**Les réseaux**

**informatiques**

**Table des matières**

**1. Généralités 7**

LAN, MAN et WAN 7

Internet, extranet et intranet 9

La notion de protocole 9

Le WAN 10

La connectique des LAN 11

La topologie physique des LAN 13

**2. Le cloud computing 15**

L'IaaS, le SaaS et le PaaS 16

Avantages 18

Inconvénients 18

Le problème de la sécurité 19

Quel avenir ? 21

**3. Les réseaux locaux 23**

Caractéristiques 23

La fibre optique 24

Les switches 25

Les routeurs 27

Le paramétrage d'un routeur sans fil 30

**4. Le modèle OSI de l'ISO 33**

Les services de chaque couche 34

Le modèle Internet 35

Protocoles de la couche Application 36

La base commune : TCP-IP 37

ARP 37

BGP-4 38

**5. Les systèmes intermédiaires 39**

Les fonctions des systèmes intermédiaires 39

Les fonctions du répéteur 40

Les fonctions du hub 40

Les fonctions du point d'accès 40

Les fonctions du pont 41

Les fonctions du switch 42

Les fonctions du switch de niveau 3 43

Les fonctions du MLS 44

Les VLAN 45

En résumé 45

Les fonctions du routeur 46

Les fonctions de la passerelle 47

Le routage interne 47

Le STP 47

Les IGP 48

Les EGP 50

**6. L'adressage IP 51**

Adresses IP v4 publiques et privées 52

Les deux parties d'une adresse IP v4 52

Le CIDR 53

Les sous-réseaux IP v4 54

Le subnetting d'un réseau /8 55

Le subnetting d'un réseau /16 55

Le subnetting d'un réseau /24 56

Le VLSM 56

IP v6 56

**7. FTP 59**

Filezilla 60

Le site manager 62

Les problèmes classiques 63

Une ouverture de session 64

Commandes principales 66

FTP et les pare-feu 67

La confidentialité 68

**8. Commandes de réseau 69**

Quand une commande ne passe pas 69 ping 70 traceroute 71 ifconfig 71 host 71 dig 71

netstat 72 finger 72 telnet et ssh 72 ftp 72 net view, net share 73 net use 73 net user, net accounts, net group 73

Automatiser les commandes 73

Une remarque juridique 74

**9. La sécurité du réseau local 77**

L'essentiel en bref 77

La boucle de Boyd 77

Moyens techniques 78

Les types de malware 79

Le pare-feu 80

La DMZ 83

Pour conclure 84

**10. Les réseaux téléinformatiques 87**

La boucle locale 87

Le réseau national et international 88

La vision « contrat » 89

La connexion sur la boucle locale 90

L'essentiel en bref 93

Le sans-fil sur la boucle locale 94

Sans-fil et sécurité 95

**11. L'Internet 97**

L'infrastructure de l'Internet 97

APNIC, ARIN et autres RIR 99

Aspects légaux 100

Le droit à l'image 102

Le droit d'auteur 103

Un droit fondamental 104

**12. Le DNS 109**

L'infrastructure DNS 110

Le DNS sur l'hôte 112

Un exemple de requête DNS 112

BIND 114

**13. Services Internet 115**

Fourniture d'accès 115

Messagerie 115

Hébergement de sites web 116

Synchronisation de données 117

Sauvegarde en ligne 117

IaaS 118

PaaS 118

SaaS 119

**14. Les systèmes Cisco 121**

Le système d'exploitation IOS 121

Les outils de configuration 122

Les modes 122

**15. La sécurité des réseaux 125**

Le social engineering 127

L'infestation 129

Les attaques par messagerie 129

L'injection SQL 131

L'administration de la sécurité du réseau 132

**1. Généralités**

Un **réseau** est un ensemble de plusieurs ordinateurs reliés entre eux par un système de communication permanent.

Si on relie momentanément deux ordinateurs pour, par exemple, copier des données de l’un sur l’autre, on ne peut pas vraiment parler de réseau.

Un réseau a trois caractéristiques fondamentales :

1° les machines fonctionnent comme un tout ;

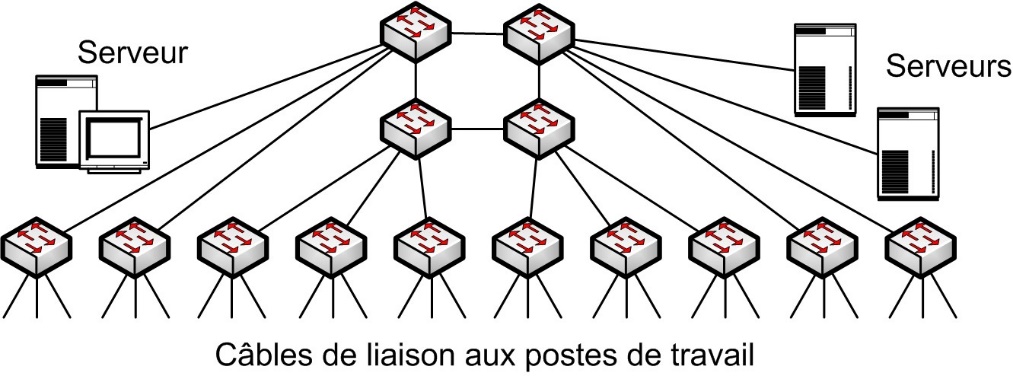
2° cet interfonctionnement est automatique ;

3° il est actif 24 heures sur 24.

Dans la plupart des cas, un réseau réunit des **postes de travail** et des **serveurs**, mais les très petits réseaux ne comprennent parfois que des postes de travail. Il inclut aussi des **imprimantes**. Si elles sont attachées directement à un PC, ce sont des imprimantes locales. Si elles sont dotées d’une électronique de réseau, ce sont des imprimantes de réseau.

Pour communiquer avec le monde extérieur, il faut un **routeur**. Cet équipement permet notamment aux utilisateurs d’envoyer et recevoir des messages électroniques et d’accéder au web.

Les postes de travail, les serveurs, les imprimantes de réseau et les routeurs sont reliés ensemble par des

**commutateurs** ou **switches**. Leur symbole standard est un carré surmonté de quatre flèches opposées deux à deux.

On peut relier des switches entre eux, ce qui permet de faire grandir le réseau. Par exemple, le schéma ci-contre montre une pyramide en trois

é t a g e s c o m p o s é e d e t ro i s

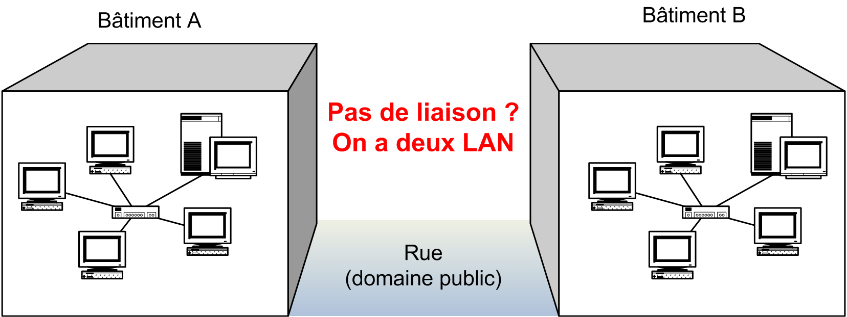
serveurs, quatre switches centraux, dix switches de groupes de travail et un certain nombre de postes de travail. On distribue les tâches comme on veut ; ici, chaque switch central gère soit trois groupes de travail soit deux groupes et un ou deux serveurs.

**LAN, MAN et WAN**

Un **réseau local** ou **LAN** (Local Area Network) s’étend sur un seul site (un ou plusieurs bâtiments, mais un seul terrain). Il ne requiert aucune autorisation de la part des autorités.

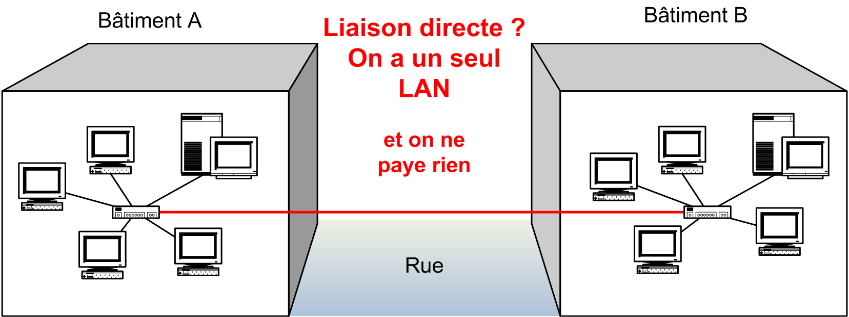
Les réseaux locaux utilisent pour leurs liaisons les normes **Ethernet**. Les débits sont en général **100 Mbps**,

**1 GE** et/ou **10 GE** (Gigabit Ethernet). Il y a en tout une vingtaine de normes Ethernet.

Un LAN peut s’étendre sur des dizaines de kilomètres s’il repose sur des fibres optiques. En théorie, il peut même couvrir des centaines de kilomètres, mais, en pratique, aucune entreprise ne possède de terrain de cette taille.

