République **A**lgérienne **D**émocratique et **P**opulaire

Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'INFORMATIQUE

DEPARTEMENT D'INFORMATIQUE

Mémoire de Fin d'Etudes
De MASTER ACADEMIQUE

Domaine : **Mathématiques et Informatique**
Filière : **Informatique**

Spécialité : **Systèmes Informatiques.**

Présenté par
Makhlouf OULD LAMARA

Thème

Conception et réalisation d'une plateforme d'administration de dispositifs informatiques à distance.

Mémoire soutenu publiquement le 02/10/ 2016 devant le jury composé de :

Président : M^{r} Dib A.
Promoteur: M^{r} Chaieb Y.
Examinateur: M^{r} Sadou S.
Examinateur : M^{r} Kerbiche.

Encadreur M^{r} : Fraihat Adlane.

Remerciements

Je tiens à exprimer ma profonde gratitude et mes sincères remerciements :

A Adlane qui m'a transmis savoir et connaissances.

A mon promotteur Mr CHAIEB Yazid.

Aux membres du jury qui nous ont fait l'honneur de bien examiner notre travail.

A tous ce qui mon soutenu et encouragé pour finalisé cette modeste contribution.

Dédicaces

Je dédie ce modeste travail

A mes chers parents, ce travail vous doit beaucoup, qu'il soit pour vous le témoignage de ma reconnaissance infinie pour ces années de compréhension et d'efforts communs.

A mon cher oncle Ferhat que j'aime beaucoup et sa femme.

Aux adorables: mes princesses Katia, Sophie, Zora, mon prince Zakari.

A mes grands-mères Ferroudja et Ouiza que Dieu nous les garde.

A ma tante Fouzia et son époux Massinissa.

A tous mes oncles et tantes, cousins et cousines maternels et paternels.

A tous mes amis(es).

A toutes les personnes que j'estime.

Makhlouf OULD LAMARA

Table des matières

Introduction Générale
Chapitre I : Tour d'horizon.

Chapitre II : Analyse et conception:

Chapitre III : Réalisation:

Liste des Figures

Liste des Figures

Liste des Tableaux

Liste des tableaux

Liste des Abréviations

Liste des Abréviations

ADSL	Asymmetric Digital Subscriber Line
AJAX	Asynchronous JAvascript and Xml
ARPANET	Advanced Research Projects Agency Network
ASP	application service provider
C.F.A.O	conception et fabrication assistées par ordinateur
CDI	disque compact interactif
CERN	Centre européen pour la recherche nucléaire
CP	Continuos Power.
CRM	customer relationship management
DARPA	Defense Advanced Research Projects Agency, soit Agence pour les projets de recherche avancée de défense.
DCC	Digital Compact Cassette , cassette numérique.
DNS	Domain name system.
DRAC	Dell OpenManage Remote Assistant Card
ERP	Enterprise Resource Planning.
FAH	Fournisseur d'Applications Hébergées
FM-200	Extincteur d'incendie.
IAB	Internet Activities Board.
IBM	International Business Machines
INRIA	Institut national de recherche d'informatique et d'automatique en France
IPS	système de prévention d'intrusion.
ISOC	Internet Society
IT	Information technology
KVM	keyboard-video-mouse switch
MILNET	Military Network
MIT	Massachussets Institute of Technology
MRTG	Multi Router Traffic Grapher.
NCP	Network Communication Protocol.

NCP	norme internet
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
NSFNET	National Science Foundation Network
PCI	Peripheral Component Interconnect
PGI	progiciel de gestion intégré.
PME	Petite et moyenne entreprise
PRP	Prime Rating Power
QoS	Quality of Service
RAT	Remote Administration Tool
RRDTool	Round-Robin database.
SDN	:software defined networking
SI	système d'information
SLA	Service Level Agreement
SMS	Short Message Service
SPOF	Single Point Of Failure, point unique de défaillance
TCP/IP	Transmission Control Protocol/ Internet Protocol.
UCLA	Université de Californie à Los Angeles
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol - Protocole de message de contrôle sur Internet
UPS	uninterruptible power supply
WAP	Wireless Application Protocol

Introduction Générale

Introduction Générale

Les besoins de l'Homme ne cessent d'augmenter en terme de rapidité de calcule, de control, de gestion et de communication, l'informatique a su répondre à ses attentes, nous allons ensemble découvrir l'évolution fulgurante de l'informatique pour ensuite voir les tendances du moment qui sont le Cloud et l'administration à distance.

L'administration d'ordinateurs à distance représente un marché gigantesque plébiscité par des besoins de control et d'assistance à distance plus en plus accrus.
Dans le présent travail, le but étant d'illustrer et de présenter une nouvelle réflexion d'administration à distance. Bien que des progrès significatifs aient été enregistrés pour de telles techniques, la performance est encore loin d'être satisfaisante, ce qui plaide d'ailleurs en faveur du développement de nouvelles techniques.

Ce mémoire est composé de trois chapitres :

Le premier chapitre est consacré au tour d'horizon de l'informatique, la convergence vers le Cloud et l'émergence de nouvelles techniques d'administration, présentera les centres de données, la délocalisation et l'externalisation, le monitoring et surtout l'administration à distance, ses outils et pratiques.

Le second chapitre est consacré pour les limites des outils et techniques d'administrations et ainsi présenter la réflexion c'est la partie analyse et conception.

Le dernier chapitre détaillera l'ensemble des technologies utilisées dans notre technique.

Nous terminons par des perspectives et une conclusion générale qui résume l'apport essentiel de notre travail.

Chapitre 1

Tour d'Horizon

1. Introduction:

L'informatique est la science du traitement automatique et rationnel de l'information considérée comme le support des connaissances et des communications.

C'est un domaine d'activité scientifique, technique et industriel concernant le traitement automatique de l'information via l'exécution de programmes informatiques par des machines des systèmes embarqués, des ordinateurs, des robots, des automates, etc.

Ces champs d'application peuvent être séparés en deux branches, l'une, de nature théorique, qui concerne la définition de concepts et modèles, et l'autre, de nature pratique, qui s'intéresse aux techniques concrètes d'implantation et de mise en œuvre sur le terrain. Certains domaines de l'informatique peuvent être très abstraits, comme la complexité algorithmique, et d'autres peuvent être plus proches d'un public profane. Ainsi, la théorie des langages demeure un domaine davantage accessible aux professionnels formés (description des ordinateurs et méthodes de programmation), tandis que les métiers liés aux interfaces homme-machine sont accessibles à un plus large public.

Dans ce chapitre nous intéresserons à l'histoire fulgurante de l'évolution de l'informatique, convergence vers le Cloud et l'émergence de nouvelles techniques d'administration.

2. Histoire de l'informatique:

L'histoire de l'informatique est très étroitement liée à celle des ordinateurs. Le terme « informatique » date de 1962. Il vient de la contraction des mots « information » et « automatique ».

L'histoire de l'informatique est justement marquée par la volonté des Hommes d'automatiser certaines tâches longtemps réalisées à la main, en particulier le calcul. C'était donc l'idée primaire qui a abouti à la conception de l'ordinateur : pouvoir procéder à des calculs plus simplement. L'être humain s'est vite rendu compte qu'il lui fallait des moyens plus élaborés s'il voulait perfectionner ses calculs. Ainsi l'évolution s'est produite selon une chronologie établie tout au fil des siècles. Cependant, les besoins de l'homme ont évolué avec, et c'est ainsi que l'ordinateur de nos temps modernes représente bien plus qu'un simple outil de calcul, et concrétise toute la pensée et l'évolution de l'esprit de l'homme que nous sommes !! L'ordinateur d'aujourd'hui nous accompagne dans beaucoup de nos travaux et de nos occupations. On peut lire, écrire, stocker des données, calculer, jouer, faire des chirurgies à distance et effectuer bien d'autres opérations sur nos ordinateurs [16].

3. Les réseaux: Du réseau ARPANET à Internet

L'origine d'internet vient d'une initiative d'une agence du département américain de la défense à la fin des années 1960, la DARPA (Defense Advanced Research Projects Agency, soit Agence pour les projets de recherche avancée de défense) visant à réaliser un réseau de transmission de données (transfert de paquets) à grande distance entre différents centres de recherche sous contrat. Il s'agit de l'ARPANET (Advanced Research Projects Agency Network) qui verra le jour en 1969. Le premier nœud de raccordement relie alors l'Université de

Californie à Los Angeles (UCLA) et l'Institut de recherche de Stanford, suivis de peu par les universités de Californie à Santa Barbara et de l'Utah puis s'étend progressivement jusqu'à connecter une quarantaine de sites en 1972.

La connexion entre tous les réseaux existants, c'est-à-dire "l'internet" proprement dit, n'est devenue possible qu'avec la définition de normes communes.

En 1970, a été créé un premier protocole de communication, le NCP (Network Communication Protocol). En 1974, les Américains Vint Cerf et Robert Kahn publient un ouvrage dans lequel ils décrivent le protocole TCP/IP qui permet à des réseaux hétérogènes de communiquer entre eux. Dans ce document le terme internet apparaît pour désigner l'interconnexion de plusieurs réseaux. Ce langage commun permet de relier tous les ordinateurs et tous les réseaux existants. En 1983, ARPANET est divisée en deux branches, MILNET étant la partie militaire et ARPANET devenant civil, mais principalement destiné à la communication entre les établissements scientifiques. ARPANET adopte alors officiellement la norme TCP/IP au détriment du NCP. C'est le démarrage d'internet, avec à l'époque environ un millier de postes utilisateurs. La même année, le système de noms de domaines (DNS) est mis au point. Il permet la correspondance entre une adresse IP et un nom de domaine et plus généralement de trouver une information à partir d'un nom de domaine. La National Science Foundation (NSF) lance, en 1986, le réseau NSFNET en réponse à l'afflux des nouveaux arrivants sur ARPANET qui provoque un phénomène de surcharge. En 1989, les particuliers et les entreprises privées accèdent au réseau. En 1990, ARPANET est intégré au réseau de la NSF qui en finance le développement jusqu'en 1995. En 1992, alors qu'un million de machines sont interconnectées, l'Internet Society (ISOC), association de droit américain à but non lucratif, voit le jour. Elle a pour rôle de promouvoir et de coordonner le développement des réseaux informatiques dans le monde. Elle intègre l'Internet Activities Board (IAB), organisme chargé d'élaborer les normes et standards d'internet [22].

3.1.1. La création du World Wide Web

Internet s'ouvre véritablement au grand public avec la création, lors du Centre européen pour la recherche nucléaire (CERN), en 1991, du World Wide Web, par Tim Berners-Lee. Il s'agit d'un système d'interface graphique, très ergonomique et très facile d'utilisation, qui permet de passer d'une page ou d'un site à un autre en "cliquant" sur un lien dit "hypertexte". La navigation sur la "Toile" devient ainsi extrêmement aisée. Le web ouvre donc le réseau à de nouveaux utilisateurs peu familiarisés avec l'informatique. En quelques mois, les sites web se multiplient. Phénomène technique et social de grande ampleur, le World Wide Web a dû se doter, en 1994, d'un consortium pour gérer son évolution afin que ce puissant instrument de publication demeure ouvert, fidèle en ceci à l'esprit d'internet. Le World Wide Web Consortium ou W3C s'est placé sous la responsabilité du Massachussets Institute of Technology (MIT) aux Etats-Unis et de l'Institut national de recherche d'informatique et d'automatique (INRIA) en France [10]

3.1.2. L'essor d'internet

Depuis lors, internet a connu une expansion planétaire et a permis, grâce à la convergence de l'informatique, de l'audiovisuel et des télécommunications, la multiplication de services de toute nature sur le World Wide Web comme la messagerie électronique, les

groupes et forums de discussion, le commerce électronique, la consultation d'informations, la diffusion d'images fixes, de fichiers audio et vidéo…

Et les outils et techniques continuent d'évoluer, avec le développement des réseaux haut débit filaires (ADSL) ou sans fil (WIFI et Bluetooth) ou de l'internet mobile (WAP), ou encore avec les technologies et produits du **web 2.0** qui renouvellent les modes d'usages et d'appropriation des services internet par les utilisateurs (RSS, blogs, wikis, outils de partage de photos, de videos, réseaux sociaux tels facebook ou LinkedIn...) [10].

3.1.3. Le Web 2.0:

Figure 1 web 2.0

L'expression fondamentale « Web 2.0 » désigne l'ensemble des techniques, des fonctionnalités et des usages du World Wide Web qui ont suivi la forme originelle du web [7], caractérisée par plus de simplicité et d'interactivité. Elle concerne en particulier les interfaces et les échanges permettant aux internautes ayant peu de connaissances techniques de s'approprier de nouvelles fonctionnalités du web. Les internautes peuvent d'une part contribuer à l'échange d'informations et interagir (partager, échanger, etc.) de façon simple, à la fois au niveau du contenu et de la structure des pages, et d'autre part entre eux, créant notamment le Web socialL'internaute devient, grâce aux outils mis à sa disposition, une personne active sur la toile.

Le Web 2.0 est donc l'évolution du Web vers l'interactivité à travers une complexification interne de la technologie mais permettant plus de simplicité d'utilisation, les connaissances techniques et informatiques n'étant pas indispensables pour les utilisateurs.

L'expression « Web 2.0 » utilisée par Dale Dougherty (en) en 2003, diffusée par Tim O'Reilly en 2004 et consolidée en 2005 avec l'exposé de position « What Is Web 2.0 » s'est imposée à partir de 2007 [17].

3.1.3.1. Présentation:

Le Web 2.0 facilite l'interaction entre utilisateurs, le crowdsourcing et la création de réseaux sociaux rudimentaires, pouvant servir de contenu et exploitant les effets de réseau, avec ou sans réel rendu visuel et interactif de pages Web. En ce sens, les sites Web 2.0 agissent plus comme des points de présence, ou portails Web centrés sur l'utilisateur plutôt que sur les

sites web traditionnels. L'évolution des supports permettant de consulter les sites Web, leurs différents formats, amènent en 2008 une approche recentrée sur le contenu plus que sur l'aspect.

Les nouveaux gabarits Web 2.0 (en anglais : template) tentent d'apporter un soin graphique, des effets, en restant compatibles avec cette diversité de supports. Dans le Web 2.0, l'internaute devient acteur en alimentant les sites en contenu, comme les blogs, ou de manière collaborative avec les wikis, voire des dispositifs très rigoureux de type science citoyenne.

Les sites internet 2.0 permettent aux utilisateurs de faire plus que d'en retirer de l'information. En augmentant ce qu'il était déjà possible de faire avec le Web 1.0, ils apportent aux utilisateurs de nouvelles interfaces et de nouveaux logiciels informatiques. Les utilisateurs peuvent maintenant apporter des informations aux sites Web 2.0 et avoir le contrôle sur certaines de celles-ci.

Du point de vue des techniques de développement web , le terme a été également beaucoup utilisé dans la seconde moitié des années 2000 pour désigner la généralisation de l'utilisation des technologies dites AJAX qui permettent de modifier l'apparence d'une page web en fonction des instructions données par le serveur sans avoir à la recharger , ce qui donne à un site web des possibilités comme interagir avec l'utilisateur lors du remplissage d'un formulaire, faire de l'auto complétion lors du remplissage d'un champ ou faire des effets visuels dynamiques intelligents sur des pages qui était au choix soit figées, soit remplis d'effets visuels sans utilités autres que cosmétiques. Même si l'ensemble de ces technologies était disponible depuis l'invention de Javascript par le navigateur Web NetScape depuis 1995, elles avaient été dans un premier temps très peu utilisées et ont même dû attendre 2005 pour se voire accoler une dénomination les désignant. Google a été à l'origine d'une prise de conscience massive de l'intérêt que pouvaient avoir ces technologie lorsqu'il a mis en place une auto complétion des recherche dans son moteur de recherche et à sorti son système de cartographie Google Map qui permettait de parcourir une carte en ne chargeant une page web qu'une seul fois. Ces technologies assez complexes et longues à mettre en place sont devenues beaucoup plus accessibles avec l'arrivée en 2006 de la bibliothèque jQuery. Dès lors, il a été souvent utilisé le terme de Web 2.0 pour désigner l'arrivée massive des sites internet qui interagissait (parfois avec outrance, on a parlé du piège du Web 2.0) avec l'utilisateur sans avoir besoin de recharger ses pages. Certaines personnes ont préférées utiliser le terme Web 3.0 en considérant qu'une autre révolution technique avait précédé le phénomène de l'AJAX, d'autres ont considéré que la facilitation de l'utilisation d'AJAX n'était pas une révolution assez importante pour la voir distinguée de la sorte [17].

4. Délocalisation :

4.1. **Définition:**

Selon le dictionnaire LAROUSSE: la délocalisation est l'action de délocaliser quelque chose. Economie, Déplacement d'unité de production d'un pays vers un autre lié à la recherche d'un coût de production plus bas. (Utilisée essentiellement par les firmes multinationales, la délocalisation a pour objectif la recherche d'un environnement juridique plus favorable en matière de réglementation du travail, de fiscalité, des changes ou d'activités polluantes.) [5].

4.2. Le processus de délocalisation:

La délocalisation est une pratique ancienne, qui consiste à déplacer une unité de production afin de bénéficier d'avantages industriels. La libre circulation des capitaux, et des personnes ont amené un regain de cette pratique.

- Pousse les pays, régions et agglomérations à des politiques de redynamisation améliorant leur attractivité économique et incitant à la création de nouvelles activités pour remplacer le « vide » économique ;
- Incite à des formes de management très décentralisées, par exemple le système de l'entreprise étendue, permettant de coordonner sans engager de grands capitaux les meilleures sources de produits et de compétences dans les divers points de la planète et d'être par ailleurs présents sur les marchés économiques les plus porteurs ;
- Induit, à l'inverse, la tentation du protectionnisme, qui risque d'être contre-productif, en isolant des flux économiques mondiaux et en amenuisant le pouvoir d'achat du fait de l'absence de concurrence qui entraîne des prix internes élevés par manque d'efforts d'amélioration et création de rente de monopoles locaux, diminuant encore davantage la compétitivité.

Il se trouve cependant dans l'histoire de l'après Seconde Guerre mondiale des pays qui ont profité d'un protectionnisme opportuniste comme le Japon ou les dragons de l'Asie (Corée, Taïwan, Hong Kong, Singapour). Dans le cas du Japon, de la Corée et de Taïwan, cette stratégie a permis une hausse particulièrement rapide du niveau de vie de la population [17].

4.3. Pays concernés:

Les délocalisations concernent deux types de pays :

- Les pays subissant les délocalisations, qui perdent leurs centres de production, en général les pays industrialisés. C'est le cas de l'Europe Occidentale ou les États-Unis.
- Les pays bénéficiant des délocalisations, qui voient s'implanter chez eux de nouveaux centres de production, en général les pays émergents.

4.4. Cause:

Les causes peuvent être schématiquement résumées autour de deux grandes problématiques : produire moins cher et vendre sur le marché local.

4.5. Avantages sur les Coûts:

- Bénéficier d'une main d'œuvre moins chère,
- S'affranchir de toutes les contraintes des pays occidentaux.
- Bénéficier d'avantages offerts. Certains pays Low Cost, en plus de la main d'œuvre moins chère, offrent des prestations supplémentaires aux grandes entreprises qui s'implantent. Terrains offerts, construction d'usine financée par les communes, exonérations d'impôts.

4.6. Réduire les coûts de transports:

Il est intéressant pour une entreprise d'essayer de vendre ses produits dans les pays émergents (autre terme utilisé pour les pays Low Cost).

- Se rapprocher des marchés de consommation,
- réduire les entraves à l'exportation.
- S'affranchir de la variation des taux de change.

4.7. Conséquences:

Si les conséquences négatives sur les pays subissant les délocalisations sont souvent mises en avant, on en oublie les conséquences positives sur les pays qui bénéficient de ces délocalisations. Nous allons pencher sur les conséquences positives sur les pays de délocalisations:

4.7.1. Conséquences positives de la délocalisation:

Les conséquences sont souvent très positives pour les pays bénéficiant des délocalisations, en particulier les pays émergents. Elles permettent notamment de :

- Créer de nouveaux emplois: Par voie de conséquence, ces délocalisations permettent de :
- Augmenter le niveau de vie de ces pays. Taïwan qui a bénéficié de nombreuses délocalisations notamment du Japon est devenu par exemple un pays riche ;
- Favoriser progressivement la démocratie dans certains pays non démocratiques, ce dernier point est souvent contesté, et la Chine est souvent citée comme un bon contre-exemple.

4.8. Solutions pour les pays en voie de développement:

Si les pays subissant les délocalisations souhaitent les limiter, il n'en est pas de même des pays bénéficiant des délocalisations, synonymes pour eux d'enrichissement. C'est pourquoi, ces derniers font tout ce qui est possible pour favoriser ces délocalisations. Les huit questions clés posées dans "le filtre Factea" [23] permettent de structurer et d'analyser de façon exhaustive les solutions possibles pour favoriser les délocalisations et donc l'implantation de nouvelles entreprises:

Question clé 1 : proximité du service / produit. Favoriser la consommation de produits et services délocalisés. Par exemple, créer des marques à forte attractivité. Rendre la fabrication dans leur pays synonyme de qualité.

Question clé 3 : infrastructures. Développer des infrastructures performantes susceptibles d'attirer les entreprises en leur permettant d'améliorer leur compétitivité avec ces infrastructures. C'est l'un des enjeux que s'est fixée l'Inde, qui souffre aujourd'hui encore d'infrastructures insuffisantes.

Question clé 4 : reproductibilité. Favoriser le transfert de technologies par tout moyen. C'est par exemple ce que fait la Chine en conditionnant l'obtention de grands marchés, au transfert de technologies, comme dans le nucléaire.

Question clé 6 : différentiel de coût. Maintenir le différentiel de coût de production des produits / services entre les pays subissant et bénéficiant des délocalisations. Notamment en freinant l'augmentation des salaires ou encore des contraintes environnementales ou autres.

Question clé 7 : capacité à délocaliser. Aider les PME à délocaliser. Par exemple, en leur proposant des modèles économiques attractifs "prêts à l'emploi" (e.g. sur le recyclage de bouteilles plastiques).

Question clé 8 : volonté de délocaliser. Convaincre les dirigeants et actionnaires de délocaliser. À défaut, racheter des entreprises dans les pays subissant les délocalisations. Puis une fois rachetée, délocalisé en continuant à bénéficier de la marque.

5. Centre de données:

5.1. Définition:

Un centre de données ou data center est un site physique sur lequel se trouvent regroupés des équipements constituants du système d'information de l'entreprise (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne et/ou externe à l'entreprise, exploité ou non avec le soutien de prestataires [9].

C'est un service généralement utilisé pour remplir une mission critique relative à l'informatique et à la télématique. Il comprend en général un contrôle sur l'environnement (climatisation, système de prévention contre l'incendie, etc.), une alimentation d'urgence et redondante, ainsi qu'une sécurité physique élevée.

Des enjeux environnementaux sont liés à la consommation d'électricité des centres de données, et à leur coproduit qu'est la chaleur, dissipée par les serveurs et les systèmes de stockage en particulier.

5.1.1. Description:

Un centre de données se présente comme un lieu où se trouvent différents équipements électroniques, des ordinateurs, des systèmes de stockage et des équipements de télécommunications. Comme son nom l'indique, il sert surtout à stocker les informations nécessaires aux activités d'une entreprise. Par exemple, une banque peut recourir à un tel centre, lui confiant les

informations relatives à ses clients. En pratique, presque toutes les entreprises de taille moyenne utilisent un tel centre. Quant aux grandes entreprises, elles en utilisent souvent plusieurs.

Les bases de données étant souvent cruciales au fonctionnement des entreprises, celles-ci sont très sensibles à leur protection. Pour cette raison, ces centres maintiennent de hauts niveaux de sécurité et de service dans le but d'assurer l'intégrité et le fonctionnement des appareils sur place.

Avant la bulle Internet, des millions de mètres carrés destinés à abriter de tels centres furent construits dans l'espoir de les voir occupés par des serveurs. Depuis, la concentration des centres s'est poursuivie, avec le développement de centres spécialisés pour lesquels les défis les plus importants sont la maîtrise de la climatisation et surtout de la consommation électrique. Ce mouvement a été intégré dans le green computing et vise à aboutir à des centres de traitement de données dits écologiques pour lesquels sont apparus des outils spécialisés [3].

5.2. Composantes:

Pour permettre les missions principales du centre, elles doivent assurer la bonne connexion réseau (internet, intranet, etc.) et une haute disponibilité du système d'information. Pour cela, différentes applications logicielles gèrent les tâches essentielles de l'activité métier des clients. Parmi ces applications, on retrouve des gestionnaires de bases de données, des serveurs de fichiers et des serveurs d'applications.

5.2.1.**Composantes physiques:**

- Climatisation (précise et stable)
- Contrôle de la poussière (filtration de l'air)
- Unité de distribution de l'énergie
- Bloc d'alimentation d'urgence, et une unité de secours (Générateur, UPS)
- Système perfectionné d'alerte d'incendie
- Extinction automatique des incendies (par micro-gouttelettes ou gaz inerte)
- Plancher surélevé
- Conduites pour câbles au-dessus et au-dessous du plancher
- Surveillance par caméras en circuit fermé
- Contrôle des accès, ainsi que sécurité physique
- Surveillance 24/7 des serveurs dédiés (ordinateurs)
- Service de sécurité continuellement présent
- Câbles de paires torsadées de cuivre en Ethernet (Fast ou Gigabit) pour liaisons inter-[jarretières/switches/routeurs/firewall]
- Fibres optiques pour liaisons inter-sites ou inter-[jarretières/switches/routeurs/firewall]

Un centre de traitement de données peut occuper une pièce, un étage ou un grand immeuble. On y retrouve des serveurs 1U ou plus, « U » correspondant à une unité de hauteur de 4,445 cm (soit 1,75 pouce) empilés dans des baies, lesquelles sont arrangés pour former des rangées simples, ce qui permet de circuler facilement parmi les serveurs, tant à l'avant qu'à l'arrière. Quelques appareils, ordinateurs centraux par exemple, sont de dimensions semblables à ces baies. Ils sont souvent placés à leurs côtés.

5.3. Climatisation:

La climatisation donne une température d'environ 20 degrés Celsius. Ce maintien est essentiel, puisque les appareils électroniques génèrent beaucoup de chaleur et deviennent défectueux lorsque la température s'élève au-delà d'une certaine limite.

Elle est également une composante fondamentale du centre de traitement, car s'il est mal conçu, il peut multiplier la consommation électrique nécessaire, pour garder une température stable des équipements et donc le coût mensuel de l'hébergement.

5.3.1. Organisation de la salle pour la climatisation:

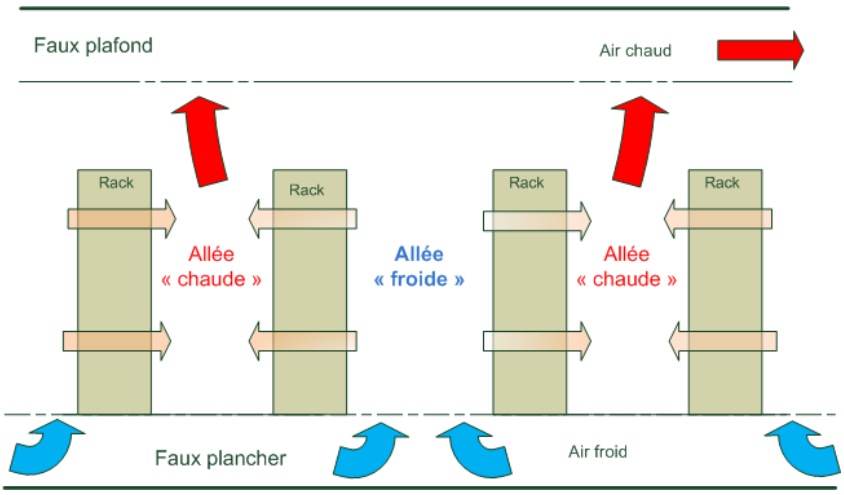


Figure 2 Principe de refroidissement des baises.

L'air chaud est aspiré et de l'air froid insufflé, sans organisation particulière, c'est le minimum indispensable, mais également le moins optimal, car l'air chaud et l'air froid se mélangent, demandant une plus grande consommation électrique pour la climatisation.

Il est généralement conseillé de mettre des caches dans les baies, aux emplacements inutilisés, afin que le flux d'air froid vers chaud se concentre dans les équipements, en dehors du cas précité, où cela ne sert à rien.

Organisation simple en couloir chaud et couloir froid, un couloir sur deux insuffle l'air froid, par le côté avant des serveurs, via des baies grillagées, l'autre couloir aspire l'air chaud par l'arrière. Il est à noter que certains équipements réseau, comme les commutateurs réseau, peuvent avoir le refroidissement avant arrière ou arrière avant, permettant d'organiser de façon plus pratique le câblage, selon les besoins. Le rendement est meilleur, mais l'air chaud peut encore partiellement se mélanger, à l'air froid en bout de rangée de baie ou par-dessus les baies [4].

Utilisation d'un cube de confinement avec corridor chaud, ou froid, selon les choix des constructeurs. Le 'cube' dans lesquelles sont placées les baies, comporte un plafond et des portes à double ou triple vitrage, réduisant considérablement les échanges de température,

seul un côté des baies échange l'air, avec les serveurs orientés en fonction du choix corridor chaud ou corridor froid. C'est aujourd'hui la solution optimale [4].

5.4. Composantes Réseaux:

Parmi les équipements réseaux qu'il contient on trouve:

- les routeurs ;
- les commutateurs ;
- le pare-feu ;
- les passerelles ;
- le système de détection d'intrusion logicielle ; ...etc.

5.5. Sécurité:

L'environnement physique des centres est sous stricte surveillance :

- La surveillance du bon fonctionnement de la climatisation, elle-même essentielle au bon fonctionnement du matériel électronique.
- L'alimentation de secours peut être fournie via un UPS (Uninterruptible Power Supply) et un générateur électrique ou via un groupe tournant (no-break) couplé à un accumulateur cinétique.
- Dans le but de prévenir une perte d'alimentation électrique, toutes les composantes électriques, y compris les systèmes de secours, sont habituellement doublées. Les serveurs dits essentiels sont de plus alimentés par un système qui fait appel à deux sources électriques indépendantes à l'intérieur du centre.
- Les centres ont habituellement un plancher surélevé de 60 cm, fait de dalles amovibles. Cet espace permet la libre circulation de l'air, tout comme il facilite le câblage d'alimentation et de données par des chemins de câble différents. Cependant, des centres de données sont sans plancher technique (alimentation par le dessus des racks, afin de supporter plus facilement des éléments lourds de type mainframe (IBM z10, etc.).
- Ils ont souvent des systèmes complexes de prévention et d'extinction des incendies. Les centres modernes sont souvent équipés de deux systèmes d'alarme. Le premier détecte les particules chaudes émises par les composantes surchauffées de l'équipement, particules qui provoquent souvent un feu. De cette façon, il est possible d'éliminer à sa source un foyer d'incendie (parfois, il suffit d'éteindre un ensemble à soudure pour éliminer le risque d'incendie). Un deuxième système sert à activer un ensemble d'activités si un début d'incendie se manifeste. Ces systèmes sont également dédiés à une portion du centre de traitement de données. Couplés à d'excellentes portes anti-feu et autres appareils de confinement, il est possible de contrôler le feu et de l'éteindre sans affecter le reste du bâtiment.
- Les systèmes conventionnels d'extinction du feu sont aussi nocifs que le feu pour les composants électroniques, c'est pourquoi des procédés alternatifs ont été développés. Certains utilisent l'azote, l'argonite, le FM-200 ou le Novec(tm)1230 FK-5-1-12, alors que d'autres se rabattent sur l'émission de fines particules d'eau ultra-pure (cette eau

n'est pas électriquement conductrice, ce qui n'endommage pas les composants électroniques).

