Dossier ressource

AX340E

Système de contrôle d'accès par serrure bio-métrique

Dossier ressource

I) Mise en situation

L'hôtel ***Beau rivage*** est un hôtel balnéaire non loin d'une plage sur la côte française. Il est principalement destiné à l'accueil des familles de passage dans la région pour des séjours touristiques. Il comprend 28 chambres sur 4 étages pour un total de 72 lits.

Il fait partie d'une chaîne hôtelière qui possède une dizaine d'établissements similaires sur le territoire. Chaque établissement a son propre fonctionnement, même si certains aspects sont communs à tous les hôtels du réseau. Voici quelques caractéristiques de l'hôtel ***Beau rivage*** :

- Une équipe de 15 personnes (1 gérant et 14 employés) assurent l'accueil et l'entretien des locaux.
- Hors saison, la réception est ouverte de 6h30 à 9h30 et de 17h00 à 21h00 en semaine, et de 7h30 à 10h30 et de 17h00 à 21h00 week-ends et jours fériés.
- Durant la saison estivale, la réception est ouverte de 6h30 à 21h00 7j/7.
- L'accès aux chambres est assuré par des serrures électroniques à reconnaissance d'empreintes digitales.
- L'hôtel possède 7 locaux techniques équipés de contrôle d'accès bio-métriques.

Le choix de ce type d'accès s'est avéré pertinent pour les gestionnaires, et ce pour plusieurs raisons :

- Les clients sont des vacanciers qui passent le plus clair de leur temps à la plage et une clé n'est pas toujours simple à gérer pour eux.
- Il était fréquent que des clients perdent leur clé ou les oublient, sans parler des clients qui cassaient leur clé dans la serrure.
- Les clients étant souvent en famille, chaque membre de la famille n'était pas toujours en possession de la clé lors de son retour à l'hôtel.
- Le personnel d'entretient devait toujours avoir un passe pour pouvoir accéder aux chambres pour le ménage ou autre.

De plus, l'accès aux locaux techniques de l'établissement (lingerie, réserves alimentaires, locaux électriques, chambres froides, bureaux etc.) posait lui aussi des problèmes de gestion :

- Le personnel change assez souvent au cours d'une année, ainsi que d'une saison sur l'autre. Certains employés partaient avec les clés ou les perdaient.
- Les clés étaient parfois prêtées à des "amis" ou "proches" pour se servir dans les réserves.
- Les employés oubliaient parfois leurs clés chez eux.

L'équipement de tous les établissements du groupe s'est fait petit à petit, mais reste en évolution constante. Chaque serrure étant équipée d'un port Ethernet, elles se raccordent tout simplement sur le réseau informatique de l'hôtel et la gestion se fait depuis un PC en toute simplicité.

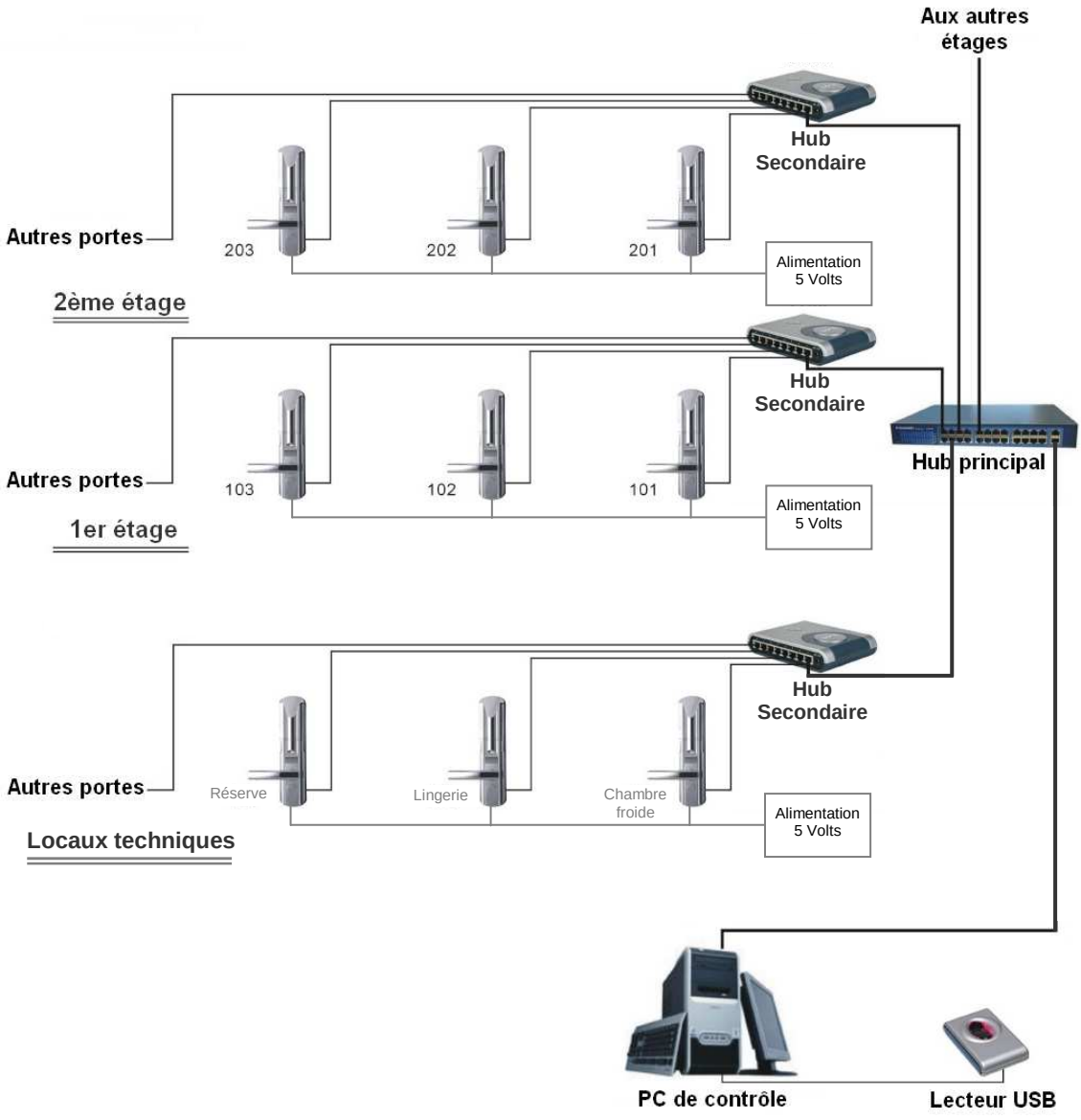
Grâce à l'utilisation de serrures bio-métriques pour la gestion des accès, l'ensemble des problèmes évoqués précédemment a pu être résolu.