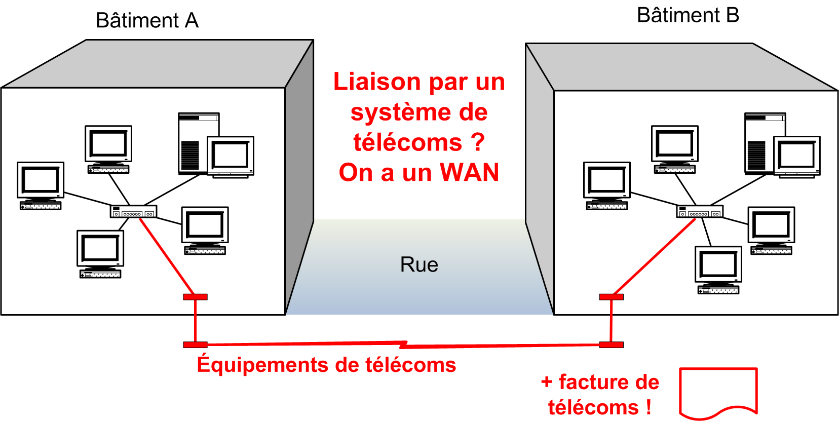
Un **réseau téléinformatique** ou **WAN** (Wide Area Network) s’étend sur plusieurs sites. Les liaisons entre sites passent par le domaine public. Ces liaisons sont assurées par un **opérateur de télécoms** (France Télécoms, Belgacom, Swisscom, etc.).

Les liaisons WAN passent par des **fibres**

**optiques** qui relient les villes entre elles. Physiquement, les câbles se trouvent souvent sous les autoroutes et les lignes de chemin de fer. Ils sont gérés

par les opérateurs de télécoms sous le contrôle de l’État.

Économiquement, ils sont vitaux pour le pays parce que presque toutes les com- munications passent par eux — l'informa- tique, la téléphonie fixe, la téléphonie mobile, etc.

Un **réseau métropolitain** ou **MAN** (Metropolitan Area Network) est un cas particulier de WAN. S’il est filaire, il réunit plusieurs réseaux locaux qui se trouvent dans une même zone géographique de quelques kilomètres carrés (souvent une agglomé-

ration) et qui appartiennent souvent à la même organisation. Par exemple, les diﬀérents sites d’une municipalité peuvent être réunis par un MAN.

Les liaisons entre les sites passent par des fibres optiques. Il s’agit souvent de fibres **Metro Ethernet** prêtes à l’emploi ou de **fibres noires**, c’est-à-dire de fibres sans signal.

Avec la solution Metro Ethernet, les liaisons sont prêtes à l’emploi. On utilise des switches Ethernet normaux, ce qui est pratique : de cette manière, le MAN forme une extension « naturelle » du LAN et sa gestion ne nécessite que des compétences en Ethernet.

Avec les fibres noires, on met en place le système de communication que l’on veut, mais cette solution n’existe que dans certaines villes.

On appelle aussi MAN les réseaux de points d’accès sans fil mis à disposition du public dans beaucoup de villes. Ces MAN municipaux sans fil sont appelés Muni Wi-Fi. Ils ne servent qu’à accéder à l’Internet. Contrairement aux MAN filaires, qui s’adressent généralement aux entreprises, ils sont destinés au public.

**Internet, extranet et intranet**

L’**Internet** est un interréseau, c’est-à-dire un ensemble de réseaux, mais il s’agit d’un système très particulier :

• il se compose de systèmes informatiques totalement indépendants les uns des autres ;

• n’importe qui peut accéder à ces systèmes ;

• il n’y a que deux canaux d’accès : le web (protocole **HTTP**) et la messagerie électronique (protocoles

**SMTP** et **IMAP**).

Un **intranet** est un Internet privé, c’est-à-dire un Internet dont l’accès est réservé aux employés de l’en- treprise concernée.

Les notions de réseau local et d’intranet n’ont rien à voir l’une avec l’autre :

• si les ordinateurs d’un site sont reliés par des câbles ou des ondes et fonctionnent ensemble, c’est un réseau local ;

• si les utilisateurs des ordinateurs d’une organisation ont accès à un site web d'entreprise (un site réservé aux employés de l’entreprise), c’est un intranet.

Un intranet peut couvrir le monde entier. Par exemple, celui de Nestlé, qui est appelé Henri (du nom du fondateur de l'entreprise, Henri Nestlé), relie les 250 000 employés de la firme dans plus de cent pays.

Si un intranet réunit plusieurs entreprises, c’est un **extranet**. L’un des plus grands extranets actuels est ENX (European Network Exchange), qui réunit des fabricants d’automobiles européens et leurs four- nisseurs ([http://www.enxo.com/lang/fr).](http://www.enxo.com/lang/fr))

**La notion de protocole**

Les normes utilisées pour permettre à des ordinateurs de communiquer entre eux s’appellent des **proto- coles**. Ethernet, IP, TCP, HTTP sont des protocoles. Un groupe de protocoles complémentaires forme une **pile de protocoles** (protocol stack).

Il y a vingt ou trente ans, plusieurs piles de protocoles coexistaient, mais, aujourd’hui, tout le monde utilise la **pile TCP-IP**, aussi appelée **protocoles Internet** parce qu’elle a été mise au point pour le réseau Arpanet, l’ancêtre de l’Internet. Dans cette pile, **IP** (Internet Protocol) gère l’adressage des paquets de données et **TCP** (Transmission Control Protocol) s’assure que les messages parviennent bien à leur destinataire.

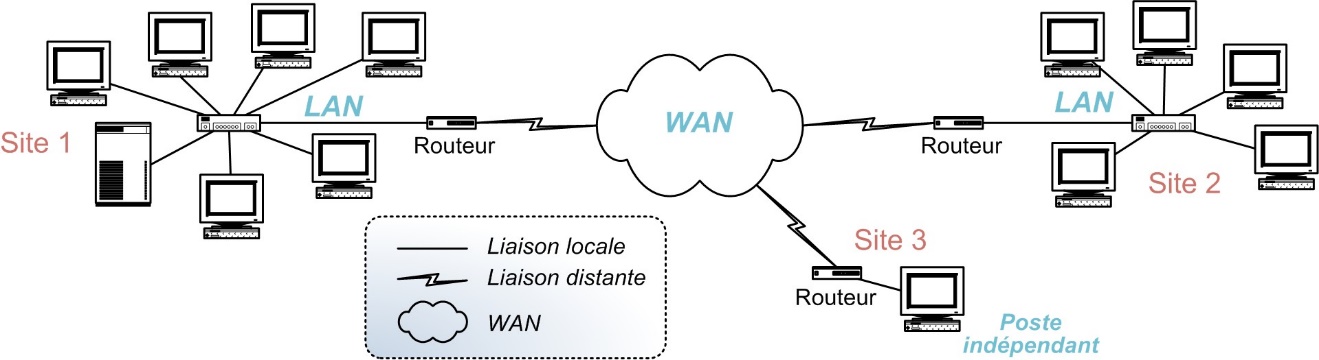
Le fait que les LAN, les MAN et les WAN reposent tous sur le même système de transport des messages est très pratique : on n’a aucun système de passerelle à mettre en place pour permettre les commu- nications entre systèmes informatiques. On est sûr que le message parviendra bien à son destinataire quel qu’il soit et où qu’il soit.

Par contre, l’usage universel de TCP-IP ne garantit pas que le programme destinataire comprendra le message qu’il a reçu. Pour cela, il faut encore que les applications soient compatibles.

**Le WAN**

Contrairement au LAN, le WAN traverse le domaine public, ce qui implique qu’on ne peut pas faire ce que l’on veut : les télécommunications sont une prérogative essentielle de l’État. Cela s'explique par le fait que, en temps de crise, il est essentiel que les communications continuent d'être assurées.

La distance entre les sites peut être courte (la largeur d’une route) ou longue (des continents).



Le nombre de sites connectés varie de deux à plusieurs milliers, voire plus.

Dans chaque site, on place un **routeur** qui sert de porte entre le réseau local et le monde extérieur. C’est lui qui gère les adresses IP.

Le routeur et le switch peuvent être intégrés dans un seul boîtier qui assure les deux fonctions de base :

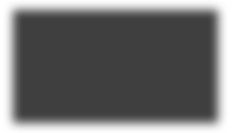
• le **routage**, c’est-à-dire le choix de l’itinéraire vers le destinataire d’un message ;

• la **commutation** (switching), c’est-à-dire la transmission du message à l’ordinateur destinataire (en suivant le

chemin choisi par le routage).

Là où il y a routage, il y a choix entre plusieurs chemins. Le rôle des routeurs est de choisir parmi ces chemins possibles un itinéraire vers un destinataire.

Le switch n’intervient qu’ensuite, une fois que le chemin a été déterminé. C’est lui qui établit la connexion vers l'ordinateur destinataire.