- La sécurité est aussi essentielle au fonctionnement de tels centres. L'accès physique à ces centres est restreint au personnel autorisé, tout comme des caméras vidéo permettent de suivre les personnes sur place. Également, des gardes de sécurité veillent si le centre est grand ou contient des informations considérées comme essentielles.

5.6. Application:

Le but principal d'un centre de traitement de données est d'exécuter des applications qui traitent des données essentielles au fonctionnement d'une société. Ces applications peuvent être conçues et développées en interne par l'entreprise cliente ou par un fournisseur de progiciel de gestion d'entreprise. Il peut s'agir typiquement d'ERP et CRM.

Souvent, ces applications sont réparties dans plusieurs ordinateurs, chacun exécutant une partie de la tâche. Les composantes les plus habituelles sont des systèmes de gestion de base de données, des serveurs de fichiers, des serveurs d'applications, des middlewares.

5.7. Classification des Datacenter:

5.7.1. Organisme de classification:

Uptime Institute est un consortium d'entreprises créé en 1993 [22] dont l'objectif est de maximiser l'efficacité des centres de traitement de données [14]. Uptime Institute est connu en particulier pour avoir défini la notion de "Tier" pour les datacenters, largement adopté dans le monde [20]. Uptime Institute a été racheté par " The 451 Group " en 2009 [19].

5.7.2. Niveaux de classification:

La classification comporte les niveaux Tier I, Tier II, Tier III et Tier IV. Un datacenter doit être certifié par l'Uptime Institute pour revendiquer un niveau de Tier. La classification d'un site est fixée par son sous-système de plus bas niveau. À noter que la notion intermédiaire de type Tier III+ n'existe pas même si on peut la rencontrer dans certaines publications commerciales. En 2015, Uptime Institute est le seul organisme à délivrer des certifications de datacenter. Les autres organismes proposant des classifications de datacenter (BICSI 002, TIA 942, Syska Hennessy) ne proposent pas de certification [17].

Chaque niveau reprend les caractéristiques des niveaux précédents, en y ajoutant certaines améliorations. Donc on a :

Tier I: Le Basique:

Site basique sans redondance (capacité N). Il doit cependant disposer au minimum de salles informatiques dédiées, d'un groupe électrogène disposant d'une réserve de fioul de 12 heures, et d'un onduleur.

Un datacenter Tier I nécessite au moins un arrêt annuel pour maintenance. Une grande partie des maintenances et pannes génèrent un arrêt du site.

Tier II: La Redondance:

Le Tier II est caractérisé par la redondance de sa production (capacité N+R). L'ensemble des composants dispose de redondance : Groupes électrogènes, cuves à fioul, onduleurs, production de froids (groupes froids, pompes, unités de froid en sales, … Les distributions (électricité et froid) n'ont pas besoin d'être redondées.

Un datacenter Tier II nécessite au moins un arrêt annuel pour maintenance. Certaines maintenances et pannes génèrent un arrêt du site, notamment sur les circuits de distribution.

Tier III: La Maintenabilité:

Tous et chacun des composants d'un datacenter Tier III sont maintenables sans arrêt de l'informatique. Le corolaire est que tous les composants et circuits de distribution sont redondants. De plus les groupes électrogènes doivent pouvoir fonctionner à charge nominale (N) sans limitation de durée. Cela implique que les valeurs de groupe à retenir est la « Continuous Power » (CP) selon la norme ISO8528.1. Un déclassement de 30% de la PRP (Prime Rating Power) est à appliquer aux groupes ne déposant de classification « CP ».

Aucune maintenance ne doit provoquer un arrêt de l'informatique. Certaines pannes, incidents ou erreurs humaines peuvent interrompre l'informatique.

Tier IV: La tolérance aux pannes:

Le datacenter Tier IV présente les grandes caractéristiques suivantes :

- Tous les composants et distributions sont maintenables sans impacter IT,
- Réponse automatique aux pannes uniques (N Capacity),
- Compartimentage coupe-feu : aucun élément de la voie A ne peut être dans le même compartiment qu'un composant de la voie B,
- Continuous Cooling : assurer le refroidissement en absence totale d'alimentation électrique,
- Continuous Power: Groupe Électrogène fonctionnant sans limitation de durée,

Le résultat est l'absence de SPOF (Single Point Of Failure, trad: point unique de défaillance).

Le Tier IV est tolérant aux maintenances, pannes (uniques), et incident même graves (incendie par exemple).

5.7.3. Taux de disponibilité:

Des statistiques ont été menées sur la disponibilité des quatre types de tier, en voici les valeurs classées dans le tableau suivant [17]:

Type de tier	Caractéristiques	Taux de disponibilité	Indisponibilité statistique annuelle	Maintenance à chaud possible	Tolérance aux pannes
Tier I	Non redondant	99,671 %	28,8 h	Non	Non
Tier II	Redondance partielle	99,749 %	22 h	Non	Non
Tier III	Maintenabilité	99,982 %	1,6 h	Oui	Non
Tier IV	Tolérance aux pannes	99,995 %	0,4 h	Oui	Oui

Tableau 1 comparatif des 4 types de tiers :

5.7.4. Principe de certification:

Seul l'Uptime Institute peut délivrer une certification. Aucun autre organisme n'est habilité à se prononcer sur le niveau de Tiering d'un Datacenter. Encore moins par auto-évaluation.

La certification repose sur la réponse à l'exhaustivité des critères. Si un seul critère n'est pas rempli le site est déclassé au niveau correspondant.

Le champ couvert par la certification est très large :

- Production de froid : Calcul des puissances, inertie thermique, alimentation des composants, nombre et positionnement des vannes, automates de pilotage, …
- Électricité : Puissance, autonomie (batteries, groupes électrogènes), nombre et positionnement des tableaux et disjoncteurs, caractéristiques techniques de chaque composant, protection foudre, terre, …
- Cheminement physique et compartimentage de tous les circuits.
- Fuel : cheminement physique, détection et réponse aux fuites, positionnement des vannes
- Arrêts d'urgence : maintenance parallèle, séparation des voies.
- Compartiments coupe-feu.
- Détection des fuites (eau et fuel).
- Équilibrage des charges.
- Automates de pilotages, supervision.
- Adduction télécom.

Les domaines non couvert par la certification sont : Les systèmes de détection incendie et extinction, la sécurité physique d'accès au site et salles.

L'absence de maintenance régulière accroît très significativement le risque d'incidents bloquants et fait perdre les bénéfices d'un Tier III ou IV. L'obtention de la certification n'est donc pas une fin en soi. Il est important de maintenir le niveau de qualité tout au long de la vie du datacenter par une maintenance régulière et exhaustive ainsi que des tests de bon fonctionnement.

Dans les faits une grande partie des datacenters, selon la méthode de certification de l'Uptime Institute relèveraient d'un niveau Tier II [17].

6. Externalisation :

6.1. Définition :

6.1.1. Etymologie : Du latin *externus,* extérieur, du dehors, étranger.

6.1.2. Définition Larousse: *n.f* Action pour une entreprise de confier une partie de ses activités à des partenaires extérieurs.

L'externalisation sous-traitance, en anglais : Outsourcing, désigne le transfert de tout ou partie d'une fonction d'une organisation (entreprise ou administration) vers un partenaire externe [25].

6.2. Description :

Elle consiste très souvent en la sous-traitance des activités jugées non essentielles et non stratégiques : pour une entreprise, il s'agit de celles qui sont les moins productrices de revenus. Il s'agit d'un outil de gestion stratégique qui se traduit par la restructuration d'une entreprise au sein de sa sphère d'activités : ses compétences de base et son activité principale (*core business* en anglais).

L'externalisation diffère de la simple prestation extérieure de services, et de la simple sous-traitance, dans la mesure où il y a :

- 2pilotage étroit par l'entreprise donneuse d'ordre ;
- engagement du prestataire externe.

Le processus inverse, c'est-à-dire la reprise à l'interne de l'entreprise des activités externalisées est parfois observée. On parle alors de réinternalisation confondue avec la relocalisation ou backsourcing [17].

6.2.1. L'externalisation du point de vue économique:

C'est un accord passé entre une organisation et un tiers pour la prise en charge, l'exploitation, la gestion continue et l'amélioration :

- de fonctions entières de l'organisation (ex. : informatique, nettoyage, ressources humaines, paie/revenus, facturation, comptabilité, marketing et communication) ;
- d'infrastructures (ex. : système d'informations, systèmes de sécurité, réseaux de télécommunications) ;
- de processus opérationnels (ex. : exploitation de matières premières, production industrielle, exploitation d'un réseau de télécommunications, stockage, logistique, transports) en amont ou aval de l'organisation.

6.2.2. L'externalisation du point de vue juridique :

L'externalisation repose en termes juridiques sur un contrat à durée fixe portant sur le transfert de toute ou partie de la fonction, du service et/ou de l'infrastructure ou du processus opérationnel de l'organisation entre l'organisation propriétaire et un opérateur. Les clauses de retour ou de réversibilité sont la clef d'une externalisation réussie.

Ce contrat peut inclure un transfert d'actifs et/ou de personnel. Le client se concentre sur la définition des résultats à atteindre.

L'externalisation est susceptible de toucher des organisations publiques et privées. C'est désormais une question de stratégie administrative qui se pose.

6.3. Démarche à suivre afin d'externaliser :

6.3.1. Identification des processus externalisables :

Avoir recours à une solution d'externalisation est semblable à l'adoption de tout nouveau processus. Les étapes initiales comprennent l'établissement d'une politique générale, la définition du cœur de métier de l'entreprise et d'une liste de fonctions susceptibles d'être externalisées, puis la sélection de fournisseurs.

6.3.2. Validation économique :

Il est nécessaire d'effectuer une analyse coûts-bénéfices pour mesurer la valeur du modèle d'externalisation ainsi qu'une analyse de risques (gestion des risques et coût du backsourcing).

6.3.3. Mise en œuvre détaillée par contrat :

La mise en œuvre auprès d'un fournisseur de services est un processus complexe qui s'étudie sérieusement et donne lieu en général après des études de faisabilité, comportant des indicateurs de services mesurables et des matrices de responsabilités réciproques, à la rédaction d'une convention de services (SLA).

Du point de vue de la technique contractuelle, un conseil juridique s'avère indispensable pour examiner les points critiques du contrat à savoir :

- la définition du service attendu selon l'état de l'art, les spécifications techniques mesurables objectivement et pratiques pour être parfaitement appréhendées ;
- la définition du niveau de(s) performance(s) qui conditionnera les malus et bonus en termes de rémunération du prestataire ;
- la responsabilité des parties et les couvertures de transferts de risques (assurance, etc) suivant la grille de risques appliquée à l'opération d'externalisation ;
- la procédure de transfert de l'activité externalisée qui comprendra des audits et inventaires préalables validés ;
- les modalités permettant la continuité du service et de la performance (en cas de changement progressif, brutal d'activité voire en cas de crise) ;
- les modalités quant à la mise en œuvre de la clause de réversibilité de l'externalisation (backsourcing) ;
- les procédures de contrôle de l'externalisation (suivi, audits).

Enfin, en termes de gestion de projet et alors que le contrat est désormais signé après un appel à la concurrence dont la négociation prendra du temps, toute externalisation réussie demandera une communication interne et externe parfaitement préparée et mise en œuvre par les cocontractants pour éviter les blocages toujours possibles des parties prenantes (autres fournisseurs, clients, salariés, syndicats, tiers) en particulier en cas de délocalisation totale ou partielle.

6.4. Motifs d'externalisation :

Les motifs d'externalisation dans une entreprise sont multiples :

- assurer une plus grande disponibilité pour se concentrer sur le cœur de métier (sur les activités à valeur ajoutée) ;
- bénéficier de compétences étendues : par-rapport à la structure interne, le prestataire de services peut mettre les meilleurs spécialistes en face de problèmes parfois complexes ;
- disposer pour sa structure économique d'une meilleure flexibilité en cas d'augmentation ou de diminution du nombre de collaborateurs/d'activité de l'entreprise ; le prestataire peut s'adapter plus facilement à toute modification de la marche de l'entreprise ; l'entreprise qui externalise n'a d'autre part pas les soucis d'absence du personnel interne pour vacances, maladie ou autre ;
- enfin et surtout avec la montée en puissance d'une compétitivité globalisée, favoriser un meilleur contrôle des coûts liés à la fonction, à l'infrastructure, au processus externalisé ; étant contractuels, donc connus d'avance et fixes (engagements très souvent forfaitaires), ils peuvent être à terme moins élevés que des coûts internes grâce à leur mutualisation.

6.5. Avantage :

Les quatre principales motivations sont les suivantes :

- Contrôler et réduire les coûts opérationnels de l'entreprise avec pour objectifs d'améliorer certains ratios, de connaitre et de prévoir les montants avec précision. L'externalisation permet une vision à moyen et long terme étant donné l'évolution plus lente des coûts externes par rapport aux coûts internes de l'entreprise.
- Investir dans les secteurs clés les plus productifs de l'entreprise. Externaliser consiste alors à se focaliser sur son cœur de métier. C'est d'autant plus intéressant lorsque les activités externalisées sont peu maîtrisées au sein de l'entreprise, et sont donc réalisées avec plus ou moins de succès dans des délais assez importants. De plus, la perspective d'un travail de qualité nécessiterait en interne des investissements élevés.
- Augmenter sa compétitivité en bénéficiant de compétences humaines, technologiques et matérielles récentes : les entreprises spécialisées dans l'externalisation effectuent sans cesse des investissements pour rester compétitives et grâce à la mutualisation, ces prestataires peuvent proposer les meilleurs profils, processus et matériels élaborés à des prix très compétitifs.
- Anticiper, afin d'accélérer des changements structurels : par exemple, lorsque le facteur temps est prioritaire, le recours à l'externalisation va fluidifier et accélérer la mise en œuvre, du fait de la rapidité du processus. Ainsi, plus l'environnement aura tendance à évoluer rapidement, plus le recours à un prestataire externe aura du sens car il pourra mettre en place les équipes et les moyens nécessaires à la situation. La flexibilité du prestataire sera appréciable, autant lors des phases de croissance que des phases de décroissance.

6.6. Inconvénient :

- La perte de maîtrise et des compétences au sein de l'entreprise ainsi que le manque de formations des employés qui n'ont pas les outils nécessaires pour accomplir leurs fonctions.
- Le sentiment d'appartenance moins importante à l'entreprise qui sous-traite et à ses projets de l'équipe externalisée par rapport à une équipe interne.
- La dépendance vis-à-vis du prestataire, comme des délais trop longs ou une détérioration du service.
- Un manque d'information et de transparence.
- La diminution des salaires versés aux employés.
- La détérioration que la qualité de la production ou du service fournies par celle-ci

6.7. Externalisation et délocalisation :

L'externalisation est fréquemment associée d'une manière erronée au phénomène de la délocalisation.

Les deux modes de gestion des organisations ne doivent pas être confondus pour autant :

- Toute externalisation n'entraîne pas de délocalisation, puisqu'elle ne fait souvent appel qu'à de la sous-traitance locale.
- Toute délocalisation n'est pas forcément de l'externalisation, par exemple dans le cas où c'est l'entreprise elle-même qui déplace l'un de ses propres sites de production.

6.7.1. Externalisation sans délocalisation :

Parmi les avantages d'une externalisation a priori sans délocalisation, les expertises locales, le respect des réglementations nationales et la maîtrise des coûts sans effet de change sont au top des motifs des dirigeants qui exige un service irréprochable pour une prestation de plus en plus complexe avec la stratification des règlementations.

6.7.2. Externalisation avec délocalisation :

Dans le domaine de la production, le secteur textile et de la confection est sans doute le premier secteur industriel à avoir connu ce phénomène dès les années 70. D'autres secteurs ont suivi : maroquinerie, chaussure par exemple pour gagner des secteurs plus sophistiqués comme aujourd'hui celui de l'automobile où les délocalisations vers l'est européen ne sont plus des chimères.

Dans le domaine des services, c'est surtout dans le secteur informatique que le mouvement a pris une ampleur très forte notamment vers l'Inde et les pays de l'Est (Russie) compte tenu de la capacité à réaliser des prestations intellectuelles à distance. On parle alors d'externalisation « offshore » ou délocalisée.

7. Convergence vers le Cloud (Le cloud computing) :

Comme nombre d'innovations, le Cloud computing tire son essence des technologies grand public qui, peu à peu, ont su conquérir le monde professionnel. Ainsi, les systèmes de messagerie (comme:Windows Live Messenger) ou les réseaux sociaux (LinkedIn,Viadeo, Twitte...), à l'origine réservés à une utilisation publique et gratuite, se sont immiscés dans la vie de l'entreprise. Les utilisateurs faisant ainsi leur première expérience professionnelle du Cloud computing [17] n'est d'ailleurs pas un hasard si, aujourd'hui, les offreurs de bout en bout sur le cloud public proviennent exclusivement du grand public.

Mais c'est quoi le cloud computing ?

7.1. Définition:

7.1.1. Selon la publication NIST :

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." [11].

7.1.2. Traduction:

Le cloud computing est un modèle qui permet un accès omniprésent, pratique et à la demande à un réseau partagé et à un ensemble de ressources informatiques configurables (comme par exemple : des réseaux, des serveurs, du stockage, des applications et des services) qui peuvent être provisionnées et libérées avec un minimum d'administration.

7.1.3. Autre définition:

Le *cloud computing*, ou l'informatique en nuage ou nuagique ou encore l'infonuagique (au Québec), est l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement l'internet. Ces serveurs sont loués à la demande, le plus souvent par tranche d'utilisation selon des critères techniques (puissance, bande passante, etc.) mais également au forfait. Le *cloud computing* se caractérise par sa grande souplesse : selon le niveau de compétence de l'utilisateur client, il est possible de gérer soi-même son serveur ou de se contenter d'utiliser des applicatifs distants en mode SaaS [13] [8] [6].

7.2. Explication:

Le nuage (anglais cloud) est un ensemble de matériel, de raccordements réseau et de logiciels qui fournit des services sophistiqués que les individus et les collectivités peuvent exploiter à volonté depuis n'importe où dans le monde. Le cloud computing est un basculement de tendance : au lieu d'obtenir de la puissance de calcul par acquisition de matériel et de logiciel, le consommateur se sert de puissance mise à sa disposition par un fournisseur via Internet [13].

Les caractéristiques essentielles d'un nuage sont la disponibilité mondiale en libre-service, l'élasticité, l'ouverture, la mutualisation et le paiement à l'usage :

Ressources en libre-service : et adaptation automatique à la demande. La capacité de stockage et la puissance de calcul sont adaptées automatiquement au besoin d'un consommateur. Ce qui contraste avec la technique classique des hébergeurs où le consommateur doit faire une demande écrite à son fournisseur en vue d'obtenir une augmentation de la capacité - demande dont la prise en compte nécessite évidemment un certain temps. En cloud computing la demande est automatique et la réponse est immédiate [2].

Ouverture : les services de cloud computing sont mis à disposition sur l'Internet, et utilisent des techniques standardisées qui permettent de s'en servir aussi bien avec un ordinateur qu'un téléphone ou une tablette [2].

Mutualisation : elle permet de combiner des ressources hétérogènes (matériel, logiciel, trafic réseau) en vue de servir plusieurs consommateurs à qui les ressources sont automatiquement attribuées. La mutualisation améliore l'évolutivité et l'élasticité et permet d'adapter automatiquement les ressources aux variations de la demande [25].

Paiement à l'usage : la quantité de service consommée dans le cloud est mesurée, à des fins de contrôle, d'adaptation des moyens techniques et de facturation [25].

Les nuages utilisent des technologies telles que la virtualisation du matériel informatique, les grilles, l'architecture orientée services et les services web. Un nuage peut être public, privé ou communautaire. Un nuage public est mis à disposition du grand public. Les services sont typiquement mis à disposition par une entreprise, qui manipule une infrastructure qui lui appartient. Un nuage privé est destiné exclusivement à une organisation, qui peut le manipuler elle-même, ou faire appel à services fournis par des tiers. Dans un nuage communautaire, l'infrastructure provient d'un ensemble de membres qui partagent un intérêt commun. Ce type de nuage est semblable à ceux montés par les milieux académiques pour des études de grande envergure [2].

Le nom « cloud computing » est né des professionnels de l'informatique qui recherchaient une désignation pour les nouveaux systèmes informatiques fonctionnant par l'action conjointe d'éléments variés réunis indifféremment de leur localisation géographique et de l'infrastructure sous-jacente [2].

7.3. Services:

Cette représentation des différents modèles de service montre comment les responsabilités sont théoriquement réparties suivant les modèles internes, IaaS, PaaS, SaaS.

Du point de vue économique, le cloud computing est essentiellement une offre commerciale d'abonnement économique à des services externes. Selon le National Institute of Standards and Technology il existe trois catégories de services qui peuvent être offerts en cloud computing [2].

7.3.1. IaaS (infrastructure as a service)

En français infrastructure en tant que service. C'est le service de plus bas niveau. Il consiste à offrir un accès à un parc informatique virtualisé. Des machines virtuelles sur lesquelles le consommateur peut installer un système d'exploitation et des applications. Le consommateur est ainsi dispensé de l'achat de matériel informatique. Ce service s'apparente aux services d'hébergement classiques des centres de traitemenst de données, et la tendance est en faveur de services de plus haut niveau, qui font davantage abstraction de détails techniques [2].

Prenons un exemple pour comprendre :

Mon entreprise doit installer 1 serveur. Voici les étapes, dans les 2 cas :

Etapes	Mode classique (sans le IaaS)	Mode IaaS
Avant	Chercher une offre ou appeler un fournisseur pour acheter un serveur.	Se connecter au site d'un hébergeur.
	Commander le serveur	Choisir le serveur.
	Attendre sa livraison, (1 jour, 2 jour, ou plus ?)	Attendre sa livraison (quelques minutes)
	Trouver une place pour le mettre (prises de courant, et prises réseau)	
	Réceptionner la livraison	
	Déballer le serveur du carton et vérifier le contenu de la livraison	
	Le brancher Electriquement et le brancher au réseau	
	Le démarrer et enfin commencer à travailler dessus	
Mon serveur est enfin opérationnel	Au final : j'ai passé plusieurs heures au minimum, et j'ai dû patienter plusieurs jours pour la livraison de mon serveur	Quelques minutes (ou quelques dizaine de minutes).
Pendant sa durée d'utilisation	il faut quand même que je vérifie si le matériel et notamment les disques ne tombent pas en panne	rien à faire, l'hébergeur s'en charge.
	Que je m'assure qu'il est toujours alimenté en électricité	rien à faire, l'hébergeur s'en charge.

Après	Il faudra que je gère son recyclage !	rien à faire, l'hébergeur s'en charge.

Tableau 2 comparatif entre le mode IaaS et le mode sans IaaS.[1]

7.3.2. PaaS (platform as a service)

En français plate-forme en tant que service. Dans ce type de service, situé juste au-dessus du précédent, le système d'exploitation et les outils d'infrastructure sont sous la responsabilité du fournisseur. Le consommateur a le contrôle des applications et peut ajouter ses propres outils. La situation est analogue à celle de l'hébergement web où le consommateur loue l'exploitation de serveurs sur lesquels les outils nécessaires sont préalablement placés et contrôlés par le fournisseur. La différence étant que les systèmes sont mutualisés et offrent une grande élasticité - capacité de s'adapter automatiquement à la demande, alors que dans une offre classique d'hébergement web l'adaptation fait suite à une demande formelle du consommateur [2].

Exemples de Paas :

- Louer un serveur, avec le logiciel Exchange déjà installé dessus. (Pour ceux qui ne savent pas ce que c'est : Exchange est un logiciel permettant de gérer la messagerie des entreprises.
- Cette location est bien en mode PaaS, car dans ce cas, vous louez : Le serveur, l'OS, et le logiciel et le tout déjà pré-installé.

- Louer un serveur avec les systèmes de virtualisation déjà pré-installés. [1]

7.3.3. SaaS (software as a service)

En français logiciel en tant que service. Dans ce type de service, des applications sont mises à la disposition des consommateurs. Les applications peuvent être manipulées à l'aide d'un navigateur web ou installées de façon locative sur un PC, et le consommateur n'a pas à se soucier d'effectuer des mises à jour, d'ajouter des patches de sécurité et d'assurer la disponibilité du service. Gmail est un exemple de tel service. Il offre au consommateur un service de courrier électronique et le consommateur n'a pas à se soucier de la manière dont le service est fourni. Autre exemple, Office 365 propose un ensemble de services en abonnement dont la suite logicielle Office qui se met automatiquement à jour, l'utilisateur ne se soucie pas de racheter un nouveau logiciel ou de le mettre à jour. On parle ici de location de services hébergés par Microsoft. D'autres exemples de logiciels mis à disposition en Saas sont Google Apps, Office Online ou LotusLive (IBM) [13].

Un fournisseur de software as a service peut exploiter des services de type platform as a service, qui peut lui-même se servir de infrastructure as a service.

Un exemple :

Vous voulez gérer votre stock.

Avant le cloud :

- il fallait acheter un logiciel,
- installer le logiciel sur votre ordinateur.
- Refaire l'opération en cas de changement d'ordinateur.
- Ne pas oublier de copier les données en cas de changement d'ordinateur.
- Penser à faire des sauvegardes pour ne pas perdre les données en cas de panne de disque dur.

Avec le cloud :

- vous choisissez le logiciel en ligne qui vous convient,
- vous payez ou pas le service et vous utilisez le logiciel [1]

➢ D'autres services sont également disponibles:

- **Data as a service**

Correspond à la mise à disposition de données délocalisées quelque part sur le réseau. Ces données sont principalement consommées par ce que l'on appelle des mashups.

- Business process as a service (BPaaS)

Il s'agit du concept de (BPaaS) qui consiste à externaliser une procédure d'entreprise suffisamment industrialisée pour s'adresser directement aux managers d'une organisation, sans nécessiter l'aide de professionnels de l'informatique

- Desktop as a service (DaaS)

Aussi appelé en français « bureau en tant que service », « bureau virtuel » ou « bureau virtuel hébergé ») est l'externalisation d'une virtual desktop infrastructure auprès d'un fournisseur de services. Généralement, le desktop as a service est proposé avec un abonnement payant.

- Network as a service (NaaS)

Le network as a service correspond à la fourniture de services réseaux, suivant le concept de software defined networking (SDN).

- Storage as a service (STaaS)

Stockage de fichiers chez des prestataires externes, qui les hébergent pour le compte de leurs clients. Des services grand public, tels que Microsoft OneDrive, SugarSync et Box.net, proposent ce type de stockage, le plus souvent à des fins de sauvegarde ou de partage de

fichiers. Voici d'autres exemples : Microsoft SharePoint, Amazon S3, Dropbox, Google Drive, HubiC, iCloud, Ubuntu One, Windows Live Mesh, Wuala.

- Communication as a service (CaaS)

Correspond à la fourniture de solutions de communication substituant aux matériels et serveurs locaux (PABX, ACD, SVI…) des ressources partagées sur Internet.

- Workplace as a service (WaaS)

Les caractéristiques du cloud sont qualifiées par les anglophones sous le vocable elastic computing capacity. Le National Institute of Standards and Technology en a donné une définition succincte qui reprend ces principes de base : « L'informatique dans les nuages est un modèle permettant d'établir un accès par le réseau à un réservoir partagé de ressources informatiques standard configurables (réseau, serveurs, stockage, applications et services) qui peuvent être rapidement mobilisées et mises à disposition en minimisant les efforts de gestion ou les contacts avec le fournisseur de service»[12].

Les caractéristiques du cloud computing intéressantes pour les entreprises sont la réduction du coût total de possession des systèmes informatiques, la facilité d'augmenter ou de diminuer les ressources. Le recours au cloud computing permet de décharger les équipes informatiques des entreprises, qui ont alors plus de disponibilité pour des activités à haute valeur ajoutée. Le cloud computing permet également aux petites entreprises d'avoir accès à des services jusque-là réservés aux grandes entreprises en raison de leur coût [25].

Emergence de nouvelles techniques d'administrations (de l'infrastructure serveur et service informatique):

Le rapport à l'application, au serveur, au stockage et au réseau a beaucoup évolué ces dernières années. Il se concentre désormais sur les moyens d'en rationaliser la gestion pour mieux soutenir la croissance des entreprises. Au cœur de cette évolution : l'infrastructure informatique, centre névralgique de l'entreprise et véritable muscle de l'activité [15].

C'est qu'améliorer les performances d'un site Web trop lent ou réagir aux plaintes des utilisateurs face à des applications peu performantes ne suffisent plus. Pour rester compétitive, une entreprise doit saisir les opportunités qui permettront à son infrastructure informatique de rester « agile ». En d'autres termes, la compétitivité d'une entreprise se mesure à son agilité - « IT agility ». Il s'agit d'un défi de tous les instants, alors que les obstacles sont nombreux et parfois imprévisibles [15].

Dans une architecture informatique classique, l'allocation trop stricte des ressources aboutit à une infrastructure figée, peu réactive. Dans le cas d'une évolution imprévue des besoins, il faut alors procéder à des interventions manuelles souvent laborieuses et appliquer des correctifs au cas par cas. Il est pourtant possible de s'y prendre autrement… et mieux, via la mise en œuvre de points stratégiques de contrôle au niveau de l'infrastructure dans son ensemble, permettant d'ajouter, de supprimer ou de redéfinir des services à la demande [15].

Le principe consiste à faire évoluer l'infrastructure pour l'aligner avec l'évolution des besoins liés à l'activité - sans pour autant négliger ceux de l'entreprise -, et à piloter la croissance de l'activité en privilégiant à l'implémentation de solutions ponctuelles et coûteuses, une vision de l'infrastructure

souple et basée sur le long terme.

Les solutions traditionnelles sont obsolètes

Une entreprise s'appuie sur son personnel, sur les applications qu'il utilise et sur les données qui constituent son expertise. Dans ce contexte, le rôle de l'informatique est de permettre l'interaction de ces trois composantes de façon rapide, libre et continue. C'est là une condition essentielle au bon fonctionnement de l'activité [15].

Une application de e-commerce trop sollicitée ne permettant pas aux consommateurs de poursuivre une opération en cours ou une bande passante insuffisante empêchant la sauvegarde de fichiers sont autant d'obstacles entre les personnes, les applications et les données. Ce sont là des contraintes majeures pour l'activité [15]. Traditionnellement, la réponse à ce genre de problèmes consiste à installer de nouveaux serveurs, à augmenter la capacité de stockage et à ajouter de la bande passante. Au mieux, cette approche allège les difficultés. Mais le plus souvent, cet allègement n'est que provisoire et on finit par obtenir l'effet inverse du résultat escompté : les coûts opérationnels augmentent. Au pire, l'ajout à une infrastructure statique d'équipements identiques à ceux en place peut créer plus de goulets d'étranglement qu'il n'en supprime [15].

« L'IT agility » consiste à créer une infrastructure capable de s'adapter en toute transparence et en toutes circonstances à l'évolution de l'activité. Cet objectif passe nécessairement par le remplacement des connexions statiques au sein de l'infrastructure par des interactions plus dynamiques et plus intelligentes. Cette approche se traduit par la virtualisation des interactions entre chaque élément de l'infrastructure - depuis les appareils clients jusqu'aux serveurs d'applications, en passant par le stockage des données -, créant des points de contrôle stratégique à tous les niveaux de l'infrastructure où transite l'information. Ce mode de contrôle permet d'accroître la capacité de l'infrastructure, de développer de nouveaux services, de déplacer des ressources et d'optimiser les performances, la sécurité et la fiabilité, tout en limitant les dépenses et l'impact des changements sur l'activité [15].

8. Délocalisation des services informatiques(Infogérance) :

8.1. Introduction :

Ces dernières années, les entreprises du monde entier ont compris les avantages considérables de la délocalisation des services informatiques, permettant à ce secteur de prendre de l'ampleur. De plus en plus de pays se sont en effet spécialisés dans la délocalisation de services informatiques en sus d'anciennes destinations offshore comme l'Inde.