II) Configuration matérielle du système

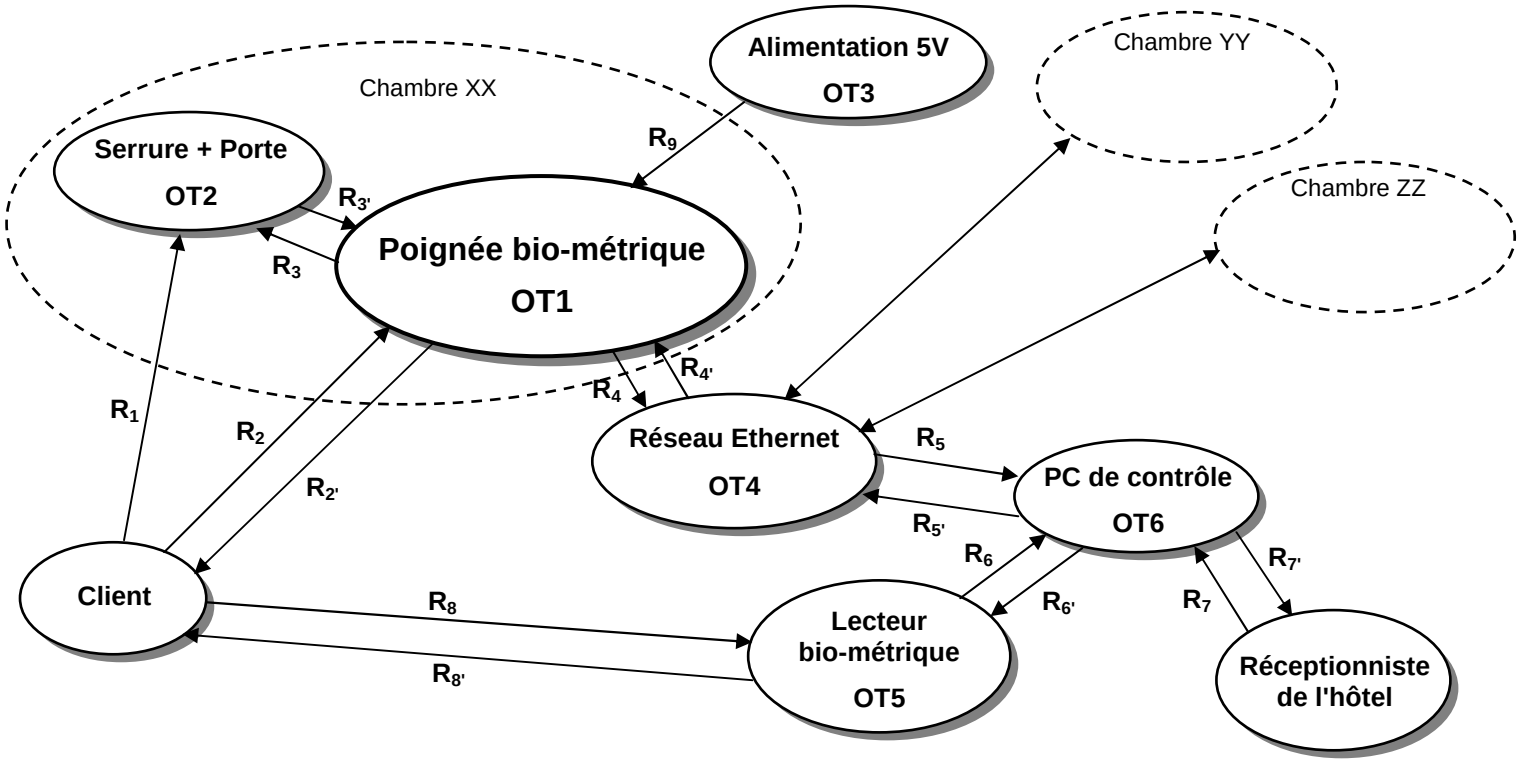
L'installation de l'hôtel ***Beau rivage*** est constituée de la façon suivante (elle est quasi identique à celles des autres hôtels du groupe) :

- Un PC de contrôle se trouvant à la réception de l'hôtel,
- Un lecteur d'empreintes digitales relié au PC de contrôle par liaison USB,
- Un HUB Ethernet principal,
- Un HUB secondaire à chaque étage,
- Une serrure par chambre.

Schéma global d'une installation



III) Diagramme sagittal



Définition des relations du diagramme sagittal :

- **R_1 :** Action du client sur la poignée de la porte.
- **R_2 :** Demande d'accès, présentation d'un doigt pour identification.
- **$R_{2'}$:** Information sonore et visuelle sur l'autorisation ou non de l'accès
- **R_3 :** Information électrique de commande de la gâche.
- **$R_{3'}$:** Information électrique sur l'état de la gâche
- **R_4 :** Information électrique relative à la demande d'autorisation d'accès.
- **$R_{4'}$:** Information électrique d'autorisation, de refus ou de paramétrage
- **R_5 :** Information électrique relative à la demande d'autorisation d'accès.
- **$R_{5'}$:** Information électrique d'autorisation, de refus ou de paramétrage
- **R_6 :** Information électrique image de l'empreinte du client.
- **$R_{6'}$:** Information électrique d'autorisation de début de lecture de l'empreinte
- **R_7 :** Saisi des données client et paramétrage du système.
- **$R_{7'}$:** Information visuelle sur l'état du système
- **R_8 :** Empreinte digitale à entregistrer.
- **$R_{8'}$:** Information sonore et visuelle sur l'enregistrement de l'empreinte digitale.
- **R_9 :** Alimentation en tension continue 5V de la serrure biométrique.

IV) Description des éléments constitutifs du système

OT1 : ***Poignée biométrique*** (Référence : AX340E)

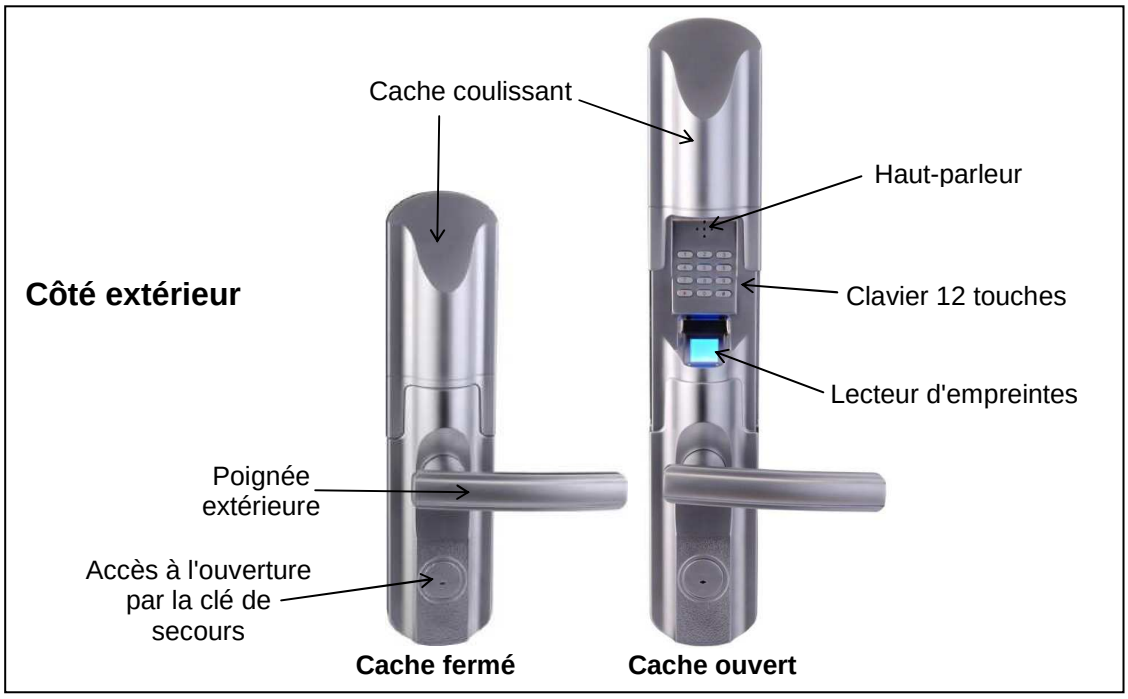
Chaque poignée bio-métrique est montée sur une porte et permet l'accès à une chambre (ou un local technique) après identification de l'empreinte digitale de la personne. Chaque poignée est paramétrée dès son installation pour être insérée au réseau.