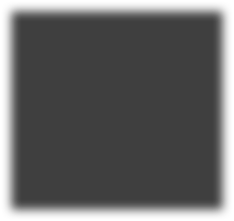


Une organisation peut gérer elle-même son WAN et, dans ce cas, elle ne demande à l’entreprise de télécommunications qu’un service de transport de données. Mais elle peut aussi demander des services supplémentaires comme la gestion de la disponibilité et de la sécurité. Ce type de WAN s’appelle un **VAN** (Value-Added Network).

Les services oﬀerts par les VAN sont notamment la messagerie électronique, le B2B (gestion de liaisons directes entre systèmes informatiques d'entreprises) et la VoIP (voice over IP, téléphonie passant par l'Internet).

Les documents échangés sur les VAN le sont souvent en **XML**, le langage standard de balisage de texte (il sert seulement à décrire et structurer un texte, il n'a rien à voir avec un « vrai » langage, qui permet de générer des traitements).

Par exemple, deux logiciels de comptabilité incompatibles peuvent s'échanger des commandes, des factures, etc., en les transmettant sous forme de documents XML. Voici un exemple très simplifié 1 :



<Facture>

! <NuméroFacture>

! ! 023604

! </NuméroFacture>

! <IntituléFacture>

! ! Appareil de photo

! </IntituléFacture>

! <MontantFacture>

! ! 590,00

! </MontantFacture>

</Facture>

Les balises sont les constructions <NomBalise> … </NomBalise>.

Il suffit que l'application A et l'application B sachent envoyer et recevoir les documents selon cette structure pour qu'elles soient en mesure de s'échanger des factures. Les deux programmes peuvent se trouver sur des systèmes informatiques incompatibles, cela ne pose pas de problèmes puisque les données envoyées et reçues sont dans un format commun.

**La connectique des LAN**

Il existe trois possibilités pour la connectique des réseaux locaux (et d'ailleurs aussi des réseaux non locaux) :

• les **ondes**,

• le câble en **cuivre**,

• la f**ibre optique** (verre).

Les trois possibilités sont conçues pour coexister : on peut utiliser un mélange des trois sur un réseau.

Les deux caractéristiques essentielles de chaque protocole sont le **débit** et la longueur maximale d’un **segment**, c’est-à-dire la distance maximale entre deux équipements. Il s’agit par exemple de la distance entre deux switches ou entre un switch et un poste de travail.

Le débit se calcule en **mégabits par seconde** (Mbps, millions de bits par seconde). Un bit est un 1 ou un

0. Ne pas confondre le bit, abrégé b minuscule, avec le byte, abrégé B majuscule, qui vaut 8 bits. Un débit de 100 Mbps équivaut donc à un débit de 12,5 MBps.

Le tableau ci-dessous donne un aperçu des normes actuelles de réseaux locaux.

1 Cet exemple suppose qu'une facture ne peut contenir qu'un seul produit, ce qui est évidemment faux.

|  |  |  |  |
| --- | --- | --- | --- |
| **Norme** | **Medium** | **Débit** | **Segment** |
| 802.11g | Ondes | 54 Mbps | 38 mètres |
| 802.11n | Ondes | 150 Mbps | 70 mètres |
| 802.11ac | Ondes | 800 Mbps | 35 mètres |
| 802.11ad | Ondes | 6 Gbps | ? |
| Ethernet 100Base-TX | Cuivre | 100 Mbps | 100 mètres |
| Ethernet 100Base-SX | Fibre optique multimode | 100 Mbps | 300 mètres |
| Ethernet 100Base-FX | Fibre optique multi ou monomode | 100 Mbps | 2 kilomètres ou plus |
| Ethernet 100Base-BX | Fibre monomode | 100 Mbps | 40 kilomètres |
| Ethernet 1000Base-CX | Cuivre | 1 Gbps | 25 mètres |
| Ethernet 1000Base-TX | Cuivre | 1 Gbps | 100 mètres |
| Ethernet 1000Base-T | Cuivre | 1 Gbps | 100 mètres |
| Ethernet 1000Base-SX | Fibre multimode | 1 Gbps | 550 mètres |
| Ethernet 1000Base-LX | Fibre multimode | 1 Gbps | 550 mètres |
| Ethernet 1000Base-LX | Fibre monomode | 1 Gbps | 5 kilomètres |
| Ethernet 1000Base-LX10 | Fibre monomode | 1 Gbps | 10 kilomètres |
| Ethernet 1000Base-BX10 | Fibre monomode | 1 Gbps | 10 kilomètres |
| Ethernet 1000Base-EX | Fibre monomode | 1 Gbps | 40 kilomètres |
| Ethernet 1000Base-ZX | Fibre monomode | 1 Gbps | 70 kilomètres |
| SFP+ ou 10GBase-CX1 | Cuivre | 10 Gbps | quelques mètres |
| Ethernet 10GBase-CX4 | Cuivre | 10 Gbps | 15 mètres |
| Ethernet 10GBase-T | Cuivre | 10 Gbps | 100 mètres |
| Ethernet 10GBase-SR | Fibre multimode | 10 Gbps | 400 mètres |
| Ethernet 10GBase-LR | Fibre monomode | 10 Gbps | 10 kilomètres ou plus |
| Ethernet 10GBase-LRM | Fibre multimode | 10 Gbps | 220 mètres |
| Ethernet 10GBase-ER | Fibre monomode | 10 Gbps | 40 kilomètres |
| Ethernet 10GBase-LX4 | Fibre multi ou monomode | 10 Gbps | 10 kilomètres |
| Ethernet 40GBase-CR4 | Cuivre | 40 Gbps | 100 mètres |
| Ethernet 40GBase-SR4 | Fibre multimode | 40 Gbps | 100 mètres |
| Ethernet 40GBase-FR | Fibre monomode | 40 Gbps | 2 kilomètres |
| Ethernet 40GBase-LR4 | Fibre monomode | 40 Gbps | 10 kilomètres |
| Ethernet 100GBase-CR10 | Cuivre | 100 Gbps | 100 mètres |
| Ethernet 100GBase-SR10 | Fibre multimode | 100 Gbps | 100 mètres |
| Ethernet 100GBase-LR4 | Fibre monomode | 100 Gbps | 10 kilomètres |
| Ethernet 100GBase-ER4 | Fibre monomode | 100 Gbps | 40 kilomètres |

Les débits indiqués sont des valeurs maximales impossibles à atteindre. En réalité, on n'atteint grosso modo que 80 % de ces valeurs en filaire et 50 % en sans-fil — pour autant que les ordinateurs connectés

soient capables de suivre le rythme. Dans beaucoup de cas, le 1 GE ne fonctionne qu’à une fraction de sa capacité parce que le goulet d’étranglement n’est pas le réseau, c’est le système d’entrée-sortie des ordinateurs.

Les distances maximales peuvent être allongées en utilisant ce qu’on appelle en franglais des **répéteurs** (en français, des répétiteurs). Leur rôle consiste à régénérer le signal et à éliminer le bruit. C’est grâce à eux que nous parvenons à envoyer des données d’un pays à l’autre et, sous les océans, d’un continent à l’autre. Des câbles intercontinentaux comme Pacrim-East ou Southern Cross connectent Hawaii à l’Aus- tralie en traversant des milliers de kilomètres.

**La topologie physique des LAN**

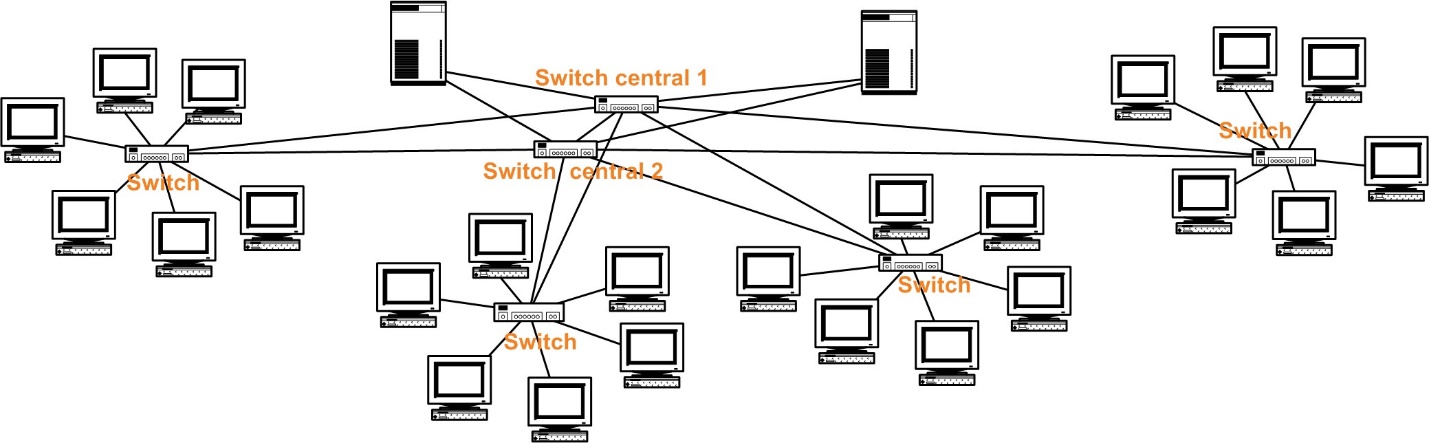
L’architecture physique des réseaux s’appelle la **topologie**.

