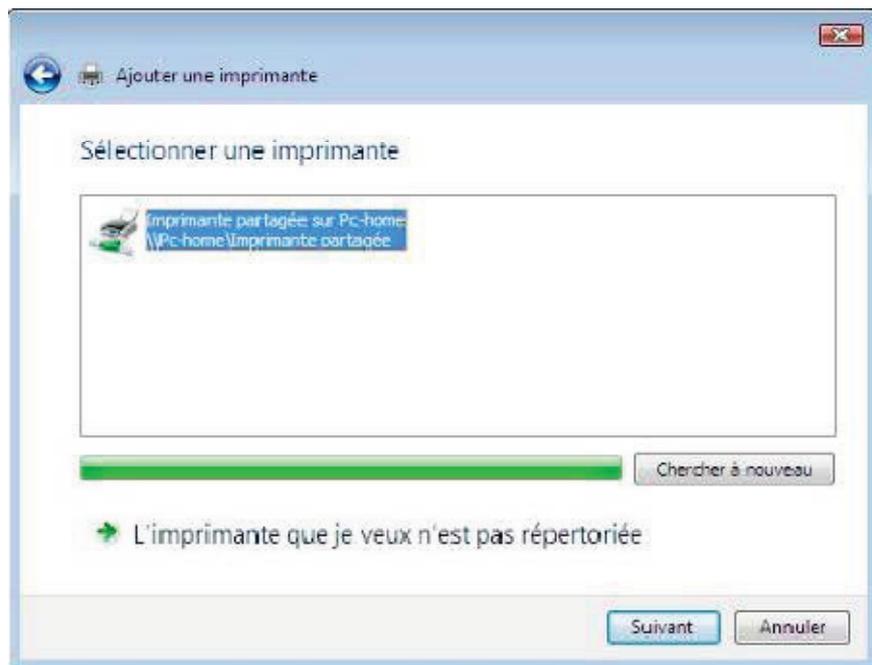


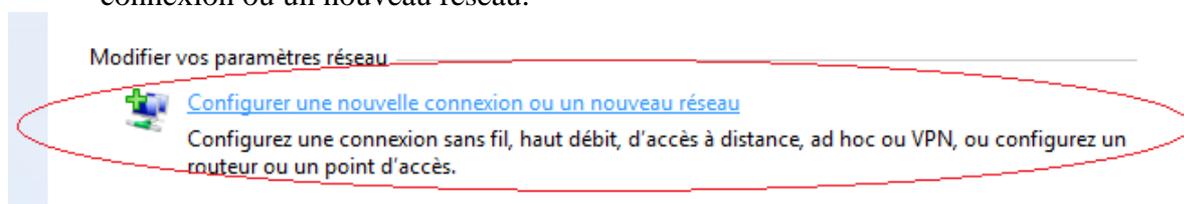
FIGURE 2.24 – Fenêtre d’ajout d’une imprimante

- Windows recherche alors les imprimantes partagées sur votre réseau. Sélectionnez l'imprimante partagée puis cliquez sur Suivant.
- Si besoin, acceptez l'installation des pilotes de l'imprimante lorsque Windows vous le propose.
- Validez le nom de votre imprimante, puis cliquez sur Suivant.
- Cochez la case Définir en tant qu'imprimante par défaut, si vous le souhaitez.
- Cliquez sur Terminer pour fermer l'assistant.

2.7.2 Partager une connexion ADSL, dossiers et imprimantes dans un réseau de type sans Infrastructure

Les étapes à suivre sont :

- Accédez au Centre Réseau et partage. Pour ce faire, sélectionnez le menu Démarrer/Panneau de configuration.
- Cliquez sur la rubrique Réseau Internet, puis Centre Réseau et partage. Dans la fenêtre Centre Réseau et partage, cliquez sur le lien Configurer une nouvelle connexion ou un nouveau réseau.



- Sélection le lien configurer un réseau sans fil ad-hoc (ordinateur à ordinateur), puis cliquer sur suivant.

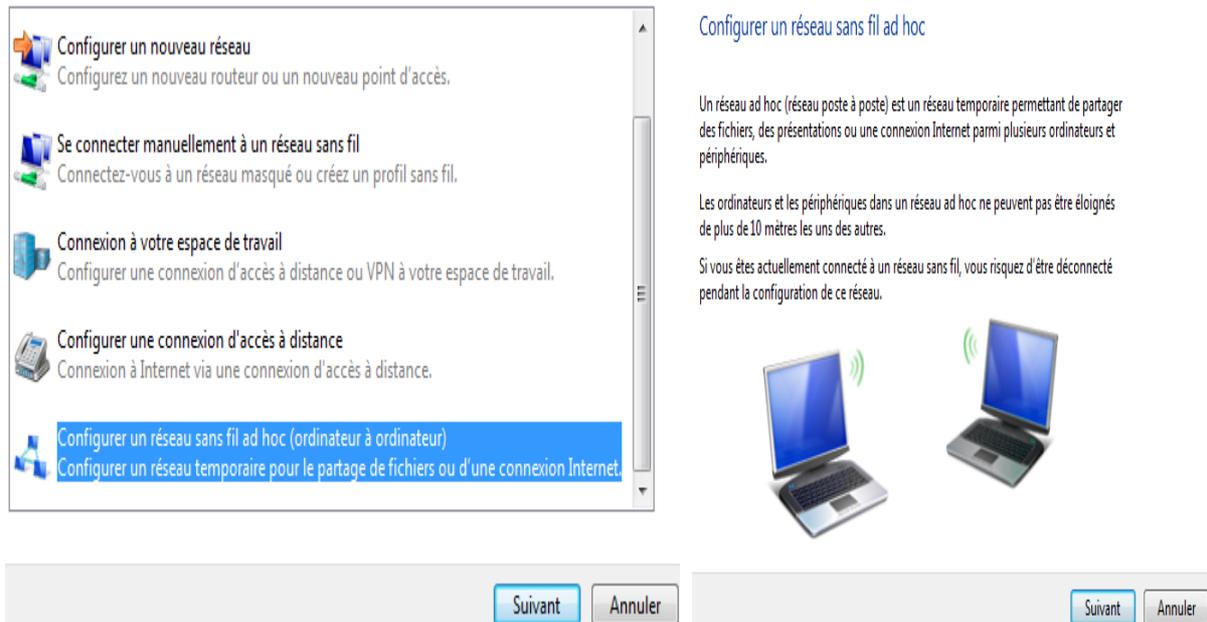


FIGURE 2.25 – Fenêtre de configuration d’un réseau Ad-hoc

- Configurer votre réseau Ad-hoc avec l’attribution d’un nom au réseau et de choisir les options de sécurité, puis cliquer sur suivant.

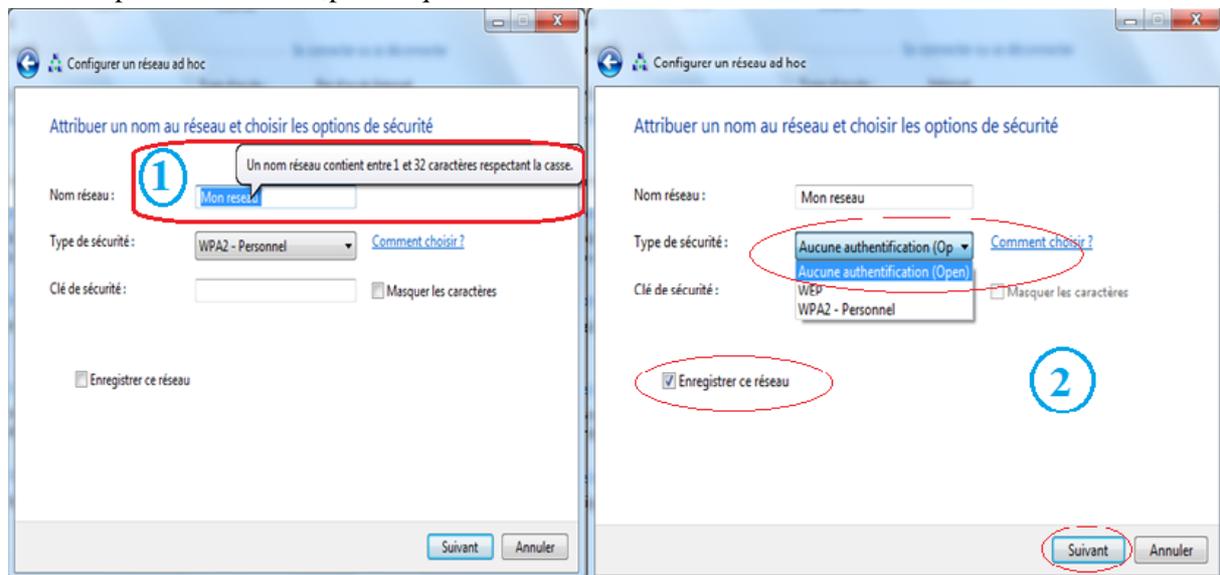


FIGURE 2.26 – Fenêtre de configuration d’authentification d’un réseau Ad-hoc

- Le type de la sécurité utilise consiste à introduire une clé WEP ou WPA2- Personnel qui permet aux utilisateurs d’authentifier leurs accès a ce réseau, et l’accès est autorise seulement pour les clients qui connaissent cette clé de sécurité crée précédemment.
- D’autre part les clients qui veulent avoir l’accès aux réseaux créer précédemment il faut d’abord introduire la clé d’authentification, pour qu’ils s’identifiés automatiquement.