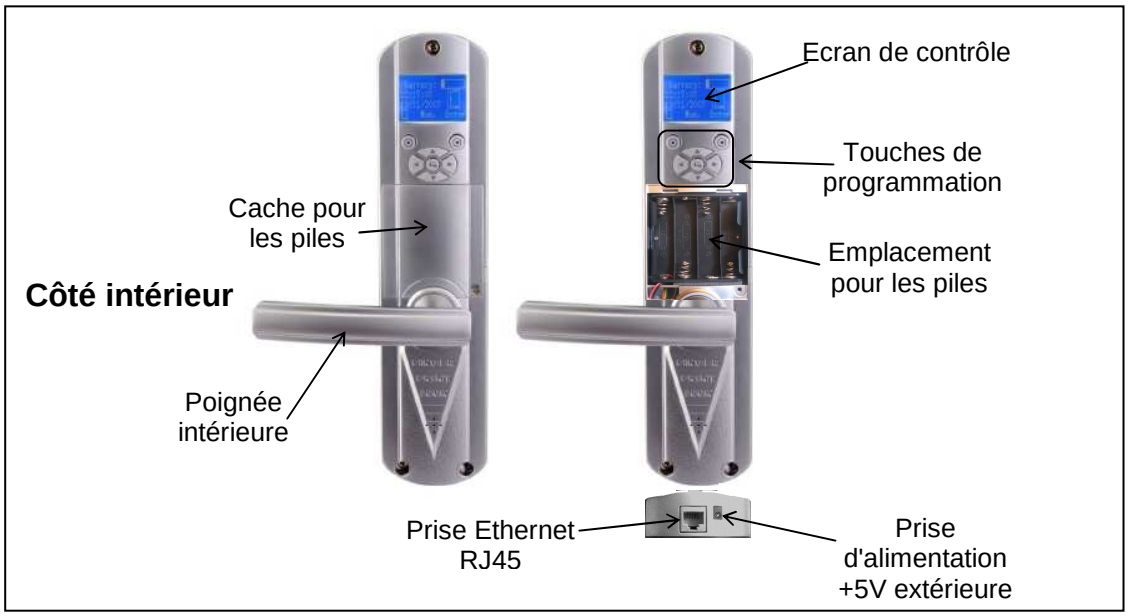
Elles peuvent être paramétrés localement, en utilisant l'écran et le clavier de la serrure, ou bien à distance par l'intermédiaire du PC via le réseau Ethernet.

Chaque poignée a besoin d'être alimentée en +5V continu qui peut être fourni par une série de piles 1,5 montées directement dans la serrure, ou bien une alimentation extérieure.

Voir Annexes 1 et 2 sur la biométrie, ainsi que les documents constructeur.

Structure de la serrure :





OT2 : ***Serrure + porte***

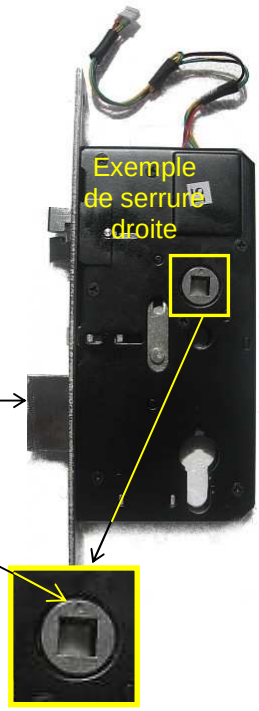
Elle a pour rôle de gérer physiquement l'accès au local concerné. Chaque porte est munie d'une serrure commandée électriquement par la poignée bio-métrique. La serrure électrique condamne ou libère l'accès à l'usager.

La serrure est mortaisée dans la porte, entre les deux parties (intérieure et extérieure) de la poignée bio-métrique.

Le déverrouillage et le verrouillage de la porte se font par l'intermédiaire du **pêne dormant**.

La poignée extérieure (avec lecteur d'empreinte) doit toujours être montée du côté du **poinçon sur la serrure**.

Il y a deux types de serrures : **gauche et droite**. L'emplacement du poinçon détermine le type de serrure.



Fonctionnement de la serrure :

La **têtière** (partie dormante) montée sur le cadre fixe de la porte est équipée d'un **galet presseur** à ressort.

Lorsque l'on ferme la porte, ce galet vient appuyer sur le **bouton de déblocage** du pêne dormant de la serrure. De ce fait, le pêne dormant est en position sortie. La porte est verrouillée. Tant que le bouton de déblocage est appuyé, le pêne dormant est actionnable par les poignées (intérieure ou extérieure)

Lorsque la porte est ouverte, rien ne vient presser le bouton de déblocage du pêne dormant. Ainsi, le pêne dormant reste en permanence rentré dans la serrure.

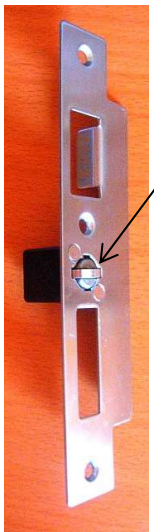


Fig. A

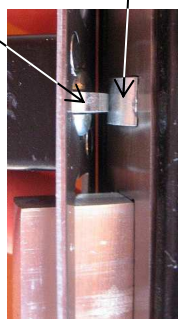


Fig. C

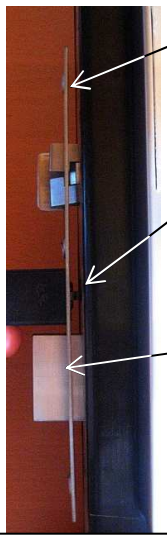


Fig. A

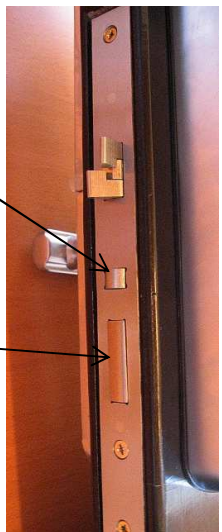


Fig. B

OT3 : ***Alimentation +5V***

Il y en a une par étage. Elles sont installées dans un local technique. Elles permettent d'alimenter plusieurs serrures en convertissant le 220V fourni par l'EDF en une tension continue de +5V.

OT4 : ***Réseau Ethernet***

Il s'agit d'un réseau Ethernet 100MB utilisant des câbles 8 conducteurs torsadés. Chaque câble est muni d'une prise RJ45 à chaque extrémité. Les distances entre les serrures et les Hub secondaires peuvent aller jusqu'à 100 mètres maximum selon le câble utilisé. Il utilise un mode de câblage 100BASE-TX en étoile avec des Hub secondaires reliés à un Hub principal.

OT5 : ***Lecteur biométrique USB***

Il permet d'enregistrer les empreintes digitales de chaque client au fur et à mesure de leur enregistrement dans l'hôtel. Il doit être paramétré pour être intégré à l'installation. Il est connecté au PC par câble USB.

OT6 : ***PC de contrôle***

Il permet de gérer l'accès aux chambres ainsi que l'ensemble de l'installation. Chaque client et membre du personnel a son empreinte enregistrée sous forme cryptée dans le PC. Il est équipé du logiciel "**Fingerprint Lock Management System**" conçu spécialement pour ce type d'application.