La solution la plus simple est de s’en passer en utilisant le sans-fil, mais cette méthode convient surtout aux réseaux de petite taille parce que le débit est proportionnel au nombre d’utilisateurs. De plus, le sans- fil nécessite que les échanges soient chiﬀrés pour assurer la sécurité.

En filaire, la topologie employée est l’**étoile** quand il n’y a pas plus de quelques dizaines d’ordinateurs connectés. Les grands fabricants oﬀrent des switches de 8, 12, 16, 32, 48 ou 96 prises, ce qui veut dire qu’on pourrait construire une étoile unique avec près de 100 ordinateurs à connecter, mais il faut penser à la résistance aux pannes et prévoir une réserve (la plupart des réseaux croissent avec le temps).

On préfère donc utiliser plusieurs switches centraux, d’autant plus qu’on peut les faire travailler ensemble comme s’il s’agissait d’un seul grand switch, ce qui est pratique pour l’administrateur du réseau. Financièrement, ce n’est guère plus cher parce qu’un switch de 48 prises coûte presque le double qu’un switch de 24 prises.

Le cœur du réseau s’appelle le **backbone**. Dans le schéma ci-dessous, il est constitué des deux switches centraux :



De cette manière, on construit une étoile simple virtuelle avec un groupe de switches centraux et on garde les avantages essentiels de l’étoile : c’est la solution la plus simple à administrer et celle qui oﬀre le meilleur débit.

Ici, on a aﬀaire à une **double étoile**. C’est une topologie classique parce que le doublement des liaisons oﬀre une bonne sécurité et que les flux des données sont bien modélisés par la forme en étoile puisque la quasi-totalité des échanges se passent entre un serveur et un poste de travail.

Une autre structure de backbone répandue est le carré de quatre switches centraux qu’on a vu au début de ce texte.

On rencontre aussi souvent un backbone formé d'un seul gros switch central qui se présente sous la forme d'un rack. Chaque « tiroir » du rack est un switch, et on peut mélanger sans problème les normes. Par exemple, un switch pourra être en 100GBase-SR10, un deuxième en 10GBase-SR et les autres en 1000Base- SX. Dans ce cas, le backbone est à l'intérieur du rack et on parle de **collapsed backbone** (« partie centrale du réseau sous forme comprimée »).

Dans une grande entreprise, la topologie est souvent à trois étages :

1° des **switches centraux** (core),

2° entourés de **switches départementaux** (distribution),

3° eux-mêmes entourés de **switches de groupes de travail** (edge).

La place des serveurs n’est pas forcément au centre du dispositif. On les relie aux switches centraux s’ils fournissent des services à l’ensemble des utilisateurs, mais, quand ils ne concernent qu’un groupe d’utili- sateurs, il vaut mieux les intégrer au groupe de travail en question.

Par exemple, le meilleur endroit où mettre le serveur qui abrite la comptabilité est le groupe de travail Comptabilité. Non seulement il n’est pas utile aux autres employés, mais son accès leur est au contraire interdit pour des raisons de confidentialité. Cela n’aurait donc aucun sens de le placer à un endroit mieux centré. De plus, placer les serveurs à l’endroit du réseau où ils sont le plus utilisés a pour résultat de minimiser le trafic sur le réseau.

**2. Le cloud computing**

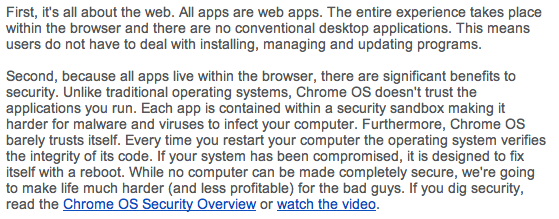
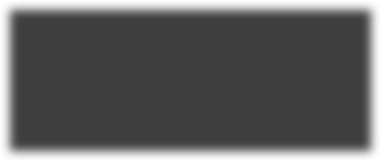
Quand on parle de LAN ou de WAN, on parle de réseaux au sens technique du terme. Sur ces infrastructures, on peut mettre en place des **services** de stockage de données ou d'applications. C'est l'idée du **cloud computing** (« informatique dans les nuages »). Il consiste à utiliser l'Internet pour accéder à des données, des applications ou des services qui se situent quelque part sur l'Internet.

Il a pour but de permettre à l'entreprise d'avoir accès à des services informatiques sans devoir investir dans des infrastructures, de payer des licences et d'engager de nouveaux administrateurs de systèmes. Avec le cloud computing, une entreprise peut se contenter de n'avoir en local qu'un réseau local qui réunit des terminaux — des PC, des Mac, des tablettes,… — et un routeur. Le seul programme installé sur les terminaux est un navigateur. Cet ensemble est le **front-end**.

Tout le reste se trouve sur l'Internet : les serveurs, les applications, le personnel qui administre les systèmes, etc. Cette partie du système est le **back-end**. On n'a rien à gérer, on se contente de payer l'utilisation des ressources partagées du back-end.

Par définition, ce modèle de fonctionnement implique évidemment que tous les programmes utilisés par l'entreprise sont des **web-based applications**, aussi appelées browser-based applications.

En bonne logique, une entreprise qui travaille uniquement avec le cloud devrait avoir des postes de travail minimalistes avec juste un système d'exploitation léger et un navigateur intégré. C'est la raison pour laquelle Chromium OS a été mis au point (<http://googleblog.blogspot.ch/2009/11/releasing-chromium-os->open-source.html).



Le cloud computing n'est pas une nouvelle technique mais une nouvelle manière d'organiser le système informatique. En fait, il s'agit même du retour du plus vieux modèle de traitement : **l'informatique centralisée**, à ceci près que ce n'est plus le WAN de l'entreprise mais l'Internet qui sert de tuyau entre les serveurs et les postes de travail. Les traitements se font sur les serveurs et les postes de travail servent seulement de terminaux (aﬀichage à l'écran et entrée des données au clavier).

Il existe plusieurs catégories de cloud computing :

1° Un **cloud public** est ouvert à tout le monde (soit les entreprises, soit les particuliers, soit les deux).

C'est la forme habituelle de cloud computing.

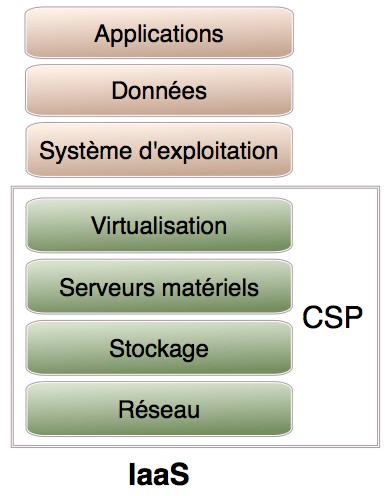
2° Un **cloud communautaire** réunit des clients qui font partie d'un même ensemble, par exemple une association de cabinets d'avocats.

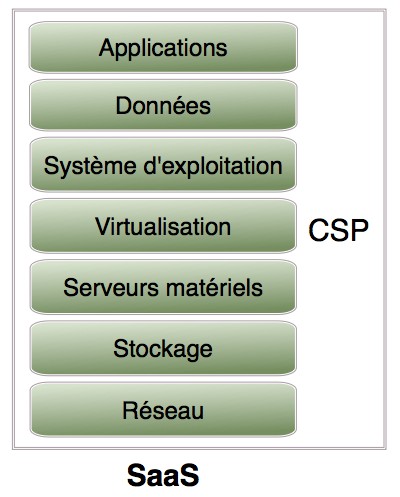
3° Un **cloud privé** est employé par une entreprise unique. C'est donc en fait un WAN d'entreprise qui fonctionne en cloud.

4° Un **cloud hybride** réunit un cloud public et un cloud privé. Le client met ses données sensibles sur le cloud privé et les autres sur le cloud public.

Le cloud computing est en train de devenir une forme de **utility computing** (« informatique vue comme un système de fourniture de services courants »), un service qui va de soi, qui fait partie de la vie courante comme, par exemple, la fourniture de l'électricité ou de l'eau courante.

**L'IaaS, le SaaS et le PaaS**

Le cloud computing existe sous trois formes : le SaaS (software as a service), le PaaS (platform as a service) et l'IaaS (infrastructure as a service). L'entreprise qui fournit des services de cloud computing s'appelle un **CSP** (cloud services provider).

L'**IaaS** consiste pour le CSP à mettre à disposition une infrastructure matérielle formée du réseau, des serveurs matériels et de la virtuali- sation 2 . Sur cette infrastructure,

le client installe ses propres

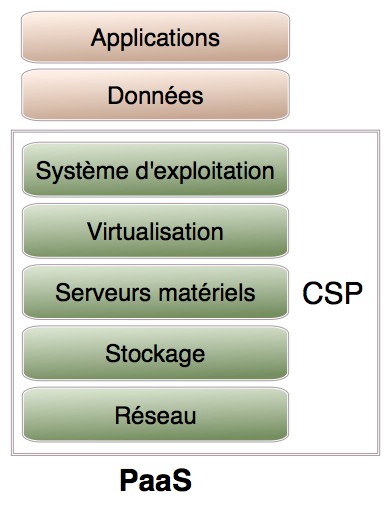
serveurs virtuels, son système d'exploitation et ses applications, et il gère ses données. C'est la forme la plus simple de cloud computing. On l'appelle aussi HaaS (hardware as a service). L'accès passe généralement par des web services (des protocoles spécialisés dans les échanges qui passent par l'Internet).