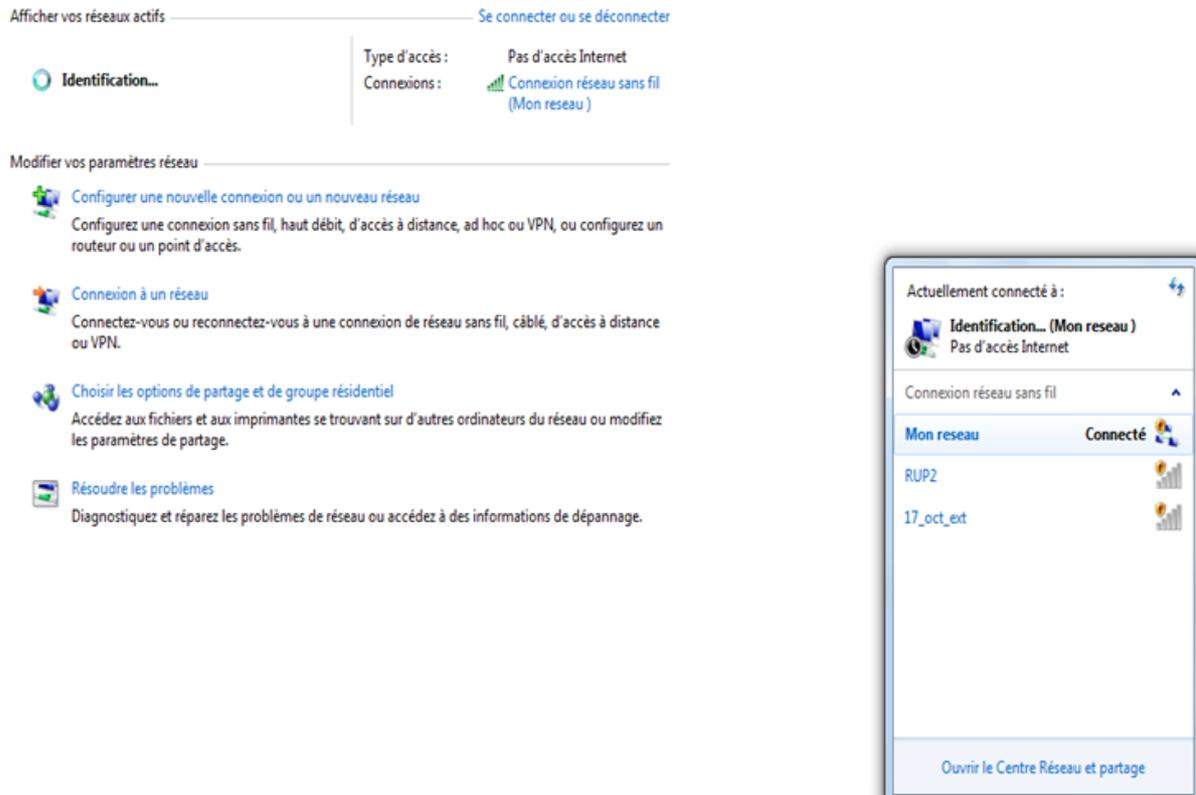


FIGURE 2.27 – Fenêtre d'identification d'un réseau Ad-hoc

Avant de passer à l'étape de partage vos dossiers, vos imprimantes ou votre connexion, vous devez activer le partage depuis le Centre Réseau et partage.

2.8 Conclusion

Certes avec tous ces concepts fondamentaux de partage des ressources nous avons fournis l'essentiel des fonctionnalités ainsi que les différentes méthodes de partages, il est évident que le partage des ressources est une étape primordial voire vital pour le bon fonctionnement d'échange de différents ressources informatique.

Chapitre 3

Serveur d'impression CUPS

3.1 Introduction

Dans ce chapitre nous allons présenter la mise en place d'un serveur d'impression CUPS. Ainsi que l'utilisation des imprimantes depuis des hôtes client Linux et Windows par l'intermédiaire de Samba.

3.2 Présentation de CUPS

CUPS est un système Commun d'Impression Unix ("Common Unix Printing System") que tous les systèmes d'exploitation de la famille Unix, utilise pour l'impression. Il permet à l'ordinateur sur lequel il est installé de fonctionner en serveur d'impression sur un réseau. Un serveur d'impression est capable d'accepter des tâches d'impression d'autres ordinateurs (les clients) et de les répartir sur les imprimantes auxquelles il a accès.

Le client peut être un hôte distant ou tout simplement l'hôte local (l'ordinateur sur lequel est implanté CUPS). Si l'ordinateur client est un hôte distant, il doit être configuré en tant que client. [8]

CUPS fournit un mécanisme qui permet aux applications d'imprimer de façon standardisée, c'est lui qui s'occupe de converser avec les imprimantes. Le système est organisé en trois couches :

1. les applications envoient les documents à imprimer à un gestionnaire de tâche sur le serveur CUPS ;
2. ce gestionnaire passe le document à travers un filtre pour le convertir dans un langage que l'imprimante peut comprendre ;
3. le document ainsi transformé est livré à un module de transport qui se charge de transmettre les données d'impression à un périphérique local ou une connexion réseau.

Le système fait l'utilisation étendue du PostScript et de la rastérisation des données pour convertir les données à un format qui convienne à l'imprimante.

- **PostScript** : Le PostScript est un langage informatique spécialisé dans la description de pages, mis au point par Adobe. Il repose sur des formulations vectorielles de la plupart de ses éléments. Il sait aussi traiter les images matricielles (en mode point). ce langage inter-plateformes permet d'obtenir un fichier unique comportant tous les éléments décrivant la page (textes, images, polices, couleurs, etc.).PostScript est devenu pratiquement un standard, la plupart des imprimantes lasers haut de gamme peuvent traiter directement le format PostScript.
- **La rastérisation** : La rastérisation est un procédé qui consiste à convertir une image vectorielle en une image matricielle destinée à être affichée sur un écran ou imprimée par un matériel d'impression.

3.3 Principe de fonctionnement de CUPS

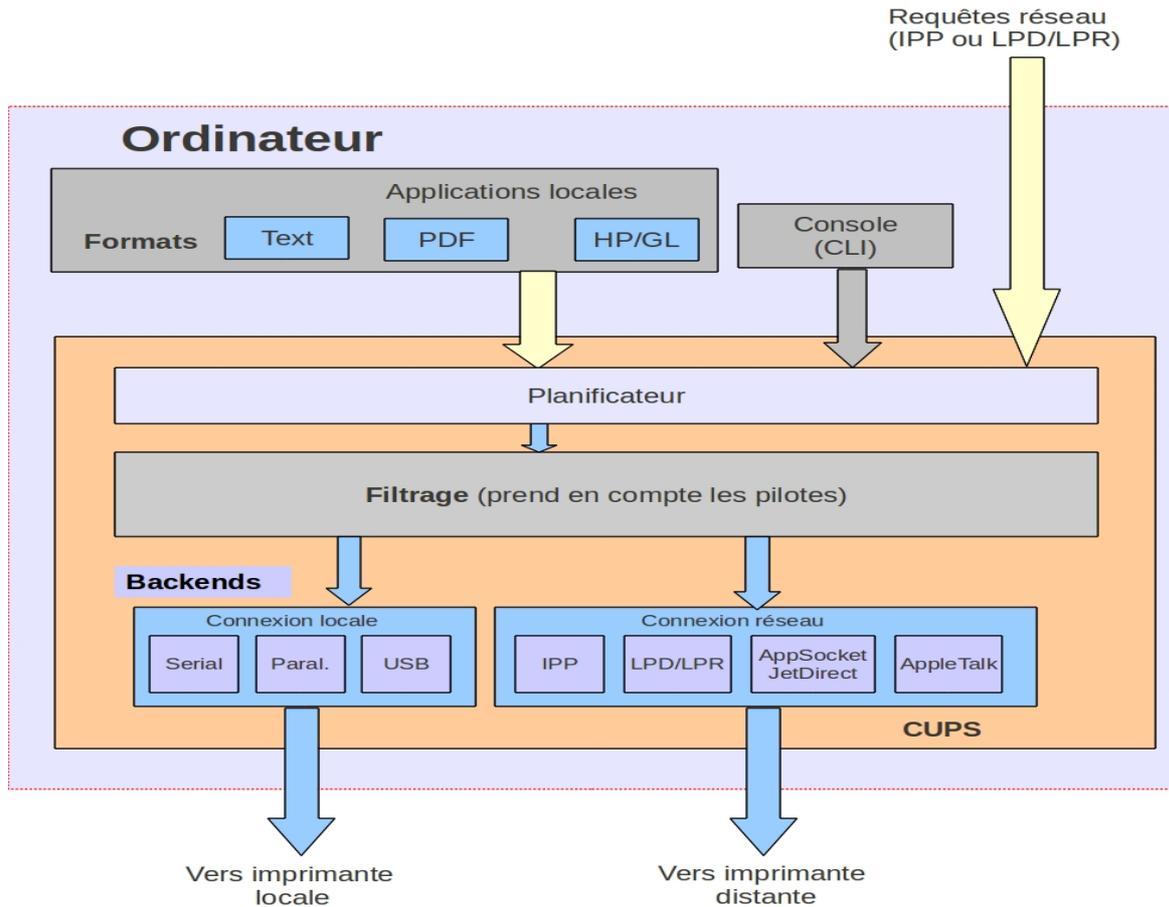


FIGURE 3.1 - Le schéma fonctionnel de CUPS

- **Planificateur** : Le planificateur reçoit les requêtes d'impression des hôtes distants ou de l'hôte local. Pour adresser ces requêtes, les clients utilisent le protocole IPP (Internet Printing Protocol) ou le protocole LPD/LPR qui est alors converti par le planificateur en IPP.