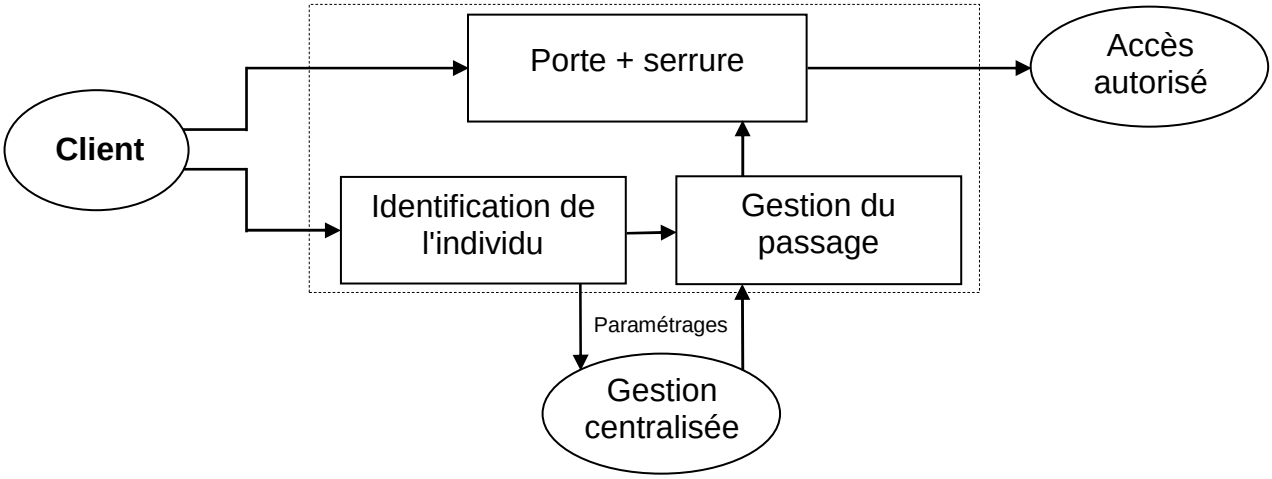
Le PC communique en permanence avec les serrures de l'installation par l'intermédiaire du réseau Ethernet.

V) Expression de la fonction d'usage

Le système de contrôle d'accès a pour rôle de :

- Permettre l'enregistrement de nouveaux usagers (clients, employés etc.).
- Identifier les personnes qui désirent accéder à un lieu (chambres, locaux techniques etc.).
- Autoriser ou refuser l'accès de ces personnes dans le lieu souhaité.

VI) Schéma fonctionnel de niveau II



VII) Synoptique de fonctionnement du système

La serrure bio-métrique est constituée de trois parties distinctes :

- La poignée "Intérieure", qui se trouve côté intérieur du lieu à contrôler (une chambre par exemple). Cette partie ne demande aucune identification, ainsi l'usager peut sortir du lieu à son gré. La poignée intérieure actionne la serrure en permanence ; il suffit d'appuyer sur la poignée pour ouvrir la porte.
- La poignée "Extérieure", qui se trouve côté extérieur du lieu à contrôler. Cette partie demande à l'usager de s'identifier pour autoriser l'ouverture. La poignée extérieure actionne la serrure seulement si l'accès est autorisé. Les deux poignées (intérieure et extérieure) sont reliées électriquement.
- La serrure électrique qui se trouve entre les deux poignés et qui libère ou bloque l'ouverture mécanique de la porte. Cette serrure est commandée électriquement par la poignée intérieure. Elle est reliée à celle-ci par 4 fils.

Mise sous tension :

A la mise sous tension, la serrure ne laisse apparaître aucun signe particulier.

Ouverture de la porte :

Etat initial : Porte fermée ; pêne dormant sorti ; porte verrouillée **(Fig. A Page 6)**

- Pour l'ouvrir depuis l'intérieur, il suffit d'actionner la poignée intérieure qui actionne systématiquement le pêne dormant.
- Pour l'ouvrir depuis l'extérieur, plusieurs solutions existent :
  1. La serrure bio-métrique est en mode "passage libre" ; la porte est alors déverrouillée, il suffit d'actionner la poignée pour ouvrir.
  2. La serrure est en mode "verrouillé". Dans ce cas, il faut s'identifier :
     - ***Identification par code seul*** : Composer le code d'accès sur le clavier. La serrure émet un bruit de vibreur ; la serrure est déverrouillée pendant 6 secondes, puis de nouveau bloquée.
     - ***Identification par empreinte digitale seule*** : Poser le doigt sur le capteur. Le système analyse (scanne) l'empreinte. Un carillon indique qu'elle est reconnue, la serrure émet un bruit de vibreur ; la serrure est déverrouillée pendant 6 secondes, puis de nouveau bloquée.
     - ***Identification par code ou empreinte***, au choix : Mêmes fonctionnements que précédemment.
     - ***Identification par code de réveil + empreinte*** : Composer tout d'abord le code de réveil, puis placer le doigt sur le capteur pour identification.

Fermeture de la porte :

Etat initial : Porte ouverte ; pêne dormant rentré ; porte déverrouillée **(Fig. B - Page 6)**

En rabattant la porte dans l'encadrement, la serrure vient se placer en face de la têtière. Le galet presseur de la têtière appui alors sur le bouton de déblocage du pêne dormant **(Fig. C - Page 6)**. Le pêne dormant sort de la serrure et verrouille la porte.

Annexe 1 : Notions de bio-métrie

1) A propos du contrôle d'accès

Les techniques de contrôle d'accès sont basées sur ce que l'on sait (par exemple, un code d'accès), sur ce que l'on possède (par exemple, un badge), sur ce que l'on est ou sur une combinaison de ces trois critères. La biométrie exploite le troisième : ce que l'on est.

Il convient de distinguer **l'identification** et **l'authentification** :

- **L'identification** permet de vérifier que l'identité d'un individu qui se présente existe bien dans la base de référence.
- **L'authentification** permet de prouver l'identité revendiquée par un utilisateur.

2) Définition

Un système de contrôle bio-métrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à l'individu.

3) Les bases de la biométrie

Les données analysées par les systèmes bio-métriques sont basées sur :

- L'analyse morphologique (empreintes digitales, forme de la main, traits du visage,...)
- Les traces biologiques (odeur, salive, ADN,...)
- L'analyse comportementale (dynamique du tracé de la signature, frappe sur un clavier d'ordinateur,...)

4) Fiabilité des systèmes bio-métriques

Les performances d'un système bio-métrique sont mesurées par deux taux d'erreur : le **FRR** (False Reject Rate) et le **FAR** (False Acceptance Rate).

- Le **FRR** se rapporte à la probabilité qu'un système bio-métrique échoue dans l'authentification d'une personne enregistrée.
- Le **FAR** se rapporte à la probabilité d'une vérification incorrecte.

Un troisième paramètre (**FER**) mesure le taux d'échec à l'enrôlement. Il traduit la probabilité d'absence d'une caractéristique bio-métrique pour un individu dans une population.

Des tests menés en 2002 aux Aéroports de Paris ont donné un taux de faux rejets (FAR) de 0,1% pour l'empreinte digitale, 0,2% pour la main et 8% pour l'iris.

5) Technologies d'identification bio-métrique

Les technologies les plus fréquemment utilisées sont au nombre de huit. Il s'agit de :

- La reconnaissance des empreintes digitales,
- La reconnaissance de la main,
- La reconnaissance de la rétine,
- La reconnaissance de l'iris,
- La reconnaissance de visages,
- La reconnaissance vocale,

- La reconnaissance de la dynamique de signature,
- La reconnaissance de la dynamique de la frappe au clavier.