La plus grande entreprise d'IaaS est AWS (Amazon Web Services), avec probablement 200'000 serveurs environ. On ne sait pas combien

il y en a exactement : un nombre inconnu de ces serveurs sont dissimulés parce que des services gouverne-

mentaux les utilisent. Ils fonctionnent sous Xen, un hyperviseur Linux. Les machines d'AWS abritent environ 15 millions de sites web.

2 La virtualisation de serveurs consiste à installer un système d'exploitation hôte, appelé hyperviseur, qui est capable de gérer des systèmes d'exploitation invités. Ainsi, un seul serveur matériel peut abriter plusieurs serveurs virtuels. VMware ESX est un exemple d'hyperviseur (c'est un dérivé de Linux).

Le **SaaS** consiste pour le CSP à mettre à disposition tout le système informatique, depuis le réseau jusqu'aux applications. Le client n'a rien à gérer lui-même à part son réseau local et ses postes de travail. L'accès aux applications s'eﬀectue au moyen d'un navigateur comme Firefox ou Chrome. Le CSP gère par exemple toute la palette des applications de gestion (comptabilité, gestion de stocks, ressources humaines, etc.) et ces applications sont employées par des milliers d'autres entreprises.

Google Apps for Business est un exemple bien connu de SaaS (http://

[www.google.com/enterprise/apps/business).](http://www.google.com/enterprise/apps/business))

Le **PaaS** consiste à mettre à disposition un système informatique complet, y compris les moyens de réaliser, déployer et gérer des web- based applications. L'accès passe soit par des web services soit par un navigateur.

Heroku (http://www.heroku.com) est un exemple de plate-forme de PaaS. Le système d'exploitation est Linux. Elle a été créée en 2007 et était d'abord compatible avec Ruby seul, mais, actuellement, elle accepte également Java (le langage le plus répandu aujourd'hui), Scala, Node.js et Python. Elle nécessite l'emploi de PostgreSQL comme SGBD (système de gestion de bases de données).

D'autres entreprises oﬀrent des services de PaaS, notamment :

• Openshift, de Red Hat (https://openshift.redhat.com/app). Il est compatible avec PHP, Perl, Java, Node.js, Python et Ruby, mais aussi avec tout programme exécutable capable de fonctionner sur RHEL, le système d'exploitation Linux de Red Hat. Les SGBD possibles sont SQLite, MySQL, PostgreSQL et MongoDB.

• App Engine, de Google (https://developers.google.com/appengine). Il est compatible avec Java et Python.

Pour la base de données, la plate-forme oﬀre un système qui lui est propre, le High Replication Data- store. Le système d'exploitation est Linux.

• Cloud Bees (http://www.cloudbees.com). Cette plate-forme accepte les applications écrites en n'im- porte quel langage fonctionnant sur la JVM (Java Virtual Machine), dont Java, Scala, Rhino ( Javascript), Jython (Python) JRuby (Ruby) et jGo (Go). Le SGBD est MySQL. Le système d'exploitation est Linux.

• Java Cloud Service d'Oracle (https://cloud.oracle.com/mycloud/f ?p=service:java:0). Les applications doivent être réalisées en Java. Le SGBD est Oracle.

Ruby on Rails est un **web framework** très utilisé sur Heroku (un web framework est un logiciel destiné à faciliter la réalisation de web-based applications).

Voici un tableau de quelques langages, frameworks et SGBD très utilisés en cloud computing :

|  |  |  |
| --- | --- | --- |
| **Langages** | **Web frameworks** | **SGBD** |
| Java Python Ruby Scala | Spring ( Java) Twitter Bootstrap Ruby on Rails (Ruby) Django (Python) | PostgreSQL MySQL MariaDB MongoDB |

Un CSP qui oﬀre des services de PaaS ou de SaaS peut lui-même être client d'un CSP qui oﬀre des services d'IaaS. Par exemple, Heroku et Cloud Bees sont hébergés par AWS (Amazon Web Services).

**Avantages**

Le cloud computing permet de se décharger d'une grand partie des soucis de l'informatique : on n'a plus besoin d'avoir un personnel d'administration de systèmes, de faire

des sauvegardes tous les jours, de gérer la redondance (résistance aux pannes), de gérer le datacentre, de prévoir l'évolution du système, etc. (mais il reste nécessaire de faire des sauvegardes hebdomadaires pour éviter qu'un problème avec le CSP ait des conséquences graves).

1° On a accès à une oﬀre étendue d'applications sans avoir à installer et donc gérer quoi que ce soit en local.

2° On n'a pas à s'occuper du système réel (serveurs, systèmes d'ex- ploitation, langages utilisés, etc.), ni des mises à jours.

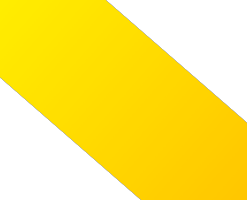
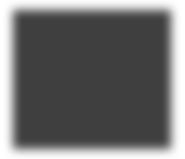
Précautions nécessaires en cloud computing :

− avoir une **copie de sauvegarde**

des données ;

− avoir une **solution de repli** pour le cas où le fournisseur fait défaut ;

− prendre des précautions pour assurer la **confidentialité** des données.



3° Les ressources sont partagées, ce qui permet d'optimiser leur utilisation.

4° Les frais sont partagés. On peut espérer une diminution de 15 à 20% environ du coût de l'infor- matique.

5° Les données et les applications sont disponibles n'importe quand, depuis n'importe quel endroit.

6° Les ressources et les services se payent à l'utilisation (pay as you go). Si un serveur reçoit soudain un grand nombre de requêtes, le système lui accorde aussitôt plus de ressources.

7° Grâce au fait que les clients utilisent un datacentre, l'aptitude à monter en puissance (scalability) est très bonne.

8° Grâce à la virtualisation et au partage du datacentre, l'élasticité est très bonne. Le client peut augmenter ou diminuer rapidement l'utilisation des ressources. Les ressources sont disponibles à la demande.

9° L'espace de stockage à disposition est très grand.

10° Les postes de travail locaux peuvent être simples et bon marché.

11° Le personnel informatique est débarrassé des tâches d'administration des serveurs et peut se consacrer aux tâches directement utiles comme la réalisation d'applications.

**Inconvénients**

Le cloud computing a aussi des inconvénients :

1° On n'a plus le contrôle de la gestion des données et des applications. Selon Steve Wozniak, cofondateur d'Apple : « Avec le cloud, vous ne possédez plus rien. Vous avez déjà signé l'abandon de

vos droits » 3 .

3 S. RICHMOND, « Apple founder warns of 'horrendous' cloud computing risks », The Telegraph, 6 août 2012.

2° Si, par exemple, un changement de version d'un programme cause des problèmes, rien ne dit que le fournisseur des services agira pour résoudre la question.

3° Si c'est une PME, le client est tout petit face au CSP. Par exemple, Google Apps a plusieurs millions de clients, et, chaque mois, ce chiﬀre augmente de plusieurs milliers.

4° Le CSP occupe une position de force, et cela s'aggrave avec le temps : plus on a de données chez lui, plus on en est dépendant.

5° Intégrer des services de cloud oﬀerts par des CSP diﬀérents est souvent diﬀicile. Par exemple, si une en- treprise a sa gestion de salaires chez le CSP A et sa comptabilité chez le CSP B, cela n'ira pas de soi d'inter-

facer les deux applications.

Première loi de l'informatique de Schofield :

« Ne mettez jamais de données dans un programme si vous ne savez pas comment les en sortir ».

6° Il est parfois diﬀicile de changer de CSP à cause des problèmes dea migration des données (voir la

Première loi de l'informatique de Schofield) 4 .

7° Si le CSP met fin au contrat, les conséquences peuvent être graves.

8° Si le CSP est à l'étranger, la législation est diﬀérente. On peut même se retrouver dans l'illégalité (par exemple, la loi sur la protection des données est bien moins restrictive aux États-Unis qu'en Europe).

9° Certaines applications sont mal adaptées au cloud computing, notamment le multimedia.

10° Dans beaucoup de cas, le client ne sait même plus dans quel pays ses données se trouvent. Si un problème se pose, ça ne sera peut-être pas simple de les récupérer.

11° Si on veut se prémunir contre une faillite ou un autre type de désastre, les sauvegardes des données doivent être faites ailleurs que chez le CPS, mais cela pose souvent des problèmes de copie de données (on retrouve la Première loi de l'informatique de Schofield).

**Le problème de la sécurité**

Le cloud computing pose de nombreux problèmes de sécurité, et ils sont potentiellement graves.