En quelques années seulement, les prestataires informatiques se sont multipliés aux quatre coins du globe. Les entreprises disposent désormais d'un large choix de sociétés délocalisées capables de mener à bien différents types de missions. De nombreux professionnels délocalisés dans ces pays sont extrêmement compétents dans le domaine de l'informatique, car les gouvernements de ces derniers œuvrent activement pour le développement des TIC dans leur propre pays.

Les entreprises qui prévoient de délocaliser leurs services informatiques peuvent ainsi comparer les offres de plusieurs prestataires et sélectionner celui qui peut leur fournir un service de qualité avec un maximum de rentabilité.

Par ailleurs, le développement de la délocalisation informatique permet à une entreprise d'étendre les services délocalisés de la simple infogérance à l'ingénierie logicielle ou au développement de solutions business, pour un gain substantiel en efficacité et en productivité [28].

8.2. Définition de l'infogérance :

L'infogérance (cas particulier d'externalisation) est un service défini comme le résultat d'une intégration d'un ensemble de services élémentaires, visant à confier à un prestataire informatique tout ou une partie du système d'information (SI) d'un client, dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de services et une durée définie (définition de l'AFNOR). En d'autres termes, c'est l'externalisation de tout ou partie de la gestion et de l'exploitation du SI à un prestataire informatique tiers (SSII nouvellement appelé ESN). Cette mission doit s'effectuer dans la durée et non de manière ponctuelle.

L'externalisation informatique est la démarche qui conduit à l'infogérance. Son objectif est donc, historiquement, de réduire les coûts. Cependant les entreprises l'utilisent de plus en plus comme vecteur de transformation de leur système d'information et de leurs processus afin d'améliorer leurs performances, ainsi que pour pouvoir se recentrer sur leur métier de base.

Actuellement, ce terme correspond aussi bien à la maintenance du parc, qu'à la gestion de projets, qu'à la sécurité informatique et même aux formations.

8.3. Historique et évolution :

Depuis les années 1980, une forme d'externalisation a été développée en réponse aux besoins et à l'évolution des systèmes d'information appelée l'infogérance. Les entreprises qui utilisent l'infogérance sont les grandes entreprises industrielles, les entreprises du monde de la finance, les administrations... Le développement des systèmes d'information et des progiciels de gestion intégrée (PGI ou ERP) datant des années 80 ont obligé les entreprises à s'adapter à ces changements.

L'infogérance est une réponse adaptée aux besoins lourds et complexes du déploiement des PGI, en garantissant des délais et des niveaux de service dans un contexte où les compétences dans ces domaines étaient rares et coûteuses.

À l'origine, peu de petites ou moyennes entreprises entraient dans ce cadre et les offres des fournisseurs n'étaient pas souvent adaptées à leurs besoins.

Depuis 2000, une nouvelle forme d'infogérance est appelée ASP (application service provider). Elle révolutionne l'infogérance « classique », en lui apportant une rapidité et une simplicité d'exécution. Seuls les terminaux utilisateurs restant dans les locaux des entreprises, l'ASP minimise (voire supprime) tous les problèmes matériels. Permettant une prise de main rapide sur les bureaux utilisateurs, l'ASP simplifie le support fonctionnel aux utilisateurs.

Depuis 2008, le développement du Cloud computing (nuage) est délivré à travers un service cloud comme par exemple le DaaS [17].

8.4. Trois métiers imbriqués :

Il existe trois métiers d'infogérance, pouvant être combinés les uns aux autres :

8.4.1. La tierce maintenance aplicative (TMA) :

Elle consiste à confier tout ou partie de la maintenance des applications à un prestataire informatique. Elle permet de garder le produit informatique dans un état optimal de fonctionnement en faisant face instantanément à tout type de problème.

Trois niveaux de maintenance existent :

- la maintenance préventive concerne les mesures d'entretien exécutées pour éviter les anomalies.
- la maintenance curative vise à corriger le système en place. Le prestataire diagnostique le matériel défectueux et corrige les anomalies ou bugs existants ;
- la maintenance évolutive permet de faire progresser, de pérenniser et de valoriser le système. Il s'agit, par exemple, de mise à niveau des logiciels [17].

8.4.2. Application Service provider (ASP) :

L'Application Service Provider est aussi appelée Fournisseur d'Applications Hébergées (FAH). C'est une entreprise qui fournit des logiciels ou des services informatiques à ses clients au travers d'un réseau. Il consiste à externaliser l'hébergement d'une application ou d'un service en ligne à travers un réseau de type Internet ou réseau privé. La sécurité des données est assurée par le fournisseur et c'est la société tierce qui est propriétaire de l'application.

Ce modèle apporte un gain de productivité, une maîtrise des coûts, plus de flexibilité, une meilleure communication (entre sites ou pour les utilisateurs nomades) [17].

8.4.3. Business Process Outsoursing (BPO) :

Il s'agit de l'externalisation d'un ou plusieurs processus métiers (exemples de fonction : gestion de la relation client, ressources humaines). Les fonctions les plus externalisées sont les achats, la comptabilité, la gestion de la relation client (CRM), les processus administratifs de gestion des ressources humaines et le Back Office dans le domaine bancaire.

Dans tous les cas, la question se pose entre la location et l'achat de matériel [17].

8.5. Le contrat d'infogérance :

La prestation fait l'objet d'un contrat entre le prestataire (l'infogérant) et l'entreprise (le client). Il s'agit d'un contrat SLA « Service Level Agreement » définissant la qualité de service (en anglais « Quality of Service » ou QoS) auquel le prestataire doit se plier pour son client. Ce contrat est complexe à mettre en place car il détient des clauses de base et des clauses spécifiques au contrat d'infogérance.

8.5.1. Les clauses de base :

- Définition du client et du prestataire;
- Les conditions de durée, de renouvellement et de résiliation du contrat;
- Les assurances;
- Les éventuelles cessions des éléments du contrat ;
- Les modalités de paiement et de révision des prix ;
- Les clauses de responsabilité ;

8.5.2. Les clauses spécifiques à l'infogérance :

Il peut être inclus dans le contrat, en fonction des besoins du client et de son budget :

- Le maintien en conditions opérationnelles du système informatique, des réseaux et télécoms
- L'amélioration de la performance de ce système
- L'assistance aux utilisateurs, à l'administrateur et au dirigeant.

Pour chaque clause, il est indispensable de vérifier les éléments suivants :

Le périmètre : on définit d'abord un périmètre de la prestation afin de savoir ce qui est inclus ou non dans le contrat. Le périmètre est défini en fonction des besoins réels du client. Par exemple, les ordinateurs, les tablettes et smartphones, les serveurs, la solution de sauvegarde des données, les routeurs, le réseau interne du client, les équipements d'impression, télécoms ou encore de sécurité.

Les interventions : on s'intéresse dans un deuxième temps à la manière dont la prestation va s'effectuer. Néanmoins, les interventions répondent à plusieurs problématiques: les délais d'interventions, le nombre de personnes chargées de cette prestation, les jours et horaires d'intervention, le contact intervenant, le numéro de téléphone ou l'adresse de courriel à utiliser pour programmer cette intervention.

Les matériels : pour finir, on détaille le matériel pris en considération dans le contrat mais également si chaque réparation ou remplacement de matériel est inclus dans le prix de la prestation. Dans ce cas, le contrat détermine comment sera fixé le prix et dans quels cas le matériel informatique sera remplacé ou réparé [17].

8.6. Les phases du projet :

1. Le contrat d'infogérance est établi à l'issue d'une phase préalable :

- Étude d'opportunité de réalisation de l'opération par rapport aux orientations stratégiques de l'entreprise et aux besoins des utilisateurs du SI ;
- Étude de faisabilité (évaluation des contraintes, des coûts, des risques…).

2. Prise de décision de la direction générale sur la poursuite du projet avec la rédaction d'un cahier des charges.

3. Lancement d'un appel d'offres, pour effectuer une « short list » (liste restreinte d'infogérants susceptibles d'être choisis).

4. Choix du prestataire le mieux qualifié et qui répond aux exigences du contrat.

5. Mise en place du contrat et des conditions de prise en charge pendant la phase de « protocole d'accord ». On procède à différents audits :

Un audit technique permet au prestataire d'obtenir une description technique complète du système, de ses performances et d'apprécier les moyens qui devront être mis en œuvre dans le cadre des opérations d'externalisation ;

Un audit juridique clarifie les droits de propriété intellectuelle (licences d'exploitation) que l'entreprise dispose sur les différents éléments de son système.

6. Conclusion du contrat.

7. Phase d'intégration, on prépare le transfert de responsabilité entre le client et le prestataire:

Le prestataire récupère la connaissance du SI, effectue un transfert de propriété, de droit d'usage et du personnel, ainsi qu'un transfert physique ou géographique.

Le client s'assure que la reprise des connaissances est suffisante et que la maîtrise de l'ensemble confié au prestataire est assurée.

8. Phase de mise à niveau permet de parvenir à un niveau de service supérieur si la qualité de service du contrat est insuffisante. L'écart entre l'état des lieux du SI et le niveau d'exigence qualité du contrat peut ainsi entraîner une mise à niveau.

9. Phase opérationnelle concerne les prestations définies dans le contrat entrecoupées de périodes d'évolution ou d'optimisation.

10. A l'échéance du contrat, ce dernier peut être reconduit, être renégocié ou prendre fin. Le cycle peut également s'interrompre en cas de résiliation anticipée à l'initiative du client ou à l'initiative du prestataire.

À la fin du contrat, il convient de respecter les modalités de fin de prestation d'infogérance et plus particulièrement celles concernant la réversibilité [17].

8.7. Avantages de l'infogérance :

Les différents avantages de l'infogérance au sein d'une organisation :

- Réduction des coûts informatiques : Des économies de 10% à 15% sur le budget informatique est généralement constatée grâce à des effets d'échelles et mutualisations des moyens.
- Recentrage sur le « cœur de métier » en développant de nouvelles activités et/ou en rationalisant les activités existantes.
- Optimiser la gestion du Système d'Information grâce aux compétences des prestataires, ce qui entraîne un gain de temps, d'argent et une plus grande flexibilité.
- Une flexibilité face à des évolutions importantes et rapides de l'activité de l'entreprise : changement d'organisation, périmètre d'activité, restructuration…

- Meilleure maîtrise de l'évolution technologique, de la qualité, et de la productivité du SI à moindre frais.
- Interlocuteur unique (prestataire) qui a des obligations de moyens et de résultats, c'est un gage de qualité. Il a une vision extérieure et peut donc aider l'entreprise cliente lors d'une réflexion sur l'évolution du SI [17].

8.8. Les risques de l'infogérance :

Les trois principaux risques :

8.8.1. Risques de perte et de maitrise du SI :

Il existe 3 types de risques :

- Risques liés à la sous-traitance :

Les donneurs d'ordres doivent vérifier que :

-Le prestataire a réellement des capacités techniques et financières nécessaires à la bonne exécution des prestations ;

-La sous-traitance ne rendra pas inefficace les contraintes de sécurité exigées par le secteur d'activité.

En cas de manquement à ces deux obligations, le donneur d'ordres peut se réserver le droit de récuser tout sous-traitant qui ne présente pas les garanties suffisantes pour exécuter les prestations conformément aux exigences de sécurité.

- Risques liés à la localisation des données :

L'ensemble des lieux d'hébergement (site principal, sites de secours, sites de sauvegarde...) doivent répondre d'une part aux exigences de sécurité du donneur d'ordres, et d'autre part aux obligations légales et réglementaires. De manière générale, le risque de divulgation d'informations sensibles dans une opération d'infogérance doit être systématiquement évalué.

De plus, une localisation de données non maîtrisée peut entraîner trois types de

Difficulté :

-Une difficulté à exercer un droit de regard et de contrôle sur les personnels du prestataire;

-Une difficulté à effectuer un audit de sécurité de l'infrastructure sous-jacente;

-Une difficulté à répondre à d'éventuelles injonctions de la justice, pour des raisons fiscales ou autres raisons (par exemple d'ordre juridique).

- Risques liés au choix technique du prestataire :

Pour des raisons économiques, le prestataire peut être dans l'incapacité de satisfaire le contrat d'infogérance. Le donneur d'ordres doit être en mesure de récupérer les

données afin d'avoir la possibilité de les confier à un autre tiers de son choix. Cette restitution doit être mentionnée dans le contrat.

8.8.2. Risques liés aux interventions à distance :

Les interventions à distance permettent une réduction significative des coûts et des délais d'intervention.

Les principaux modes d'intervention à distance sont :

-Le télédiagnostic par la supervision d'équipements réseau et sécurité, diagnostic d'anomalies sur une application…;

-La télémaintenance par la réalisation, après le diagnostic, des opérations à distance sur le dispositif ;

-La télédistribution par une mise à jour d'une application à distance.

Les principaux risques liés aux dispositifs dédiés aux interventions à distance sont :

-L'intrusion dans le système d'information par une personne non autorisée

-L'indisponibilité du système d'information qui va avoir un impact sur la confidentialité ou sur l'intégrité des données

-L'abus de droits d'un technicien lors d'une intervention qui peut accéder à des données confidentielles ou encore modifier des données sur le système d'information.

Pour éviter les risques liés à la télémaintenance, le donneur d'ordre doit mettre en place une passerelle informatique sécurisée. Ce dispositif va :

-Authentifier la machine distante et la personne chargées du support ;

-Prévenir l'exploitation de vulnérabilité (par exemple les systèmes d'exploitation des dispositifs non tenus à jour ou encore l'absence de traçabilité des actions…) sur le dispositif de télémaintenance ;

-Garantir la confidentialité et l'intégrité des données sur le SI (système d'information) ;

-Assurer une traçabilité des actions effectuées par le technicien;

-Garantir l'absence de fuite d'informations vers l'extérieur.

Parallèlement, la mise en place d'un audit régulier va permettre de confirmer si, les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité [17].

8.8.3. Risques liés à l'hébergement mutualisé :

L'hébergement mutualisé consiste à héberger plusieurs services sur un seul et même serveur, afin de rationaliser les ressources. Les principaux risques liés à ce choix sont :

- La perte de disponibilité : Lors d'une attaque externe ou interne, puisque les services sont hébergés sur le même serveur, l'ensemble des équipements peuvent être indirectement victimes de l'attaque.
- La perte de confidentialité : le partage des services dans un même environnement physique peut conduire à des croisements d'information (contenu des fichiers clients de plusieurs sites dans la même base de données, ou le même sous répertoire, etc.).
- La perte d'intégrité : lorsque l'un des services hébergés subit une attaque, un changement de logiciel (voulu ou non) peut avoir une répercussion indirecte sur un service hébergé (non compatibilité, erreurs, etc.) ;

Pour lutter contre ces risques, le contrat d'infogérance doit prévoir une récupération rapide de toutes les données. Les quatre domaines suivants doivent être impérativement détaillés :

-Les journaux d'événements

-Le suivi du service hébergé (les mises à jour, les maintenances, sauvegardes....)

-Les modalités de prévention d'une attaque

-La réaction à la suite de l'incident.

8.9. Le marché de l'infogérance dans le monde :

D'après une étude réalisée par « Les Echos », l'infogérance se développe grâce aux services de Cloud computing.

Ce marché est monopolisé par les géants historiques de l'infogérance (SSII, équipementiers informatiques) d'envergure mondiale et par les pionniers mondiaux du Cloud computing (Google, Amazon). Toutefois, le marché compte également de nombreuses SSII de taille moyenne qui se focalisent davantage sur des marchés de spécialités (externalisation de fonctions par exemple) ou distribuent des solutions développées par les informaticiens (IBM, Bull...) et les éditeurs (Microsoft, Oracle...).

Ces acteurs proposent des services innovants (CRM, gestion de la paie et sécurité des données) qui attisent les convoitises des leaders. Depuis 2011, les leaders ont tendance à racheter ces sociétés innovantes.

En 2014, la valeur totale des contrats d'externalisation IT (Information Technology) a progressé de 7% pour atteindre 9,5 milliards d'euros. Malgré une baisse de 1% du nombre de contrats signés sur l'année (588 en 2014, contre 595 en 2013), le marché reste attractif grâce à une hausse des « mégas contrats ». Les pays européens tels que l'Allemagne, le Royaume-Uni et la France ont largement contribué au dynamisme du secteur [17].

9. Le monitoring :

9.1. Définition :

Selon de dictionnaire LAROUSSE :

Synonyme de monitorage ; Monitorage : Processus de contrôle d'un son ou d'une image au cours d'une transmission, d'un enregistrement ou d'une reproduction.

Autre définition :

Le monitoring est l'anglicisme du terme surveillance et définit la mesure d'une activité (humaine, économique, électrique, d'un organe, etc.)

En informatique, le monitoring désigne la mesure (et parfois les systèmes ou appareils de mesure) d'un système électronique ou électrique, dans le cadre de la supervision d'un parc.

Donc le monitoring ou monitorage est une activité de surveillance et de mesure d'une activité informatique. On parle aussi de supervision.

Les raisons peuvent être variées :

- mesure de performance, en termes de temps de réponse par exemple.
- mesure de disponibilité, indépendamment des performances.
- mesure d'intégrité, l'état des processus sur une machine Unix par exemple, ou bien qu'une page web n'a pas été modifiée (sécurité informatique).
- mesure de changement, surveillance de sites de News avec Google Actualités.

9.2. Domaines de surveillance :

On peut surveiller :

- l'état physique d'une machine : température, disques (S.M.A.R.T)
- la charge d'une machine : nombre d'utilisateur, de requêtes, la CPU, débit réseau ...
- disponibilité applicative : présence de processus et leur réponse par exemple
- les messages inscrits en logs systèmes (Event-Viewer) concernant une application ou un composant système
- les performances du réseau : débit, latence, taux d'erreur, QoS ...
- la nature des protocoles d'un réseau et leur taux relatif : UDP, TCP, ICMP, idem pour la couche 4 ...
- les attaques connues sur un Pare-feu par exemple
- les réponses protocolaires (simulation partielle d'une session)
- les modifications, suivant le but de la surveillance et dans certain cas, sont souhaitables ou au contraire signalent une anomalie.
- la qualité du travail lors de montage audio/vidéo sur des périphériques professionnel

9.3. Type de résultats :

Les mesures donnent des résultats :

- booléen : oui ou non ceci est disponible ?
- numériques : quel est son temps de réponse ?
- qualitatif : quand j'effectue telle requête, j'obtiens une erreur 404, ou montrer les dernières nouvelles

Ces types de réponses permettent certains traitement, par exemple il est naturel de grapher des résultats numériques. Les traitements statistiques seront aussi différents suivant les types de valeurs. La présentation des résultats peut être très différente, cela va d'un graphe à la présentation de pages web qui ont été modifiées.

9.4. Actions liées :

Le monitoring permet donc de faire des mesures, qui sont alors utilisée pour :

- Alerter les administrateurs d'un dysfonctionnement, ceci par interface "temps réel", mail, SMS, PUSH ...
- Exécuter des actions programmées comme redémarrer un service ou alors couper le réseau en cas d'attaque comme dans le cas des IPS (système de prévention d'intrusion).
- Construire des graphes (avec RRDTool ou Graphite par exemple), afin de visualiser les performances et de voir les tendances ;

9.5. Modes de surveillance :

La surveillance peut s'opérer :

- soit par un logiciel dédié, installé sur la/les machines à surveiller (solutions type MRTG)
- soit par une solution externe en mode ASP (Application Service Provider, signifiant fournisseur d'applications en ligne) via Internet (solutions type ServeurMonitor ou WebLiveAlert).

9.6. Aspects particuliers :

- Un domaine particulièrement développé est le Monitoring de site web.
- La surveillance de serveur peut également s'accompagner de fonctions d'inventaire de parc pour disposer d'informations sur tous les postes de travail connectés au même réseau.

9.7. Logiciels de surveillance :

Il y a une multitude de logiciels de monitoring, en voici quelque uns :

Applications Manager : solution de Zoho Corporation, BoardVisor de IDCWARE : solution de Business Activity Monitoring (Supervision et Gestion Budgétaire), Cacti, Centreon, Ganglia, Evidian OpenMaster de Bull, Eyesofnetwork, Icinga, Monit, Nagios, NetCrunch 5, Multi Router, Traffic Grapher, Munin, Observium : surveillance réseau plug&play récente (détection automatique, mappage dynamique, derniers événements, ...), OpenNMS: outil de supervision, monitoring opensource, Overmon : Solution intégrée de Gestion de Parc, incluant Nagios, Centreon, GLPI, FusionInventory et Mediawiki, PRTG, RRDTool, ServeurMonitor de Kalimoni : surveillance système, applicative et inventaire de parc en ASP, Shinken : outil de supervision, métrologie, monitoring (mode cluster possible, compatible avec les configurations Nagios) écrit en python, Sysun Secure : sécurisation du réseau, anti-spams, accès distant sécurisé, sécurité de la messagerie électronique et des accès au Web, contrôle et gestion des trafics, contrôle des logiciels du parc informatique.

10. Administration à distance (outils et pratiques d'administration) :

10.1. Définition :

Un outil d'administration à distance RAT (Remote Administration Tool) est un logiciel permettant la prise de contrôle totale, à distance, d'un ordinateur depuis un autre ordinateur. Il est constitué de deux parties : le "client" et le "serveur". Le "client" est installé sur l'ordinateur de celui qui prend le contrôle et le "serveur" est installé sur l'ordinateur contrôlé [26].

10.2. Description :

Grace à l'usage d'un RAT, une personne distante se retrouve dans une situation totalement identique à ce qu'elle serait si elle était devant la machine contrôlée. Son clavier devient le clavier de la machine distante, son écran devient l'écran de la machine distante, sa souris devient la souris de la machine distante etc. ... sans aucune limitation ni contrainte. Les seules limitations sont celles du profil du compte sous lequel est lancée la partie "serveur" :

- sous un compte "Administrateur", la personne distante à tous les droits les plus étendus sur la machine contrôlée
- sous un compte "Utilisateur Limité", la personne distante est limitée aux droits du compte limité sous lequel est lancé le serveur.

La personne distante peut être à des centaines ou des milliers de kilomètres de la machine contrôlée. On conçoit donc que les RAT puissent constituer des agressions de la plus extrême gravité. [26]

10.3. Autres noms (alias) :

Diverses erreurs d'usage et de transcription créent une grande confusion :11

10.3.1. Terme admis :

- Remote Administration Tool est le seul terme exact. Ses déclinaisons et abréviations correctes sont:
- Remote Administration Tools
- Remote Admin Tool
- Remote Admin Tools
- RAT
- RATs. [26].

10.3.2. Termes erronés désignant d'autres classes de produits totalement différentes

- Trojan et tous ses synonymes et déclinaisons (trojans, troyen, troyens, trojan horse, trojan horses, cheval de Troie, chevaux de Troie et toutes les orthographes de la ville de Troyes...) sont des termes employés à tort et à travers qui ne doivent jamais désigner un RAT. Un Trojan n'est pas un RAT.
- Backdoor L'emploi de ce terme est totalement faux (bien que certains Backdoor sophistiqués puissent contenir des fonctionnalités d'un RAT). Il est vrai, par contre, qu'un RAT (sa partie "serveur" sur la machine contrôlée) comporte obligatoirement un Backdoor. [26]

Exemples de logiciels RAT :
Poison Ivy2, Bihrat, Njrat, BlackShades NET, ProRat.

10.4. Le RAT est légitime ou illégitime :

Un RAT peut être :

- légitime lorsqu'une personne ou une société a donné son accord à une autre personne ou une autre société pour prendre le contrôle à distance de son ordinateur. Le cas le plus habituel est celui de la télémaintenance et de la télé diagnostique qu'une entreprise délègue à son fournisseur de produits et services informatiques. Ce dernier peut intervenir bien plus rapidement et efficacement en prenant le contrôle de l'ordinateur de son client sans quitter ses bureaux et sans perdre de temps en déplacement, surtout si le client est à plusieurs centaines ou milliers de kilomètres de là. Le serveur doit être lancé au dernier moment, lorsque le fournisseur et prêt à prendre le contrôle. Le serveur ne doit jamais rester en veille permanente. Il doit, en outre, n'être activable que sur présentation d'un solide mot de passe renouvelé après chaque intervention. Les droits du compte sous lequel la personne exerce sa prise de contrôle à distance devraient être limités au stricte nécessaire et au strict minimum (principe de moindre privilège) [26].

- Illégitime lorsqu'il a été implanté à l'insu de l'utilisateur. C'est un Trojan qui a probablement s1ervi à le véhiculer et l'implanter ou une personne qui a accès physiquement à l'ordinateur. Dans les 2 cas il y a, outre la malveillance introduite, une faille de sécurité quelque part qui a permis son installation [26].

11. Switch KVM :

11.1. Définition :

Commutateur écran-clavier-souris ou commutateur KVM (switch KVM ou keyboard-video-mouse switch en anglais) est un commutateur qui permet de partager clavier, écran et souris entre plusieurs ordinateurs.

11.2. Description :

Plusieurs ordinateurs sont reliés au même KVM mais un seul est vu à la fois. L'utilisateur peut choisir à tout moment l'ordinateur qu'il souhaite contrôler, et commute instantanément (quelques centièmes de secondes) de l'un à l'autre. Quelques commutateurs KVM récents permettent aussi de partager non seulement des périphériques USB, mais aussi audio (hautparleurs, micro…), bien que la commutation de ces derniers ne soit pas toujours plus avantageuse que le simple mixage.

L'utilisateur connecte un écran, un clavier et une souris au périphérique KVM. Il utilise ensuite des câbles pour connecter le commutateur KVM aux ordinateurs qu'il veut contrôler. L'utilisation des boutons du commutateur KVM permet de choisir l'ordinateur contrôlé parmi ceux qui sont connectés au commutateur, car celui-ci transmet les signaux

entre un ordinateur d'une part et le clavier, la souris et l'écran d'autre part en fonction de l'ordinateur sélectionné. La plupart des commutateurs KVM permettent aussi de choisir l'ordinateur contrôlé en utilisant des commandes spéciales sur le clavier (comme par l'appui sur certaines touches, souvent Scroll Lock, rapidement deux ou trois fois de suite). Certains périphériques KVM envoient aussi des signaux aux ordinateurs qui ne sont pas actuellement sélectionnés pour garantir que ceux-ci ne se croient pas déconnectés de l'écran, de la souris et du clavier.

Les commutateurs KVM diffèrent par le nombre d'ordinateurs qui peuvent y être connectés, ce nombre pouvant varier de 2 à 64. Des périphériques KVM de classe entreprise peuvent aussi être mis en chaîne pour permettre à un nombre encore supérieur d'ordinateurs d'être contrôlés depuis un même ensemble de clavier, moniteur et souris.

Les commutateurs KVM-P (P pour Peripheral en anglais) possèdent un hub USB permettant d'y connecter et de partager imprimantes, scanners, appareils photos numériques, etc. [17]

11.3. Avantages et inconvénients

- **Avantages d'un switch KVM**
  - Économique : un jeu de périphériques pour plusieurs ordinateurs.
  - Pratique : lorsqu'un même opérateur doit contrôler plusieurs ordinateurs. [26]

- Inconvénients :
  - Risque de perdre des informations si la commutation vers l'écran n'est pas automatique ou si l'un des ordinateurs a besoin que l'un des périphériques soit connecté en permanence. [17]

12. Carte Management(Serveur) :

12.1. Définition :

Une carte d'administration à distance des serveurs permet, à travers une simple connexion Web, de prendre la main sur la console du serveur, de redémarrer, éteindre ou allumer le serveur. La carte reste accessible même serveur éteint (tant qu'il reste branché au courant électrique). La prise en main est possible dès le boot, permettant par exemple de modifier des paramètres du BIOS.

Grâce à un plugin, il est possible de "monter" un lecteur CD local ou une image ISO afin d'installer à distance un système d'exploitation (ou un logiciel) sur le serveur.

Cas de la carte Management DRAC de Dell :

La carte DRAC (Dell OpenManage™ Remote Assistant Card) est une carte en option de gestion de système qui fournit des capacités de gestion à distance pour les systèmes Dell™ PowerEdge™. La carte DRAC permet aux administrateurs système de gérer et de surveiller un système PowerEdge par l'intermédiaire d'une connection par modem ou par réseau même lorsque le système lui-même ne fonctionne pas.

12.2. Fonctions de la carte DRAC

La DRAC offre une solution matérielle et logicielle complète au défi posé par la gestion d'un système distant. L'une des principales fonctions de la carte DRAC est de permettre aux administrateurs d'accéder à distance à un système hors service et de le remettre en 8état de fonctionnement aussi vite que possible. La carte DRAC envoie 1-2 Guide d'utilisation un avertissement d'alerte lorsque le système est hors service et permet un accès total à ce dernier. De plus, la carte DRAC tient un journal des causes probables de la panne du système et sauvegarde l'affichage de l'erreur actuelle.

La carte DRAC version .x est une carte PCI (Peripheral Component Interconnect) équipée de son propre microprocesseur et de sa propre mémoire. La carte est alimentée par le système lorsque le système est alimenté ou elle peut fonctionner sur son module à batterie intégrée. De plus, un adaptateur d'alimentation externe est fourni pour que la carte DRAC puisse être alimentée lorsque le système est éteint.

La carte DRAC peut alerter les administrateurs système des pannes probables d'un système. En communiquant avec le matériel de gestion de système intégré du système, elle peut émettre des avertissements ou des erreurs concernant les tensions, les températures et les vitesses du ventilateur.

12.3. Les caractéristiques de la carte DRAC comprennent :

• Accès distant par l'intermédiaire d'une connexion réseau 10Base-T, d'un modem ou d'un port série RS232.

• Capacité d'effectuer un réacheminement intégral de console (textes ou graphiques) dont celui du clavier et de la souris.

• Capacité d'alerter un administrateur en cas de panne du système.

• Les alertes peuvent être communiquées en composant le numéro d'une station de gestion, en envoyant un message à un pager numérique ou alphanumérique, ou encore en envoyant une interception SNMP (Simple Network Management Protocol [protocole de gestion de réseau simple]) par l'intermédiaire de la connexion en réseau

• Surveillance de la santé du système comprenant des informations sur les tensions, les températures et l'état du ventilateur du système via la communication avec le matériel ESM (Embedded System Management [gestion de système intégrée])

• Capacités de gestion hors bande.

• Capacité d'afficher les journaux des événements système et les codes POST (Power-On Self-Test [auto-test de démarrage])

• Capacité d'effectuer un arrêt puis de restaurer et de contrôler l'alimentation du système à partir d'une console à distance.

• Interface bus conforme à PCI 2.1 [27].

13. Conclusion :

Au cours de ce premier chapitre d'introduction à la technologie d'administration à distance, nous avons tout d'abord donné un aperçu de l'évolution de l'informatique et de différentes technologies d'administrations à distances existantes.

Bien que chacune des techniques présente un intérêt particulier suivant les applications visées, nous constatons que ces dernières ont des inconvénients et des limites.

Le chapitre suivant est dédié à la présentation des limites des technologies utilisés jusqu'à maintenant, posé notre problématique et proposé no notre solution.

Chapitre 2

Analyse et Conception

1. Introduction

1.1. Réflexion et limite des outilles d'administration classique :

Après avoir suivie l'évolution des outils et conjoncture technologique dans le chapitre précèdent nous nous arrêtons en soulignant l'importance capitale que représente les outille d'administration jumelé à ce de monitoring.

Dans ce contexte la et ayant développé les notions de délocalisation qui a fait naitre les data center et celui de l'extermination qui à donner lieu au concept de cloud et d'infogérance il demeure clair que pour renforcé l'aspect service une évolution des outille d'administration et de contrôle est un impératif.

Se désamorcer du présentiel pour une réel administration et ou maintenance des plateformes délocalisé avec éventuellement des services externalisé est à l'ordre du jour.