Le planificateur assure également la gestion des autorisations d'accès et l'ordonnancement des tâches d'impression à l'aide de files d'attente, ainsi que l'interprétation des commandes en ligne traditionnelles des différents systèmes permettant d'interagir avec les imprimantes.

- **Filtrage** : Les données de différents types sont envoyées vers le serveur CUPS qui les convertit en un format que l'imprimante comprendra et sera capable d'imprimer. C'est au niveau de cette couche que les formats des diverses applications sont traduits en un format compréhensible par l'imprimante, en tenant compte, entre autres, de la spécificité de l'imprimante grâce aux pilotes. Au niveau du processus global de CUPS les pilotes sont pris en compte au niveau de l'étage de filtrage.

- **Transport :** Pour communiquer avec les imprimantes, CUPS utilise des modules de transport (backend). Il existe des modules de transport pour les protocoles utilisant les ports parallèle, série et USB mais aussi des modules de transport opérant à travers un réseau via les protocoles IPP (Internet Print Protocol), JetDirect (AppSocket), Line Printer Daemon (LPD/LPR) ou SMB.

3.4 Avantage CUPS

Un des principaux avantages de CUPS est qu'il peut interpréter une grande variété de formats de données pour le serveur d'impression. Il convertit les données à imprimer dans le langage/format final via une série de filtres. Il utilise pour cela les types MIME (Multipurpose Internet Mail Extensions). MIME est un standard internet pour le format des courriers électroniques mais il est communément utilisé dans d'autres systèmes pour déterminer le type de fichier que le système est en train de traiter.

- Il peut accepter et envoyer les travaux d'impression à peu près partout.
- Il fournit l'infrastructure nécessaire pour appuyer l'impression moderne et les imprimantes.
- Il est aujourd'hui inclus avec presque toutes les distributions Linux et est disponible gratuitement pour tous les systèmes d'exploitation UNIX.
- Il fournit des interfaces graphiques pour l'impression pour les utilisateurs finaux.

3.5 Les différentes situations d'une architecture de partage d'imprimante

Parmi les différentes situations qui défini l'architecture de partage des imprimantes en peut y avoir deux situations :

3.5.1 Situation 1 : l'imprimante est connectée directement à l'ordinateur

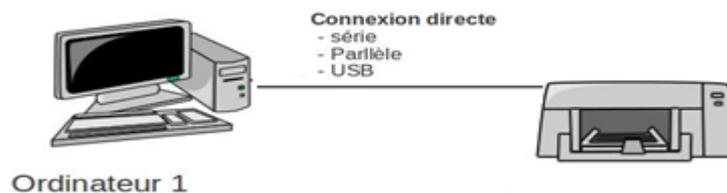


FIGURE 3.2 - L'imprimante connectée directement à l'ordinateur

C'est le cas des imprimantes qui ne disposent que d'un port USB, d'un port parallèle (ou encore les deux à la fois) ainsi que des imprimantes connectées par Bluetooth. Ce peut-être également un choix délibéré de la part de l'utilisateur.

Cette option n'exclut pas le partage avec d'autres ordinateurs si votre ordinateur est raccordé à un réseau et qu'il reste allumé quand les autres ont besoin d'imprimer. Dans ce cas, CUPS est

installé sur l'ordinateur (hôte local) et joue le rôle de serveur d'impression pour les différentes applications locales et pour les commandes en ligne.

Pour communiquer avec l'imprimante dans cette situation il faut :

- Si cet ordinateur n'a pas lieu d'accepter des demandes d'impression d'autres ordinateurs, simplement y installer l'imprimante.
- Par contre, si l'ordinateur doit en plus accepter des demandes d'impression venant d'autres ordinateurs ; il faudra en plus, le configurer en serveur d'impression.

3.5.2 Situation 2 : L'imprimante est accessible via un réseau

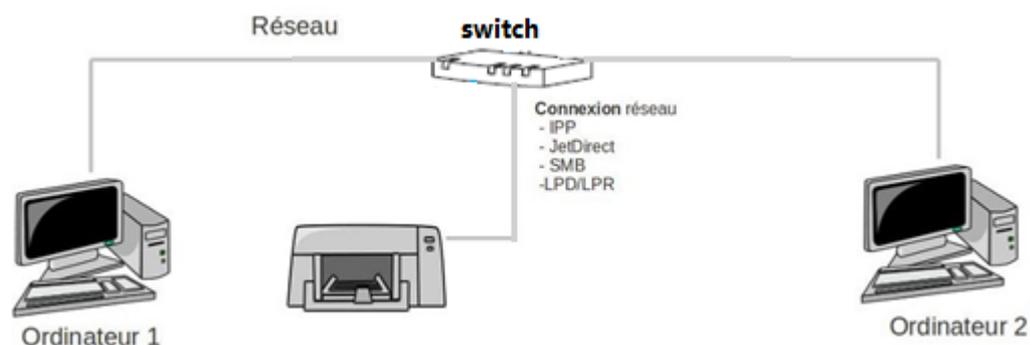


FIGURE 3.3 - L'imprimante est accessible via un réseau

Pour communiquer avec une imprimante via un réseau, il faut qu'entre votre ordinateur et l'imprimante s'intercale un serveur d'impression.

Un serveur d'impression permet le partage d'une ou plusieurs imprimantes entre des ordinateurs situés sur un réseau. Il dispose donc :

- ✓ D'une connexion au réseau par laquelle il communique selon un protocole réseau (TCP/IP par exemple).
- ✓ D'une ou plusieurs connexions directes avec une ou plusieurs imprimantes.

Il y a pour cela plusieurs possibilités :

- l'imprimante dispose d'une carte de raccordement direct au réseau (imprimante réseau), C'est la carte réseau de l'imprimante qui assure la gestion et l'ordonnancement des tâches reçues des divers ordinateurs du réseau
- l'imprimante est raccordée à un boîtier électronique, qui comporte ce serveur d'impression, qui peut être un boîtier dédié, une passerelle résidentielle.
- l'imprimante est (ou sera) en communication directe avec un autre ordinateur relié au réseau qui inclut un serveur d'impression.

Pour communiquer avec l'imprimante dans cette situation il faut :

- Raccorder physiquement l'imprimante au réseau et configurer ce réseau. Il est conseillé de configurer le réseau pour que l'imprimante ait une adresse IP fixe.
- Installer l'imprimante sur votre ordinateur, c'est-à-dire : ajouter l'imprimante aux imprimantes prises en charge par CUPS sur votre ordinateur en lui fournissant les pilotes et en lui précisant les moyens d'accès (module de transport et adresse IP).
- Configurer l'ordinateur en client d'un serveur d'impression.