1° Les attaques ciblées (spear-phishing) sont facilitées par la logique du cloud, comme l'explique Rick

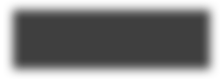
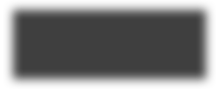
Ferguson, de Trend Micro :

Un des premiers endroits qu'un pirate va visiter est LinkedIn. Que faisons-nous sur ce site ? Nous rendons tout notre CV visible dans le monde entier. Vous pouvez voir toutes les entreprises pour lesquelles j'ai travaillé dans le passé. Vous pouvez voir tout mon réseau, tous les gens avec qui j'ai travaillé,

Deuxième loi de l'informatique de Schofield :

« Les données n'existent pas vraiment tant qu'on n'en a pas deux copies ».

tous ceux que je connais. Ainsi un pirate peut feindre d'être une de ces personnes et faire référence à des choses qui sont arrivées dans ma vie professionnelle. Et j'ai bien plus de chances d'ouvrir une pièce jointe à votre message électronique parce qu'il est beaucoup plus crédible 5 .



2° Le piratage est également facilité par la logique du cloud.

[…] Le journaliste de Wired Mat Honan a vu ses comptes Gmail et Twitter piratés, ce qui n'est pas si rare. Ce qui a rendu l'histoire "épique" est que les pirates ont utilisé son compte iCloud pour

4 Jack SCHOFIELD, Technology Blog, The Guardian., [http://www.guardian.co.uk/technology/askjack.](http://www.guardian.co.uk/technology/askjack)

5 Patrick KINGSLEY, « Danger: hackers at work », The Guardian, 16 juin 2011.

eﬀectuer un "eﬀacement distant" de son iPhone, son iPad et son MacBook, supprimant toutes ses données. Pis que tout, il n'avait pas de sauvegarde 6.

3° Les attaques de type DoS (denial of service) sont facilitées : un flot de requêtes invalides envoyées à un serveur logiciel peuvent avoir pour résultat que le serveur matériel est débordé et ne peut plus traiter les requêtes des utilisateurs dans un délai raisonnable. Si un mécanisme de répartition de la charge existe, les dommages peuvent s'étendre à d'autres serveurs matériels du datacentre. Dans

certains cas, les frais dus à ce pic d'utilisation sont facturés au

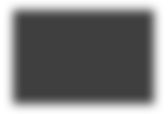
client victime de l'attaque.

4° Le maintien de la confidentialité ne va pas de soi sur certains sites de SaaS. Par exemple, des membres de Facebook se sont plaints en septembre 2012 de voir de vieilles conversations privées apparaître sur leur mur. En réalité, il semble qu'il s'agissait de messages publics, ce qui veut dire que c'est non pas Facebook mais les

membres concernés qui sont responsables du problème :

Troisième loi de l'informatique de Schofield :

« Plus il vous est facile d'accéder à vos données, plus il est facile à quelqu'un d'autre d'accéder à vos données ».



Les messages découverts en catastrophe sur les profils des membres français du réseau social seraient en fait de vieilles conversations publiques tenues entre membres. Ces discussions, longtemps présentées sous une forme discrète, sont ressorties à la surface à la faveur d'un chan- gement d'interface de Facebook 7.

Que la cause de la réapparition de ces messages soit la sottise des utilisateurs et non pas Facebook ne change toutefois pas grand chose au problème, qui est que des messages ou des photos sont vues par des personnes qui ne devraient pas les voir. Cela a même donné naissance à l'expression de « licen- ciements Facebook ». Selon Jean-Marc Manach, du Monde, le problème est lié à la logique des réseaux sociaux :

[…] il n'y a pas de "vie privée" sur Facebook : sur un "réseau social", on mène une "vie sociale", voire une "vie publique" 8.

5° L'espionnage industriel est facilité. Ce problème touche surtout le secteur financier et les industries

(armement, pharmaceutique, chimique, etc.). Selon le New York Times :

[Un rapport de l'université de Toronto] montre que le réseau d'espionnage dirigé contre l'Inde a fait un usage intensif de services Internet comme Twitter, Google Groups, Blogspot, blog.com, Baidu Blogs and Yahoo! Mail pour automatiser la maîtrise des ordinateurs une fois qu'ils ont été infectés 9 .

6° Le fait que les clients se partagent les ressources d'un seul et unique datacentre implique le risque qu'un client puisse attaquer d'autres clients.

7° Les données doivent rester disponibles : il ne faut pas que l'utilisateur se retrouve dans l'impossibilité d'accéder à ses fichiers, par exemple à la suite d'une attaque de type déni de service 10 . C'est arrivé à un certain Nick Saber, dont Google a désactivé le compte, ce qui l'a empêché d'accéder à ses

messages, mais aussi à ses photos (stockées sur Picasa), à Google Docs et à ses fichiers. Schofield :

6 Jack SCHOFIELD, « How to avoid being hacked like Honan », The Guardian, 9 août 2012.

7 Benjamin FERRAN, « Facebook : la Cnil calme le jeu », Blogs, Le Figaro, 26 septembre 2012.

8 Jean-Marc MANACH, « Facebook et le "paradoxe de la vie privée" », Blogs, Le Monde, 25 septembre 2012.

9 John MARKOFF et David BARBOZA, « Researchers Trace Data Theft to Intruders in China », The New York Times, 5 avril 2010.

10 Jenna WORTHAM, Andrew E. KRAMER, « Professor Main Target of Assault on Twitter », The New York Times, 7 août 2009 (une attaque de ce type consiste à bombarder le site cible de requêtes pour provoquer l'engorgement des connexions avec ce site).

[…] si vous avez des données en ligne, vous pouvez perdre l'accès à elles à tout moment, que ce soit à la suite de piratage, d'une lubie sans fondement, d'une simple erreur ou d'un quelconque désastre financier ou même naturel 11 .

À cause de cela, beaucoup d'entreprises interdisent à leurs employés d'utiliser des services comme

Google Docs pour stocker des données sensibles, à moins d'avoir l'autorisation expresse de la direction.

8° Les données sensibles doivent être chiﬀrées. Or il arrive qu'un bug rende impossible le déchiﬀrement, ce qui cause la perte des données.

9° Étant donné qu'un CSP peut avoir des millions de clients, il constitue une cible de choix pour les malfaiteurs, qui sont prêts à investir beaucoup de temps et d'argent pour casser ses défenses.

10° Si un malfaiteur parvient à s'introduire chez un CSP, les clients touchés n'ont aucun moyen de le savoir puisqu'ils ne gèrent pas le système.

11° Si un malfaiteur parvient à s'introduire, le CSP lui-même risque de ne pas s'en apercevoir : les grands clouds ont des millions d'utilisateurs. Trouver un malfaiteur dans cette masse énorme peut se révéler diﬀicile.

12° En cas de faillite du CSP, on peut perdre toutes les données.

Le risque de faillite est très réel : il suﬀit qu'un CSP soit attaqué avec succès par des malfaiteurs pour que sa réputation souﬀre, qu'il perde des clients et qu'il risque de ne pas pouvoir s'en relever.

On entend souvent dire que le cloud computing est plus sûr que l'informatique traditionnelle parce que les CSP font généralement plus attention à leur sécurité que les autres entreprises, mais cela n'empêche pas qu'un problème de sécurité a potentiellement des conséquences beaucoup plus graves s'il se produit chez un CSP que s'il se produit dans un autre type d'entreprise. Ce point a été soulevé en été 2012 avec deux interruptions de service d'AWS (Amazon Web Services) l'une le 14 et l'autre le 29 juin, due à une tempête. Ces ruptures ont montré que le principal datacentre d'AWS n'est pas équipé de deux circuits indépendants d'alimentation électrique avec deux génératrices diesel indépendantes, ce qui montre que les CSP ne font pas toujours plus attention à leur sécurité que les autres entreprises 12 .

Pour les données importantes, le CSP doit oﬀrir des mécanismes de sécurité dans toutes les situations :

• les données transmises ;

• les données stockées ;

• les données en cours d'utilisation dans les applications ;

• les données supprimées.

**Quel avenir ?**

Avec le cloud computing, les clients ne possèdent pas l'infrastructure mais se contentent de louer des ressources et des services. Ce nouveau modèle informatique réduit les coûts et délivre les entreprises d'une bonne partie des tracas de l'informatique. On peut donc s'attendre à son essor. La majorité des PME

pourraient bien travailler de cette manière dans quelques années.

11 Jack SCHOFIELD, « When Google owns you… your data is in the cloud », The Guardian, 6 août 2008.

12 On peut vérifier si et quand une rupture de service a eu lieu chez un fournisseur en recherchant sur Google l'expression formée du nom du fournisseur et du mot outage (exemple : amazon cloud outage).

Pour l'instant, il y des freins, en particulier le prix des télécommunications, les obstacles à l'interfonction- nement (problèmes de migration des données et d'interfaçage des applications) et la sécurité, mais ces freins devraient perdre de leur importance ces prochaines années :

• Les États vont probablement agir pour abaisser le prix des télécommunications car des télécommuni- cations bon marché soutiennent la croissance économique.

• En SaaS, le problème de l'interfonctionnement peut être résolu en ayant tout l'applicatif chez un seul fournisseur.