C'est dans ce contexte la que s'inscrit notre attribution et réflexions à travers notre adhésion au projet de l'organisme d'accueil que représente la SARL ISTERLAB.

Le projet en question porte sur une plateforme pour l'administration à travers une prise de contrôle à distance.

Bien que des solutions existe en souligne les limitations suivante :

Pour les solutions software la limitation est d'ordre conceptuel or tout programme ne pourrait opérer hors système d'exploitation (du matériel haute) d'où tout disfonctionnement de cette OS entrainerait la perte de contrôle ce qui n'est pas souhaitable.

Pour les solutions hardware : nous notons la mise sur le marché des carte de contrôle qui sont généralement greffé sur un des ports de la carte mère elle-même ce qui limite dans la plus part des cas l'accès globale au bios ou au dispositif se chargeant avant ce dernier tel les cartes RAID (à titre d'illustration) ; de plus ce type d'équipement est généralement propriétaire et ne compte la prise de contrôle que d'un seul équipement (sur lequel il est déployée) ce qui engendre une nécessité d'une lourde gestion dans le cas d'un centre de donnée ; ajouté à quoi la non administration des équipement réseau.

Ayant constaté cela de visu, notre projet porte sur une solution à deux niveau : software et hardware qui permettrait de pallier au manque et désagrément soulignés.

Pour se faire notre réflexion porte l'élaboration d'une plateforme (software/hardware) permettant tout simplement le transfert à distance de la donnée soit en entrée ou en sortie des portes (de communication) des équipements et dispositif informatique ou réseau.

Bien que cette solution de ports déportés que nous avons nommé Plateforme d' Administration et de Contrôle A Distance **PACAD** semble simple elle n'est pas pour autant simpliste.

Afin d'illustrer l'insertion de cette plateforme, nous vous proposons de consulter la figure suivante :

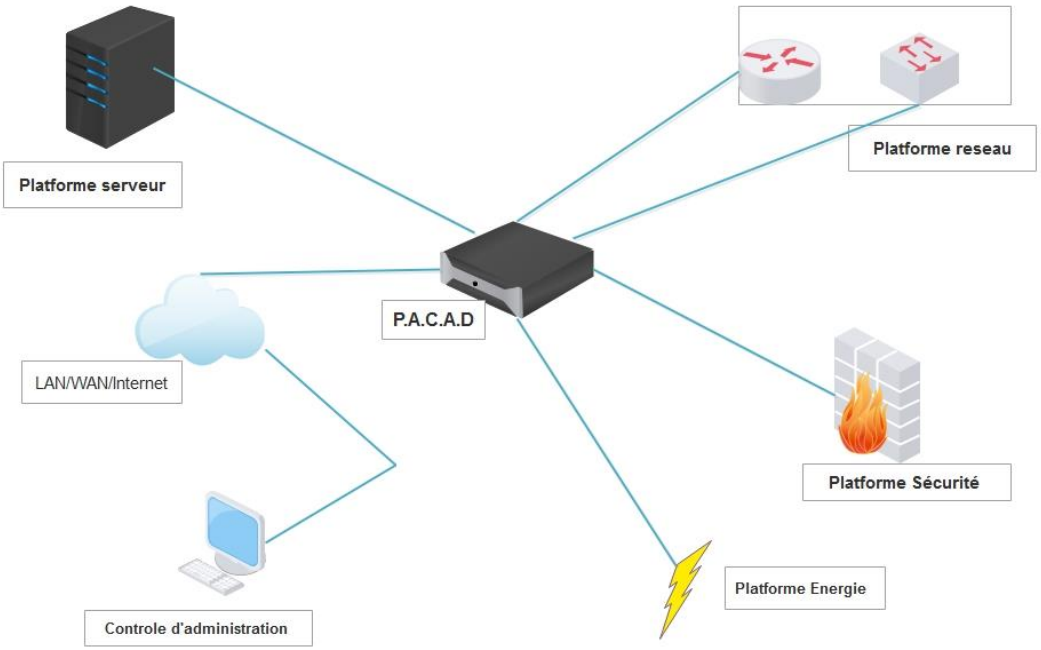


Figure 3 Insertion de la plateforme PACAD dans l'environnement de travail

Or si on se réfère à cette illustration nous remarquerons déjà que nous sommes dans une configuration à deux tiers soit client-serveur ou la console représenterait le client et le dispositif hardware muni de la solution software représentait le tiers serveur.*

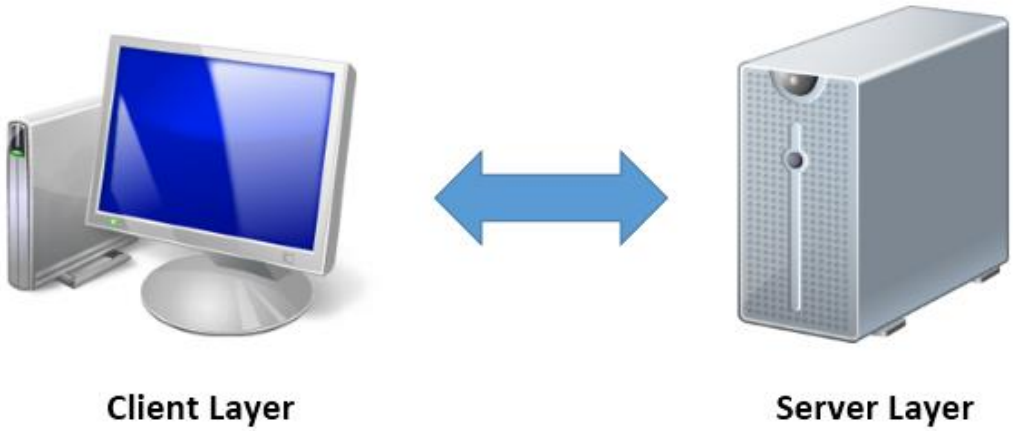


Figure 4 Architecture 2-tiers

2. Architecture :

Pour ce faire nous avons fait le choix fonctionnel de subdivisé la plateforme en trois couche :

Une couche d'administration du système : qui a pour rôle de permettre le paramétrage de l'ensemble des fonctionnalités de la plateforme.

Une couche de transfert des contrôle : se chargeant de transféré les flux échangé à travers le interface réseaux disponible.

Une couche de sécurité : charger de garantir les différant service de sécurité.

Ce qui se traduit en cette vue d'ensemble que nous proposons :

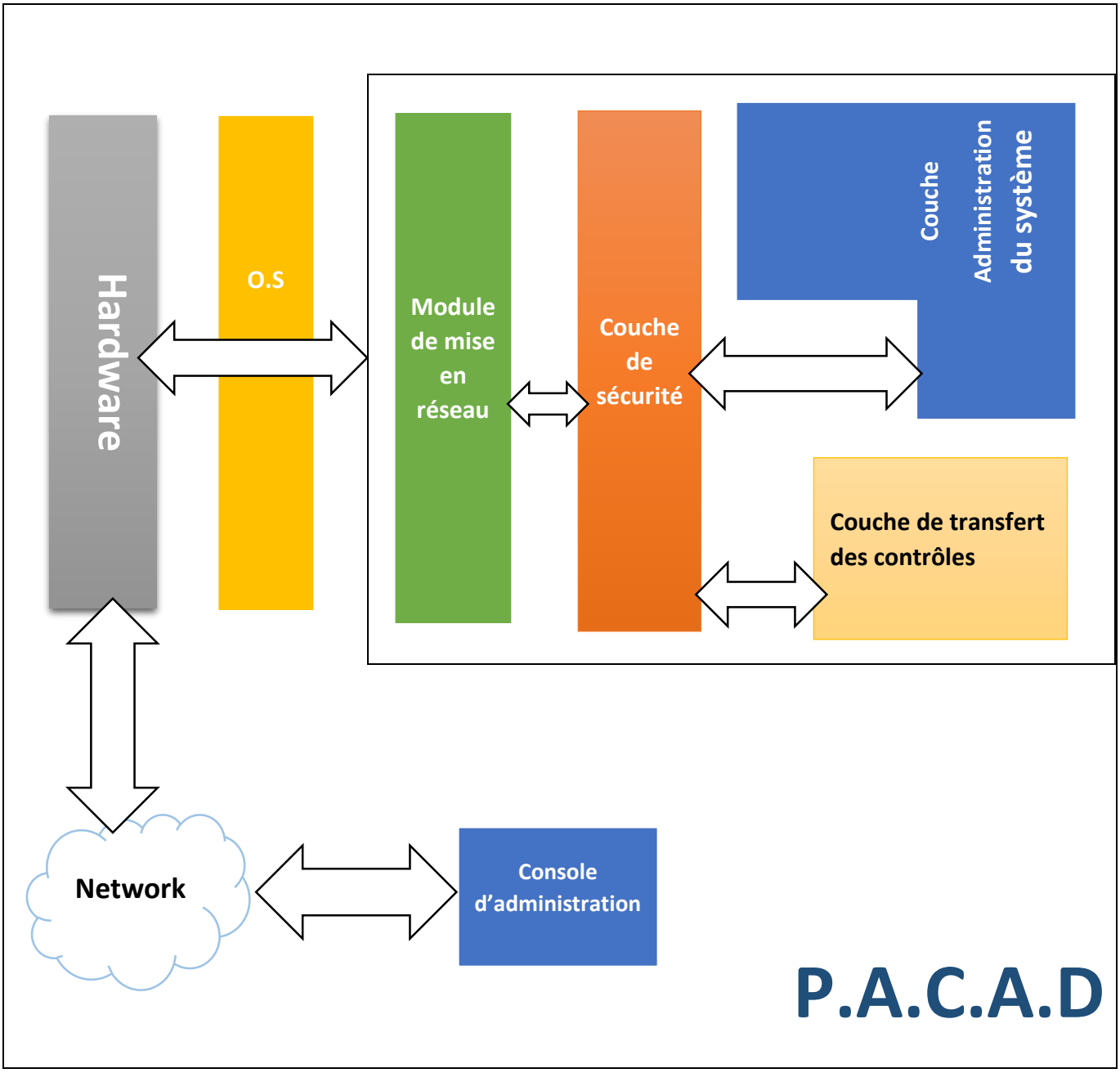


Figure 5 Vue en couche de P.A.C.A.D

2.1. La couche sécurité :

Etant donné que la sécurité occupe la place nodale dans tout système nous avons fait le choix de dédier tout une annexe pour décrire globalement ces services et dans le détaille les composantes utilisées.

Pour ce qui est des services nous pouvons déjà énumérer un certain nombre à compter :

A) En transit

- **La confidentialité :** vise à empêcher l'accès à l'information par toute entité qui n'y soit pas habilité ou sa diffusion non autorisé (même par des entités habilitées à y accéder).
- **Intégrité :** devrait garantir la perception de toute modification ou altération de l'information.

- **Authentification :** permet de s'assurer de l'origine d'un message, ainsi que l'identité du destinataire. On peut distinguer deux types d'authentification :

L'authentification d'un tiers et l'authentification de la source des données.

-L'authentification d'un tiers consiste pour ce dernier à prouver son identité

-L'authentification de la source des données sert à prouver que les données reçues viennent bien d'un tel émetteur déclaré.

- **Non-répudiation :** Vise l'intra protection des protagonistes d'un échange, et ce au moins sur un ensemble des trois points :

-Non-répudiation d'origine : l'émetteur ne pourrait nier avoir créé l'information.

-Non-répudiation de réception : le receveur ne pourrait nier l'avoir reçue.

-Non-répudiation de transmission : l'émetteur ne pourrait nier avoir transmis l'information.

B) Hors Transit

- **Contrôle d'accès :** Assurant la position de médiation entre un utilisateur légitime d'un système et ses ressources, son rôle porte sur la détermination des activités permise de ce même usagé. Ceci inclurait :
  - **Imputabilité :** ou (selon la définition de Larousse) la possibilité d'attribuer à un individu la responsabilité d'une infraction ; ceci ne pourrait se faire le recours aux mécanismes :

    - D'Identification

    - Et de Traçabilité

  - **Autorisation.**
- **Disponibilité :**

Dans un but d'illustration, nous proposons le shéma d'imbrication des appels et collaboration (figure 1) entre les différents services vu jusqu'à lors et ce dans le but de souligner l'impact qu'aurait l'assurance ou la défaillance de l'un sur l'autre ou les autres services qui aurait comme objectif de lever tout leurre qui ferait croire qu'un service a plus d'importance que les autres.

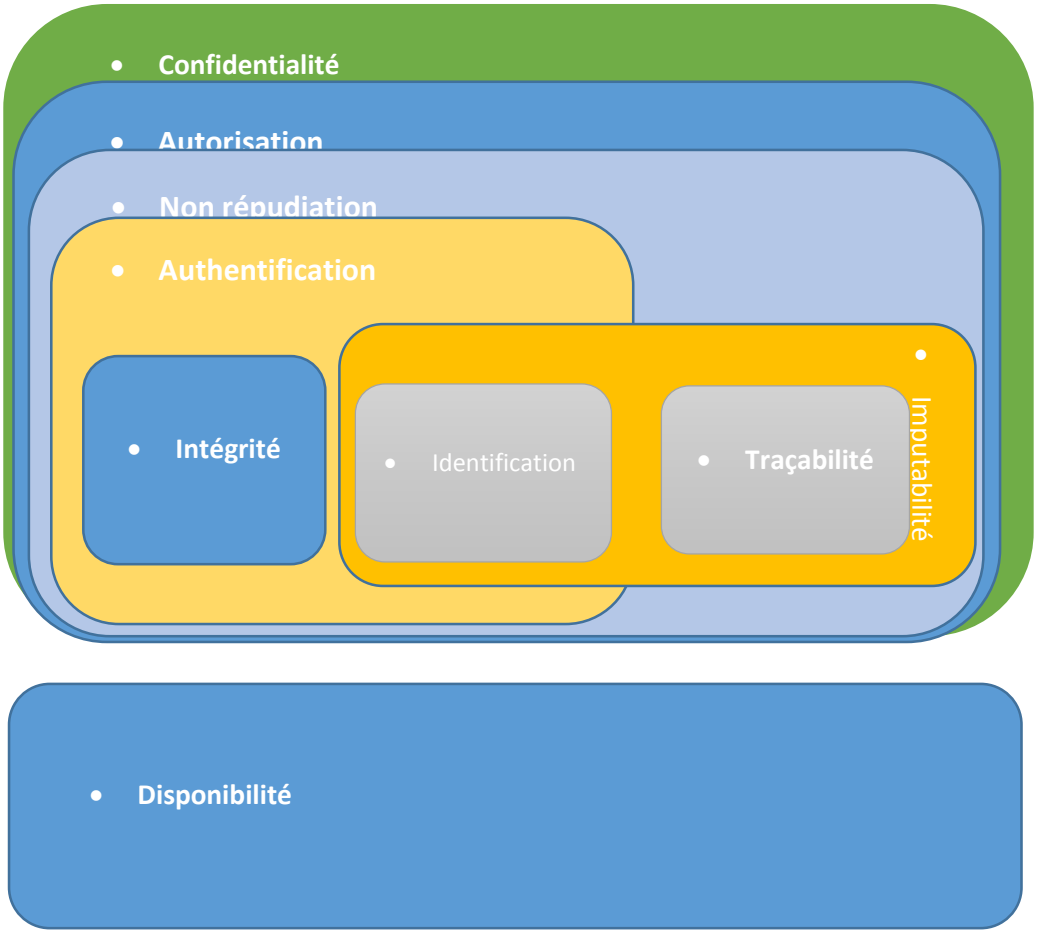


Figure 6 Services de sécurité

3. La couche d'administration :

Selon les fonctionnalités nous proposons sa subdivision en sept modules à compter :

3.1.1. Le module présentation :

Charger de l'interface permettant l'accédé et la modification des divers paramètres gérant la plateforme il inclurait l'interface homme machine IHM et M to M machine à machine, il est important de noté que dans 90% des cas c'est la console qui se charge des interfaces IHM.

3.1.2. Le module de paramétrage :

Seule disposant des droits de visualisation et de modification des divers ficher de paramètre des différents services tournant sur la plateforme et cela bien évidement à travers la module de la couche de sécurité.

3.1.3. Le module d'évaluation de la charge :

charger d'effectuée un prévisionnelle sous la base d'une bibliothèque de fonction de probabilité opérant sur des statistique prélevé par les sondes du module d'analyse de charge afin de prévenir d'une éventuelle dégradation des ressource ou désagrément lors de la mise en service de la console d'administration or le niveau de service escompté dépond clairement de la seul appréciation de l'usager derrière la console.

3.1.4. Le module d'analyse de charges :

Incluant un ensemble de sonde permettant le suivit et prélèvement des donnée concernant les taux d'utilisation des ressource qu'elle soit systèmes, réseaux ou autres.

3.1.5. Le module statistique :

Il est chargé de la translation des données des sondes (**module d'analyse**)

Et de les communiquer au **module d'archivage**.

3.1.6. Module de gestion des logs :

La journalisation étant un impondérable à tout management un module lui est dédié.

Ce qui est représenté sur le schéma suivant :

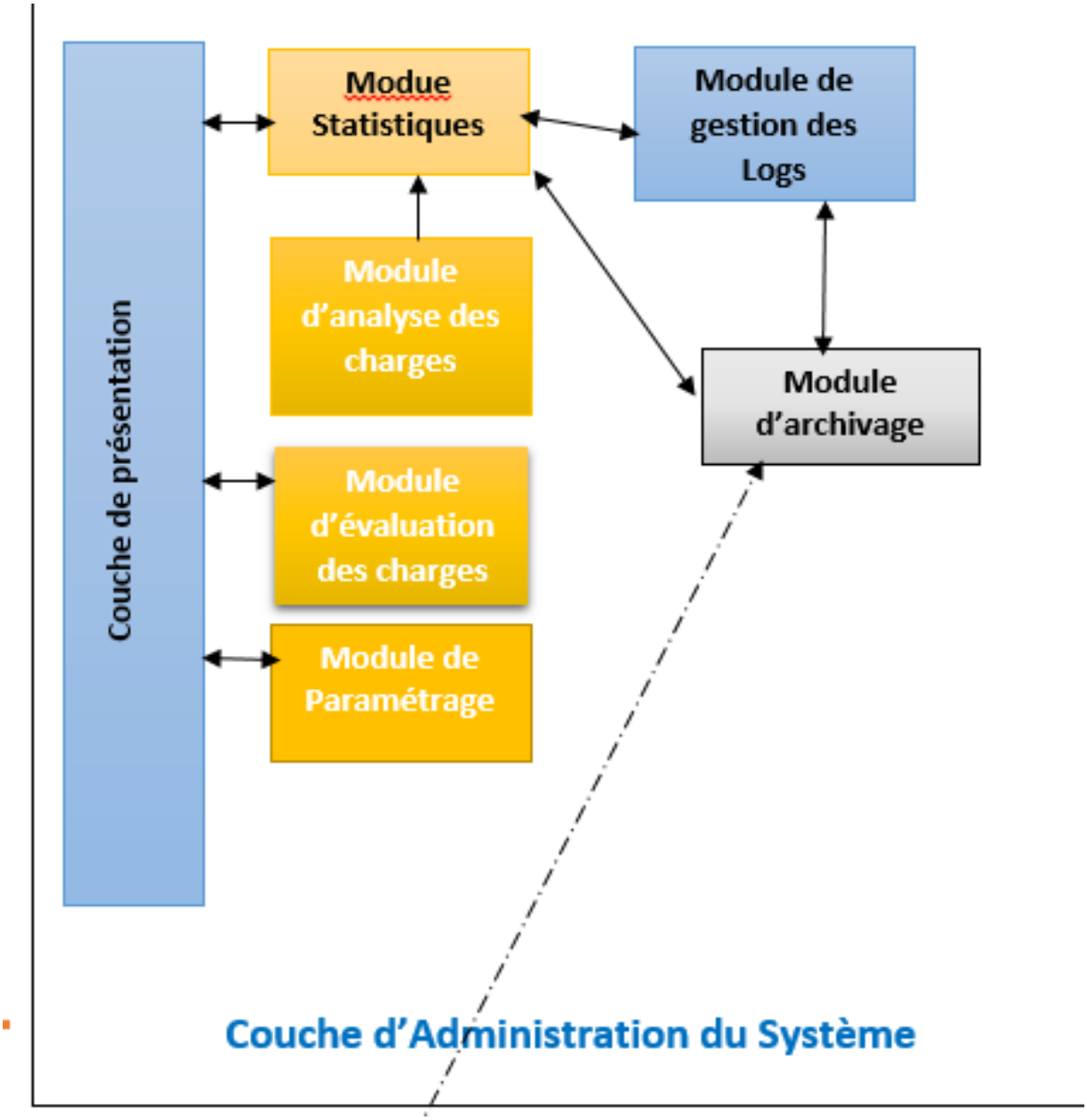


Figure 7 P.A.C.A.D: Couche d'administration système.

3.2. Couche transfert des contrôles :

Ayant comme objectif la fonction clefs de la plateforme, la couche de transfert des contrôles permet le transfert en délocalisation après sérialisation et virtualisation des ports d'E/S des équipements à administrer pour ce faire, Elle dispose d'un :

3.2.1. Module de transfert des contrôles :

Charger de l'acquisition et restitution des flux respectivement en sortie ou en entrée des ports d'E/S des équipements à administrer d'où sa subdivision conceptuelle en deux parties.

3.2.2. Module d'encapsulation :

Étant donné que les acquisition/restitution peuvent être multiple une encapsulation est de rigueur pour garantir l'étanchéité entre les diverses données.

3.2.3. Module de mise en forme et présentation :

Opérant en complémentarité avec le module d'encapsulation, il permet de formaté les différentes données échangées afin de les préparer au transport ou à la restitution.

3.2.4. Module d'optimisation :

Afin de garantir une utilisation rationnel voir optimale des ressource rare tel le transport (accès au réseau) ce module comptera à titre d'illustration des fonctions tel la compression après quoi les trames PACAD son mise en ligne à travers le module de mise en réseau après sécurisation.

3.2.5. Module recorder :

À usage de trouble shooting le recoder est charger d'enregistrer l'ensemble ou une partie des flux d'un ou plusieurs dispositif et ce à travers le module d'archivage de la couche administration.

Dans un but d'illustration nous vous invitons à étudier la figure suivante :

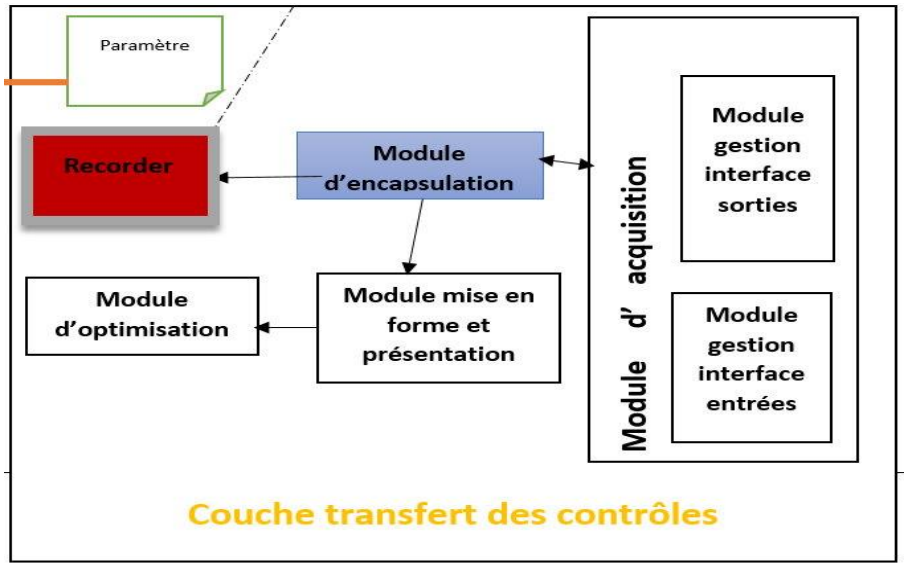


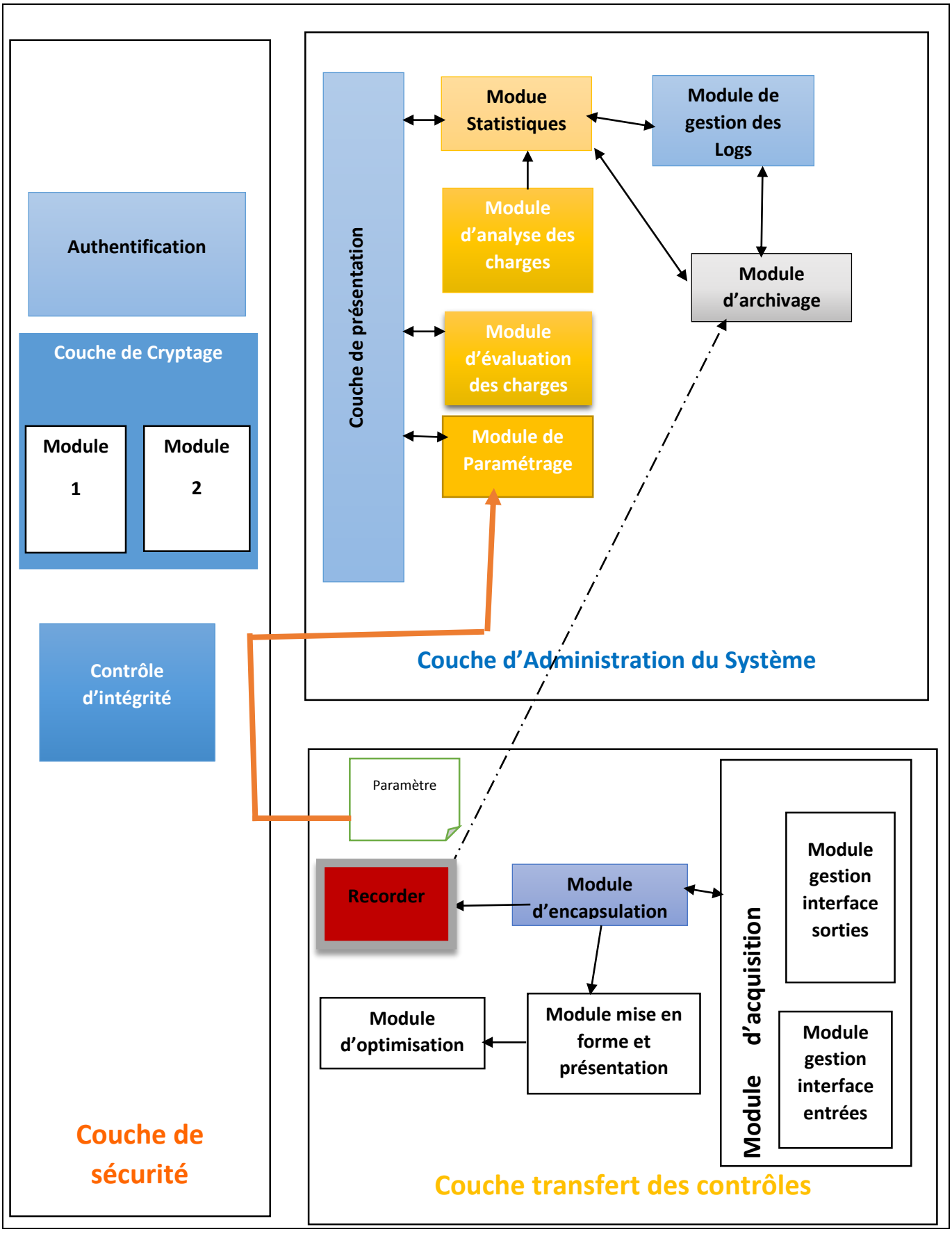
Figure 8 P.A.C.A.D: Couche transfert des contrôles.

Il est important de souligner le fait que tous les échanges se font à travers les services de la couche de sécurité ;

4. Conslusion :

Afin de permettre une vision globale nous clôturons ce chapitre par une vue d'ensemble de notre proposition d'architecture.

Figure 9: P.A.C.A.D: Vue d'ensemble



Chapitre 3

Réalisation

1. Introduction :

Dans cette dernière partie, nous allons nous intéresser au côté développement du P.A.C.A.D pour ce faire nous nous référons toujours au schéma tracé lors de la conception.

Pour commencer :
En nous basons sur la figure 5 la premier couche à sélectionner est la couche matériel.

2. Couche Hardware :

Comme support de la plateforme, le hardware occupe une place nodale, de ce fait nous aurons à sélectionner les éléments de cette couche avec le plus grand soin.

Etant donnée la réalité du terrain dans notre pays du point de vue normative, conformité des salles machines et environnement de travail des équipements à administrer il est préférable de tenir compte des dégradations environnemental sur les points :

- Humidité.
- Température.
- COURTS CIRCUITS.
- Décharge électrostatique.
- Interférence électromagnétique.

C'est dans cette orientation que l'organisme d'accueil SARL ISTERLAB, dans une quête la satisfaction du client et qualité élevé de service, nous contraint à nous conformer aux standards militaire MIL-STD.

3. MIL-STD :

Une norme du Département de la Défense des États-Unis, aussi appelée « norme militaire américaine », MIL-STD ou MIL-SPEC, est utilisée dans le but d'obtenir la normalisation de différents objectifs fixés par le Département de la Défense des États-Unis.

- La normalisation augmente l'interopérabilité et assure que certains équipements atteignent certains critères :
- compatibilité entre eux ;
- fiabilité d'opération ;
- coût total de possession ;
- compatible avec les systèmes de logistique ;
- autres critères qui facilitent l'atteinte d'objectifs liés à la défense du territoire américain.

Ces normes sont aussi utilisées par d'autres organismes gouvernementaux, des organismes techniques et l'industrie en général.

Sous cette orientation nous avons optés pour le standard MIL-STD-810G.

Et pour s'y conformé nous avons opté pour une carte mère avec :

DRMOS

Un DrMOS est un mosfet de dernière génération utilisé pour délivrer l'alimentation au processeur. Le mosfet DrMOS de MSI ne gaspille pas d'énergie, reste à bonne température et est plus efficace en énergie que toute autre solution d'économie d'énergie. Et du fait que ce mosfet soit composé d'une puce 3-en-1, il délivre plus de puissance en nécessitant moins de composants électroniques.

CONDENSATEURS HI-C CAP

Un condensateur Hi-C Cap est un condensateur petit mais très efficace. En plus d'assurer suffisamment d'espace autour du processeur afin de pouvoir y placer un large système de refroidissement, il permet également une efficacité énergétique de 93%. Grâce aux Hi-C Cap, les cartes mères gaming MSI font partie des modèles les plus économes en énergie actuellement proposés sur le marché.

BOBINES SUPER FERRITE CHOKE

Les bobines SFC (Super Ferrite Chokes) disposent d'un noyau en ferrite offrant une excellente perméabilité magnétique. Celle-ci permet aux bobines SFC de fonctionner à une température réduite de 35°, d'avoir une résistance à la charge électrique 30% supérieure, une efficacité énergétique améliorée de 20% et une stabilité optimale lors d'un overclocking.

CONDENSATEURS DARK CAP

Grâce à leur noyau en aluminium, les condensateurs Dark CAP sont des éléments de base essentiels dans la conception des cartes mères haut de gamme car ils offrent une faible résistance-série équivalente (ESR) ainsi qu'une durée de vie supérieure à 10 ans.

Ce qui nous permet déjà d'avoir un équipement de classe 4 selon le même standard.

Cette sélection est juste à titre d'illustration des critères de même niveau d'exigence sont à pourvoir du point de vue stockage, refroidissement et traitement.

Mais afin de mettre en service ces équipements une sélection de la seconde couche illustré sur la figure 5 est à effectuer c'est :

4. Choix du Système d'exploitation :

4.1. Pour le tier serveur :

Devant la multitude de système d'exploitation mis sur le marché une sélection se voie rude or un certain nombre de critère est à établir :

Une large compatibilité avec les équipements : ce qui nous évite les os propriétaire

Un aspect ouvert pour forcer le développement et l'intégration même dans les couches basse du système d'exploitation : ce qui élimine les systèmes commerciaux.