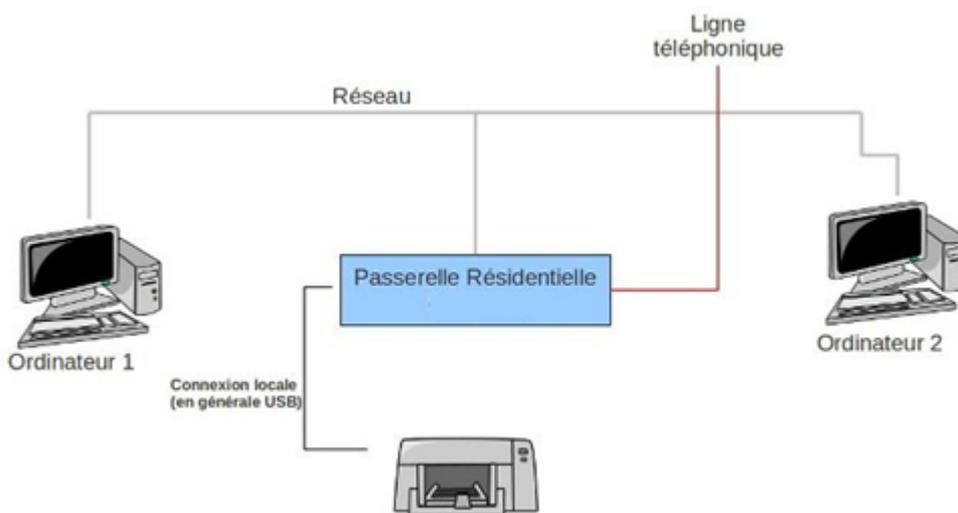
Si votre imprimante est raccordée à un boîtier électronique qui comporte ce serveur d'impression

FIGURE 3.4 - L'imprimante raccordée à un boîtier

Pour communiquer avec l'imprimante dans cette situation il faut :

- Raccorder l'imprimante au boîtier contenant le serveur d'impression.
- Configurer le serveur d'impression et le raccorder au réseau.
- Configurer un ordinateur en client d'un serveur d'impression. L'imprimante publiée par l'ordinateur serveur apparaît alors dans la liste des imprimantes utilisables.

Si l'imprimante est en communication directe avec un autre ordinateur relié au réseau qui inclut un serveur d'impression.

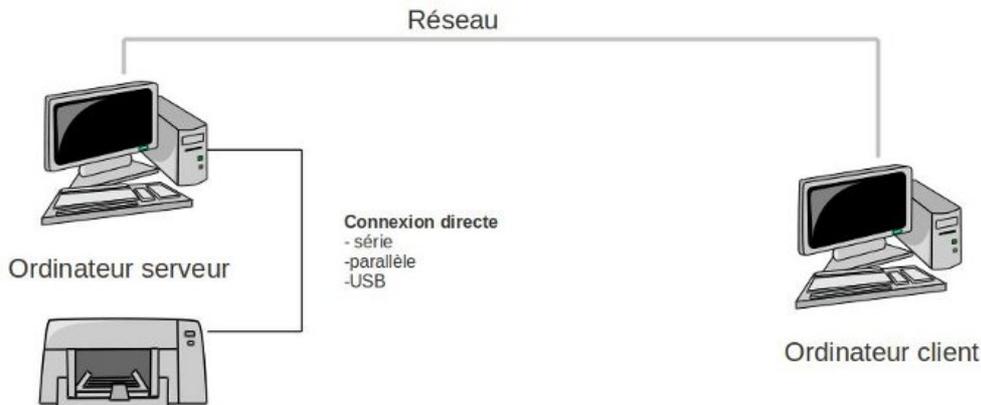


FIGURE 3.5 - L'imprimante communiquée à un ordinateur relié au réseau

Dans ce cas, votre ordinateur est dit "**ordinateur client**" et l'ordinateur distant est dit "**ordinateur serveur**".

Pour communiquer avec l'imprimante dans cette situation il faut :

- Raccorder et installer l'imprimante sur l'ordinateur distant.
- Configurer l'ordinateur distant en "serveur d'impression".
- Configurer votre propre ordinateur en client et le mettre en relation avec l'imprimante.

3.6 Présentation de Samba

Samba est un serveur de fichiers pour Linux (en licence GNU GPL, donc libre) compatible avec les réseaux Microsoft Windows. C'est-à-dire qu'il permet de partager les fichiers et les imprimantes d'un serveur linux avec les ordinateurs d'un réseau Microsoft Windows, et de manière totalement transparente : Linux passe pour un serveur Windows NT aux "yeux" des clients Windows. Les clients pour Microsoft Windows deviennent alors en quelque sorte des clients Linux...

Samba utilise le protocole SMB pour partager les fichiers et les imprimantes sur une connexion réseau. Les systèmes d'exploitation qui prennent en charge ce protocole incluent Microsoft Windows (à travers son **Voisinage Réseau**), OS/2 et Linux.

3.7 Les fonctionnalités de samba

- partager des systèmes de fichiers,
- partager une imprimante sur un serveur Unix avec des clients Windows/Unix,
- jouer le rôle de contrôleur de domaine Windows 2003/2000/NT.

- fournir un serveur WINS (Windows Internet Name Service).

3.8 Architecture de Samba

Samba est constituée d'un serveur et d'un client, ainsi que de quelques outils permettant de réaliser des services pratiques ou bien de tester la configuration.

Grâce à **un client samba**, vous pouvez :

- Accéder à des imprimantes partagées par un PC sous Windows.
- Vous accéderez à des dossiers et des imprimantes partagés.
- Votre machine sera vue sur le réseau, elle pourra avoir un compte machine sur le domaine.

Grâce à **un serveur Samba** vous pouvez :

- partager différents dossiers et des imprimantes.
- Un serveur Linux équipé de samba peut être configuré comme machine partageant des données dans un workgroup Windows,
- Comme serveur membre d'un domaine Windows,
- Comme contrôleur de domaine principal (PDC) d'un domaine Windows...
- Il peut s'insérer dans une Active Directory MS.

Le serveur est constitué de deux applications (appelées *démons*) :

- **smbd** : noyau du serveur, fournissant les services d'authentification et d'accès aux ressources.
- **nmbd** : permettant de montrer les services offerts par Samba (affichage des serveurs Samba dans le voisinage réseau, ...).

3.9 Conclusion

L'utilisation de CUPS nous offre l'opportunité de configurer l'impression sur un réseau étendu d'une manière simple, en configurant globalement les imprimantes réseau, ce qui permet de gérer les demandes d'impressions provenant des utilisateurs locaux ou distants.

3.10 Introduction

Dans cette partie pratique nous allons configurer et administrer le serveur CUPS ainsi que la configuration de serveur SAMBA à fin de permettre aux utilisateurs Windows d'accéder au serveur d'impression.

3.11 Etape de configuration du serveur d'impression CUPS

- D'abord il faut identifier un administrateur et l'authentifier par un login et un mot de passe, ceci à partir du Shell en introduisant la commande suivante :

`Lppasswd -a (le nom choisi)`

- Il va vous demandez d'introduire le mot de passe se dernier doit contenir 6 caractères et au moins un chiffre :

Entrez le nouveau mot de passe : (le mot de passe choisi)

- Ensuite il faut redémarrer CUPS avec la commande :

`/etc/init.d/cups restart`

Afin de procéder à la configuration du serveur d'impression il faut modifier le fichier `/etc/cups/cupsd.conf`

- Pour donner un nom au serveur on utilise la directive suivante :

`ServerName (le nom du serveur)`

- Pour définir le langage à utiliser pour les connexions avec les clients on utilise la directive :

`DefaultLanguage fr`

- Pour préserver l'historique des travaux complètes, annulés ou abandonnés sur disque ou non on utilise la directive :

`PreserveJobHistory off/on`

- Pour purger les travaux d'impression lorsque ils ne sont plus nécessaire au vue de quotas on utilise la directive :

`AutoPurgeJobs No/Yes`

- Pour limiter le nombre des pages autorisés pour chaque utilisateur on utilise la directive :

`MaxCopies (nombre de pages)`

- Pour limiter le nombre maximum de travaux d'impression qui sont conservés en mémoire on utilise la directive :

`MaxJobs` (nombre de travaux)

- Pour limiter le nombre maximum des travaux actifs qui sont autorisés pour chaque imprimante ou classe d'imprimante on utilise la directive :

`MaxJobsPerPrinters` (nombre)

- Pour limiter le nombre maximum des travaux d'impression qui sont autorisés pour chaque utilisateur on utilise la directive :

`MaxJobsPerUser` (nombre)

- Si on connecte une imprimante dotée d'un Fax support on peut gérer le nombre maximum d'essais à faxé, on utilise la directive :

`FaxRetryLimit` (nombre)

- Pour fixer l'intervalle entre deux essais on utilise la directive :

`FaxRetryInterval` (nombre unité en seconde)

- Pour définir l'emplacement du fichier de certificat SSL utilisé par le serveur, on utilise la directive :

`ServerCertificate` (emplacement de certificat)

- Pour indiquer l'emplacement du fichier de clé privée SSL utilisé par le serveur, on utilise la directive :

`ServerKey` (emplacement de fichier)

- Pour définir sur quel port le serveur d'impression CUPS sera en attente de connexion on utilise la directive :

`Port` (N° de port)

- Pour les connexions sécurisées on utilise la directive :

`SSLPort` (N° de port)

- Pour limiter le nombre maximum de clients simultanés qui seront autorisés par le serveur on utilise la directive :

`MaxClients` (nombre)

- Pour limiter la taille maximum des fichiers d'impression on utilise la directive :

`MaxRequestSize` (taille de fichier en Mo)

- Pour l'activation ou non de l'exploration réseau des imprimantes on utilise la directive :

Browsing On/Off

- La directive **SystemGroup** indique le groupe système d'administration pour l'authentification de type système :

SystemGroup lpadmin

- On peut autoriser l'administration CUPS par l'interface web ou la refuser ceci avec la directive :

Allow From (@reseau)

Deny From (@, All ...)