• En IaaS et en PaaS, le problème de l'interfonctionnement peut être résolu en réalisant des applications qui sont toutes du même type, par exemple des applications Ruby on Rails sur le SGBD PostgreSQL.

• Avec les connaissances actuelles, on est capable de construire une bonne infrastructure de sécurité. Par exemple, les interruptions de service d'AWS auraient été évitées s'ils avaient prévu un système de fail- over (reprise automatique sur incident par un système de secours).

Toutefois, le cloud computing n'est pas pour les entreprises qui ont besoin d'un haut niveau de sécurité (secteur bancaire, industries de pointe, etc.) car les grandes puissances ont des moyens importants en matière d'espionnage électronique.

Dans le cas des États-Unis, ces moyens sont légaux (PATRIOT Act) 13 . Les États-Unis ont un service, le Signals Intelligence Directorate, qui se consacre à cette tâche et qui compte plusieurs milliers de collaborateurs. Son travail est facilité par le fait que la plupart des fournisseurs de services de cloud sont basés aux États-Unis.

Cela a conduit les gouvernements européens à réagir. Ainsi, en France, l'entreprise d'armement Thales s'est alliée en 2012 à la Caisse des dépôts et à Orange pour créer un CSP appelé Cloudwatt, et un cloud concurrent, Numergy, a été lancé par Bull et SFR. Les deux projets sont soutenus par l'État français 14 .

Cette réponse au problème est toutefois très fragile sachant qu'il suﬀit pour casser la sécurité du réseau que l'ordinateur d'un employé soit infecté par un logiciel espion comme Flame 15 .

Quant au chiﬀrement des données, il ne constitue pas non plus une garantie sûre car l'existence d'une porte dérobée est toujours possible.

13 Laura POITRAS, « The Program », The New York Times, 22 août 2012 ; « Le Patriot Act, dix ans d'incertitude », http://

[www.ovh.com/fr/all/a574.le\_patriot\_act\_dix\_ans\_dincertitude,](http://www.ovh.com/fr/all/a574.le_patriot_act_dix_ans_dincertitude) OVH, 18 novembre 2011.

14 « Thales lance Cloudwatt avec Orange », Le Figaro, 6 septembre 2012.

15 Skywiper Analysis Team, « sKyWIper (a.k.a. Flame a.k.a. Flamer) : A complex malware for targeted attacks », http:// [www.crysys.hu/skywiper/skywiper.pdf,](http://www.crysys.hu/skywiper/skywiper.pdf) Laboratory of Cryptography and System Security, University of Technology and Economics, Budapest, 31 mai 2012.

**3. Les réseaux locaux**

Un **réseau local** ou **LAN** (Local Area Network) est un réseau qui s’étend sur **un seul site**. Il peut être limité à une seule pièce ou réunir tout un groupe de bâtiments, mais il doit occuper un seul terrain.

Il relie au minimum deux postes de travail, et il n’y a pas vraiment de limite supérieure. Les plus grands

LAN réunissent des dizaines de milliers de machines. Il comprend généralement un ou plusieurs serveurs.

Un serveur est un ordinateur dont la fonction consiste à mettre des ressources à disposition des utili- sateurs. Quelques exemples :

• serveur de bases de données (PostgreSQL, MySQ, Oracle, DB2, etc.) ;

• serveur de fichiers, souvent pour le stockage de fichiers de bureautique ;

• serveur de messagerie ;

• serveur HTTP, aussi appelé serveur web ;

• serveur d’application.

Un réseau peut rassembler des postes de travail et des serveurs de plusieurs types (Windows, Mac OS, Linux, Solaris, etc.). Tous les mélanges sont possibles.

**Caractéristiques**

Un LAN présente les caractéristiques suivantes :

• Pour connecter les éléments matériels du réseau entre eux, on utilise soit un **câblage**, soit un système

**sans fil**, soit un mélange des deux. Les deux techniques coexistent sans problème.

• La norme utilisée sur les réseaux sans fil est presque toujours **Wi-Fi** (**IEEE 802.11**) . Le débit maximal peut atteindre des centaines de Mbps (mégabits par seconde), mais, dans le meilleur des cas, le débit réel est environ deux fois plus faible que le débit nominal. La bande passante est partagée, ce qui veut dire qu’un réseau sans fil qui réunit douze machines ira grosso modo trois fois plus lentement qu’un réseau qui en compte quatre. Un **WAP** (wireless access point) relie les nœuds entre eux. Tous les échanges passent par lui.

• Un WAP peut typiquement gérer jusqu’à vingt ou trente postes de travail dans un rayon de quelques dizaines de mètres, pour autant qu’il n’y ait pas d’obstacles. Un simple mur peut être infranchissable, notamment s’il est en béton armé.

• Sauf exception, la norme des réseaux filaires (câblés) est **Ethernet** (**IEEE 802.3**).

• Le débit est généralement de 100 ou 1’000 Mbps. Dans les LAN à fort trafic, les switches centraux sont souvent en 10 Gbps.

• Il existe une vingtaine de normes Ethernet. Certaines utilisent un câble en **cuivre** et d’autres la **fibre optique**.

• S’il ne compte pas plus de quelques dizaines de postes, un LAN filaire se présente sous la forme d’une **étoile**. S’il est plus grand que cela, il se présente sous la forme d’un **ensemble d’étoiles**. La partie centrale est le **backbone**.

• Au centre de chaque étoile, il y a un **commutateur** ou switch. C’est un boîtier à prises multiples qui centralise les connexions entre les éléments du réseau et pilote le trafic.

• Les serveurs, les postes de travail, les serveurs, les imprimantes en réseau, les routeurs sont au bout des branches.

• Pour qu’ils puissent communiquer avec le monde extérieur, les LAN comprennent un **routeur**. Quand on envoie un message, c’est au routeur du réseau du destinataire qu’on l’envoie — la seule adresse d’un réseau visible de l’extérieur est celle de son routeur.

• Certains des éléments matériels d’un réseau n’ont pas d’**adresse**, ce qui les rend invisibles, mais la plupart en ont une. Dans ce cas, on les appelle des **nœuds**. Un poste de travail, un serveur, une impri- mante de réseau, un routeur sont des exemples de nœuds.

• Le système d’adressage que tout le monde utilise aujourd’hui est **IP**. Ce protocole fournit un service d’adressage où chaque adresse est unique au monde, ce qui permet de faire voyager un message de routeur en routeur depuis l’expéditeur jusqu’au destinataire d’un paquet de données. **TCP** complète IP en fournissant un service de connexion. Il s’assure que le programme destinataire reçoit bien tous les paquets de données envoyés par l’expéditeur.

• Ensemble, TCP et IP suﬀisent pour relier deux ordinateurs de manière fiable.

La plupart des systèmes d’exploitation incluent TCP-IP et l’activent par défaut. On n’a donc rien à faire de particulier pour le mettre en place, cela se fait tout seul.

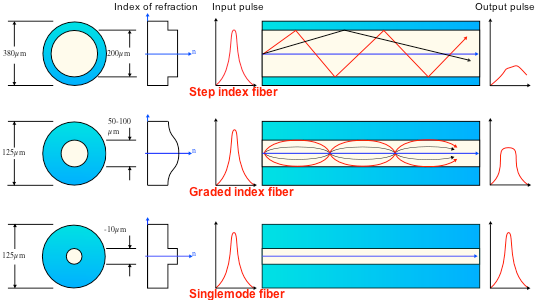
Dans beaucoup d’endroits publics (places, cafés, gares, aéroports, etc.), on trouve des hot spots, des WAP mis à disposition du public, le plus souvent gratuitement. À ces endroits, toute personne ayant un ordinateur portatif doté d’une interface 802.11 peut se connecter à l’Internet.

**La fibre optique**

En simplifiant, la fibre optique se comporte comme un tuyau dont la surface intérieure serait un miroir. Quand un signal voyage dans ce tube, il finit par toucher la paroi interne, mais celle-ci le réfléchit et le renvoie vers le cœur.

Une fibre peut être **multimode** (MMF, multimode fibre) ou **monomode** (SMF, monomode fibre). Dans le second cas, le cœur est beaucoup plus fin, ce qui permet de transporter le signal plus loin. Avec les meilleures fibres, le signal peut traverser des centaines de kilomètres, voire plus, avant d’être illisible.

Le schéma ci-dessous montre comment les signaux sont transmis dans une MMF à saut d’indice (step index), dans une MMF à gradient d’indice (graded index) et dans une SMF 16 :



La fibre est préférable au cuivre parce qu’elle est insensible au bruit électromagnétique (aux interférences), qu’elle transporte le signal sur une distance bien plus grande et qu’elle est légère, ce qui simplifie la mise en place du câblage.

Par contre, la fibre est plus compliquée à installer. Le plus infime décalage dans une prise est interdit : le tube de lumière d’une SMF mesure environ un centième de millimètre de diamètre.

**Les switches**

Les switches comprennent généralement 8, 12, 16, 24, 32, 48 ou 96 **ports** (prises de réseau).

Ci-dessous, voici la face avant d’un switch Ethernet 10/100BaseT à 24 ports en deux rangées de 12. Les deux « ailes » permettent de fixer le switch à un rack.