Une prise en charge complète des services de sécurité avec une garantie de transparence ce qui oriente le choix vers un réel opensource.

De ce fait nous aurons à choisir parmi :

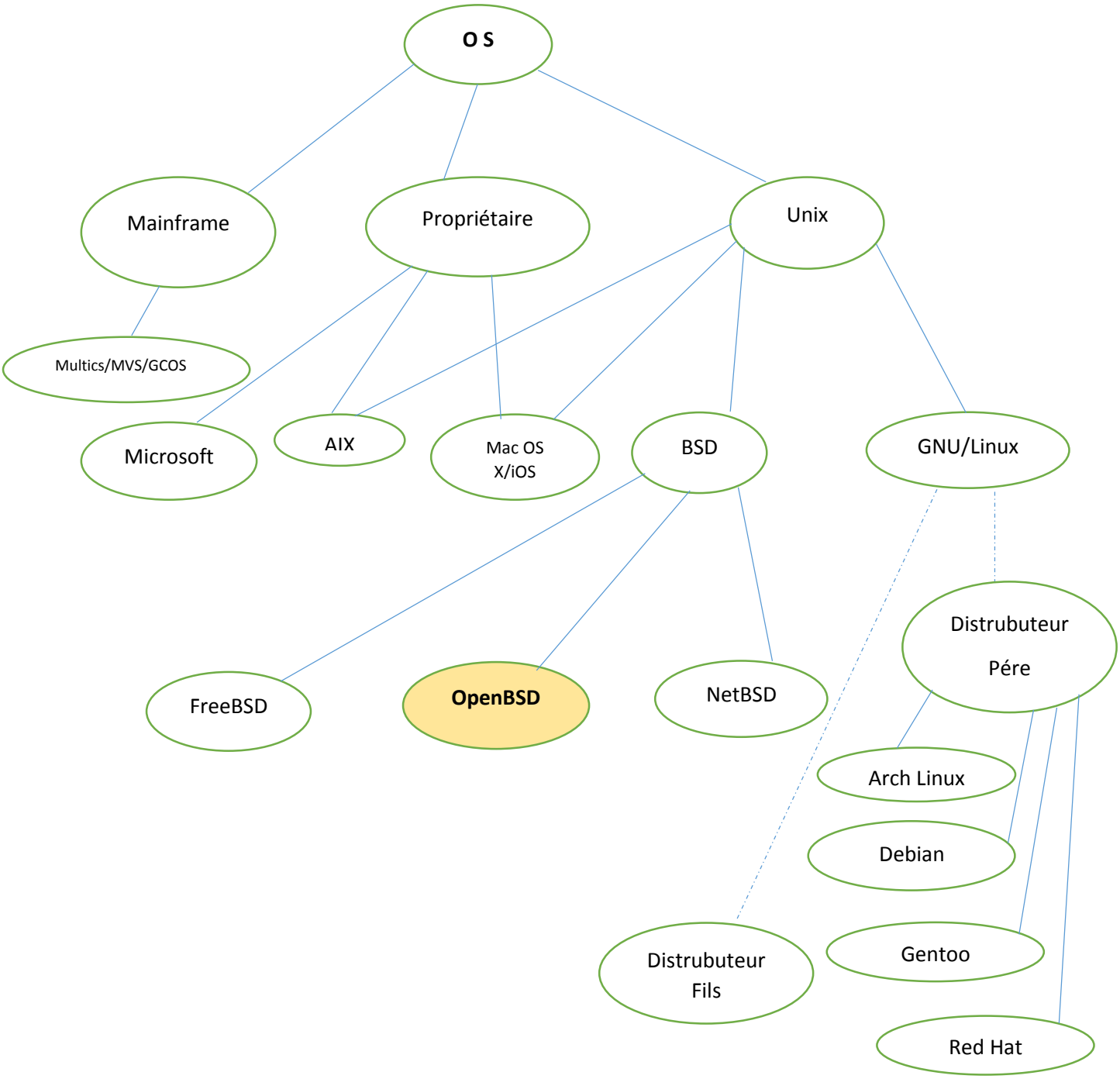


Figure 10 Arborescence des O.S

Suivant nos critère et logique de sélection, nous avons évité de travailler avec les OS suivants pour des raisons suivantes :

- Microsoft Windows (dernière version : Windows 10 (désormais plus en beta) : les systèmes d'exploitation de Microsoft sont actuellement préinstallés sur plus de 90 % des ordinateurs personnels son inconvénient est qu'il est propriétaire.

- C'est-à-dire qui ne permet pas légalement ou techniquement, ou par quelque autre moyen que ce soit, d'exercer simultanément les quatre libertés logicielles que sont l'exécution du logiciel pour tout type d'utilisation, l'étude de son code source (et donc l'accès à ce code source), la distribution de copies, ainsi que la modification et donc l'amélioration du code source, et aussi les couts engendrés.

- les systèmes d'exploitation *mainframes* (« grands systèmes ») :
  - Multics (père d'UNIX) et héritier de CTSS
  - IBM : MVS, VM, DOS/VSE, TPF
  - Bull : GCOS
  - Siemens : BS2000
  - ITS, TOPS-10 et TOPS-20
    - Les raisons sont que ces OS sont destinés pour des équipements spécifiques

1. Dérivés d'Unix (sous différentes déclinaisons : BSD, System V, etc.) dont :
   - Mac OS X et iOS (ex-iPhone OS) : systèmes préinstallés sur la majorité des ordinateurs et appareils mobiles vendus par Apple.
     - c'est-à-dire destinés aux équipements Apple.
   - GNU/Linux : un système d'exploitation libres appuyant sur le noyau Linux et les outils GNU installés sur + de 1 % du parc informatique mondial toutes distributions confondues.
     - Systèmes GNU/Linux pères : Arch Linux Debian, Gentoo, Red Hat, SUSE, Slackware, …
     - Systèmes GNU/Linux fils.
     - Nous n'avons pas travaillé sur Linux car au niveau du noyau le (.bin) n'est pas open source ce qui ne nous permet pas de travailler avec la couche matériel.
   - la famille BSD : un effort réussi pour rendre sa liberté au système de Berkeley comprenant :
     - NetBSD, FreeBSD, OpenSolaris de Sun.
   - les Unix dits « propriétaires » :
     - AIX (IBM, SystemV), A/UX (Apple, SystemV), BOS (Bull Operating System),IRIX (Silicon Graphics, SystemV), HP-UX(Hewlett Packard, SystemV), LynxOS(LynuxWorks), NeXTSTEP (NeXT,

BSD),Sinix (Siemens), Solaris (Sun, SystemV),SunOS (Sun, BSD), Tru64 (Compaq).

- Même raison que celle citée pour Windows. Sont des OS propriétaires c'est-à-dire qui ne permet pas légalement ou techniquement, ou par quelque autre moyen que ce soit, d'exercer simultanément les quatre libertés logicielles que sont l'exécution du logiciel pour tout type d'utilisation, l'étude de son code source (et donc l'accès à ce code source), la distribution de copies, ainsi que la modification et donc l'amélioration du code source, et aussi les couts engendrés.

Mac OS : le premier système d'exploitation des ordinateurs Macintosh d'Apple, qui a succédé aux systèmes Lisa et Apple II, et a été remplacé par Mac OS X ;

- c'est-à-dire destinés aussi aux équipements Apple.

Nous avons opté pour le système d'exploitation **OpenBSD**, en voici les raisons :

- OpenBSD est un système d'exploitation libre de type Unix.
- Réputé pour son intransigeance sur la liberté du logiciel et du code source donc accès au Karnel,
- La qualité de sa documentation,
- L'importance accordée à la sécurité et la cryptographie intégrée.

Pour le tiers serveur le choix c'est axé sur Open BSD

4.2. Pour le tier client (console) :

Afin de garantir une accessibilité optimale nous nous devons de nous greffé sur les os les plus utilisé par les usagé sur des équipements terminaux pour ce faire nous nous référents au derniers statistiques :

Statistique collectée par W3Schools. Source http://www.w3schools.com/browsers/browsers_os.asp

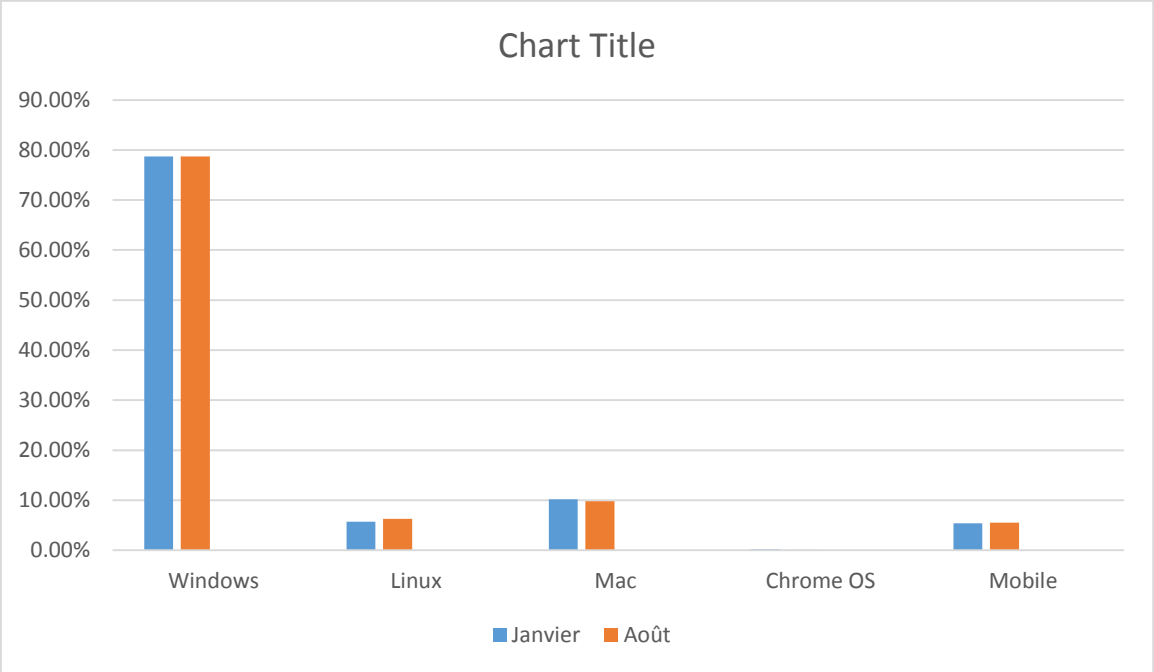


Figure 11 Graphe illustrant les principaux OS utilisés, on se basant sur les statistiques collectés par le site www.w3schools.com/browsers.

- Vu l'aspect critique de la fonction d'administration, il nous est obligé d'adapter notre Console aux les OS lus plus répondu coté client afin de permettre à ce dernier de travailler avec le système qu'il juge approprier à ses utilisations.

Les critères de sélection du matériel et la sélection des systèmes d'exploitation de l'ensemble des tiers étant effectué nous nous devons de sélectionner des outils pour le développement des modules inclus dans les couches de la plateforme PACAD et des l'ensemble du software coté console ou station.

5. Sélection des outils de développement :

5.1. Pour le software de la Station :

Nous allons prendre les statistiques faites par l'IEEE (L'Institute of Electrical and Electronics Engineers ou IEEE, en français l'« Institut des ingénieurs électriciens et électroniciens », est une association professionnelle. L'IEEE compte plus de 400 000 membres et possède différentes branches dans plusieurs parties du monde. L'IEEE est constituée d'ingénieurs électriciens, d'informaticiens, de professionnels du domaine des télécommunications, etc. L'organisation a pour but de promouvoir la connaissance dans le domaine de l'ingénierie électrique (électricité et électronique). Juridiquement, l'IEEE est une organisation à but non lucratif de droit américain [17].) Pour l'année 2016 pour appuyer notre choix du langage de programmation.

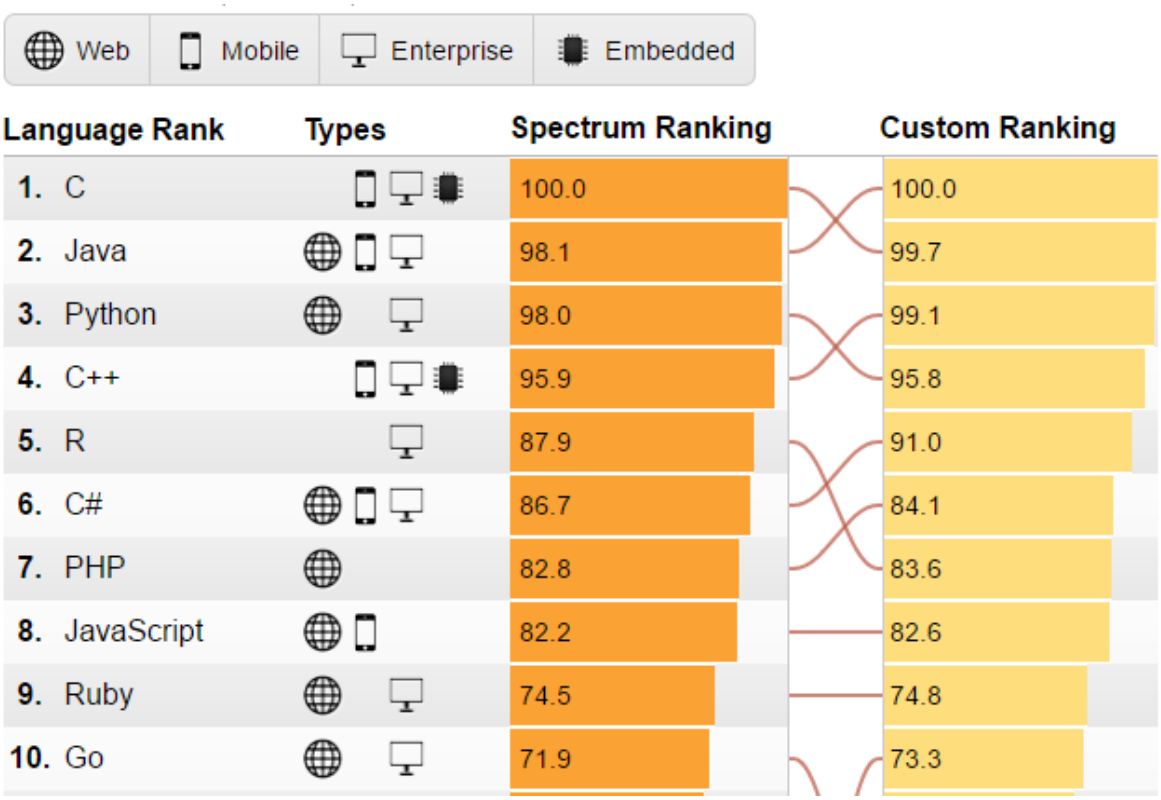


Tableau 3 IEEE : top 10 des meilleurs langages de programmation de l'année 2016

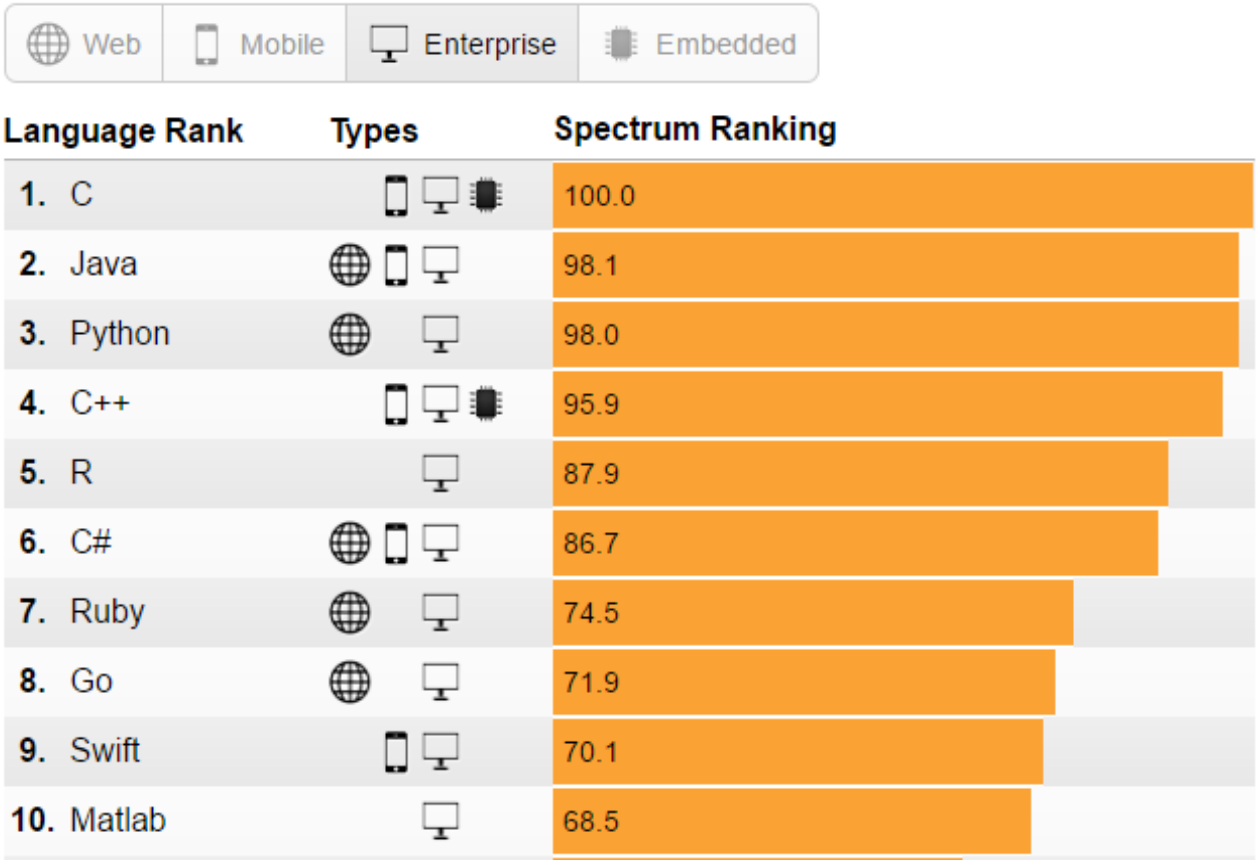


Tableau 4 Meilleurs langages pour le développement de systèmes embarqués

Selon la publication 2016 de l'IEEE(*Institute of Electrical and Electronics Engineers*), ''C'' est classé numéro 1 avec 100 % au classement général, et numéro 1 au classement des langages de programmation en forte croissance, numéro 1 au classement des langage les plus demandés par les employeurs, également numéro 1 au classement des langages de développement pour les systèmes embarqués, c'est sur ce dernier point qui est choisi ce langage en plus de sa rapidité et sa stabilité pour la réalisation des interface serveur.

« C » est un langage de programmation impératif et généraliste. Inventé au début des années 1970 pour réécrire UNIX, « C » est devenu un des langages les plus utilisés. De nombreux langages plus modernes comme C++, Java et PHP reprennent des aspects de C.

5.2. Choix de l'A.G.L pour la console:

5.2.1. Comparatif entre les deux principaux outils : Visual Studio et Windev.

Visual Studio (IDE C#)	Windev
Technologie	**Technologie**
-à termes on a vite fait le tour des possibilités **-plusieurs langages en 1 EDI** **- contiennent le nécessaires pour apprendre les – rudiments de leur langage respectif** **-problème de portabilité** Définition : **Microsoft Visual Studio est une suite de logiciels de développement pour Windows conçue par Microsoft. La dernière version s'appelle Visual Studio 2015.** **Visual Studio est un ensemble complet d'outils de développement permettant de générer des applications Web ASP.NET, des Services Web XML, des applications bureautiques et des applications mobiles. Visual Basic, Visual C++, Visual C# et Visual J# utilisent tous le même environnement de développement intégré (IDE, Integrated Development Environment), qui leur permet de partager des outils et facilite la création de solutions faisant appel à plusieurs langages. Par ailleurs, ces langages permettent de mieux tirer parti des fonctionnalités du Framework .NET, qui fournit un accès à des technologies clés simplifiant le développement d'applications Web ASP et de Services Web XML grâce à Visual Web Developer.**	-rapidité de développement, même pour novice -n'est pas un bon moyen pour débuter dans la programmation -peut être utilisé sous linux et windows -WinDev utilise son propre "langage de programmation", le WLangage, ressemblant beaucoup à du pseudo-langage - Permet de développer plus vite, et donc de libérer du temps pour se consacrer à l'aspect «métier» - La compatibilité WINDEV/WEBDEV/WINDEV Mobile permet de créer des applications qui fonctionneront sur un PC, un Mac, sous tous les Navigateurs Web, sur Tablette, sur srmatphone et sur terminal, sans concession sur les fonctionnalités **Définition :** WinDev est un atelier de génie logiciel (AGL) édité par la société française PC SOFT et conçu pour développer des applications, principalement orientées données pour Windows10, 8, 7, Vista, XP, 2008, 2003, 2000, mais également pour Linux, .Net et Java. Il propose son propre langage, appelé le WLangage. La première version de l'AGL est sortie en 1993. Apparenté à WebDev et WinDev Mobile.
Coût	**Coût**
-Outils gratuits Microsoft: **-gratuits (Visual Studio Express)** **-version étudiante de Visual Studio gratuite avec licence illimitée personnel** **-Version avancée payante (entre 350€ et 17 000€)**	-version gratuite limitée dans le temps -Version avancée payante (1650€)

Sécurité	**Sécurité**
-Cryptage des données intégré	-Possibilité de crypter les données
Veille techno	**Veille techno**
Version mise à jour régulière par Microsoft https://www.microsoft.com/france/visual-studio/1 Communauté importante	http://pcsoft.fr/st/telec/index.html
Convivialité	**Convivialité**
-IDE classique -Entièrement en français -Utilisation de WYSIWYG	-Permet de générer des interfaces graphiques -Tout est générés, aucun code à mettre en place - Produits faciles à prendre en main : environ 1 semaine suffit - Entièrement en français

Tableau 5 Tableau 8 Comparatif entre les deux principaux outils : Visual Studio et Windev.

Nous avons opté pour WinDev de PC SOFT Car :

- Il génère le code binaire pour l'ensemble des plateformes.
- Sa capacité a intégré des modules écrient en d'autre langages tel que le C.
- ça permet de créer des IHM (Interface Homme-Machine) par glisser-déplacer.
- Il permet également de choisir un modèle de charte graphique parmi un ensemble proposé et d'en créer de nouveaux.
- Sa gestion avancée de documentation et sa prise en charge de la partie conception.
- L'équipe de développement travaille sur cet éditeur d'interface graphique,

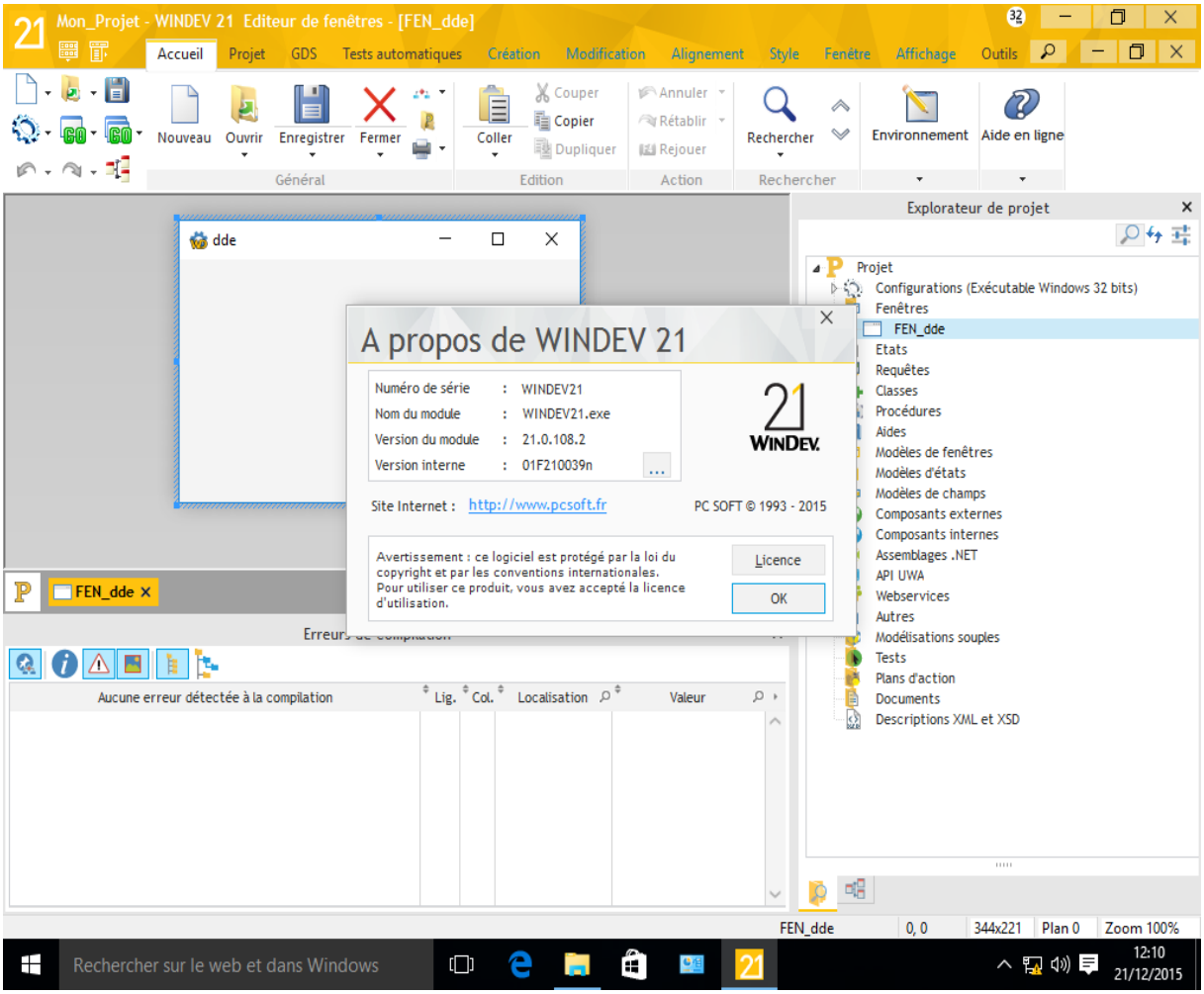


Figure 12 Image de l'interface de WinDev.

Les outils de développement étant choisies nous pouvons passer en se référant à la figure 5 à la couche sécurité et si en reprend les services de cette dernier énuméré à la figure 6 nous pouvons déjà souligner le fait de contribuer au service de disponibilité à travers le critère de sélection hardware d'une part et pour le reste des fonctionnalités nous notons hâtivement que la cryptographie et le hachage permettes de couvrir nombre de ces services de ce fait :

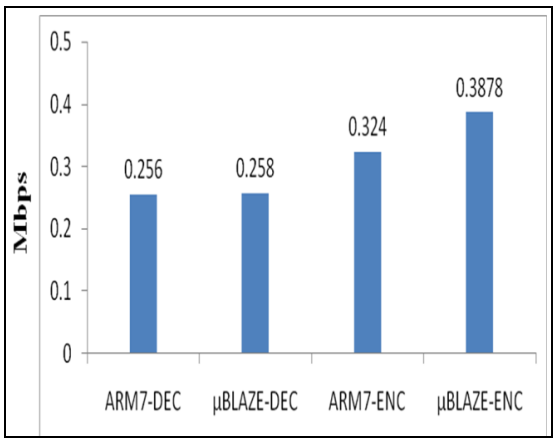
6. Couche sécurité :

Pour la cryptographie nous avons sélectionné un jeu de trois premiers algorithmes classés par le concours de la NSA (voir annexe 1) à savoir :

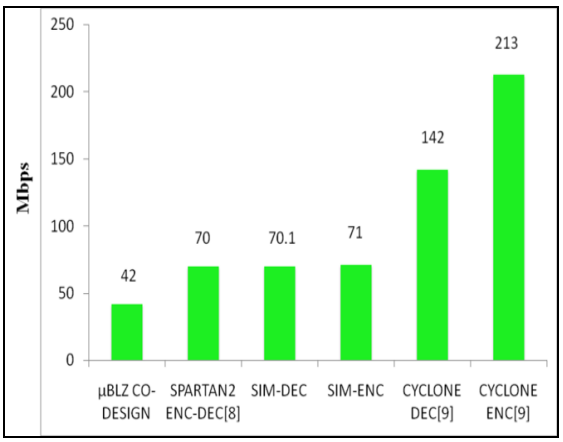
- AES
- SERPENT
- BLEUFISH

Cependant le cryptage/décryptage à un cout qui n'est pas à négliger surtout en termes de vitesse de traitement ce qui risquerait de contraindre la vitesse en sortie ou en entrée ce qui nous a forcé après test à pencher sur une implémentation hardware de la composante cryptographique.

Or si nous prenons l'exemple de l'AES nous pouvons apprécier le comparatif entre implémentation hardware et software ainsi que le rapport performance :



AES Logiciel



AES Hardware

Figure 13 Comparaison entre AES en logiciel et AES en Hardware

De ce fait pour notre implémentation nous avons opté pour la solution hardware et en attendant l'implémentation des trois algorithme sur FPGA nous avons entamé les premiers tests proto avec

- Atmel® CryptoAuthentication™ USB Dongle Demo-Evaluation Kits

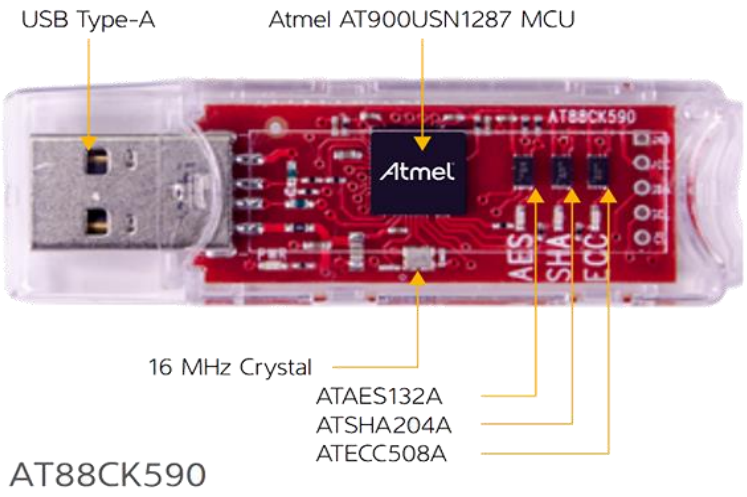


Figure 14 Implémentation Hardware d'AES.

Cependant il est à noter que ce choix n'est pas arbitraire or la compatibilité avec l'OS station n'est pas à négliger, je vous rassure qu'il est pris en charge.

7. Couche transfert des contrôles :

7.1. Module d'acquisition :

Pour ce qui est du module acquisition de la couche transfert des contrôle nous soulignant le fait qu'une sélection hardware s'impose pour certain interface et nous dirons même qu'elle est incontournable tel le cas de la fonction affichage graphique du module de gestion des interface de sortie or si nous devons pallier au manque des carte d'administration propriétaire nous devons être indépendant du hardware des équipements serveur pour le transfert de l'affichage et ce d'une manière exclusive de ce fait : Afin de transmettre l'image, nous devons avoir un dispositif hardware permettant le sérialisation et le transfert des flux vidéo émanant des ports graphique tel que HDMI, SDI, DVI, VGA ;

7.1.1. Module gestion d'interfaces de sorties :

Après recherche notre sélection à pencher vers le produit d'EPIPHAN, model AV.IO HD permettant la sérialisation des données à travers le port USB 3.0.