3.12 Configuration du mot de passe pour l'administration CUPS

- Ajouter un utilisateur (soit exister ou non sur le serveur) avec la directive :

Server : ~# lppasswd -a printadmin

Entrer password : (introduire votre mot de passe)

Entrer le mot de passe again : (confirmez votre mot de passe)

3.13 Création du certificat et de la clef SSL pour CUPS

- Créer un répertoire `/etc/cups/ssl/` et copiez le fichier `/etc/ssl/openssl.cnf` vers `/etc/cups/ssl/openssl-cups.cnf`
- Tapez ces commandes pour générer votre clef et certificat SSL

Server : ~# cd /etc/cups/ssl/

Server : /etc/cups/ssl # openssl req -new -x509 -config /etc/cups/ssl/openssl -

cups.cnf -keyout /etc/cups/ssl/server.key -out /etc/cups/ssl/server.crt -days 365 -nodes

L'option **-nodes** permet de ne pas crypter le certificat et la clef SSL sinon CUPS ne sera pas capable de les changer.

- Pour relancer (Redemarrer) le serveur CUPS on utilise la directive :

Server : /etc/cups/ssl # /etc/init.d/cupsys restart

3.14 Configuration de Samba pour les clients Windows

Nous utilisons une authentification locale pour accéder à notre serveur d'impression Samba => CUPS

Il faut modifier le fichier `/etc/samba/smb.conf` :

```
#===== Global Settings =====
```

```
[global]
```

```
# Server Naming Options:
```

```
#
```

```
# workgroup = NT-Domain-Name or Workgroup-Name
```

```
workgroup = WORKGROUP
```

```
# netbios name, but defaults to your hostname
```

```
netbios name = IMPRIMANTE-LINUX
```

```
# server string is the equivalent of the NT Description field
```

```
server string = Samba Server %v
```

```
# Security :
```

```
#
```

```
# On demande une authentification pour se connecter au serveur.
```

```
security = user
```

```
encrypt passwords = yes
```

```
passdb backend = tdbsam guest
```

```
# Printing Options:
```

```
# On charge les imprimantes
```

```
load printers = yes
```

```
# Définition du style d'impression
```

```
printing = cups
```

```
printcap = cups
```

```
# Définit les droits d'administration (@group)
```

```
printer admin = root, @lpadmin
```

```
show add printer wizard = yes
```

```
# Logging Options:
```

```
log file = /usr/local/samba/var/log.%m
```

```
# Put a capping on the size of the log files (in Kb).
```

```
max log size = 5
```

```

# Security and Domain Membership Options:
#
# hosts allow = 192.168.1. 192.168.2. 127. EXCEPT 192.168.2.1
hosts allow = 127.0.0.1 192.168.0.0/24
hosts deny = 0.0.0.0/0

interfaces = eth* lo
bind interfaces only = yes
dns proxy = no
#===== Print Definitions =====

[printers]
comment = Spool d'impression
path = /tmp
browseable = no
public = no
writable = no
printable = yes

[print$]
comment = Pilotes d'imprimantes
path = /var/lib/samba/printers
browseable = yes
guest ok = no
read only = yes
write list = root, @lpadmin

```

3.15 Attribution des adresses IP pour les imprimantes réseau

Il existe trois méthodes différentes pour attribuer une adresse ip à votre imprimante soit :

- ✓ En utilisant ARP
- ✓ En utilisant RARP
- ✓ En utilisant BOOTP

La méthode la plus simple pour installer l'adresse ip d'un matériel réseau est d'utiliser la commande ARP . Elle envoie un paquet ARP (Address Resolution Protocol) à l'adresse MAC indiquée tout en lui indiquant son adresse IP comme suit :

- ✓ Arp -s adresse IP adresse MAC
- ✓ Arp -s printx.(le nom du serveur) 08 :00 :F9 :00 :12 :3D
- ✓ Arp -s (adresse ip choisi ex : 192.168.0.20) 08 :00 :F9 :00 :12 :3D

Sinon vous pouvez saisir dans votre serveur DHCP (dhcp.conf) les coordonnées de vos imprimantes puisque leur adresse MAC est connue utilisant la directive suivante :

```

host EpsonStylusC45 {
hardware ethernet 08:00:F9:00:12:3D;
fixed-address 192.168.0.20;
option host-name " EpsonStylusC45.(le nom du serveur)";
}

```

3.16 Connexion et administration du serveur CUPS

La gestion d'impression avec CUPS est possible à travers plusieurs interfaces :

3.16.1 Interface d'administration Web

- Tapez l'adresse suivante sur votre navigateur : `https://localhost/` ou `https://localhost:631`
- Vous arrivez sur la page principale qui vous propose différents menus.

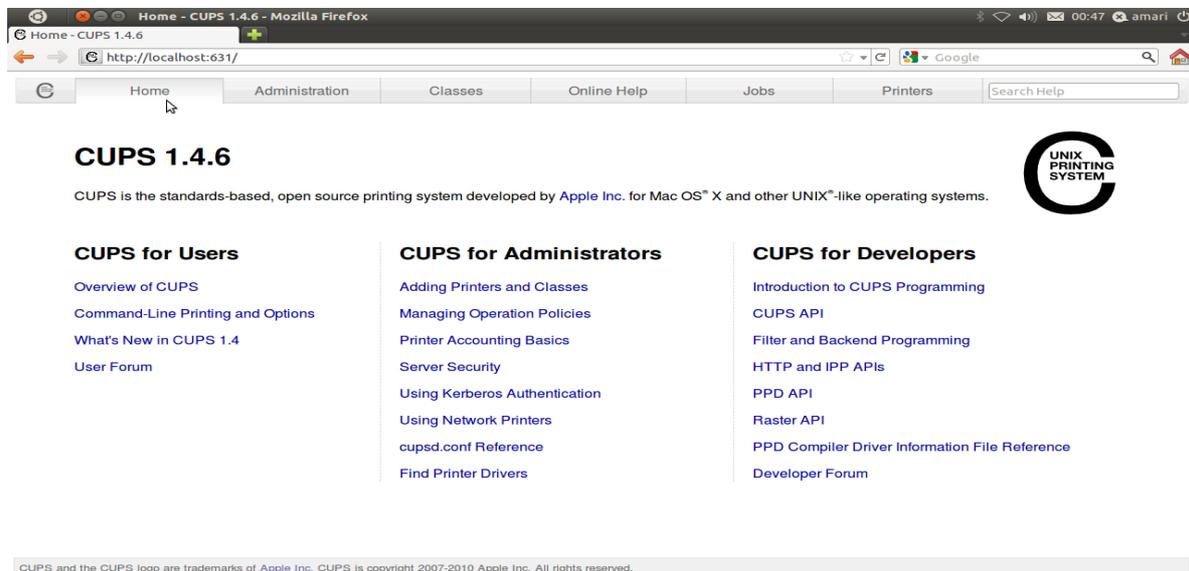


FIGURE 3.6 – Interface d'administration Web

- Selon les actions que vous allez exécuter, le mot de passe « Administrateur » vous sera demandé.

Cliquez sur **ADMINISTRATION** des imprimantes du serveur CUPS :

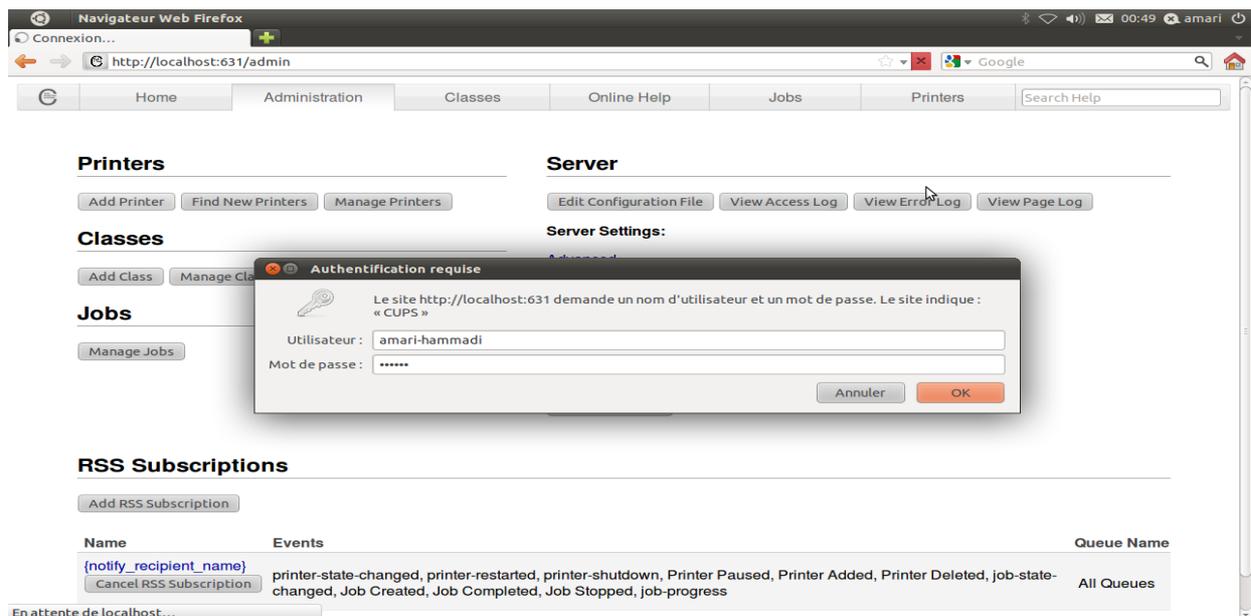


FIGURE 3.7 – Ajouter une imprimante

Cliquez sur Ajouter imprimante pour ajouter une nouvelle imprimante, vous pouvez déclarer votre imprimante dans l'interface.