Les six premières analysent des caractéristiques morphologiques ; les deux dernières, des caractéristiques comportementales.

La reconnaissance des empreintes digitales

Cette technologie de reconnaissance s'appuie sur les structures périodiques des empreintes digitales. Ces structures sont appelées "***minuties***". Les minuties les plus fiables sont conservées lors de l'enrôlement.

L'acquisition des données est faite par un capteur électronique de type optique, thermique, capacitif ou à ultrasons. Cette dernière est considérée comme la plus fiable, mais aussi la plus coûteuse.

Il convient de prendre garde aux contrefaçons. Un faux doigt peut en effet être créé à partir d'une empreinte, comme l'ont notamment montré deux "pirates" allemands ! Ce type d'attaque peut fonctionner avec plusieurs types de capteurs (capteur de température, capteur de battements cardiaques, capteur de conductivité ou mesure de la constante diélectrique relative), principalement à cause de la marge d'erreur qu'ils autorisent.

La reconnaissance de la main

Cette technologie se base sur la géométrie de la main dans l'espace. 90 caractéristiques sont prises en compte comme la longueur et la largeur des doigts, la largeur et l'épaisseur des paumes, la forme des articulations, les dessins des lignes de la main,...

Très utilisée aux Etats-Unis, cette technologie a aussi les faveurs de la CNIL en France, plutôt que la reconnaissance des empreintes digitales.

La reconnaissance de la rétine

Fiable (mais aussi coûteuse), la reconnaissance de la rétine est utilisée pour des applications de haute sécurité, notamment dans les domaines militaires et nucléaires. Cette technologie se base sur un nombre de points de repères allant jusqu'à 92. Malheureusement, quelques risques pour la santé ont été relevés.

La reconnaissance de l'iris

Comme la reconnaissance de la rétine, la reconnaissance de l'iris est une technologie fiable : Il est prouvé que la probabilité de trouver deux iris identiques est inférieure à l'inverse du nombre d'humains ayant vécu sur terre.

La reconnaissance de visages

Cette technologie se base sur des caractéristiques telles que l'écart entre les yeux, la forme de la bouche, le tour du visage, la position des oreilles,... En tout, plus de 60 critères fondamentaux existent.

***Photo de gauche** : estimation de la position de la tête*

***Photo de droite** : estimation de la position de caractéristiques faciales*

Elle présente une fiabilité moyenne (incapacité de différencier de vrais jumeaux, utilisation d'un maquillage ou d'un masque en silicone, perturbation par des éléments tels que les lunettes, la barbe, la moustache, le piercing, une blessure,...) et elle est souvent perçue par les utilisateurs comme intrusive.

Elle se révèle par contre utile dans des systèmes de télésurveillance intelligente.

La reconnaissance vocale

La technologie de reconnaissance vocale se base sur les caractéristiques de la parole, constituée par une combinaison de facteurs comportementaux (vitesse, rythme,...) et physiologiques (tonalité, âge, sexe, fréquence, accent, harmonique,...)

Elle est vulnérable (utilisation d'un enregistrement, par exemple) mais peu intrusive.

La reconnaissance de la dynamique de signature

Cette technologie recourt à une table à digitaliser électronique et analyse les mouvements du stylo : Vitesse de la signature, variation du rythme du stylo, calcul de la distance pendant laquelle le stylo est suspendu entre deux lettres,...

La reconnaissance de la dynamique de la frappe au clavier

Cette technologie correspond grosso modo à la transposition de la graphologie aux moyens électroniques. Sont pris en compte : La vitesse de frappe, la suite de lettres, la mesure des temps de frappe, la pause entre chaque mot, la reconnaissance de mots précis,...

D'autres technologies existent comme, par exemple :

- Les empreintes génétiques (réservées en France pour les crimes sexuels depuis 1998, ainsi que, depuis 2003, à la sécurité intérieure),
- La reconnaissance du réseau veineux.

Prometteuse, cette dernière technique sonde par infrarouge le dessin du réseau de veines soit du doigt soit de la main. Elle est notamment développée par Hitachi pour les établissements bancaires.

Aux Etats-Unis, 82% des personnes interrogées en août 2002 ont fait l'expérience de la reconnaissance des empreintes digitales, contre 46% pour la signature dynamique, 27% pour la voix, 22% pour le visage, 20% pour les yeux, 19% pour la géométrie de la main et 7% pour la dynamique de la frappe au clavier.

6) Contraintes légales liées aux systèmes bio-métriques

En France, l'utilisation des technologies bio-métriques est réglementée par la **C**ommission **N**ationale de l'**I**nformatique et des **L**ibertés (**CNIL**). L'objectif de la CNIL est de prévenir l'usage abusif des fichiers et des outils informatiques, y compris dans le futur (et y compris en cas de changement de régime politique !).

En pratique, s'il n'y a pas de stockage de critères morphologiques dans une base de données (si, par exemple, les données sont stockées sur une carte à puce), il n'y a pas de problème. Par contre, lorsqu'une base de données existe, la CNIL contrôle la finalité et sa proportionnalité avant d'accepter :

Par exemple, il est arrivé qu'un système de reconnaissance d'empreinte digitale destiné à la gestion des horaires du personnel d'une entreprise ait été jugé disproportionné.

En France, le CLUSIF (Club de la Sécurité des Systèmes d'Information Français) a également proposé une comparaison (avantages / inconvénients) des principales technologies bio-métriques.

Techniques	Avantages	Inconvénients
Empreintes digitales	Coût, ergonomie moyenne, facilité de mise en place, taille du capteur	Qualité optimale des appareils de mesure (fiabilité), acceptabilité moyenne, possibilité d'attaques (rémanence de l'empreinte,...)
Forme de la main	Très ergonomique, bonne acceptabilité	Système encombrant, coût, perturbation possible par des blessures et l'authentification des membres d'une même famille
Visage	Coût, peu encombrant, bonne acceptabilité	Jumeaux, psychologie, religion, déguisement, vulnérabilité aux attaques
Rétine	Fiabilité, pérennité	Coût, acceptabilité faible, installation difficile
Iris	Fiabilité	Acceptabilité très faible, contrainte d'éclairage
Voix	Facilité	Vulnérable aux attaques
Signature	Ergonomie	Dépendant de l'état émotionnel de la personne, fiabilité
Frappe au clavier	Ergonomie	Dépendant de l'état physique de la personne

7) Quelques applications de la biométrie

La biométrie est notamment utilisée dans les applications suivantes :

- Le contrôle d'accès logique (contrôle d'accès à un ordinateur, login d'ouverture de sessions réseaux, accès distants connexions VPN,...),
- Le contrôle d'accès physique à des locaux (salle informatique, service de recherche, site nucléaire,...),
- L'identification judiciaire,
- Les machines pointeuses.
- ...