Ce choix non plus n'est pas « innocent » or ce dispositif est os indépendant est assure une conversion en haute qualité (confirmé par les LAB Test)

Figure 15 Epiphan AV.io HD

Caractéristiques techniques :

Interface	**USB 3.0, USB 2.0.**	
pilotes OS	UVC et UAC dispositif	
Dimensions	3.54 "x 2.36" x 0.91 ", 90 mm × 60 mm × 23 mm	
Connecteurs	DVI-I (intégré, numérique et analogique), connecteur USB 3.0 type B	
Contribution	HDMI (y compris audio), DVI, VGA	
Résolution d'entrée	Jusqu'à 1920 × 1200	
frame rate de sortie Notez que le logiciel tiersque vous utilisez définit la taille d'image et le bitrate.	**Résolution de sortie**	**taux de trame disponibles**
	640 × 360	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps
	640 × 480	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps
	848 × 480	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps

	960 × 540	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps
	1024 × 768	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps
	1280 × 720	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps
	1280 × 1024	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps
	1600 × 1200	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps
	1920 × 1080	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps
	1920 × 1200	15, 23,97, 24, 25, 29,97, 30, 50, 59,94, 60 fps
Sortie espace couleur	YUV 4: 2: 2	
réglages VGA	Luminosité, contraste, décalage horizontal, déplacement vertical	
capture de latence	Proche de zéro. Cependant, les applications tierces peuvent contribuer à capturer retard.	
HDMI Audio (entrée)	16-bit et 24-bit codé MIC audio à 32 kHz, 44,1 kHz et 48 kHz Taux d'échantillonnage	
Sortie audio	16 bits 48 kHz Taux d'échantillonnage stéréo	
LED	Une LED pour indiquer l'état de l'AV.io HD (puissance, la préparation et le fonctionnement en cours)	
Soutien OS	Windows 7, Windows 8.1, Windows 10, Mac OS X 10.10 et plus, la distribution Linux avec un noyau 3.5.0 ou plus pris en charge.	
la conformité HDCP	High-bandwidth protection de contenu numérique (HDCP) est une forme de protection numérique de copie destiné à empêcher la copie illégale de données vidéo et audio content.AV.io HD ne peut pas capturer à partir de sources vidéo protégés par HDCP.	
Pays d'origine	Fabriqué en Amérique du Nord (Canada)	

Tableau 6 Caractéristiques techniques AV.io HD d'Epiphan

7.1.2. Module gestion des interfaces en entrées (voir E /S):

De ce fait et étant donnée qui nous somme dans la quasi-certitude de faire tendre tout port d'E/S (Annexe 2) par conversion en un port USB le chalenge software de base fonctionnel ce vois rétrécir en le transfert des ports USB par la création d'un dispositif USB virtuel attaché à la console puis le reste est Plutôt simple or il suffit de reprendre le contenu des buffer de la station (tiers serveur) et le restitué sur cette même console cependant il est à noter l'utilisation du multithreading et multi processus pour l'acquisition et la restitution de même que l'ajustement des débit par le module d'évaluation des charges.

8. Cas illustrant la connectivité des différents éléments avec la PACAD :

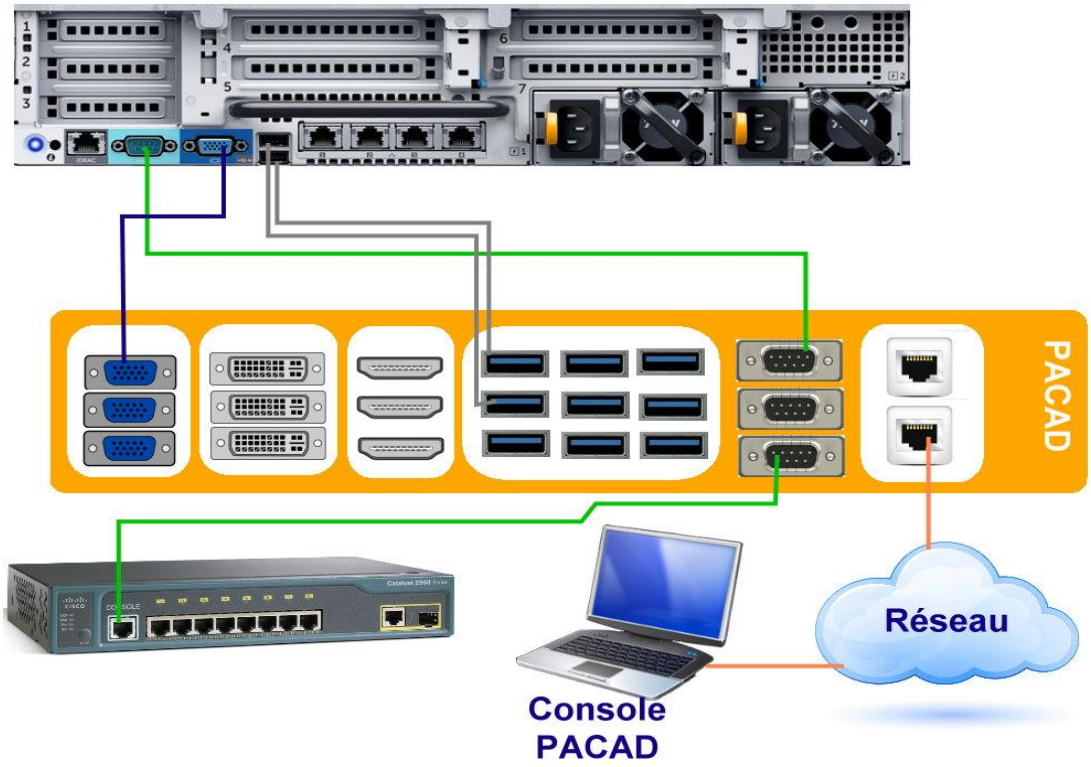


Figure 16 Représentation d'une connectivité des différents équipements avec la PACAD.

9. Conclusion :

Arrivé à ce niveau nous sommes en mesure de dire que nous nous trouvons face à un embryon d'une nouvelle génération d'outils d'administration et que nous avons l'honneur et le plaisir d'y avoir apporté notre modeste contribution.

Conclusion Générale

Conclusion générale

Dans un monde ou l'avancée technologique ne constitue plus un critère de différenciation mais un défi pour les nations.

Dans une tentative de côtoyer cette avancée et d'embrasser le monde des réalisations technologiques nous avons eu à travers ce mémoire à travailler dans une structure organisationnelle tout en intégrant des équipes pluridisciplinaire enrichissantes et complétantes nos acquis théorique académique avec cette fenêtre sur le monde professionnelle avec ses contraintes, ses apports et ses défis et par-dessus tout son côté opérationnel.

Cette expérience nous a aussi permis de touché du doigt le monde du développement architecturale de plateforme avec ses réflexion, conception développement et intégration d'où une capitalisation du savoir-faire et le plaisir de participation.

Dans un espoir de continuité d'approfondissement que nous clôturons notre mémoire.

Annexe 1

Sécurité

La Sécurité

Etant donné que la sécurité occupe la place nodale dans tout système nous avons fait le choix de dédier tout une annexe pour décrire globalement ces services et dans le détaille les composantes utilisées.

Pour ce qui est des services nous pouvons déjà énumérer un certain nombre à compter :

B) En transit

- **La confidentialité :** vise à empêcher l'accès à l'information par toute entité qui n'y soit pas habilité ou sa diffusion non autorisé (même par des entités habilitées à y accéder).
- **Intégrité :** devrait garantir la perception de toute modification ou altération de l'information.

- **Authentification :** permet de s'assurer de l'origine d'un message, ainsi que l'identité du destinataire. On peut distinguer deux types d'authentification :

L'authentification d'un tiers et l'authentification de la source des données.

-L'authentification d'un tiers consiste pour ce dernier à prouver son identité

-L'authentification de la source des données sert à prouver que les données reçues viennent bien d'un tel émetteur déclaré.

- **Non-répudiation :** Vise l'intra protection des protagonistes d'un échange, et ce au moins sur un ensemble des trois points :

-Non-répudiation d'origine : l'émetteur ne pourrait nier avoir créé l'information.

-Non-répudiation de réception : le receveur ne pourrait nier l'avoir reçue.

-Non-répudiation de transmission : l'émetteur ne pourrait nier avoir transmis l'information.

B) Hors Transit

- **Contrôle d'accès :** Assurant la position de médiation entre un utilisateur légitime d'un système et ses ressources, son rôle porte sur la détermination des activités permise de ce même usagé. Ceci inclurait :
  - **Imputabilité :** ou (selon la définition de Larousse) la possibilité d'attribuer à un individu la responsabilité d'une infraction ; ceci ne pourrait se faire le recours aux mécanismes :

    - D'Identification

    - Et de Traçabilité

  - **Autorisation.**

- **Disponibilité :**

Dans un but d'illustration, nous proposons le shéma d'imbrication des appels et collaboration (figure 1) entre les différents services vu jusqu'à lors et ce dans le but de souligner l'impact qu'aurait l'assurance ou la défaillance de l'un sur l'autre ou les autres services qui aurait comme objectif de lever tout leurre qui ferait croire qu'un service a plus d'importance que les autres.

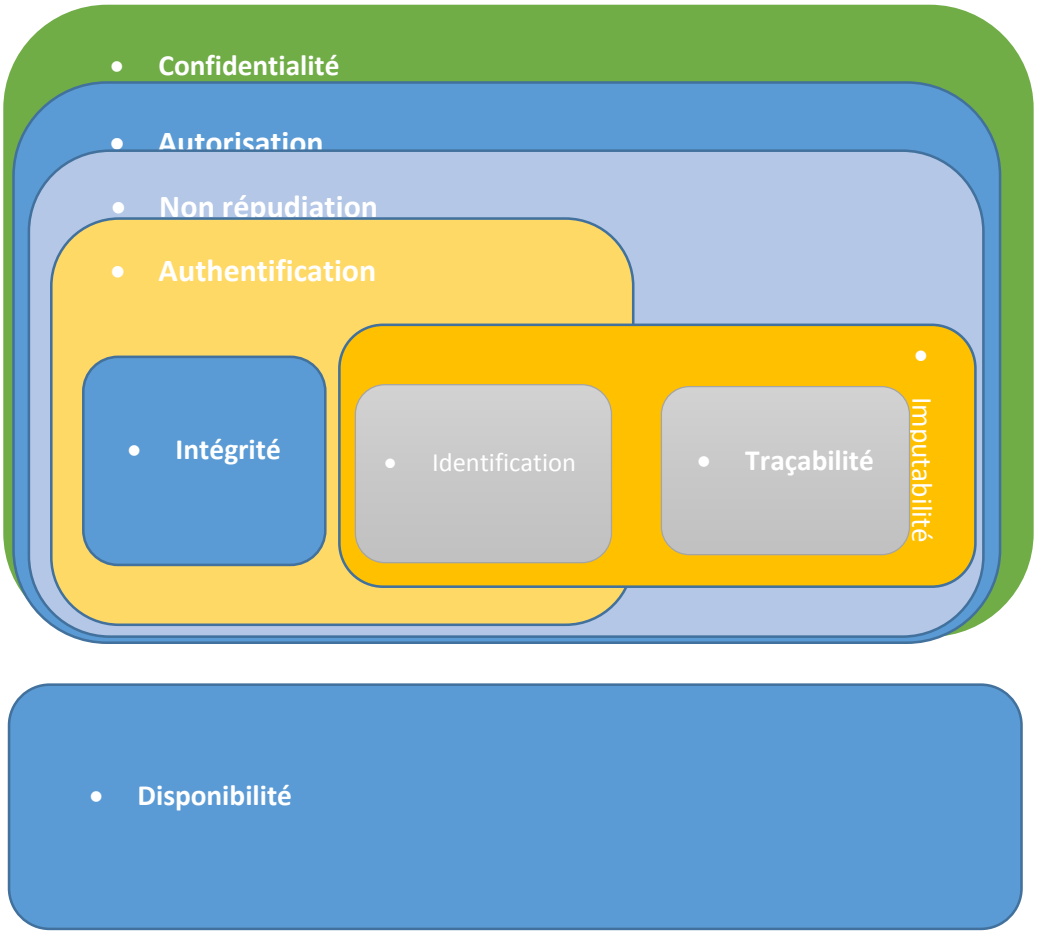


Figure 1 Les services de sécurité

Un certain nombre de ces services est traité par la science que représente la cryptologie :

Cryptologie :

La cryptologie, étymologiquement la science du secret, ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie — l'écriture secrète – et la cryptanalyse – l'analyse de cette dernière.

La cryptologie est un art ancien et une science nouvelle : un art ancien car les Spartiates l'utilisaient déjà (la scytale) ; une science nouvelle parce que ce n'est un thème de recherche scientifique académique, c'est-à-dire universitaire, que depuis les années 1970.

Cryptographie :

Cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés. Elle se distingue de la stéganographie qui fait passer inaperçu un message dans un autre message alors que la cryptographie rend un message inintelligible à autre que qui-de-droit.

Utilisation :

Les domaines d'utilisations de la cryptographie sont très vastes et vont du domaine militaire, au commercial, en passant par la protection de la vie privée.

Algorithmes de Cryptographie symétrique (à clé secrète) :

Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. L'un des problèmes de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre. La mise en œuvre peut s'avérer difficile, surtout avec un grand nombre de correspondants car il faut autant de clés que de correspondants. Nous allons voir les trois principaux algorithmes les plus utilisés.

Advanced Encryption Standard (AES):

Standard de chiffrement avancé en français, aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique. Il remporta en octobre 2000 le concours AES, lancé en 1997 par le NIST et devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il a été approuvé par la NSA (National Security Agency) dans sa suite B des algorithmes cryptographiques. Il est actuellement le plus utilisé et le plus sûr [29]

Fonctionnement :

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(2^8) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un OU exclusif XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.

Recommandation de la NSA :

La NSA a annoncé que tous les finalistes qui avaient participé au concours AES pouvaient être considérés comme sûrs et qu'ils étaient suffisamment robustes pour chiffrer les données non-

classifiées du gouvernement américain. Pour les données classifiées, le gouvernement américain a annoncé en juin 2003 à propos de l'algorithme AES :

« L'architecture et la longueur de toutes les tailles de clés de l'algorithme AES (128, 192 et 256) sont suffisantes pour protéger des documents classifiés jusqu'au niveau « SECRET ». Le niveau « TOP SECRET » nécessite des clés de 192 ou 256 bits. L'implémentation de l'AES dans des produits destinés à la protection des systèmes et/ou documents liés à la sécurité nationale doit faire l'objet d'une analyse et d'une certification par la NSA avant leur acquisition et leur utilisation»[30].

Blowfish :

C'est un algorithme de chiffrement symétrique (c'est-à-dire « à clef secrète ») par blocs conçu par Bruce Schneier en 1993.

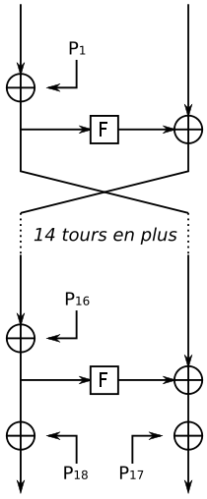
Blowfish utilise une taille de bloc de 64 bits et la clé de longueur variable peut aller de 32 à 448 bits. Elle est basée sur l'idée qu'une bonne sécurité contre les attaques de cryptanalyse peut être obtenue en utilisant de très grandes clés pseudo-aléatoires.

Blowfish présente une bonne rapidité d'exécution excepté lors d'un changement de clé, il est environ 5 fois plus rapide que Triple DES et deux fois plus rapide que IDEA. Malgré son âge, il demeure encore solide du point de vue cryptographique avec relativement peu d'attaques efficaces sur les versions avec moins de tours. La version complète avec 16 tours est à ce jour entièrement fiable et la recherche exhaustive reste le seul moyen pour l'attaquer.

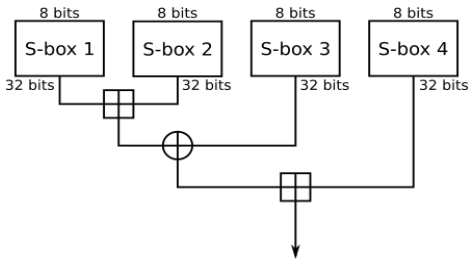
Il a été placé dans le domaine public par son créateur ; il n'est protégé par aucun brevet, et son utilisation n'est pas soumise à licence. Cela explique en partie son succès, car ce fut un des premiers algorithmes de chiffrement dont l'utilisation était libre. Il est utilisé dans de nombreux logiciels propriétaires et libres (dont GnuPG et OpenSSH)[17].

Fonctionnement :

Blowfish utilise une taille de bloc de 64 bits et la clé, de longueur variable, peut aller de 32 à 448 bits. Blowfish est basé sur un schéma de Feistel avec 16 tours et utilise des S-Boxes de grande taille qui dépendent de la clé. Il ressemble à CAST-128 qui a adopté, quant à lui, des S-Boxes au contenu fixé d'avance.



Le schéma à droite montre la structure principale de Blowfish. Chaque ligne représente 32 bits. L'algorithme gère deux ensembles de clés : les 18 entrées du tableau P et les quatre S-Boxes de 256 éléments chacune. Les S-Boxes acceptent un mot de 8 bits en entrée et produisent une sortie de 32 bits. Une entrée du tableau P est utilisée à chaque tour. Arrivé au tour final, la moitié du bloc de donnée subit un XOR avec un des deux éléments restants dans le tableau P



Le deuxième schéma montre la F-fonction de Blowfish. Elle sépare une entrée de 32 bits en quatre morceaux de 8 bits et les utilise comme entrées pour accéder aux S-Boxes. Les sorties sont additionnées avec une somme modulo 232 et l'algorithme effectue un XOR entre les deux sous-totaux pour produire la sortie finale de 32 bits. En tant que schéma de Feistel, Blowfish peut être inversé simplement en appliquant un XOR des éléments 17 et 18 du tableau P sur le bloc chiffré. Il faut ensuite utiliser les entrées du tableau P dans l'ordre inverse.

La préparation de la structure à partir de la clé commence avec l'initialisation du tableau P et des S-Boxes avec des valeurs qui sont tirées du nombre Pi exprimé en hexadécimal. On opère ensuite un XOR entre la clé secrète et les entrées du tableau P pour obtenir les nouvelles entrées du tableau P (avec une extension cyclique de la clé si nécessaire). Un bloc de 64 bits, tous à zéro, est ensuite chiffré avec cette version temporaire de Blowfish. Le résultat chiffré remplace ensuite le premier et le deuxième élément du tableau P. On réitère l'opération de chiffrement avec cette nouvelle version et ceci sur le résultat précédent. On obtient alors le troisième et quatrième élément de P. L'algorithme continue ainsi en remplaçant tout le tableau P et les éléments des S-Boxes. Finalement, ce sont 72 octets de données qui doivent être générés pour le tableau P, et 1 024 octets de données par S-Box, soit un total de 4 168 octets, et Blowfish effectue 521 itérations pour y parvenir. [17]

De par ces contraintes, Blowfish est lent quand il faut changer de clé mais très rapide pour le chiffrement pris séparément.

Le principe d'initialisation consistant à effectuer un XOR entre le tableau P long de 576 bits et les bits de la clé étendus de façon cyclique sur 576 bits, de nombreuses implémentations permettent d'utiliser des clés d'une taille atteignant 576 bits pour augmenter la sécurité. Bien que ce soit tout à fait possible, la limite de 448 bits a été fixée de façon que chaque bit de chaque valeur du tableau P et des S-Boxes dépende de tous les bits de la clé les quatre dernières valeurs du tableau P n'affectant pas tous les bits du bloc chiffré. Ce point doit être pris en considération pour déterminer la longueur de clé maximale d'une implémentation de l'algorithme d'un nombre différent de tours, car même si l'extension de la taille de la clé (indépendamment d'une extension du nombre de tours) fournit une meilleure sécurité face à une recherche exhaustive, elle affecte la sécurité garantie par l'algorithme. Car hormis les évidents bénéfices qu'offrent une clé de taille accrue, aucune étude à ce jour n'a étudié l'impact sur la sécurité qu'a le non-respect de cette règle, ce qui mène de nombreux éditeurs de logiciels à la respecter. En effet, étant donné la longue et complexe initialisation de Blowfish à chaque changement de clé, il est doté d'une protection naturelle contre les recherches exhaustives car le temps de calcul s'en trouve grandement accru. Ainsi à l'heure actuelle, le gain obtenu ne justifie pas vraiment l'utilisation d'une clé de taille supérieure à 448 bits, ce qui est déjà bien au-delà des capacités de calcul par recherche exhaustive, ainsi que de nombreux algorithmes considérés comme sécurisés.

Serpent :

Serpent est un algorithme de chiffrement par bloc finaliste pour le concours AES. Il obtiendra finalement la 2e place (59 votes contre 86 votes pour Rijndael). Serpent a été conçu par Ross Anderson, Eli Biham et Lars Knudsen.

Tout comme les autres candidats pour AES, Serpent a une taille de bloc de 128 bits et supporte des clés de 128, 192 ou 256 bits, mais également d'autres longueurs inférieures (multiple de 8 bits). L'algorithme comporte 32 tours d'un réseau de substitution-permutation opérant sur quatre mots de 32 bits. Chaque tour utilise 32 copies de la même S-Box de 16x16 éléments, il y a 8 S-Boxes en tout qui sont utilisées chacune tous les 8 tours. Leur contenu provient d'une opération déterministe simple sur les S-Boxes de DES (les auteurs levaient ainsi une partie des soupçons sur des faiblesses volontairement insérées). Après avoir opéré la substitution, une transformation linéaire (voir diagramme) modifie le bloc pour le tour suivant. Celle-ci a fait l'objet d'une analyse poussée pour vérifier sa robustesse et améliorer l'effet avalanche.

Serpent a été conçu pour travailler en parallèle avec 32 tranches de 1 bit. Cela maximise le parallélisme, mais fait également appel à la cryptanalyse intensive dont DES a été l'objet.

Serpent a été jugé plus prudent que Rijndael, le vainqueur d'AES, en termes de sécurité. Les concepteurs sont partis du principe que 16 tours suffisaient à repousser les attaques conventionnelles, mais pour contrer la cryptanalyse à venir, ils ont opté pour 32 tours.

Serpent est souvent considéré comme l'un des systèmes de chiffrement les plus sûrs actuellement disponibles.

Il existe aussi une version peu répandue de Serpent, capable de travailler avec des clés de 512 bits.

Fonction de Hachage :

On nomme fonction de hachage, de l'anglais hash function (hash : pagaille, désordre, recouper et mélanger) par analogie avec la cuisine, une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Les fonctions de hachage sont utilisées en informatique et en cryptographie.

Principe générale :

Une fonction de hachage est typiquement une fonction qui, pour un ensemble de très grande taille (théoriquement infini) et de nature très diversifiée, va renvoyer des résultats aux spécifications précises (en général des chaînes de caractère de taille limitée ou fixe) optimisées pour des applications particulières. Les chaînes permettent d'établir des relations (égalité, égalité probable, non-égalité, ordre...) entre les objets de départ sans accéder directement à ces derniers, en général soit pour des questions d'optimisation (la taille des objets de départ nuit aux performances), soit pour des questions de confidentialité.

En terme très concret, on peut voir une fonction de hachage (non cryptographique) comme un moyen de replier l'espace de données que l'on suppose potentiellement très grand et très peu rempli pour le faire entrer dans la mémoire de l'ordinateur. En revanche, une fonction de hachage cryptographique est ce que l'on appelle une fonction à sens unique, ce qui veut dire que le calcul de la fonction de hachage est facile et rapide tandis que le calcul de sa fonction inverse est infaisable par calcul et donc non calculable en pratique. Grâce à la valeur de hachage, on peut discriminer deux objets apparemment proches, ce qui peut être utilisé pour garantir l'intégrité des objets, autrement dit leur non modification par un acteur malveillant.

Terminologie :

Le résultat d'une fonction de hachage peut être appelé selon le contexte somme de contrôle, empreinte, empreinte numérique, hash, résumé de message, condensé, condensat, signature ou encore empreinte cryptographique lorsque l'on utilise une fonction de hachage cryptographique.

MD5 :

L'algorithme MD5, pour Message Digest 5, est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier (on parle souvent de message). Il a été inventé par Ronald Rivest en 1991.

L'utilisation de cette fonction de hachage dans les signatures numériques peut conduire à de multiples scénarios d'attaque et n'est plus considérée comme un composant fiable de l'infrastructure à clés publiques. Cependant dans le calcul de la « signature » d'un fichier il reste plutôt fiable, même si l'on ne peut pas assurer qu'il y a unicité entre l'empreinte calculée et le fichier ou message source.

Exemple :

Voici l'empreinte (appelée abusivement signature) obtenue sur une phrase :

MD5 (ould lamara)= ff5e829f1b7638f6078b369670dd23f4

En modifiant un seul caractère, cette empreinte change radicalement :

MD5 (ould Lamara)= 272b5254aa9449abb2208b6632415638

Très concrètement, la vérification de l'empreinte ou somme de contrôle MD5 peut être réalisée de la façon suivante : lors du téléchargement d'un programme, on note la série de caractères nommée « Signature MD5 » indiquée sur la page de téléchargement. Quand ce téléchargement est terminé, on lance un utilitaire de calcul MD5 comme HashCalc ou md5sums, qui indique entre autres la somme de contrôle correspondant au fichier. Si les deux valeurs correspondent, on peut alors raisonnablement considérer que le fichier n'a pas été corrompu (volontairement ou non d'ailleurs). On constate plusieurs fragilités dans ce processus : la page d'origine a pu être modifiée, et l'utilitaire de calcul peut être adapté pour fournir la signature attendue. C'est pourquoi il faut impérativement utiliser un utilitaire provenant d'une source de confiance. Il est aussi possible d'utiliser une extension pour le navigateur Mozilla Firefox comme MD Hash tool afin d'automatiser ce contrôle.

SHA -1 :

SHA-1 (Secure Hash Algorithm) est une fonction de hachage cryptographique conçue par la National Security Agency des États-Unis (NSA), et publiée par le gouvernement des États-Unis comme un standard fédéral de traitement de l'information (Federal Information Processing Standard du National Institute of Standards and Technology (NIST)). Elle produit un résultat (appelé « hash » ou condensat) de 160 bits.

SHA-1 n'est plus considéré comme sûr contre des adversaires disposant de moyens importants. En 2005, des cryptanalystes ont découvert des attaques sur SHA-1, suggérant que l'algorithme pourrait ne plus être suffisamment sûr pour continuer à l'utiliser dans le 4futur. Depuis 2010, de nombreuses organisations ont recommandé son remplacement par SHA-2 ou SHA-3. Microsoft, Google et Mozilla ont annoncé que leurs navigateurs respectifs n'accepteraient plus les certificats SHA-1 au plus tard en 2017.

Fonctionnement du SHA-1 :

Le SHA-1 prend un message d'un maximum de 264 bits en entrée. Son fonctionnement est similaire à celui du MD4 ou MD5 de Ronald Rivest. Quatre fonctions booléennes sont définies, elles prennent 3 mots de 32 bits en entrée et calculent un mot de 32 bits. Une fonction spécifique de rotation est également disponible, elle permet de déplacer les bits vers la gauche (le mouvement est circulaire et les bits reviennent à droite). Une de ces rotations n'était pas présente dans le SHA-0, elle permet de casser certaines caractéristiques linéaires dans la structure. Cela permet d'éviter une attaque sur les bits neutres décrite par Eli Biham, technique reprise pour calculer la collision complète sur SHA-0 (Antoine Joux et al.).

Le SHA-1 commence par ajouter à la fin du message un bit à 1 suivi d'une série de bits à 0, puis la longueur du message initial (en bits) codée sur 64 bits. La série de 0 a une longueur telle que la séquence ainsi prolongée a une longueur multiple de 512 bits. L'algorithme travaille ensuite successivement sur des blocs de 512 bits.

Pour chaque bloc l'algorithme calcule 80 tours (ou rondes, « rounds » en anglais) successifs et applique une série de transformations sur l'entrée. La première étape consiste à calculer 80 valeurs sur 32 bits. Les 16 premières valeurs sont obtenues directement à partir du bloc « message » en entrée. Les 64 autres sont calculées successivement. Le SHA-1 les obtient grâce à une rotation (absente dans SHA-0) qui est appliquée sur le résultat d'un XOR, il utilise pour cela 4 mots obtenus dans les itérations précédentes. On définit ensuite cinq variables qui sont initialisées avec des constantes (spécifiées par le standard), le SHA-1 utilise encore 4 autres constantes dans ses calculs. Si un bloc de 512 bits a déjà été calculé auparavant, les variables sont initialisées avec les valeurs obtenues à la fin du calcul sur le bloc précédent.

Il s'ensuit 80 tours qui alternent des rotations, des additions entre les variables et les constantes. Selon le numéro du tour, le SHA-1 utilise une des quatre fonctions booléennes. L'une de ces fonctions est appliquée sur 3 des 5 variables disponibles. Les variables sont mises à jour pour le tour suivant grâce à des permutations et une rotation. En résumé, le SHA-1 change sa méthode de calcul tous les 20 tours et utilise les sorties des tours précédents.

À la fin des 80 tours, on additionne le résultat avec le vecteur initial. Lorsque tous les blocs ont été traités, les cinq variables concaténées (5 × 32 = 160 bits) représentent la signature.

SHA-3 :

Keccak (prononciation: [kɛtʃak], comme “ketchak”) est une fonction de hachage cryptographique conçue par Guido Bertoni, Joan Daemen, Michaël Peeters et Gilles Van Assche à partir de la fonction RadioGatún.

SHA-3 est issu de la NIST hash function competition qui a élu l'algorithme Keccak le 2 octobre 2012. Elle n’est pas destinée à remplacer SHA-2, qui n’a à l'heure actuelle pas été compromise par une attaque significative, mais à fournir une alternative suite aux possibilités d'attaques contre les standards MD5, SHA-0 et SHA-1.

Keccak est une fonction éponge dans laquelle les blocs du messages sont XORés avec des bits initiaux, ensuite permutés de manière réversible.

Réseau privé virtuel :

En informatique, un réseau privé virtuel, VPN ailleurs, de l'anglais Virtual Private Network, est un système permettant de créer un lien direct entre des ordinateurs distants. On utilise notamment ce terme dans le travail à distance, ainsi que pour l'accès à des structures de type cloud computing.

Fonctionnement :

La connexion entre les ordinateurs est gérée de façon transparente par le logiciel de VPN, créant un tunnel entre eux. Les ordinateurs connectés au VPN sont ainsi sur le même réseau local (virtuel), ce qui permet de passer outre d'éventuelles restrictions sur le réseau (comme des pare-feux ou des proxys).

Intérêt :

Un VPN permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local. On peut ainsi avoir un accès au réseau interne (réseau d'entreprise, par exemple).

Un VPN dispose généralement aussi d'une passerelle permettant d'accéder à l'extérieur, ce qui permet de changer l'adresse IP source apparente de ses connexions. Cela rend plus difficile l'identification et la localisation approximative de l'ordinateur émetteur par le fournisseur de service. Cependant, l'infrastructure de VPN (généralement un serveur) dispose des informations permettant d'identifier l'utilisateur. Cela permet aussi de contourner les restrictions géographiques de certains services proposés sur Internet.

Le VPN permet également de construire des réseaux overlay, en construisant un réseau logique sur un réseau sous-jacent, faisant ainsi abstraction de la topologie de ce dernier.

L'utilisation de VPN n'est généralement pas légalement restreinte.

Chiffrement :

Les connexions VPN ne sont pas nécessairement chiffrées. Cependant, si l'on ne chiffre pas, cela peut permettre à des éléments intermédiaires sur le réseau d'accéder au trafic du VPN, ce qui peut être problématique si les informations qui y transitent sont sensibles. De plus, des techniques de DPI permettent à des pare-feux de filtrer le trafic du VPN s'il n'est pas chiffré.