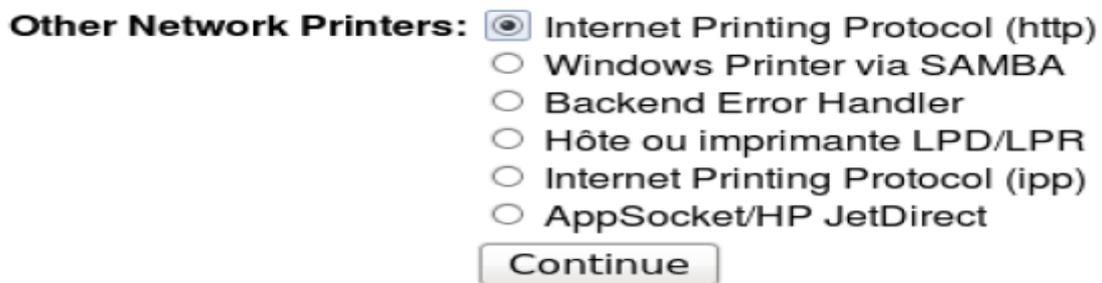


FIGURE 3.8 – choix de l'interface

Introduisez l'adresse et le nom exact de l'imprimante.

Add Printer

Connection:

Examples:

```
http://hostname:631/ipp/  
http://hostname:631/ipp/port1  
  
ipp://hostname/ipp/  
ipp://hostname/ipp/port1  
  
lpd://hostname/queue  
  
socket://hostname  
socket://hostname:9100
```

See "Network Printers" for the correct URI to use with your printer.

FIGURE 3.9 – choix de la connexion

Indiquez le nom de l'imprimante, sa description, puis l'emplacement où elle est installée (zone location).

Add Printer

Name:
(May contain any printable characters except "/", "#", and space)

Description:
(Human-readable description such as "HP LaserJet with Duplexer")

Location:
(Human-readable location such as "Lab 1")

Connection: ipp//192.168.0.11:631/Printers/

Sharing: Share This Printer

FIGURE 3.10 – Fiche d' descriptive d'imprimante

Cochez **Share this printer** si l'imprimante doit être utilisée par d'autres clients CUPS (machines Linux ou Mac).

D'abord en sélectionnant le fabricant, puis le modèle. Dans ce premier écran, si vous choisissez un constructeur (make), le programme vous proposera les différents pilotes existants. Sinon, vous pouvez également indiquer l'emplacement de votre fichier PPD :

Add Printer

Name: teste0
Description: epson
Location: mon bureau
Connection: ipp//192.168.0.11:631/Printers/
Sharing: Share This Printer
Make:

- Citizen
- Citoh
- Compaq
- DEC
- Dell
- DNP
- Dymo
- Epson
- Fujifilm
- Fujitsu

Or Provide a PPD File:

FIGURE 3.11 – Le choix de pilotes

Sélectionnez le modèle de votre imprimante

Add Printer

Name: teste0
Description: epson
Location: mon bureau
Connection: ipp//192.168.0.11:631/Printers/
Sharing: Share This Printer
Make: Epson

Model:

- Epson Stylus DX4050 - CUPS+Gutenprint v5.2.6 Simplified (en)
- Epson Stylus DX4200 - CUPS+Gutenprint v5.2.6 (en)
- Epson Stylus DX4200 - CUPS+Gutenprint v5.2.6 Simplified (en)
- Epson Stylus DX4250 - CUPS+Gutenprint v5.2.6 (en)
- Epson Stylus DX4250 - CUPS+Gutenprint v5.2.6 Simplified (en)
- Epson Stylus DX4400 - CUPS+Gutenprint v5.2.6 (en)
- Epson Stylus DX4400 - CUPS+Gutenprint v5.2.6 Simplified (en)
- Epson Stylus DX4450 - CUPS+Gutenprint v5.2.6 (en)
- Epson Stylus DX4450 - CUPS+Gutenprint v5.2.6 Simplified (en)
- Epson Stylus DX4800 - CUPS+Gutenprint v5.2.6 (en)

Or Provide a PPD File:

FIGURE 3.12 – Choix des modèles d'imprimante

Une fois l'imprimante créée, le programme vous propose alors d'indiquer les paramètres par défaut :

Set Default Options for TEST

Query Printer for Default Options

[Options installées](#) [General](#) [Finisseur](#) [Printing Modes](#) [Code technique](#) [Mot de passe de l'impression privée](#) [Code du service](#) [Livret](#) [Qualité](#) [Bannières](#)
[Règles](#) [Moniteur de port](#)

Options installées

Finisseur:

Bacs supplémentaires:

FIGURE 3.13 – Les paramètres par default

Notre imprimante est maintenant configurée, et prête à l'utilisation. Maintenant on peut y avoir accéder à tout les paramètres de notre imprimante.

3.16.2 Interface d'administration à travers le gestionnaire d'impression

Il existe une autre manière de configurer et partage d'une imprimante avec CUPS en passant par le gestionnaire d'impression à travers le gestionnaire d'impression.

Cliquez sur gestion du système / impression / Ajouter.

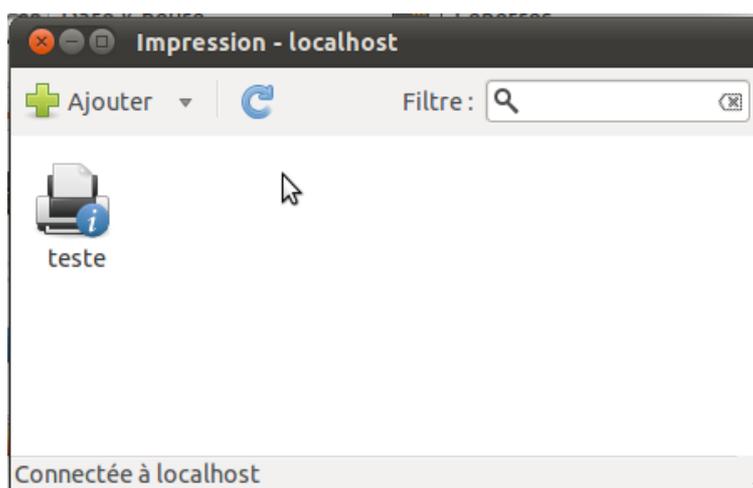


FIGURE 3.14 – Le gestionnaire d'impression

Choisissez le type d'imprimante, et introduisez l'adresse et le nom exact de l'imprimante.

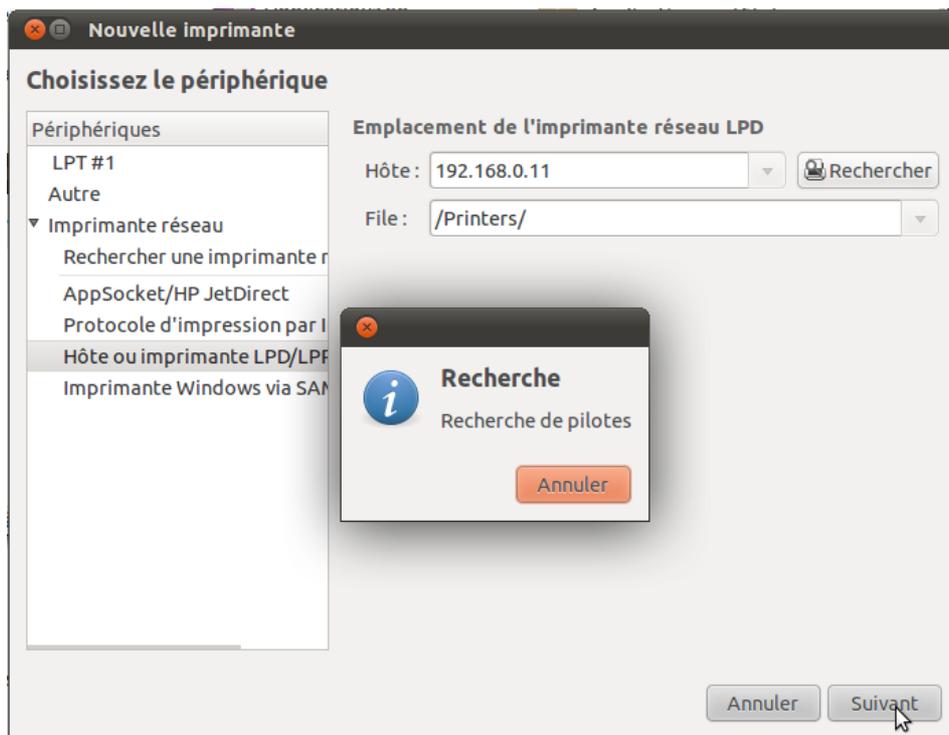


FIGURE 3.15 – Choix de périphérique

Le programme vous proposera les différents pilotes existants, choisissez le pilote convenant à votre imprimante.