Annexe 2 : La reconnaissance d'empreintes digitales

1) Introduction

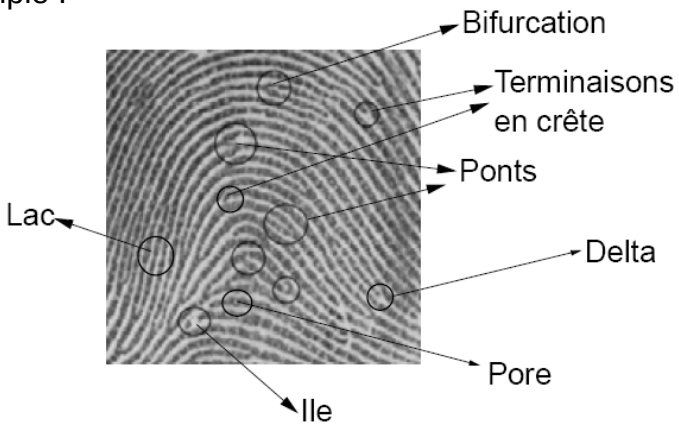
La technique des empreintes digitales est une des techniques d'identification les plus anciennes qui soit. Elle a été développée vers la fin du 19ème siècle par Alphonse Bertillon, fondateur de la police scientifique en France. A cette époque, et jusqu'à récemment, une tablette et un encreur sont le matériel utilisé pour la capture d'empreinte. Le premier système automatique d'authentification a été commercialisé au début des années 1960.

2) Définitions

Les minuties : Codifiées à la fin des années 1800 en "Caractéristiques de Galton[1]", les minuties sont composées, de façon rudimentaire, de terminaisons en crêtes (le point où la crête s'arrête), et de bifurcations (le point ou la crête se divise en deux).

Le noyau : C'est le point intérieur situé en général au milieu de l'empreinte. Il sert souvent de point de repère pour situer les autres minuties. D'autres termes existent également : ***Le lac***, ***le pont***, ***le croisement***, ***le delta***, ***la vallée***, ***le pore*** etc.

Notons que dans l'analyse des minuties, une douzaine de variables doivent être prises en compte. Exemple :



3) Principe de fonctionnement

L'authentification par empreintes digitale repose sur la concordance entre le fichier d'enregistrement, ou "Signature", obtenu lors de l'enrôlement, et le fichier obtenu lors de l'authentification.

Ces deux fonctions se décomposent chacune en plusieurs étapes :

Enrôlement :

- Capture de l'image de l'empreinte. Les données d'un doigt sont en principe suffisantes à l'enrôlement, mais la plupart des systèmes enregistrent au moins deux doigts (un par main, par exemple) pour parer l'indisponibilité résultant de petites blessures.
- Numérisation de l'image afin d'extraire les minuties, ou éléments caractéristiques.
- Enregistrement sur un support (carte à puce, disque dur…)

[1] Du nom de Sir Francis Galton

Authentification :

- Capture de l'image de l'empreinte.
- Numérisation de l'image afin d'extraire les minuties, ou éléments caractéristiques.
- Comparaison entre l'échantillon et le gabarit de référence (la "signature").
- Prise de décision.

Lors de la capture de l'image, celle-ci est toujours constituée à partir des points de contact du doigt sur le capteur.

Etapes de traitement :

- Lorsque la capture de l'image est réalisée, elle doit être convertie dans un format approprié. L'extraction des minuties est réalisée grâce à différents algorithmes. Il s'agit ensuite par une technique mathématique (segmentation) d'éliminer les informations non-utiles du système : Niveau de bruit trop élevé (image sale, doigt mal placé).
- L'image est numérisée. Afin de localiser précisément les terminaisons et les bifurcations, les crêtes sont affinées de 5 à 8 pixels à 1 pixel. A ce stade, l'image a des distorsions (des déformations) et de fausses minuties, qui peuvent être dues à des cicatrices, de la sueur, un défaut de propreté du doigt comme du capteur. Les minuties vont être filtrées afin de ne conserver que les plus fiables.

Les avis divergent sur le rapport de proportion entre minuties extraites pour l'enrôlement et minuties suffisamment fiables pour la vérification. A partir de 31 minuties extraites, seulement 10 pourront correspondre lors de l'authentification.

A titre d'information, une empreinte numérisée occupe en moyenne entre 250 et 1000 octets.

Il existe plusieurs techniques de lecture de l'empreinte digitale :

- La technique optique
- La technique silicium
- La technique ultrason

Nous ne traiterons que la technique optique

4) La technique optique

C'est, après l'encre, la technique la plus ancienne et qui a fait ses preuves.

Le principe physique utilisé est celui de "la réflexion totale frustrée" : Le doigt est placé sur un capteur éclairé par une lampe. Une caméra CMDs (Charge Modulation Device) avec CCD (Charged Couple Device – en français : DTC : Dispositif de Transfert de Charges) convertit l'image, composée de crêtes foncées et de vallées claires, en un signal vidéo retraité d'afin d'obtenir une image utilisable.

Nous pouvons différencier les terminaux en lumière visible :

- à fenêtre sèche
- à fenêtre à film liquide

La fenêtre est l'emplacement où l'utilisateur met le doigt.

Dans ce dernier cas, la fenêtre est nettoyée avant prise de vue par un mélange d'eau et d'éthanol injecté sous le doigt. Des terminaux à image infra-rouge par capteur

linéaire intégré sont parfois utilisés, mais présentent les mêmes inconvénients que ceux à lumière visible.

La technique optique

Avantages	Inconvénients
• Son ancienneté et sa mise à l'épreuve	• Il est possible que l'empreinte d'un utilisateur précédent reste latente, d'où une possibilité de dégradation de l'image par sur-impression.
• Sa résistance aux changements de température, jusqu'à un certain point.	• Apparition possible de rayures sur la fenêtre.
• Son coût abordable	• D'autre part, le dispositif CCD peut s'user avec le temps et devenir moins fiable.
• Sa capacité à fournir des résolutions de plus de 500 dpi	• Problèmes de contrastes (un doigt propre et sec devient trop clair tandis qu'un doigt humide et recouvert d'un film gras devient très foncé), problème résolu grâce au film liquide mais système mal accepté par les gens (il mouille le doigt !)

Annexe 3 : L'adressage IP

1) *Qu'est-ce qu'une adresse IP*

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP (*Internet Protocol*), qui utilise des adresses numériques, appelées adresses IP, composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Exemple : 194.153.205.26.

Ces adresses servent aux ordinateurs du réseau pour communiquer entre-eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau.

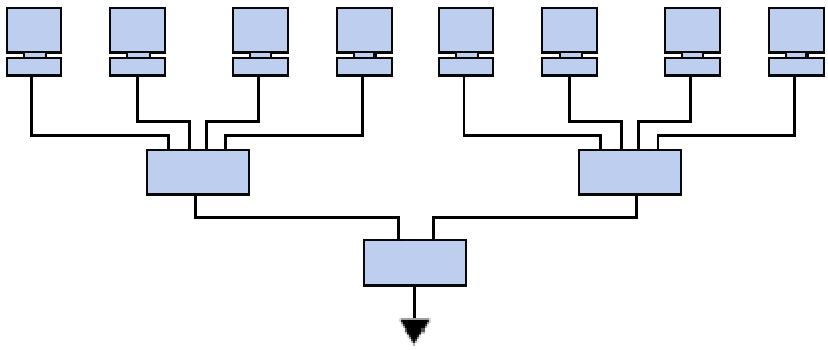
C'est l'**ICANN** (Internet Corporation for Assigned Names and Numbers, remplaçant l'IANA, Internet Assigned Numbers Agency, depuis 1998) qui est chargée d'attribuer des adresses IP publiques, c'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public internet.