Protocoles :

Les principaux protocoles permettant de créer des VPN sont :

- GRE, souvent remplacé par L2TP, tous deux développés par Cisco.
- PPTP (Point-to-Point tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco Systems, Nortel et Shiva. Il est désormais quasi-obsolète.
- L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 3931) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- IPsec est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.
- SSL/TLS offre une très bonne solution de tunnelisation. L'avantage de cette solution est de permettre l'utilisation d'un navigateur Web comme client VPN.
- SSH permet, entre autres, d'envoyer des paquets depuis un ordinateur auquel on est connecté.

Annexe 2

Hardware

Connectiques en informatique:

Introduction:

La connectique regroupe toutes les techniques liées aux connexions physiques des liaisons électriques ainsi que des transmissions de données, c'est-à-dire les connecteurs et prises.

La connectique est omniprésente dans nos vies que ce soit pour relier nos appareils électriques à des prises d'alimentation électrique ou pour relier les différents éléments de nos systèmes informatiques, nos systèmes audio ou vidéo.

Le défi des manufacturiers et des ingénieurs est de maximiser la standardisation des connexions tout en conservant la fonctionnalité de ces connexions. La maximisation de la standardisation réduit les coûts et facilite la vie des consommateurs mais cette standardisation ne doit pas se faire au détriment de la puissance et de la fonctionnalité des appareils.

Connecteurs:

Définition:

Les connecteurs informatiques, généralement appelés « connecteurs d'entrée-sortie » (notés E/S ou en anglais I/O pour Input/Output), sont des interfaces permettant de relier des équipements à l'aide de câbles. Ils se composent généralement d'une prise mâles, avec des broches (en anglais pin) saillantes, venant s'insérer dans des prises femelles (en anglais socket), constituées de douilles d'accueil. Il existe néanmoins des prises dites hermaphrodites faisant office de prise mâle et femelle et pouvant s'insérer l'une dans l'autre.

Brochage:

Les broches et douilles des connecteurs sont généralement reliés à des fils électriques constituant le câble. Ainsi, l'association des broches à chaque fil du câble est appelé brochage (en anglais pin layout).

Chaque broche numérotée correspond en règle générale à un fil du câble, mais il arrive qu'une des broches ne soit pas utilisé.

Par ailleurs, dans certains cas, il peut arriver que deux broches soient reliées entre-elles auquel cas on parle de « pont ».

Port informatique

Origine du mot :

Port, en informatique, est une traduction erronée de l'anglais port (en) ; l'étymologie du mot au sens informatique est le latin porta (→ porte), et non portus (→ port).

Il existe en informatique deux types de ports que le sens et l'utilisations diffèrent:

Le port matériel:

Un port matériel est conçu pour brancher un certain type de périphérique, soit directement, soit au moyen d'un câble. Il est soumis à des normes aussi bien sur ses caractéristiques physiques (forme, considérations électriques ou optiques) que logiques (à quoi sert chaque quel fil/patte/connecteur, que signifie tel ou tel signal en entrée, en sortie).

Les ports matériels se répartissent en :

- ports internes destinés soit à relier à une carte mère des périphériques internes au boîtier de l'ordinateur (disques, barrettes de mémoire ou même processeur en considérant un socket comme un port matériel) soit à insérer une carte d'extension enfichable sur un bus interne (on parle alors de connecteur d'extension).

- ports externes permettant de communiquer avec différents périphériques, souvent via un câble, quoiqu'on trouve aussi notamment dans le cas des portables des connecteurs d'extension reliés à un bus (par exemple PC-Card).

Port logiciel

Correspondant à la couche de transport du modèle OSI, la notion de port logiciel permet, sur un ordinateur donné, de distinguer différents interlocuteurs. Ces interlocuteurs sont des programmes informatiques qui, selon les cas, écoutent ou émettent des informations sur ces ports. Un port est distingué par son numéro.

Explication et utilités :

Pour simplifier, on peut considérer les ports comme des portes donnant accès au système d'exploitation : (Microsoft Windows, Mac OS, GNU/Linux, Solaris…). Pour fonctionner, un programme (par exemple un jeu à accélération 3D/2D, ou un logiciel de retouche photo) ouvre des portes pour entrer dans le système d'exploitation, mais lorsque l'on quitte le programme, la porte n'a plus besoin d'être ouverte.

Grâce à cette abstraction, on peut exécuter plusieurs logiciels serveurs sur une même machine, et même simultanément des logiciels clients et des serveurs, ce qui est fréquent sur les systèmes d'exploitation multitâches et multiutilisateurs.

De nombreux programmes TCP/IP peuvent être exécutés simultanément sur Internet (vous pouvez par exemple ouvrir plusieurs navigateurs simultanément ou bien naviguer sur des pages HTML tout en téléchargeant un fichier par FTP). Chacun de ces programmes travaille avec un protocole, toutefois l'ordinateur doit pouvoir distinguer les différentes sources de données.

Comment se fait l'attribution des ports:

Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine, codée sur 16 bits, Il existe donc un maximum de 65 535 ports (2^{ 16}-1) par ordinateur: un port= (la combinaison adresse IP + port est alors une adresse unique au monde, elle est appelée socket).

L'adresse IP sert donc à identifier de façon unique un ordinateur sur le réseau tandis que le numéro de port indique l'application à laquelle les données sont destinées. De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port, les données sont envoyées vers l'application correspondante. S'il s'agit d'une requête à destination de l'application, l'application est appelée application serveur. S'il s'agit d'une réponse, on parle alors d'application cliente.

L'attribution des ports est faite par le système d'exploitation, sur demande d'une application. Cette dernière peut demander que le système d'exploitation lui attribue n'importe quel port disponible. L'application peut ensuite l'utiliser comme bon lui semble.

Lorsqu'un logiciel client veut dialoguer avec un logiciel serveur, aussi appelé service, il a besoin de connaître le port écouté par ce dernier. Les ports utilisés par les services devant être connus par les clients, les principaux types de services utilisent des ports qui sont dits réservés. Par convention, l'IANA(Internet Assigned Numbers Authority) une organisation dont le rôle est la gestion de l'espace d'adressage IP d'Internet, et des autres ressources partagées de numérotation requises soit par les protocoles de communication sur Internet, soit pour l'interconnexion de réseaux à Internet et gère également les numéros de protocoles de nombreux protocoles différents sur IP ainsi la publication notamment de la liste des numéros de ports TCP et UDP. Cette liste est reprise par les différents systèmes d'exploitation (Windows, Mac Os, Unix5, Linux, etc.).

- Les ports 0 à 1023 sont les «ports reconnus» ou réservés («Well Known Ports»). Ils sont, de manière générale, réservés aux processus système (démons) ou aux programmes exécutés par des utilisateurs privilégiés. Un administrateur réseau peut néanmoins lier des services aux ports de son choix. Le fichier services indique la liste de ces services dits well-known. Sous UNIX, ce fichier est directement dans /etc ; sous Windows, ce fichier est par défaut dans C:\Windows\System32\drivers\etc.

- Les ports 1024 à 49151 sont appelés «ports enregistrés» («Registered Ports»).

- Les ports 49152 à 65535 sont les «ports dynamiques et/ou privés» («Dynamic and/or Private Ports»).

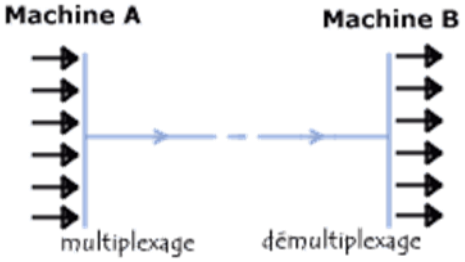
Port	Service ou Application
21	FTP
23	Telnet
25	SMTP
53	Domain Name System
63	Whois
70	Gopher
79	Finger
80	HTTP
110	POP3
119	NNTP

Ainsi, un serveur (un ordinateur que l'on contacte et qui propose des services tels que FTP, Telnet, ...) possède des numéros de port fixes auxquels l'administrateur réseau a associé des services. Ainsi, les ports d'un serveur sont généralement compris entre 0 et 1023 (fourchette de valeurs associées à des services connus).

Du côté du client, le port est choisi aléatoirement parmi ceux disponibles par le système d'exploitation. Ainsi, les ports du client ne seront jamais compris entre 0 et 1023 car cet intervalle de valeurs représente les ports connus.

La fonction de multiplexage:

Le processus qui consiste à pouvoir faire transiter sur une connexion des informations provenant de diverses applications s'appelle le multiplexage. De la même façon le fait d'arriver à mettre en parallèle (donc répartir sur les diverses applications) le flux de données s'appelle le démultiplexage.



Ces opérations sont réalisées grâce au port, c'est-à-dire un numéro associé à un type d'application, qui, combiné à une adresse IP, permet de déterminer de façon unique une application qui tourne sur une machine donnée.

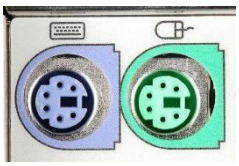
Comparaison entre un connecteur et un port:

Connecteur:

Un connecteur est la fin unique d'une fiche, la prise ou le bord d'une carte qui se connecte sur un port. Par exemple, tous les ordinateurs de bureau ont des cartes d'extension disposent d'un connecteur qui permet à la carte de se relier dans une fente sur la carte mère. Lorsqu'on se réfère à des câbles, le connecteur est l'extrémité du câble qui se connecte à un port. Par exemple, la fin d'un câble USB comporte un connecteur qui permet de se connecter à un port USB.

Port:

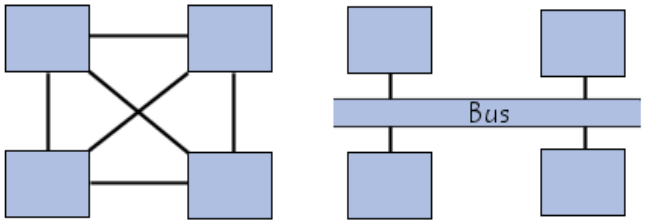
Le Port a soit des trous ou une fente qui correspond à la prise ou de la carte étant connectés dans le port. La photo montre un exemple d'un port PS / 2 qui se trouve à l'arrière de l'ordinateur qui permet à un clavier et à la souris avec un connecteur PS / 2 pour se connecter à l'ordinateur.


Port PS/2

Bus informatiques:

On appelle bus, en informatique, un ensemble de liaisons physiques (câbles, pistes de circuits imprimés, etc.) pouvant être exploitées en commun par plusieurs éléments matériels afin de communiquer.

Les bus ont pour but de réduire le nombre de « voies » nécessaires à la communication des différents composants, en mutualisant les communications sur une seule voie de données. C'est la raison pour laquelle la métaphore d'« autoroute de données » est parfois utilisée.



Caractéristiques d'un bus

Un bus est caractérisé par le volume d'informations transmises simultanément. Ce volume, exprimé en bits, correspond au nombre de lignes physiques sur lesquelles les données sont envoyées de manière simultanée. Une nappe de 32 fils permet ainsi de transmettre 32 bits en parallèle. On parle ainsi de « largeur » pour désigner le nombre de bits qu'un bus peut transmettre simultanément.

D'autre part, la vitesse du bus est également définie par sa fréquence (exprimée en Hertz), c'est-à-dire le nombre de paquets de données envoyés ou reçus par seconde. On parle de cycle pour désigner chaque envoi ou réception de données.

De cette façon, il est possible de connaître le débit maximal du bus (ou taux de transfert maximal), c'est-à-dire la quantité de données qu'il peut transporter par unité de temps, en multipliant sa largeur par sa fréquence. Un bus d'une largeur de 16 bits, cadencé à une fréquence de 133 MHz possède donc un débit égal à :

16 * 133.106 = 2128*106 bit/s,

Soit 2128*106/8 = 266*106 octets/s

Soit 266*106 /1000 = 266*103 Ko/s

Soit 259.7*103 /1000 = 266 Mo/s

Sous-ensembles de bus (Bus internes):

En réalité chaque bus est généralement constitué de 50 à 100 lignes physiques distinctes, classées en trois sous-ensembles fonctionnels :

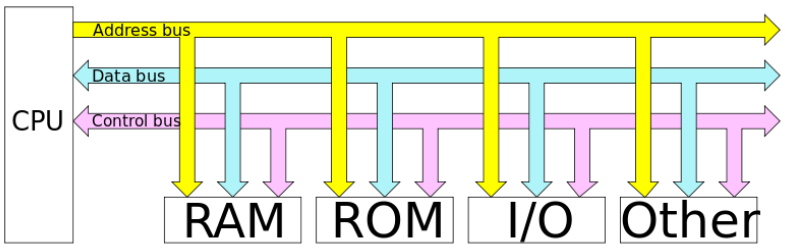
Le bus d'adresses (appelé parfois bus d'adressage ou bus mémoire) transporte les adresses mémoire auxquelles le processeur souhaite accéder pour lire ou écrire une donnée. Il s'agit d'un bus unidirectionnel.

Le bus de données véhicule les instructions en provenance ou à destination du processeur. Il s'agit d'un bus bidirectionnel.

Le bus de contrôle (parfois bus de commandes) transporte les ordres et les signaux de synchronisation en provenance de l'unité de commande et à destination de l'ensemble des composants matériels. Il s'agit d'un bus directionnel dans la mesure où il transmet également les signaux de réponse des éléments matériels.

Bus externes (bus d'extension):

Ce bus parfois appelé bus d'entrée/sortie, permet aux divers composants de la carte-mère (USB, série, parallèle, cartes branchées sur les connecteurs PCI, disques durs, lecteurs et graveurs de CD-ROM, etc.) de communiquer entre eux mais il permet surtout l'ajout de nouveaux périphériques grâce aux connecteurs d'extension (appelés slots) connectés sur le bus d'entrées-sorties.



Bus parallèle :

Matériel :

D'un point de vue physique, ce type de bus est un ensemble de conducteurs électriques parallèles. À chaque cycle de temps, chaque conducteur transmet un bit.

Ces bus ont donc une taille en nombre de conducteurs, et une taille en bits. Les tailles les plus courantes (en bits) sont : 8, 16, 32, 64 ou plus. Lorsqu'on parle de la taille d'un bus, cela signifie qu'il s'agit du nombre d'informations (ou bits) que le bus peut transmettre en un cycle, sans compter les informations de contrôle.

Certains conducteurs supplémentaires sont affectés à la transmission des signaux de contrôles du bus et de validation des signaux de donnée.

Fonctionnement:

Le bus sert à transmettre un entier informatique de la taille du bus. Les différents bits du bus ont chacun un poids différent numéroté de zéro à N-1 où N est la taille du bus. Par exemple pour un bus quatre bits on peut transmettre 16 valeurs différentes (24 = 16).

L'émetteur positionne au même instant tous les bits du bus. Au moment adéquat le composant lecteur lira tous les bits en même temps. Cet instant adéquat peut être déterminé par un des signaux de contrôle qui changera de valeur pour signaler au dispositif lecteur qu'il est temps de lire les données sur le bus.

Ce type de bus souffre d'un défaut inhérent à son principe : bien que l'émetteur positionne au même instant tous les bits, les câbles qui les transportent jusqu'au récepteur peuvent ne pas avoir précisément les mêmes caractéristiques électriques (une nappe de conducteurs tordue par exemple) ou même ne pas avoir la même longueur : cela force l'émetteur à maintenir l'état de chaque groupe de bits à transmettre pendant un temps suffisant pour garantir une réception sans erreur à l'autre bout de la liaison, ce qui réduit le débit maximal d'information.

Cas d'utilisation:

Lecture et écriture de la mémoire vive par un processeur. Quatre bus distincts sont utilisés, un bus de données de 128 bits, un bus d'adresse (d'environ 36 bit sur un PC de 2008[réf. nécessaire]), un bus de contrôle et le bus d'horloge. Le bus d'adresse est utilisé pour sélectionner les cellules mémoires qui doivent être lues ou écrites, le bus de données servant à transmettre le contenu de la mémoire elle-même, le bus de contrôle indiquant s'il s'agit d'une lecture ou d'une écriture. Les bus changent d'état sur une transition du bus d'horloge, le transfert se fait sur une transition inverse. Ce type de bus est extrêmement rapide : un PC de 2008 permet ici des transferts à 6,4 gigaoctets (Go) par seconde[réf. nécessaire]. Ces bus sont des bus au sens de l'électrotechnique, avec leur limitation de longueur. Plus le transfert est rapide, plus ils doivent être courts.

Interconnexion de disques durs SCSI. Une nappe à 68 conducteurs relie chaque disque à l'adaptateur et transporte tour à tour les signaux de commandes et de données sur 16 bits. Ce type de bus est très rapide quand la nappe est de haute qualité, il peut atteindre 320 Mo/s.

Connecteurs PCI des cartes d'extension d'un ordinateur personnel, ils permettent des transferts à environ 130 Mo/s.

Bus série :

Matériel :

Un bus série permet de transmettre les informations bit par bit. Toutefois il comporte plus d'une ligne permettant de transmettre des informations par l'addition d'éventuels signaux de contrôle et généralement par l'utilisation de deux lignes distinctes permettant ainsi à ces bus d'être bidirectionnels afin de permettre la transmission d'information dans les deux directions simultanément.

Fonctionnement:

Le bus série transmettant les données bit par bit, il est nécessaire lorsque l'on veut par exemple transmettre un mot de 32 bits de sérialiser l'information pour sa transmission. Le lecteur devra effectuer l'opération inverse pour reconstruire le mot de 32 bits à partir des bits reçus.

L'intérêt principal de ce type de bus (outre un câblage simplifié par rapport à un bus parallèle) est que pour un coût moindre (grâce au faible nombre de conducteurs de données) il permet -

en faisant appel à des composants électroniques de haute qualité - de dépasser les débits atteints par des bus parallèles.

Cas d'utilisation :

Certains périphériques informatiques tels que les souris utilisent un port série;

Une liaison USB peut être apparentée à un bus série;

Les disques durs récents utilisent un bus série (FC, SAS ou SATA). Les débits peuvent ici atteindre plusieurs Go/s.

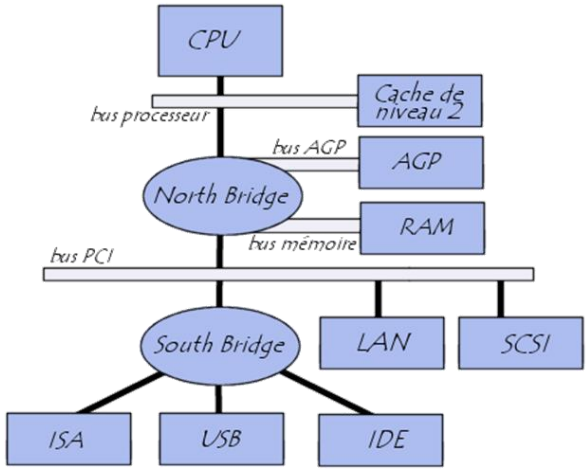
Le chipset

On appelle chipset (en français jeu de composants) l'élément chargé d'aiguiller les informations entre les différents bus de l'ordinateur afin de permettre à tous les éléments constitutifs de l'ordinateur de communiquer entre eux. Le chipset était originalement composé d'un grand nombre de composants électroniques, ce qui explique son nom. Il est généralement composé de deux éléments :

Le NorthBridge (Pont Nord ou Northern Bridge, appelé également contrôleur mémoire) est chargé de contrôler les échanges entre le processeur et la mémoire vive, c'est la raison pour laquelle il est situé géographiquement proche du processeur. Il est parfois appelé GMCH, pour Graphic and Memory Controller Hub.

Le SouthBridge (Pont Sud ou Southern Bridge, appelé également contrôleur d'entrée-sortie ou contrôleur d'extension) gère les communications avec les périphériques d'entrée-sortie. Le pont sud est également appelé ICH (I/O Controller Hub).

On parle généralement de bridge (en français pont) pour désigner un élément d'interconnexion entre deux bus.



Il est intéressant de noter que, pour communiquer, deux bus ont besoin d'avoir la même largeur. Cela explique pourquoi les barrettes de mémoire vive doivent parfois être appariées <sur certains systèmes (par exemple sur les premiers Pentium, dont la largeur du bus

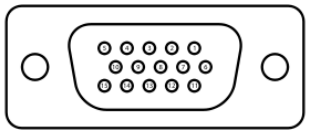
processeur était de 64 bits, il était nécessaire d'installer des barrettes mémoire d'une largeur de 32 bits par paire).

Les différents types de connectiques informatiques:

Pour compléter l'idée sur tout ce qu'on a traité précédemment, des exemples avec illustrations des connectiques sont nécessaires, nous intéressons aux plus utilisés.

Vidéo

VGA sont les initiales de Video Graphics Array, mais le VGA est aussi le premier standard de connecteur vidéo de l'histoire de l'informatique. Le signal se transporte dans un connecteur DE-15 avec 15 broches.



Le connecteur VGA avec 15 broches (schéma).

Le VGA transporte un signal analogique, c'est pourquoi il y a autant de broches. À la base, il fonctionnait sur les anciens écrans cathodiques, souvent en 640x480 ou 800x600, mais il fonctionne bien sur les écrans récents avec sa résolution maximale de 2048x1536 à 85Hz.

Je détaillerai la VGA dans les prochaines pages.

Le HDMI

Le HDMI est un connecteur vidéo numérique 19 broches utilisé principalement pour la télévision et l'image haute définition. Il permet de diffuser un signal HD voire 3D jusqu'en 4096x2160.

Il permet de transférer jusqu'à 18 Gbit/s en HDMI 2.0 et se trouve sur la plupart des cartes graphiques récentes.

Audio

Le XLR

Le connecteur XLR est un connecteur audio ou vidéo utilisé surtout dans le domaine du spectacle ou de l'audio professionnel car il comporte un système d'annulation des parasites.

Connecteur XLR

Ce système assez simple est facile à comprendre, La broche 1 du câble (à droite sur les prises femelles) représente la masse.

Les broches 2 et 3 (point chaud et point froid) sont respectivement le signal audio original et le signal avec la polarité inversée.

On peut donc s'exprimer ainsi : si le signal original, appelons-le S, est positif, et que S1 et le point chaud et S2 le point froid, on peut donc écrire l'équation suivante :

S1 = S

S2 = -S

-- APPARITION DES PARASITES, SOIT P --

Soit S1' et S2' les signaux avec leurs parasites,

S1' = S1+P = S+P

S2' = S2+P = -S+P

S1' - S2' fera donc 2S, sans les parasites.

Parce que même si le point froid est négatif et le point chaud positif, le parasite sera positif des deux côté.

Les périphériques :

L'USB

L'USB (Universal Serial Bus) est le port périphérique le plus utilisé en ce moment pour les ordinateurs et autres appareils informatiques. Il a été créé en 1996 par IBM, Microsoft et d'autres fabricants.

De gauche à droite :

- Micro-B (présent sur la plupart des mobiles Samsung)
- UC-E6 (sur quelques appareils photos)
- Mini-B (sur les anciens téléphones)
- Standard-A (femelle)
- Standard-A (mâle)
- Standard-B.

Le FireWire

Le FireWire est un connecteur, ou plutôt le nom donné par Apple à la prise originale IEEE 1394, qui est une prise série multiplexée permettant de véhiculer à la fois des données mais aussi des instructions ou des signaux de commandes aux appareils qu'elle relie.

Connecteur FireWire 400 mâle

Il est principalement utilisé pour les caméscopes vidéo (protocole DV) et pour certains disques durs externes. Il était aussi utilisé pour les connecteurs iPod et Iphone jusqu'en 2003 où Apple l'a remplacé par la prise Dock propriétaire.

Le port série

Le port série, appelé aussi RS-232, Les appareils branchés sur les ports séries sont représentés par les noms COM1, COM2, etc. sous MS-DOS et Windows.

Port série DB-9

Les appareils branchés sur les ports séries sont représentés par les noms COM1, COM2, etc. sous MS-DOS et Windows.

Le port parallèle

Le port parallèle est un connecteur série utilisé majoritairement pour connecter les imprimantes à un compatible PC.

Port parallèle DB-25

Le Thunderbolt

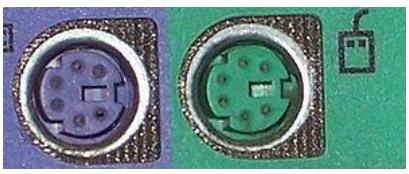
Thunderbolt est un connecteur informatique conçu par Intel sous le nom de code Light Peak. Il est prévu que Thunderbolt utilise dans ses prochaines versions la fibre optique. Il utilise un connecteur mini-DisplayPort. La vitesse maximale est de 10 Gbit/s, soit 1.25 Go/s, par canal sur le 1.0 et 20 Gbit/s, soit 2.5 Go/s, par canal sur le 2.0.

Connecteur Thunderbolt

Connecteur Thunderbolt

Le PS/2

Le port PS/2 est port utilisé pour connecter un clavier et une souris à un ordinateur. Ce port disparait peu à peu aujourd'hui, remplacé par l'USB et autres. Il s'agit en fait d'un port mini-DIN 6 broches.



Prise PS/2

La communication

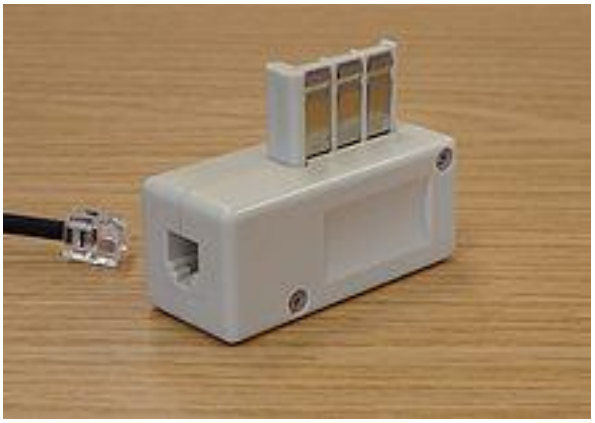
Les RJxx

Les ports RJ (Registered Jack) sont des ports le plus souvent utilisés pour la communication, et le réseau. Les formes les plus utilisées sont le RJ11 4 broches, le RJ45 8 broches et quelques autres.

Port RJ11 6 pins

La prise en T :

La "prise en T" ou F-010 est le connecteur téléphonique historique en France.



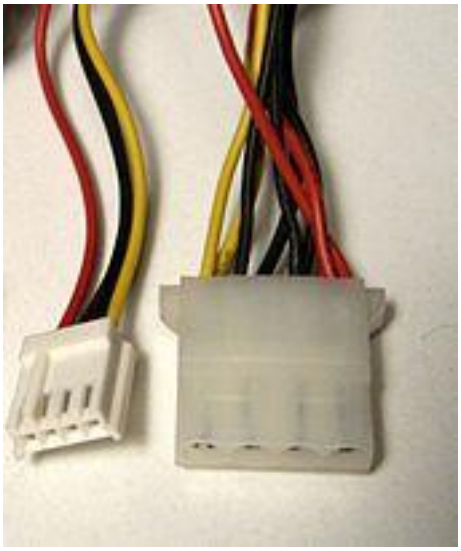
Adaptateur prise en T/RJ11

Cette prise équipait toutes les installations de France Télécom jusqu'en 2003 où elle fut remplacée par la prise RJ45 (8P8C).

Les prises internes:

Le Molex

Les prises Molex sont les prises utilisées pour alimenter les composants de l'ordinateur comme le lecteur CD/DVD, le disque dur, le lecteur de disquettes, etc.



Les 2 types de connecteurs Molex

Il existe 2 connecteurs : un normal, grand, à droite sur la photo, qui est utilisé par presque tous les composants, et un plus petit, qui n'est presque plus utilisé, qui servait pour les lecteurs de disquettes.

L'IDE

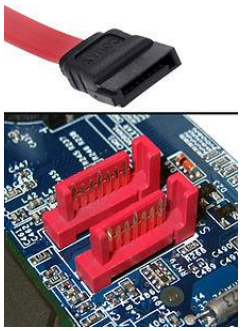
L'IDE (ou Parallel ATA, PATA) est le connecteur historique pour le disques durs, lecteurs optiques, etc. Le plus souvent sous forme de nappe, ainsi qu'on peut le voir sur cette photo :

PATA

Il n'est utilisé que pour les lecteurs internes, et est assez lent : 133 Mo/s maximum.

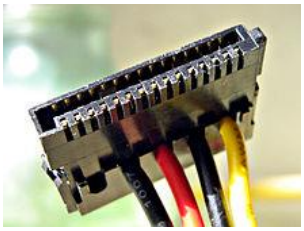
Le SATA

Le SATA, ou Serial ATA est un connecteur pour lecteur interne créé en 2003. Il succède au PATA (IDE) qui disparaitra peu à peu.



Câble et port SATA

Le SATA a eu un débit maximal de 1.5 Gbit/s, soit 192 Mo/s, mais a connu plusieurs versions qui changèrent ceci : le SATA II a doublé la vitesse avec 3 Gbit/s (384 Mo/s) puis le SATA III avec 6 Gbit/s (768 Mo/s). Il dispose de son propre câble d'alimentation :



Connecteur d'alimentation SATA

Universal Serial Bus:

Le Universal Serial Bus (USB, en français Bus universel en série, dont le sigle, inusité, est BUS) est une norme relative à un bus informatique en transmission série qui sert à connecter des périphériques informatiques à un ordinateur. Le bus USB permet de connecter des périphériques à chaud (quand l'ordinateur est en marche) et en bénéficiant du Plug and Play (le système reconnaît automatiquement le périphérique). Il peut alimenter les périphériques peu gourmands en énergie (disques SSD en particulier). Apparu en 1996, ce connecteur s'est généralisé dans les années 2000 pour connecter souris, clavier d'ordinateur, imprimantes, clés USB et autres périphériques bon marché sur les ordinateurs personnels.

Les performances de l'USB, notamment concernant les débits, se sont grandement améliorées au fil des versions (USB 2.0, 3.0…). Un futur standard 3.1 a été annoncé en 2013 et ses spécifications techniques publiées en août 2014.

Pour plus de clarté, les débits dans cet article seront indiqués en octets et non en bits (pour rappel, 1 octet = 8 bits).

Évolution de la norme USB

L'USB a été conçu au milieu des années 1990 afin de remplacer les nombreux ports externes d'ordinateurs, lents et incompatibles les uns avec les autres. Différentes versions de la norme

ont été développées au fur et à mesure des avancées technologiques, chacune étant vouée à remplacer les précédentes car plus performante.

USB 1

En 1996, la première version de la norme, l'USB 1.0, est spécifiée par sept partenaires industriels (Compaq, DEC, IBM, Intel, Microsoft, NEC et Northern Telecom). Mais elle reste théorique et n'a jamais vraiment été appliquée : par manque de composants, il faudra attendre la seconde version de la norme 1998, intitulée USB 1.1, pour que l'USB commence à être effectivement utilisé1. Ce que nous appelons couramment "USB 1" est donc en réalité de l'USB 1.1.

L'USB 1.1 apporte des corrections à la norme 1.0 et définit également deux vitesses de communication :

- le mode lent (Low Speed) a un débit de 190 Ko/s. Il permet de connecter des périphériques qui ont besoin de transférer peu de données, comme les claviers et souris ;
- le mode pleine vitesse (Full Speed) débite à 1,5 Mo/s. Il est utilisé pour connecter des imprimantes, scanners, disques durs, graveurs de CD et autres périphériques ayant besoin de plus de rapidité. Néanmoins, il est insuffisant pour beaucoup de périphériques de stockage de masse (ce mode permet la vitesse « 10 X » des CD).

En août 1998, avec la sortie de l'iMac G3, Apple est le premier2 constructeur à proposer un appareil disposant uniquement de ports USB en remplacement des ports d'ancienne génération, ce qui a fait décoller2 le marché des périphériques USB.

USB 2

En avril 2000 est publiée la norme USB 2.0, qui optimise l'utilisation de la bande passante1 et surtout ajoute introduit un troisième débit à 60 Mo/s, baptisé Haute vitesse (High Speed). Il est utilisé par les périphériques rapides : disques durs, graveurs… Mais au moment de sa sortie, la plupart des périphériques ont une vitesse inférieure à ce que permet l'USB 2.0.