FIGURE 3.16 – Choix de pilote

Indiquez le nom de l'imprimante, sa description, puis l'emplacement où elle est installée.

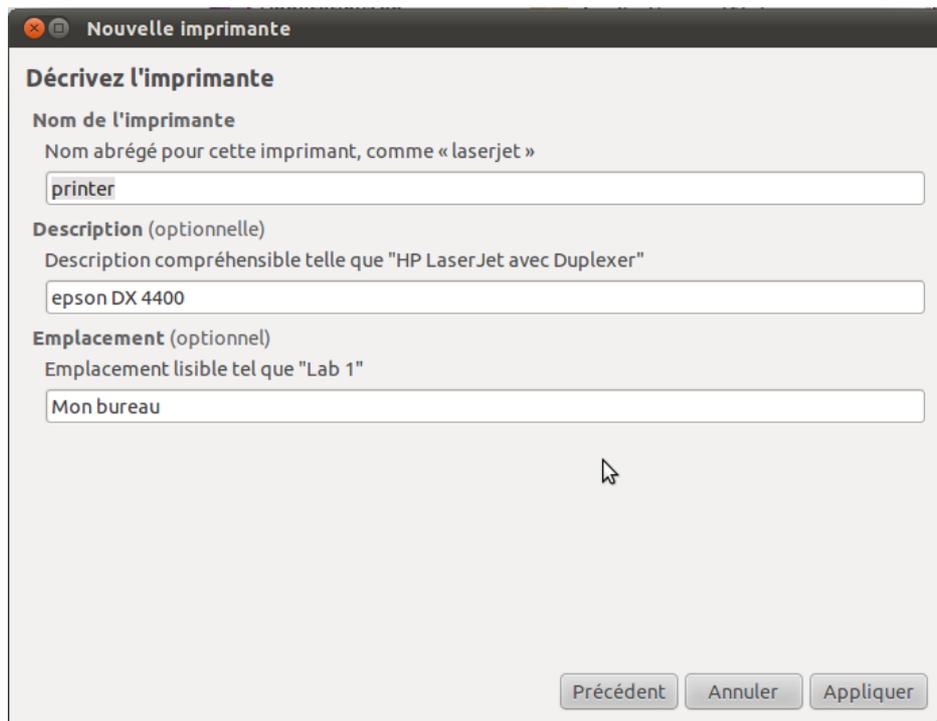


FIGURE 3.17 – Description d'imprimante

Notre imprimante est maintenant installée, et prête à l'utilisation.

Pour modifier les propriétés de l'imprimante, il existe plusieurs possibilités tels que :

- ✓ Les paramètres d'imprimante

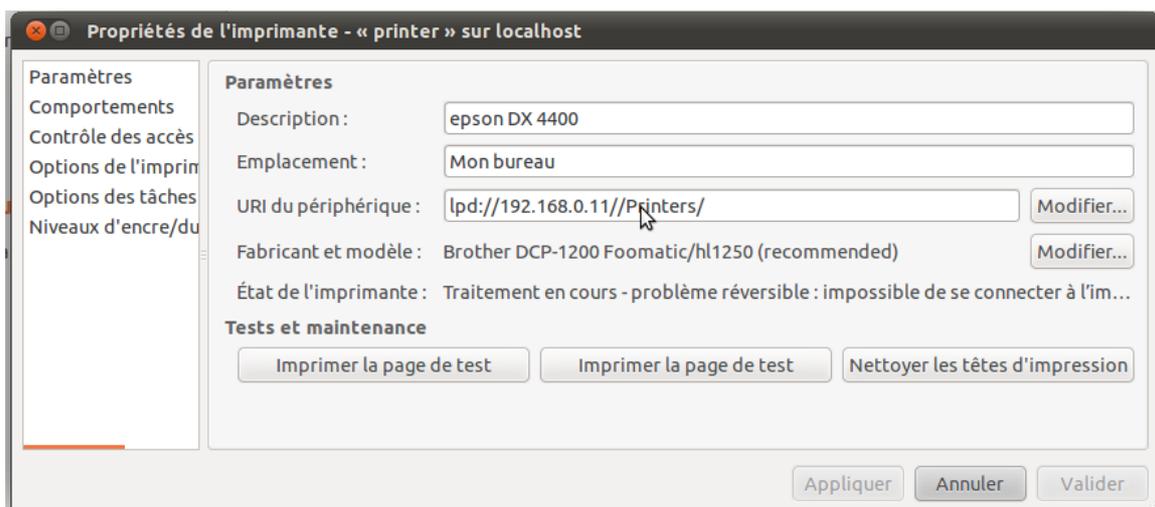


FIGURE 3.18 – Paramètres de l'imprimante

- ✓ Le comportement (activée, partagée ...)

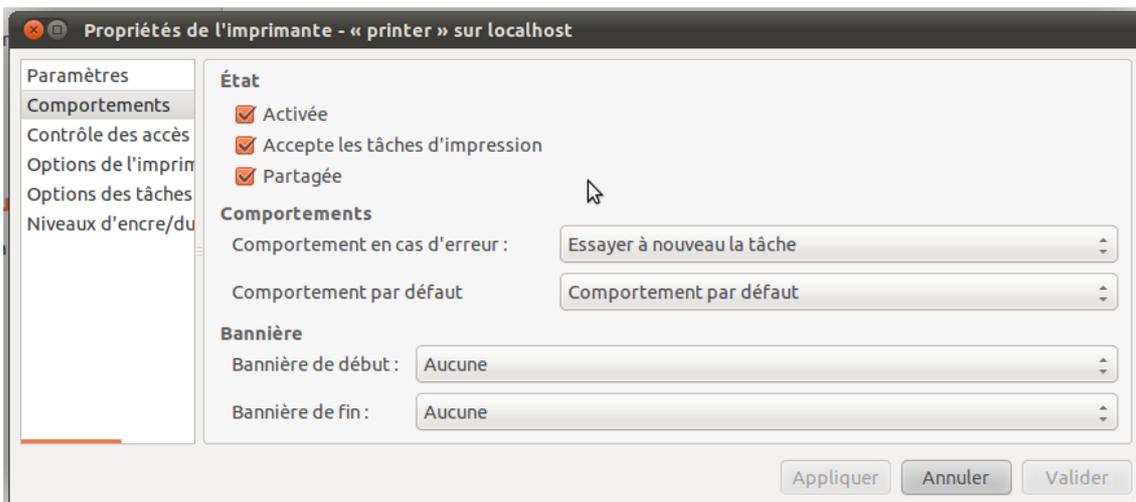


FIGURE 3.19 – Comportements de l'imprimante

- ✓ Le contrôle d'accès (autoriser ou interdire l'impression pour les utilisateurs)