2) *Déchiffrement d'une adresse IP*

Une **adresse IP** est une adresse 32 bits, généralement notée sous forme de 4 nombres entiers séparés par des points. On distingue en fait deux parties dans l'adresse IP :

- Une partie des nombres à gauche désigne le réseau. Elle est appelée **ID de réseau** (en anglais *net-ID*)
- Les nombres de droite désignent les ordinateurs de ce réseau. Elle est appelée **ID d'hôte** (en anglais *host-ID*)

Soit l'exemple ci-dessous :



Notons le réseau de gauche *194.28.12.0*. Il contient les ordinateurs suivants :

194.28.12.1 à 194.28.12.4

Notons celui de droite *178.12.0.0*. Il comprend les ordinateurs suivants :

178.12.77.1 à 178.12.77.6

Dans le cas ci-dessus, les réseaux sont notés *194.28.12* et *178.12.77*, puis on numérote un à un chacun des ordinateurs le constituant.

Imaginons un réseau noté *58.0.0.0*. Les ordinateurs de ce réseau pourront avoir les adresses IP allant de *58.0.0.1* à *58.255.255.254*. Il s'agit donc d'attribuer les numéros de telle façon qu'il y ait une organisation dans la hiérarchie des ordinateurs et des serveurs.

Ainsi, plus le nombre de bits réservé au réseau est petit, plus celui-ci peut contenir d'ordinateurs.

En effet, un réseau noté *102.0.0.0* peut contenir des ordinateurs dont l'adresse IP peut varier entre 102.0.0.1 et 102.255.255.254 (256 x 256 x 256 – 2 = 16777214 possibilités), tandis qu'un réseau noté *194.26* ne pourra contenir que des ordinateurs dont l'adresse IP sera comprise entre 194.26.0.1 et 194.26.255.254 (256 x 256 – 2 = 65534 possibilités), c'est la notion de **classe d'adresse IP**.

3) *Adresses particulières*

Lorsque l'on annule la partie *host-ID*, c'est-à-dire lorsque l'on remplace les bits réservés aux machines du réseau par des zéros (par exemple *194.28.12.0*), on obtient ce que l'on appelle l'**adresse réseau**. Cette adresse ne peut être attribuée à aucun des ordinateurs du réseau.

Lorsque la partie *net-ID* est annulée, c'est-à-dire lorsque les bits réservés au réseau sont remplacés par des zéros, on obtient l'**adresse machine**.

Lorsque tous les bits de la partie *host-ID* sont à 1, l'adresse obtenue est appelée l'**adresse de diffusion** (en anglais **broadcast**). Il s'agit d'une adresse spécifique, permettant d'envoyer un message à toutes les machines situées sur le réseau spécifié par le *net-ID*.

A l'inverse, lorsque tous les bits de la partie *net-ID* sont à 1, l'adresse obtenue constitue l'**adresse de diffusion limitée** (**multicast**).

Enfin, l'adresse **127.0.0.1** est appelée **adresse de rebouclage** (en anglais **loopback**), car elle désigne la **machine locale** (en anglais *local-host*).

4) *Les classes de réseaux*

Les adresses IP sont réparties en classes, selon le nombre d'octets qui représentent le réseau.

Classe A

Dans une adresse IP de classe A, le premier octet représente le réseau.

Le bit de poids fort (le premier bit à gauche) est à zéro, ce qui signifie qu'il y a 2^7 (0000 0000 à 0111 1111) possibilités de réseaux, soit 128 possibilités. Toutefois, le réseau 0 (0000 0000) n'existe pas, et le nombre 127 est réservé pour désigner votre machine.

Les réseaux disponibles en classe A sont donc les réseaux allant de **1.0.0.0** à **126.0.0.0** (les derniers octets sont des zéros ce qui indique qu'il s'agit bien de réseaux et non d'ordinateurs !).

Les trois octets de droite représentent les ordinateurs du réseau, le réseau peut donc contenir un nombre d'ordinateur égal à : 2^{24} - 2 = 16 777 214 ordinateurs.

Une adresse IP de classe A, en binaire, ressemble à ceci :

0	xxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
Réseau		Ordinateurs		

Classe B

Dans une adresse IP de classe B, les deux premiers octets représentent le réseau.

Les deux premiers bits sont 1 et 0, ce qui signifie qu'il y a 2^{14} possibilités de réseaux, soit 16384 réseaux possibles. Les réseaux disponibles en classe B sont donc les réseaux allant de **128.0.0.0** à **191.255.0.0**

Les deux octets de droite représentent les ordinateurs du réseau. Le réseau peut donc contenir un nombre d'ordinateurs égal à :
2^{16} - 2 = 65534 ordinateurs.

Une adresse IP de classe B, en binaire, ressemble à ceci :

10	xxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
Réseau			Ordinateurs	

Classe C

Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les trois premiers bits sont 1,1 et 0, ce qui signifie qu'il y a 2^{21} possibilités de réseaux, c'est-à-dire 2 097 152. Les réseaux disponibles en classe C sont donc les réseaux allant de **192.0.0.0** à **223.255.255.0**

L'octet de droite représente les ordinateurs du réseau, le réseau peut donc contenir:
2^{8} - 2 = 254 ordinateurs.

Une adresse IP de classe C, en binaire, ressemble à ceci :

110	xxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx
Réseau				Ordinateurs

5) *Attribution des adresses IP*

Le but de la division des adresses IP en trois classes A, B et C est de faciliter la recherche d'un ordinateur sur le réseau. En effet avec cette notation il est possible de rechercher dans un premier temps le réseau que l'on désire atteindre, puis de chercher un ordinateur sur celui-ci. Ainsi, l'attribution des adresses IP se fait selon la taille du réseau.

Classe	Nbre de réseaux possibles	Nbre d'ordinateurs maxi sur chacun
A	126	16777214
B	16384	65534
C	2097152	254

Les adresses de classe A sont réservées aux très grands réseaux, tandis que l'on attribuera les adresses de classe C à des petits réseaux d'entreprise par exemple

6) *Adresses IP réservées*

Il arrive fréquemment dans une entreprise ou une organisation qu'un seul ordinateur soit relié à Internet, et c'est par son intermédiaire que les autres ordinateurs du réseau accèdent à Internet (on parle généralement de ***proxy*** ou de passerelle).

Dans ce cas de figure, seul l'ordinateur relié à Internet a besoin de réserver une adresse IP auprès de l'ICANN. Toutefois, les autres ordinateurs ont tout de même besoin d'une adresse IP pour pouvoir communiquer ensemble en interne.

Ainsi, l'ICANN a réservé une poignée d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à Internet sans risquer de créer des conflits d'adresses IP sur le réseau des réseaux. Il s'agit des adresses suivantes :

- **Adresses IP privées de classe A** : 10.0.0.1 à 10.255.255.254, permettant la création de vastes réseaux privés comprenant des milliers d'ordinateurs.
- **Adresses IP privées de classe B** : 172.16.0.1 à 172.31.255.254, permettant de créer des réseaux privés de taille moyenne.
- **Adresses IP privées de classe C** : 192.168.0.1 à 192.168.0.254, pour la mise en place de petits réseaux privés.

7) *Masques de sous-réseau*

a) Masque de sous-réseau

En résumé, on fabrique un masque contenant des 1 aux emplacements des bits que l'on désire conserver, et des 0 pour ceux que l'on veut annuler. Une fois ce masque créé, il suffit de faire un ET logique entre la valeur que l'on désire masquer et le masque afin de garder intacte la partie souhaitée, et annuler le reste.

Ainsi, un **masque réseau** (en anglais *netmask*) se présente sous la forme de 4 octets séparés par des points (comme une adresse IP), il comprend (dans sa notation binaire) des zéros au niveau des bits de l'adresse IP que l'on veut annuler (et des 1 au niveau de ceux que l'on désire conserver).

b) Intérêt d'un masque de sous-réseau

Le premier intérêt d'un masque de sous-réseau est de permettre d'identifier simplement le réseau associé à une adresse IP.