En 2005, le Wireless USB, une version sans-fil de l'USB, est spécifiée par le Wireless USB Promoter Group. Elle promet 50 Mo/s à une distance de 3 m et 14 Mo/s à 10 m3.

L'extension On-The-Go (OTG), ajoutée à la norme USB 2.0 en 2007, permet d'effectuer des échanges de données point à point entre deux périphériques sans avoir à passer par un hôte (généralement un ordinateur personnel). La norme OTG s'impose désormais comme un standard.

USB 3

En 2008, l'USB 3.0 introduit le mode vitesse supérieure (SuperSpeed), qui débite théoriquement à 625 Mo/s4. Mais ce nouveau mode utilisant un codage des données de type8b/10b, la vitesse de transfert réelle est de seulement 500 Mo/s. L'USB 3 délivre une puissance électrique de 4,5 watts.

Les nouveaux périphériques disposent de connexions à 6 contacts au lieu de 4, mais la compatibilité ascendante des prises et câbles avec les versions précédentes est assurée. En revanche, la compatibilité descendante est impossible, les câbles USB 3.0 de type B n'étant pas compatibles avec les prises USB 1.1/2.05, mais il existe des adaptateurs.

Début 2010, l'USB 3 est introduit dans des produits grand public. Les prises femelles correspondantes sont signalées par une couleur bleue. Apparition aussi des prises femelles USB rouges, signalant une puissance électrique disponible supérieure, et appropriée au chargement rapide de petits appareils y compris (à condition de le paramétrer dans le BIOSou l'EFI) lorsque l'ordinateur est éteint.

À venir : l'USB 3.1

Un standard 3.16 à 10 Gb/s est annoncé en août 2013 ; ses spécifications techniques sont finalement publiées par le consortium USB Implementers Forum en août 2014.

L'USB 3.1 promet des débits doubles de ceux de l'USB 3.0, soit 1,2 Go/s. Le nouveau standard (câbles, interface) sera rétro compatible avec l'USB 3.0 et l'USB 2.07. Toutefois la connectique change, elle sera plus fine et n'imposera pas de sens de branchement. Pour tout de même permettre la connexion vers des connecteurs USB 2.0 et 3.0, le standard devra prendre en compte la possibilité d'avoir des adaptateurs passifs (à l'inverse des adaptateurs Lightning, le connecteur réversible qu'Apple a lancé avec l'iPhone 5 en 2012), pour garder une taille réduite et un coût de fabrication mesuré8. Cette nouvelle connectique se nommera Type C9.

Résumé des débits

Lorsque l'on parle d'un équipement USB, il est nécessaire de préciser la version de la norme (1.1, 2.0 ou 3.0) mais également la vitesse (low/full/high/super speed). Une clef USB spécifiée en USB 2.0 n'est pas forcément High Speed si cela n'est pas précisé par un logo «High Speed ».

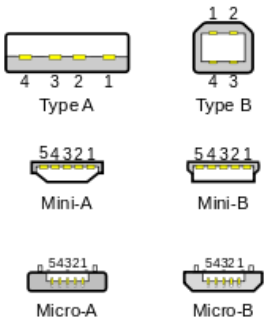
Le bus USB reste plus lent que des interfaces internes comme PCI ou AGP ou SATA / e-Sata (dans sa version 1.x et 2.0).

Débit des normes USB						
Version	USB 1.0	USB 1.1	USB 2.0	Wireless USB	USB 3.0	USB 3.1
Année	1996	1998	2000	2005	2008	2013
Débit	1,5 Mbit/s 0,19 Mo/s	12 Mbit/s 1,5 Mo/s	480 Mbit/s 60 Mo/s	480 Mbit/s 60 Mo/s	5 Gbit/s 600 Mo/s	10 Gbit/s 1,2 Go/s

Évolution des prises USB :

Différents connecteurs de type USB 1 et 2, de gauche à droite :

- micro B mâle,
- UC-E6 propriétaire (non USB),
- mini B mâle 5 pin,
- A femelle,
- A mâle
- B mâle.



Différents types de prises USB 1 et 2.

Fiche Micro-B USB 3.

Les premiers connecteurs : les types A et B

De base, le bus USB ne permet pas de relier entre eux deux périphériques ou deux hôtes : le seul schéma de connexion autorisé est un périphérique sur un hôte. Pour éviter des branchements incorrects, la norme spécifie deux types de connecteurs : le type A, destiné à être situé sur l'hôte, et le type B, destiné à être situé sur le périphérique.

Un hub USB peut comporter à la fois un connecteur B, qui permet de le relier à l'hôte, et des connecteurs A, qui permettent d'y relier des périphériques. Les appareils (hôte et périphériques) sont équipés de connecteurs femelles. Les câbles de connexion ont toujours une extrémité de type A mâle, et une extrémité de type B mâle, ce qui garantit le respect de la

topologie du bus. Il peut aussi exister des câbles de prolongation équipés de connecteurs de même type mais de genres différents.

Les mini connecteurs :

Chaque type (A ou B) existait dans les deux genres (mâle ou femelle), ce qui fait qu'il existait au départ quatre connecteurs. Par la suite, devant le développement des appareils compacts (téléphones portables, appareils photo numériques), une mise à jour de la norme USB 2 a introduit une version miniature du connecteur B : le mini B. Elle est fonctionnellement équivalente au connecteur B, mais de dimensions nettement réduites.

L'USB 2 a ensuite introduit connecteur mini AB, utilisé dans le cadre de l'extension « On-The-Go ». Il permet aux appareils compatibles de jouer indifféremment le rôle d'hôte ou rôle de périphérique, contrairement à l'USB classique où l'hôte se branche sur obligatoirement sur un connecteur de type A et le périphérique sur un connecteur de type B (voir plus haut).

Les micro-connecteurs :

Les appareils mobiles s'étant encore réduits, les connecteurs mini B sont devenus à leur tour trop gros. En janvier 2007, le nouveau connecteur micro B a été annoncé. Il est non seulement plus fin que le mini B, mais également prévu supporter pour un grand nombre de cycles de connexion/déconnexion (jusqu'à 10 00010), ce qui le rend particulièrement bien adapté aux appareils mobiles car ils souvent branchés et débranchés (tablettes tactiles, Smartphones…).

Pour les mêmes raisons, une nouvelle norme micro AB est venue remplacer le mini AB (voir plus haut), qui est aujourd'hui officiellement déprécié.

La nouvelle norme : le type C

Un nouveau connecteur a été introduit dans la norme le 11 août 2014 : le type C, destiné à remplacer tous les connecteurs précédents. Il a la particularité d'être réversible, c'est-à-dire qu'il n'a plus de sens haut/bas11. Outre l'aspect pratique, il est compatible à la fois avec les standards USB 3.1 (qui doublent le débit théorique à 10 Gbps) ainsi qu'avec l'USB Power Delivery (jusqu'à 100 watts dans les deux sens).

Applications de l'USB

Pour le transfert des données :

USB a supplanté divers bus qui équipaient auparavant les ordinateurs : port série RS-232, port parallèle, port PS/2, port joystick (ou port MIDI), port SCSI, et même des bus internes comme PCI pour la connexion de certains dispositifs (par exemple cartes son ou cartes de réception TV).

La gamme des périphériques utilisant le bus USB est extrêmement vaste :

- périphériques d'interaction avec l'utilisateur : claviers, souris, joystick, guitare ;
- périphériques de stockage : disques durs externes, appareils photo, lecteurs multimédia, et surtout clés USB, un concept apparu spécifiquement pour le bus USB. Il s'agit de

l'association d'une mémoire flash et d'une interface USB, le tout contenu dans un petit boîtier évoquant une clé par sa taille et sa forme ;

- multimédia et imagerie : imprimantes, scanners, cartes son, webcams, tuners TV, écran secondaire (intégrant son propre contrôleur vidéo), microphone ;

- adaptateurs de réseau ou de communication : Wi-Fi, Ethernet, Bluetooth, infrarouge IrDA, Modem ;

- Bus et interfaces : port série RS-232, port parallèle, port PS/2, port joystick, Bus CAN, GPIB (IEEE-488), port série RS-485.

Le bus USB est également utilisé en interne dans certains ordinateurs pour connecter des périphériques tels que webcams, récepteurs infrarouges (c'est le cas par exemple sur lesMacBook Pro) ou lecteurs de cartes mémoire.

Pour l'alimentation électrique :

Le bus USB peut alimenter en énergie les périphériques, dans une certaine limite de courant consommé (2 A pour une application haute puissance, 100 mA pour une application normale12). Ceci est notamment mis à profit pour permettre la recharge d'appareils portables, pour lesquels on voit apparaître des adaptateurs secteur disposant d'une connectique USB limitée à l'alimentation électrique.

La connectique USB a ainsi une diffusion au-delà des périphériques informatiques stricto sensu, en tant que connecteur électrique de faible puissance. Un certain nombre de gadgets alimentés par port USB qui ne sont pas des périphériques informatiques sont apparus sur le marché : lampes d'appoint, petits ventilateurs, etc.

Pour les périphériques qui demandent plus de courant que ce que peut fournir un port USB, par exemple certains disques durs externes, on complète l'alimentation par un branchement sur un second port USB. Une telle utilisation est discutable car le périphérique monopolise à lui seul deux ports. Une prise électrique ordinaire serait plus adaptée, la fonction première de l'USB étant de transférer des données et non de distribuer du courant.

Spécifications techniques :

Caractéristiques générales :

L’Universal Serial Bus est une connexion à haute vitesse qui permet de connecter des périphériques externes à un ordinateur (hôte dans la terminologie USB). Il permet le branchement simultané de 127 périphériques par contrôleur (hôte). Le bus autorise les branchements et débranchements à chaud (« Hot-Plug », sans avoir besoin de redémarrer l’ordinateur) et fournit l’alimentation électrique des périphériques sous 5 V, dans la limite de 0,5 A, soit 2,5 W.

D'un point de vue logiciel, le bus possède une topologie arborescente (dite également en étoile) : les feuilles de cet arbre sont les périphériques ; les nœuds internes sont des hubs qui permettent de greffer des sous-arborescences dans l'arborescence principale. On trouve dans le commerce ces hubs sous forme de petits boîtiers alimentés soit sur le bus, soit sur le secteur,

et qui s'utilisent comme des multiprises. Certains périphériques intègrent également un hub (moniteurs, claviers…). Cependant, tout bus USB possède au moins un hub situé sur le contrôleur : le hub racine, qui peut gérer les prises USB de l'ordinateur. Le nombre de hubs connectés en cascade est limité : hub racine compris, il ne doit pas exister plus de 7 couches dans l'arborescence13.

À plus bas niveau, il s'agit d'un anneau à jeton (ou Token Ring) : chaque nœud dispose successivement du bus. Il n'y a pas de collision de paquets comme en Ethernet, mais le nombre maximal de nœuds est prédéfini. Pour cette raison, l'USB n'est pas adapté aux communications réseau : l'apparition des "modems" ADSL USB était un moyen de diffuser l'ADSL à une époque où la plupart des PC bas de gamme disposaient du port USB mais pas d'Ethernet.

Protocole :

La bande passante est partagée temporellement entre tous les périphériques connectés. Le temps est subdivisé en trames (frames) ou microtrames (microframes) pendant lesquels plusieurs transferts peuvent avoir lieu.

La communication entre l'hôte (l'ordinateur) et les périphériques se fait selon un protocole basé sur l'interrogation successive de chaque périphérique par l'ordinateur. Lorsque l'hôte désire communiquer avec un périphérique, il émet un jeton (un paquet de données, contenant l'adresse du périphérique, codée sur sept bits) désignant un périphérique. Si le périphérique reconnait son adresse dans le jeton, il envoie un paquet de données (de 8 à 255 octets) en réponse. Les données ainsi échangées sont codées selon le codage NRZI. Puisque l'adresse est codée sur 7 bits, 128 périphériques (27) peuvent être connectés simultanément à un port de ce type. Il convient en réalité de ramener ce chiffre à 127 car l'adresse 0 est une adresse réservée.

USB définit quatre types de transferts :

- transfert de commande, utilisé pour l'énumération et la configuration des périphériques. Il convient pour des données de taille restreinte ; il y a garantie de livraison (renvoi des paquets erronés) ;

- transfert d'interruption, utilisé pour fournir des informations de petite taille avec une latence faible. Ce ne sont pas des interruptions au sens informatique du terme : le périphérique doit attendre que l'hôte l'interroge avant de pouvoir effectuer un tel transfert. Ce type de transfert est notamment utilisé par les claviers et les souris ;

- transfert isochrone, utilisé pour effectuer des transferts volumineux (bande passante garantie), et en temps réel. Il n'y a pas de garantie sur l'acheminement des données. Ce type de transfert est utilisé pour les flux audio et vidéo ;

- transfert en masse (bulk), utilisé pour transférer des informations volumineuses, avec garantie d'acheminement, mais sans garantie de bande passante. Ce type de transfert est utilisé par les dispositifs de stockage.

Il est possible de structurer la communication entre un hôte et un périphérique en plusieurs canaux logiques (pipes et endpoints) pour simplifier la commande du périphérique du port USB.

Connexion à chaud et Plug and Play : processus d'énumération

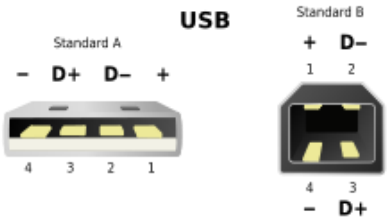
Les ports USB supportent la connexion à chaud et la reconnaissance automatique des dispositifs (Plug and Play). Ainsi, les périphériques peuvent être branchés sans éteindre l'ordinateur.

Lors de la connexion du périphérique à l'hôte, ce dernier détecte l'ajout du nouvel élément grâce au changement de la tension entre les fils D+ et D-. À ce moment, l'ordinateur envoie un signal d'initialisation au périphérique pendant 10 ms, puis lui fournit du courant grâce aux fils GND et VBUS (jusqu'à 100 mA). Le périphérique est alors alimenté en courant électrique et peut utiliser temporairement l'adresse par défaut (l'adresse 0). L'étape suivante consiste à lui fournir son adresse définitive et à obtenir sa description : c'est la procédure d'énumération.

En effet, après avoir reçu son adresse, le périphérique transmet à l'hôte une liste de caractéristiques qui permettent à ce dernier de l'identifier (type, constructeur, nom, version). L'hôte, disposant de toutes les caractéristiques nécessaires est alors en mesure de charger le pilote approprié.

Les périphériques sont regroupés en types ou classes dans la terminologie USB. Tous les dispositifs d'une classe donnée reconnaissent le même protocole normalisé. Il existe par exemple une classe pour les périphériques de stockage de masse (mass storage class, MSC), implémentée par la quasi-totalité des clés USB, disques durs externes, appareils photo et par certains baladeurs. La plupart des systèmes d'exploitation possèdent des pilotes génériques, pour chaque type de périphérique. Ces pilotes génériques donnent accès aux fonctions de base, mais des fonctions avancées peuvent manquer.

Alimentation électrique :



Prises USB de type A et B, vue de face. USB 1 et 2.

L'architecture USB a pour caractéristique de fournir aussi l'alimentation électrique aux périphériques. Il utilise pour cela un câble composé de quatre fils pour les USB 1 et 2 (la masse GND, l'alimentation VBUS et deux fils de données appelés D- et D+) et de six fils pour l'USB 3 (séparation des données IN/OUT). Les fils D+ et D- forment une paire torsadée et utilisent le principe de la transmission différentielle afin de garantir une certaine immunité aux bruits parasites de l'environnement physique du périphérique ou de son câble.

USB Battery Charging 1.0 à 1.2

USB Power Delivery

USB Power Delivery permet de délivrer jusqu'à 100 W de puissance sur une tension maximale de 20 V au travers de l'USB, tout en maintenant la communication. L'alimentation électrique est désormais bidirectionnelle, elle peut se faire dans les deux sens.

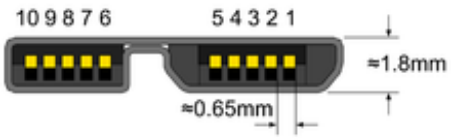
Lors de la connexion, les deux périphériques négocient la puissance à délivrer par l'intermédiaire de contrôleurs spécifiques et chaque port USB pourra ainsi indiquer les tensions et intensités qu'il supporte.

La norme prévoit 5 profils :

- Profil 1 : 5V / 2A → 10W
- Profil 2 : 5V / 2A et 12V / 1.5A → 18W
- Profil 3 : 5V / 2A et 12V / 3A → 36W
- Profil 4 : 5V / 2A et 12V ou 20V / 3A → 60W
- Profil 5 : 5V / 2A et 12V ou 20V / 5A → 100W

Brochage

Types A et B



Description prise Micro-B USB 3

• 1 : Alimentation (VBUS)

• 2 : USB 2.0 paire différentielle (D−)

• 3 : USB 2.0 paire différentielle (D+)

• 4 : USB OTG ID pour identifier les lignes

• 5 : Masse

• 6 : USB 3.0 ligne de transmission du signal (−)

• 7 : USB 3.0 ligne de transmission du signal (+)

• 8 : Masse

• 9 : USB 3.0 ligne de réception du signal (−)

• 10 : USB 3.0 ligne de réception du signal (+)

Le brochage des connecteurs de type A et B est le suivant :

Fonction	Couleur	Numéro de broche pour les types A et B	Numéro de broche pour le type mini B
Alimentation +5 V (VBUS)	Rouge	1	1

Données (D-)	Blanc	2	2
Données (D+)	Vert	3	3
Masse (GND)	Noir	4	5[14]

Type C

Le brochage de la prise de type C, vue de face, est le suivant :

A12	A11	A10	A9	A8	A7	A6	A5	A4	A3	A2	A1
GND	RX2+	RX2-	VBus	SBU1	D-	D+	CC	VBus	TX1-	TX1+	GND
GND	TX2+	TX2+	VBus	VConn			SBU2	VBus	RX1-	RX1+	GND
B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12

La broche CC indique l'orientation du connecteur, la broche VConn pour l'alimentation.

Le brochage du connecteur de réception de type C, vue de face, est le suivant :

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
GND	TX1+	TX1-	VBus	CC1	D+	D-	SBU1	VBus	RX2-	RX2+	GND
GND	RX1+	RX1+	VBus	SBU2	D-	D+	CC2	VBus	TX2-	TX2+	GND
B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1

L'alimentation passe par les broches VBus et GND. Les signaux de configurations par CC1 et CC2 et il y a 2 broches SBU (SideBand Use).

RS-232

RS-232 (parfois appelée EIA RS-232, EIA 232 ou TIA 232) est une norme standardisant un bus de communication de type série sur trois fils minimum (électrique, mécanique et protocole). Disponible sur presque tous les PC jusqu'au milieu des années 2000, il est communément appelé le « port série ». Sur les systèmes d'exploitation MS-DOS et Windows, les ports RS-232 sont désignés par les noms COM1, COM2, etc. Cela leur a valu le surnom de « ports COM », encore utilisé de nos jours. Cependant, il est de plus en plus remplacé par le port USB.

Le standard RS-232 recouvre plusieurs autres standards : les recommandations UIT-T V.24 (définition des circuits) et V.28 (caractéristiques électriques), ainsi que la norme ISO 2110 pour la connectique.

Les liaisons RS-232 sont fréquemment utilisées dans l'industrie pour connecter différents appareils électroniques (automate, appareil de mesure, etc.).

Description

Prise femelle extrémité de câble type DE-9

La connectique de cette liaison se présente fréquemment sous la forme du connecteur DE-9 ou DB-25, mais peut aussi être d'un autre type (RJ25). Seule la version DB-25 est vraiment standardisée, la DE-9 (très souvent appelée DB-9 dans le commerce) est une adaptation d'IBM lors de la création du PC AT. La transmission des éléments d'information (ou bit) s'effectue bit par bit, de manière séquentielle. Cette transmission est décrite sur la page communication série.

Utilisation

Un connecteur DE-9 (Improprement appelé DB-9) mâle utilisé comme port série sur un ordinateur personnel

Vous pouvez voir au-dessus du port sur la photo ci-contre, le symbole pour les liaisons séries, représenté par les bits 0, 1 puis 0.

Placé à l'arrière de l'ordinateur, il était souvent occupé par une souris ou un modem de type RTC, il pouvait aussi être utilisé pour le transfert des clichés numériques depuis l'appareil photo vers le disque dur du PC.

Bien que ce port de communication ait tendance à être remplacé par l'USB sur les PC, il reste encore très utilisé dans l'industrie, notamment grâce à sa robustesse et à sa simplicité. Ainsi, ce port est toujours d'actualité, en particulier dans les systèmes automatisés : le transfert deGrafcets ou bien de lignes de programme pour machines-outils à commande numérique s'effectuent toujours par liaison RS-232.

De même, de nombreux terminaux embarqués (qu'ils soient GPS, modems, terminaux graphiques, etc.) utilisent le RS-232 comme méthode principale de communication avec l'extérieur. Fréquemment, les périphériques réseau (routeurs, commutateurs, etc.) sont équipés d'un port RS-232 au travers duquel il est possible de les configurer.

Néanmoins, les pc portables munis de ports séries deviennent de plus en plus difficile à trouver. En effet, très peu de constructeurs proposent encore ce type de ports.

En cas d'absence de port RS 232, il existe des adaptateurs USB/port série.

Haute disponibilité :

Pour la haute disponibilité, une liaison RS-232 est parfois utilisée : deux serveurs fonctionnent en cluster et ils se surveillent l'un l'autre via une liaison RS-232. C'est le cas par exemple de Heartbeat.

Spécification :

Le standard RS-232 permet une communication série, asynchrone et duplex entre deux équipements.

Portée du standard :

En règle générale une jonction numérique entre un Équipement terminal de traitement de données (ETTD, en anglais DTE) et un équipement terminal de circuit de données (ETCD, en anglais DCE), située au niveau 1 du modèle OSI, se définit par trois paramètres : les circuits, les niveaux électriques et le brochage. Ce sont ces trois éléments qui sont couverts par le standard RS-232.

Plus précisément, le standard RS-232 spécifie :

- La fonction de chaque circuit de jonction. Cela correspond à la norme UIT-T V.24, dans laquelle ces circuits sont numérotés dans la série 100 (102 retour commun, 103 émission de données, 104, etc.).
- Les caractéristiques électriques de la liaison : niveaux de tension, débits possibles, etc. Cela correspond à la norme UIT-T V.28.
- Les caractéristiques mécaniques pour les connecteurs et l'identification des contacts. Dans le cas d'un connecteur DB-25, cela correspond à la norme ISO 2110.

Par contre le standard ne définit pas :

- Le codage des caractères (ASCII, Code Baudot ou EBCDIC par exemple).
- La façon dont les caractères sont répartis en trames.
- Les protocoles de détection d'erreur ou les algorithmes de compression de données.
- Les débits de transmission : seule une limite supérieure de 20 000 bauds est indiquée.
- La fourniture de courant électrique à des périphériques.

Mécanique :

- Le standard spécifie initialement l'utilisation de connecteurs DB-25 mâle du côté DTE (Data Terminal Equipement), et DB-25 femelle du côté DCE (Data Communications Equipment) (modem).

- Les connecteurs DE-9 ont rapidement remplacé les DB-25, pour des raisons de taille de connecteur et d'économie de câblage, tous les signaux n'étant pas indispensables à la communication.

- Entre un DTE et un DCE, le câblage est droit : les broches sont connectées une à une de part et d'autre. Un tel câble est muni de connecteurs de genres différents (un mâle et un femelle). Ces câbles peuvent être connectés en série (comme des « rallonges »).

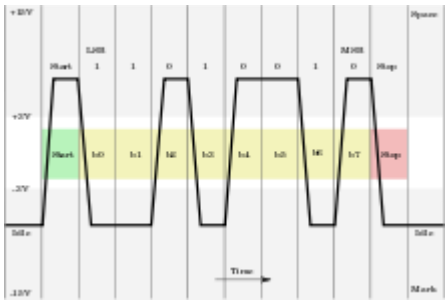
- Dans les configurations où deux DTE sont directement connectés (c'est-à-dire en l'absence de modem), un câble de liaison croisé dit « Null modem » doit être utilisé. Il est muni de connecteurs femelle à chaque extrémité, et possède un câblage spécifique, qui n'était pas prévu par la norme.

Schéma usuel de raccordement d'un câble « Null modem » à 25 broches (symétrique) ; en gras les signaux croisés : Attention, câblage à vérifier.

	Dir			Dénomination (côté DTE)
1	---	1	PG	Masse de blindage (protection électromagnétique)
3	←	2	TxD	Données à transmettre
2	→	3	RxD	Réception des données
5	←	4	RTS	Demande de transmission
4	→	5	CTS	Prêt pour transmission
20	→	6	DSR	Envoyez les données
7	---	7	SG/GND	0 Volt électrique
20	→	8	DCD	Détection d'un signal sur la ligne
9	---	9		+ Tension
10	---	10		- Tension
11	---	11		
12	---	12	SDCD	Deuxième Détection de signal sur la ligne
19	→	13	SCTS	Deuxième Prêt pour transmission
16	←	14	STD	Deuxième Transmission des données
17	→	15	ST	Signal d'horloge pour transmission de données
14	→	16	SRD	Deuxième Réception des données
15	→	17	RT	Signal d'horloge pour réception de données
		18		DTE demande le rebouclage du DCE local
13	←	19	SRTS	Deuxième Demande de transmission
6	←	20	DTR	Données prêtes
		21		DTE demande le rebouclage du DCE distant
22	→	22	RI	Indicateur de sonnerie
		23		Signal de sélection de vitesse
17,24	←	24	TT	Horloge de transmission
		25		DCE en test de rebouclage

Note : l'éventuel signal d'horloge émis par le terminal (DTE) en pin 24 est reçu par l'ordinateur (DCE) en pin 17. L'éventuel signal d'horloge émis par le DCE en pin 15 est reçu par le DTE en pin 17.

Protocole :



Oscillogramme de la transmission du caractère K (01001011), avec un bit de départ et un bit d'arrêt.

Pour établir une communication effective via RS-232, il est nécessaire de définir le protocole utilisé : notamment, le débit de la transmission, le codage utilisé, le découpage en trame, etc. La norme RS-232 laisse ces points libres, mais en pratique on utilise souvent des UART qui découpent le flux en trames d'un caractère ainsi constituées :

- 1 bit de départ ;
- 7 à 8 bit de données ;
- 1 bit de parité optionnel ;
- 1 ou plusieurs bits d'arrêt.

Le bit de départ a un niveau logique "0" tandis que le bit d'arrêt est de niveau logique "1". Le bit de donnée de poids faible est envoyé en premier suivi des autres.

Application: pour générer un signal électrique alternatif carré (rapport cyclique 1:1) sur le port série, imprimer une suite consécutive de U(01010101) ce qui donne dans le temps 0(départ)10101010(U, du lsb au msb)1(arrêt) donc 0101010101 (0101010101010101010101010101010101 = UUU) avec 8 bits de donnée, 1 bit départ, 1 bit arrêt et 0 bit de parité. Les niveaux électriques sont inversés (voir ci-dessous)

La spécification RS-232 prescrit des débits inférieurs à 20 000 bit/s. Cependant, les débits utilisés en pratique varient entre 75 bit/s et 115 200 bit/s.

Electrique :

Un niveau logique "0" est représenté par une tension de +3V à +25V et un niveau logique "1" par une tension de -3V à -25V (codage NRZ). D'ordinaire, des niveaux de +12V et -12V sont utilisés.

La norme V.28 indique qu'un 1 est reconnu si la tension est inférieure à -3 V, et un 0 est reconnu si la tension est supérieure à +3 V.

Limites :

Longueur maximum de câble RS232

Débit (bit/s)	Longueur (pieds)	Longueur (m)
19 200	50	15
9 600	500	150
4 800	1 000	300
2 400	3 000	900

Bibliographie

Webographie

Bibliographie et webographie

1. administrateur du site, c'est quoi le cloud (partie 2), www.culture-informatique.net, 2014.
2. Brian J.S. Chee, Curtis Franklin Jr., Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center, CRC Press, 2010 (ISBN 9781439806173);
3. Climatisation et serveurs : vers des salles informatiques plus vertes [archive], Thierry Lévy-Abégnoli, ZDNet France, le 5 décembre 2007.
4. Des couloirs chauds et froids [archive], Christophe Auffray, ZDNet France, le 14 janvier 2010.
5. Encyclopédie Larousse.
6. Judith Hurwitz, Robin Bloor, Marcia Kaufman et Fern Halper, Cloud Computing for Dummies, John Wiley & Sons, 2009 (ISBN 9780470484708).//
7. Le Monde Informatique, n°1139.
8. Lee Gillam, Cloud computing, Springer, 2010 (ISBN 9781849962414).
9. Livre Blanc « Datacenters, une chance pour la France » [archive], sur le site globalsecuritymag.fr.
10. Medoweb80, Internet origine et développement, www.propulser.net, 30/08/2015.
11. National Institute of Standards and Technology Special Publication 800-145, Septembre 2011
12. NIST.gov – Computer Security Division – Computer Security Resource Center , Csrc.nist.gov.
13. Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, Cloud Computing: Principles and Paradigms, John Wiley & Sons, 2010 (ISBN 9781118002209).
14. searchdatacenter.techtarget.com/definition/Uptime-Institute-Inc.
15. Vincent Lavergne, L'infrastructure informatique, organe vital de l'entreprise, www.jornaldunet.com,17/12/2009.
16. Walid KADRI, Introduction à l'Informatique" Principes et Généralités", Faculté de Sciences Politiques et de Droit, Université d'ORAN, 2010-2011.
17. Wikipédia.
18. www.cio.com.au/article/385193/uptime_exec_data_center_ratings_aid_cloud_choice/
19. www.datacenterknowledge.com/archives/2009/10/23/the-uptime-institute-sold-to-451-group/
20. www.glohse.com/?tag=uptime-institute
21. www.investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=78943204 .
22. www.ladocumentationfrancaise.fr
23. www.slideshare.net/Management.com/factea-offshoring-filter-presentation-871378
24. www.dictionnaire.phpmyvisites.net/definition-OUTSOURCING-4852.htm
25. Zaigham. Mahmood - Richard Hill, Cloud Computing for Enterprise Architectures, Springer, 2011 (ISBN 9781447122364).
26. Pierre Pinard, encyclopédie de la sécurité informatique, Assiste.com - 1999 – 2012
27. www.foxclan69.free.fr/eBook/DELL/DRAC.pdf

28. www.offshore-developpement.com/
29. www.nsa.gov
30. www.web.archive.org/web/20070927035010/http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf

Abstract

In a global environment where economic concepts affecting the technological future, as the relocation to inspire the creation of data centers and the last pair with the concepts of sharing and outsourcing have contributed greatly to the emergence of the Cloud, we wanted to include our contribution through work at the remote administration of the TMA.
Our contribution is summed up in a hardware and software unit for remote physical communication port together through an Ethernet connection (LAN / MAN / WAN / Internet) for playback at a management console (Remote).

Keywords: TV Maintenance, Remote Administration, TMA, Cloud services.

Résumé

Dans un environnement mondial où les concepts économiques influent sur le devenir technologique, tel la délocalisation à inspirer la création des centres de données et ces dernier jumelés avec les concepts de mutualisation et d'externalisation ont fortement contribué à l'émergence du Nuage, nous avons voulu inscrire notre contribution à travers un travail au niveau du volé Administration à distance de la TMA.

Notre contribution se résume en une unité matérielle et logicielle permettant de déporté un ensemble de port de communication physique à travers une connexion Ethernet (LAN/MAN/WAN/internet) pour une restitution au niveau d'une console d'administration (Distante).

Mots Clés : Télé Maintenance, Administration à distance, TMA, services Cloud.