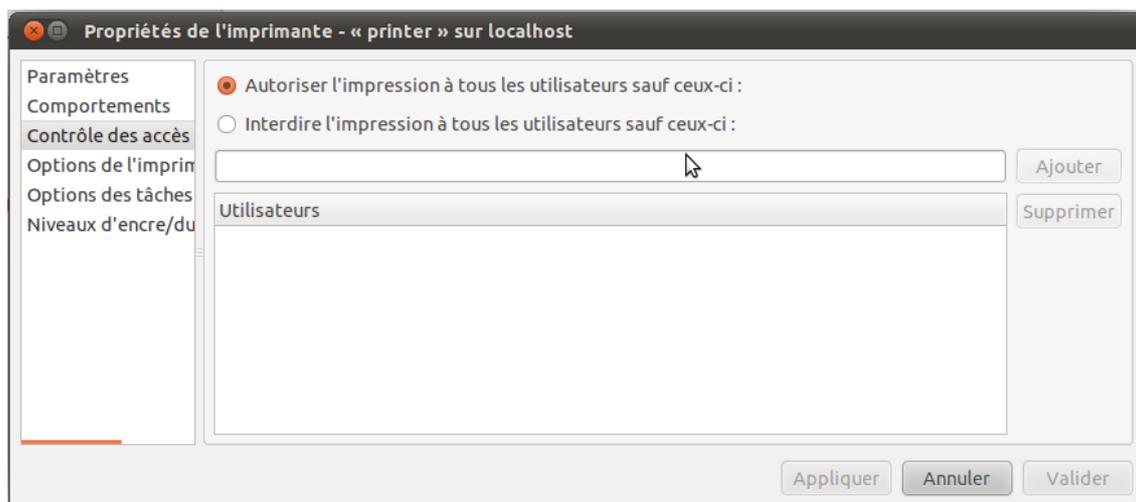


FIGURE 3.20 – Contrôle des accès de l'imprimante

3.17 Fiche descriptive du serveur

Liste des opérations génériques		
Action	Paquetage concerné	Commentaires
Installation de l'OS		
Installation des mises à jour	apt-get update apt-get upgrade	
Paramétrage complet du réseau	/etc/resolv.conf search mondomaine.com nameserver 192.168.xx.xx nameserver 192.168.xx.yy /etc/network/interfaces iface eth0 inet static address 192.168.xx.xx netmask 255.255.08.0 gateway 192.168.xx.yy auto eth1 iface eth1 inet dhcp puis /etc/init.d/networking restart	
Mise à l'heure automatique	ntp	Serveur de temps
Installation de la prise en charge des acl	acl	
Installation logiciels complémentaires	sysv-rc-conf	désactivé le démarrage de winbind
Installation samba	samba, samba-client, winbind tdb-tools	- configuration smb.conf - désactiver le démarrage de winbind - définir les dossiers en partage
Sauvegarde des bases de données samba	cat backupSamba.sh #!/bin/bash mkdir -p /root/backup/samba/cache/printing cd /root/backup/samba/cache tdbbackup /var/cache/samba/*.tdb 2>/var/log/errortdb mv -f /var/cache/samba/*.bak . mkdir -p /root/backup/samba/var/lib cd /root/backup/samba/var/lib tdbbackup /var/lib/samba/secrets.tdb 2>>/var/log/errortdb	Script pour sauvegarder les bases de données SAMBA

	<pre>mv -f /var/lib/samba/secrets.tdb.bak . cd /root/backup/samba/cache/printing tdbbackup /var/cache/samba/printing/*.tdb 2>>/var/log/errortdb mv -f /var/cache/samba/printing/*.bak . if [-s /var/log/errortdb]; then mail -s "Echec sauvegarde fichiers tdb sur \$HOSTNAME" root </var/log/errortdb fi chmod +x /root/backupSamba.sh cd /etc/cron.daily ln -s /root/backupSamba.sh</pre>	
Paramétrage CUPS		
Installation CUPS	<pre>cups cups-pdf openprinting-ppds openprinting-ppdsextra</pre>	<pre>tar xvf ... cd /opt/softs/cups- windows-6.0 make install</pre>
Paquets complémentaires	<pre>foomatic-filters-ppds openprinting-ppds printfilters-ppd ppdfilt</pre>	
Modification de smb.conf	<pre># Configuration CUPS printing = cups printcap name = cups load printers = yes [printers] comment = Imprimantes # postscript = yes browseable = no printable = yes writable = no path = /var/spool/samba guest ok = yes [print\$] comment = Pilotes imprimantes path = /var/lib/samba/printers browseable = yes guest ok = no read only = no writeable = yes write list = root, [donnees] writeable = yes path = /opt/donnees public = yes [pdf] path=/opt/donnees/pdf writeable = yes public = yes browseable = yes</pre>	

<p>Modification de /etc/cups/cupsd.conf</p>	<pre># Only listen for connections from the local machine. #Listen localhost:631 Port 631 Listen /var/run/cups/cups.sock # Show shared printers on the local network. Browsing Off BrowseOrder allow,deny BrowseAllow all BrowseLocalProtocols CUPS dnssd BrowseAddress @LOCAL # Default authentication type, when authentication is required... DefaultAuthType Basic # Restrict access to the server... <Location /> Order allow,deny Allow @LOCAL Allow from 192.168.X.X </Location> # Restrict access to the admin pages... <Location /admin> Order allow,deny Allow @LOCAL Allow from 192.168.X.X </Location> # Restrict access to configuration files... <Location /admin/conf> AuthType Default Require user @WORKGROUP Order allow,deny Allow @LOCAL Allow from 192.168.X.X </Location> # All administration operations require an administrator to authenticate... <Limit CUPS-Add-Modify-Printer CUPS- Delete-Printer CUPS-Add-Modify-Class CUPS-Delete- Class CUPS-Set- Default CUPS-Get-Devices> AuthType Default Require user @ WORKGROUP Order deny,allow </Limit> # All printer operations require a printer operator to authenticate...</pre>	
--	--	--

	<pre><Limit Pause-Printer Resume-Printer Enable-Printer Disable- Printer Pause-Printer-After-Current-Job Hold-New-Jobs Release-Held-New-Jobs Deactivate-Printer Activate-Printer Restart-Printer Shutdown-Printer Startup- Printer Promote-Job Schedule-Job-After CUPS-Accept-Jobs CUPS-Reject-Jobs> AuthType Default Require user @ WORKGROUP Order deny,allow </Limit></pre>	
Modification des droits pour stockage des pilotes Windows	<pre>cd /var/lib/samba/printers/ setfacl -R -m g:msi:rwx * setfacl -R -m d:g:msi:rwx *</pre>	
Attribution des droits de gestion d'imprimantes Windows	<pre>net rpc rights grant msi SePrintOperatorPrivilege</pre>	
Drivers Windows	<pre>Récupération depuis cups.org de cupswindows- 6,0-source apt-get install libcupsys2-dev</pre>	
Configuration génération des fichiers PDF	<pre>mkdir -p /opt/donnees/pdf chmod -R 770 /opt/donnees/ cd /opt setfacl -m g:draf:rx donnees/ setfacl -m g:msi:rwx donnees/ cd donnees setfacl -m g:draf:rwx pdf setfacl -m d:g:draf:rwx pdf setfacl -R -m g::- /opt/donnees setfacl -R -m d:g::- /opt/donnees</pre>	
Vidage quotidien des	<pre>/etc/vidagePdf.sh : #!/bin/bash</pre>	

fichiers PDF générés	rm -Rf /opt/donnees/pdf/* crontab -l : 0 21 * * * /root/vidagePdf.sh	
Configuration CUPSPDF	/etc/cups/cups-pdf.conf Out /opt/donnees/pdf /etc/apparmor.d/usr.sbin.cupsd @ {HOME}/PDF/ rw, @ {HOME}/PDF/* rw, /opt/donnees/pdf/ rw, /opt/donnees/pdf/* rw,	
Déclarer l'imprimante	Dans l'interface web, puis : cupsaddsmb -H localhost -U login -v PDF_Printer Configuration Windows en suivant. 44	

TABLE 3.1 – Fiche d descriptive du serveur

3.18 Conclusion

La réalisation de cette partie pratique nous a permis de découvrir CUPS et de se familiariser avec ces différents services, ainsi que l'ensemble des directives de configuration de serveurs d'impression.

conclusion générale

Conclusion Générale

L'objectif de notre travail est la proposition de la mise en place d'un serveur d'impression CUPS.

Durant la réalisation de notre travail nous avons été confrontés à plusieurs difficultés telles que la mise en place d'une architecture réseau accessible par différents hôtes clients Linux et Windows ainsi que l'adressage.

L'implémentation et le bon fonctionnement de notre serveur d'impression CUPS au sein d'une entreprise, administration ou autre, dépend de l'état du réseau de ces derniers, à fin de centraliser les tâches d'impression sur l'ensemble du réseau et offrir aux administrateurs la possibilité de distribuer des pilotes, avec connexion automatique possible entre systèmes Linux, de gérer des files d'attente, de gérer des droits d'accès par l'intermédiaire du serveur CUPS.

Bibliographie

BIBLIOGRAPHIE

OUVRAGES

- [1] Guy Pujolle, « **LES RESEAUX** », ÉDITIONS EYROLLES, 2007
- [2] Jean-Luc Montagnier, « **RESEAU D'ENTREPRISE PAR LA PRATIQUE** », ÉDITIONS EYROLLES.2005
- [3] Lydie Bundschuh, « **INSTALLEZ ET DEPANNEZ VOTRE RESEAU A DOMICILE** », ÉDITIONS YALLOU.2009
- [4] Laurent LEVIER Cédric LORENS , « **TABLEAU DE BORD DE LA SECURITE RESEAU** », EDITIONS EYROLLES 2006.
- [6] Stalling keurque, « **LES RESEAUX LAN** », prentice hall .2000
- [7] Remi Badonnel, « **SUPERVISION DES RESEAUX ET SERVICES AD-HOC** », THESE DOCTORAT, université HENRI POINCARÉ - Nancy, 2006

WEBO-GRAPHIE

<http://www.supinfo.com> : / visité en 05 mai 2012

- ✓ Campus BOOSTER
- ✓ La grande école d'informatique de Nantes.
- ✓ La grande école d'informatique de Bordeaux.

[5] <http://lesdefinitions.fr/materiel-informatique> : / visité en 12 mai 2012

<http://www.cups.org> : / visité en 27 mai 2012 ;

<http://www.padl.com> : / visité en 03 juin 2012.