En effet, le réseau est déterminé par un certain nombre d'octets de l'adresse IP (1 octet pour les adresses de classe A, 2 pour les adresses de classe B, et 3 pour la classe C). Or, un réseau est noté en prenant le nombre d'octets qui le caractérise, puis en complétant avec des 0. Le réseau associé à l'adresse *34.56.123.12* est par exemple *34.0.0.0*, car il s'agit d'une adresse IP de classe A.

Pour connaître l'adresse du réseau associé à l'adresse IP *34.56.123.12*, il suffit donc d'appliquer un masque dont le premier octet ne comporte que des 1 (soit 255 en notation décimale), puis des 0 sur les octets suivants.
Le masque est: *11111111.00000000.00000000.00000000*
Le masque associé à l'adresse IP *34.208.123.12* est donc *255.0.0.0*.
La valeur binaire de *34.208.123.12* est: *00100010.11010000.01111011.00001100*
Un ET logique entre l'adresse IP et le masque donne ainsi le résultat suivant :

```
00100010.11010000.01111011.00001100
                  ET
11111111.00000000.00000000.00000000
                  =
00100010.00000000.00000000.00000000
```

Soit *34.0.0.0*. Il s'agit bien du réseau associé à l'adresse *34.208.123.12*

En généralisant, il est possible d'obtenir les masques correspondant à chaque classe d'adresse :

- Pour une adresse de **Classe A**, seul le premier octet doit être conservé. Le masque possède la forme suivante *11111111.00000000.00000000.00000000*, c'est-à-dire **255.0.0.0** en notation décimale ;
- Pour une adresse de **Classe B**, les deux premiers octets doivent être conservés, ce qui donne le masque suivant *11111111.11111111.00000000.00000000*, correspondant à **255.255.0.0** en notation décimale ;

- Pour une adresse de **Classe C**, avec le même raisonnement, le masque possédera la forme suivante *11111111.11111111.11111111.00000000*, c'est-à-dire **255.255.255.0** en notation décimale

c) Création de sous-réseaux

Reprenons l'exemple du réseau 34.0.0.0, et supposons que l'on désire que les deux premiers bits du deuxième octet permettent de désigner le réseau.

Le masque à appliquer sera alors : 11111111.11000000.00000000.00000000

C'est-à-dire 255.192.0.0

Si on applique ce masque, à l'adresse 34.208.123.12 on obtient : 34.192.0.0

En réalité, il y a 4 cas de figures possibles pour le résultat du masquage d'une adresse IP d'un ordinateur du réseau 34.0.0.0

- Soit les deux premiers bits du deuxième octet sont **00**, auquel cas le résultat du masquage est **34.0.0.0**
- Soit les deux premiers bits du deuxième octet sont **01**, auquel cas le résultat du masquage est **34.64.0.0**
- Soit les deux premiers bits du deuxième octet sont **10**, auquel cas le résultat du masquage est **34.128.0.0**
- Soit les deux premiers bits du deuxième octet sont **11**, auquel cas le résultat du masquage est **34.192.0.0**

Ce masquage divise donc un réseau de classe A (pouvant admettre 16 777 214 ordinateurs) en 4 sous-réseaux - d'où le nom de *masque de sous-réseau* - pouvant admettre 2^{22} ordinateurs, c'est-à-dire 4 194 304 ordinateurs.

Il est intéressant de noter que dans les deux cas, le nombre total d'ordinateurs est le même, soit 16 777 214 (4 x 4 194 304 - 2 = 16 777 214).

Le nombre de sous-réseaux dépend du nombre de bits attribués en plus au réseau (ici 2). Le nombre de sous-réseaux est donc :

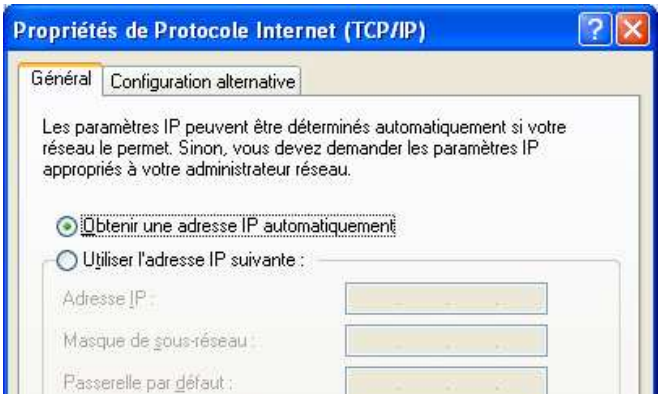
Nombre de bits	Nombre de sous-réseaux
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8 (impossible pour une classe C)	256

8) *Sur un PC :*

L'attribution de l'adresse IP et de son masque de sous réseau se fait dans la fenêtre ***Propriété de Protocole Internet***.

Généralement, l'adresse est obtenue automatiquement, sauf dans des cas particuliers.

L'adresse du PC doit être différente de celles des autres appareils branchés sur le réseau.



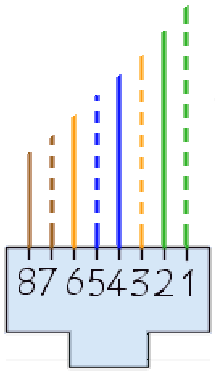
Annexe 4 : Les câbles réseaux RJ45

1) *Constitution d'un câble RJ45*

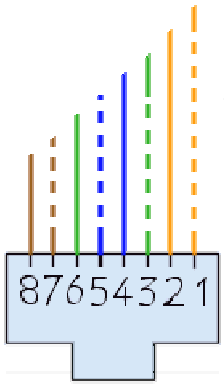
Les câbles utilisés pour les réseaux Ethernet RJ45 sont appelés *paires torsadées* (en anglais *twisted pairs*) car ils sont constitués de 4 paires de fils torsadés. Chaque paire de fils est constituée d'un fil de couleur unie et d'un fil possédant des rayures de la même couleur. Il est fortement recommandé d'utiliser du câble de catégorie 5.

Il existe deux standards de câblage différant par la position des paires orange et verte, définis par le ***E**lectronic **I**ndustry **A**ssociation* / ***T**elecommunications **I**ndustry **A**ssociation* (**EIA/TIA**):

TIA/EIA 568A



TIA/EIA 568B



Connecteur RJ45 sur une prise mâle vue de face, contacts vers le haut.

TIA/EIA 568B

Le contact 1 est à gauche sur une prise femelle (carte réseau ou bien prise murale) et à droite sur une prise mâle, connecteur vers soi, contacts vers le haut !

2) *Les câbles droits*

Lorsqu'un ordinateur est connecté à un hub ou un switch, le câble utilisé est un câble droit (*patch cable*), ce qui signifie qu'un fil relié au contact 1 d'un côté est relié au contact 1 de l'autre côté. La norme de câblage généralement utilisée pour réaliser des câbles droits est la norme TIA/EIA T568A, cependant il existe des câbles droits selon la norme TIA/EIA T568B. Seules les couleurs de certains fils changent, cela n'a aucune incidence sur le fonctionnement car les fils sont reliés de la même façon.

3) *Les câbles croisés*

Lorsque deux ordinateurs sont reliés directement, on utilise un câble croisé (*cross cable* ou *crossover*). On utilise pour ce type de câble la norme *TIA/EIA T568A* pour une des extrémités et la norme *TIA/EIA T568B* pour l'autre. Ce type de câble s'achète dans le commerce, mais il est très facile de le réaliser soi-même.