Les switches d’entrée de gamme ne sont pas configurables et n’ont pas d’adresse. En revanche, ceux qui sont configurables ont toujours une adresse.

Les switches sont souvent conçus pour être placés dans un rack ou pour être empilés (stack). Ils forment alors un ensemble intégré et s’administrent comme une seule entité. Par exemple, quatre switches empilés

de 24 ports se gèrent comme s’il s’agissait d’un seul switch de 96 ports.

16 MRZEON, Wikipedia, [http://en.wikipedia.org/wiki/File:Optical\_fiber\_types.svg,](http://en.wikipedia.org/wiki/File%3AOptical_fiber_types.svg) 21 septembre 2007.

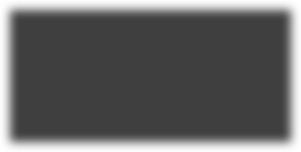
On peut faire coexister des normes inhabituelles de réseaux comme FDDI, ATM, Token Ring, etc., avec les normes Ethernet et Wi-Fi. Par cela, on peut utiliser des switches multinorme (qui comprennent par exemple des prises Ethernet et des prises FDDI).

Aujourd’hui, les communications s’eﬀectuent en **full-duplex**, ce qui veut dire qu’on peut avoir un signal sortant et un signal entrant en même temps.

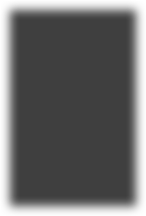
En revanche, le 10BaseT est généralement en **semi-duplex**. L’émission et la réception ne peuvent pas avoir lieu en même temps.

Avant l'avènement des switches, une **collision** se produisait si deux interlocuteurs commençaient en même temps à se parler (comme quand, dans un groupe, deux personnes se mettent à parler au même moment). Pour gérer ce problème, les normes Ethernet détectent les collisions et mettent chaque expéditeur en attente un instant variable. Le premier qui arrive au terme de son temps d’attente vérifie que le câble est silencieux et émet à nouveau le paquet de données.

Voici une pile de trois switches à 24 ports. Les LED (Light Emitting Diodes) qui se trouvent dans la partie gauche indiquent les ports actifs.



L’image ci-contre montre un détail des branchements. On voit bien les deux LED de part et d’autre de chaque prise. L’une est pour le canal d’émission (Tx, transmit) et l’autre



pour le canal de réception (Rx, receive).

De manière générale, les LED peuvent indiquer les statuts suivants :

• hors ligne ;

• inactif (prêt) ;

• actif (en cours de transmission) ;

• en panne.

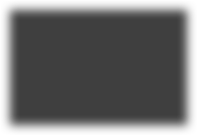
On peut configurer les switches en auto-négociation, ce qui veut dire qu’ils se contactent les uns les autres pour savoir quel débit maximal est possible et si c’est en semi-duplex ou en full-duplex. Pour que cela fontionnne, il faut que l’auto-négociation soit activée sur tous les switches — un protocole ne peut fonctionner que si les deux interlocuteurs l’utilisent.

Une erreur se produit assez souvent : si l’administrateur a configuré certains

switches en full-duplex et d’autres en auto-négociation, le résultat sera que le premier va travailler en full-

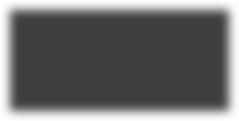
duplex et le second en semi-duplex. Cela va donner lieu à un grand nombre de collisions de paquets et les échanges seront anormalement lents. Si cela arrive, il faut vérifier que tous les switches sont bien configurés de manière identique.

L’image ci-contre montre des connecteurs optiques de type LC (Lucent Connector). Ils sont très répandus.



Par souci de standardisation, il vaut évidemment mieux utiliser un seul type de connecteur pour chaque type de fibre dans l’ensemble de l’organisation.

Les switches s’administrent depuis un poste de travail normal a u m o y e n d’une **con-**

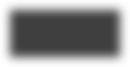


**nexion Console**. Il faut un câble spécial (photo ci- contre). Sur le switch, on le connecte à la prise appelée Console. Sur le poste de travail, on emploie soit une prise sérielle, soit une prise USB.

La prise sérielle DE-9 est très importante dans le monde des réseaux. C’est une prise mâle à 9 contacts

souvent symbolisée par le signe 010 ou 10101 (photo ci-dessous). On l’utilise pour administrer les

équipements de réseaux (switches, routeurs, pare-feu, etc.). Malheureusement, beaucoup de cartes-mères ne comprennent plus de prise DE-9. Dans ce cas, on peut installer une carte d’extension ou acheter un adaptateur de type Serial to USB.

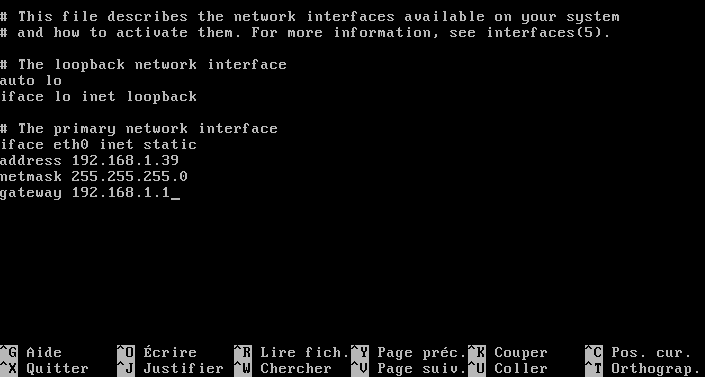
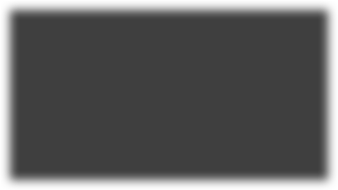


À l’exception des modèles d’entrée de gamme, les switches contiennent un

véritable système d’exploitation avec lequel on dialogue au moyen d’une émulation de terminal. Avec Windows, on peut utiliser HyperTerminal, et, avec Linux ou Mac OS, Minicom (<http://alioth.debian.org/>projects/minicom).

**Les routeurs**

Les routeurs gèrent les paquets de données qui entrent et sortent du réseau local. Vu de l’extérieur, un réseau local a une seule adresse, celle du routeur, et il en va de même dans l’autre sens : tout paquet sortant est envoyé au routeur.



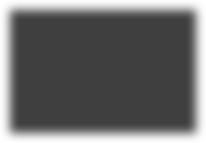
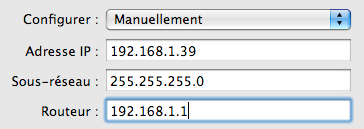
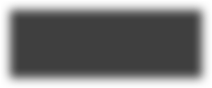
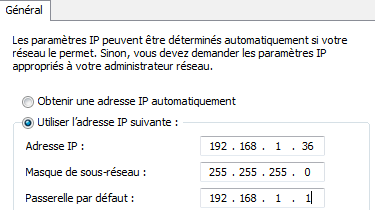
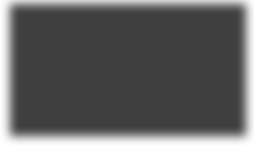
L’adresse du routeur se gère dans le système d’exploitation des ordinateurs du LAN.

Sous Linux, on la trouve dans le fichier de configuration du réseau. Dans le cas de Debian et Ubuntu, c’est la ligne gateway x dans le fichier /etc/network/interfaces. On y accède par exemple en tapant nano /etc/ network/interfaces (image ci-contre).

Sous Windows, le chemin est le suivant : Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Modifier les paramètres de la carte → Connexion au réseau local, clic droit, Propriétés → Protocole Internet version 4 → Propriétés. Le routeur s’appelle Passerelle par défaut (voir l’image ci-dessous à gauche).

Sous Mac OS, le chemin est Préférences système →Réseau et le routeur s’appelle Routeur (ci-dessous à droite).

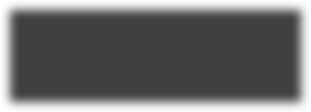
On a deux possibilités : indiquer manuellement l’adresse à utiliser ou laisser le système gérer automati- quement l’adressage. C’est le travail du serveur **DHCP** (Dynamic Host Configuration Protocol), un logiciel qui se trouve sur le routeur ou sur un serveur. Sous Windows,



on active le service DHCP en cochant Obtenir une adresse IP automatiquement. Sous Mac OS, c’est Configurer via DHCP. Sous Debian et ses dérivés, ce sont les lignes auto eth0 et iface eth0 inet dhcp dans le fichier /etc/network/interfaces.

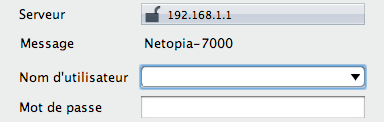
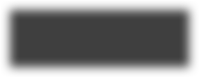
Voici ci-contre un équipement à triple fonction : c’est un routeur VDSL (Very high bit rate DSL), un switch et un WAP. Ce genre d’appareil peut atteindre 100 Mbps. Il est destiné aux privés et aux petits sites d'entreprises.

Le Cisco 1700 de la photo ci-dessous est un exemple de routeur pour une entreprise de quelques dizaines de salariés.



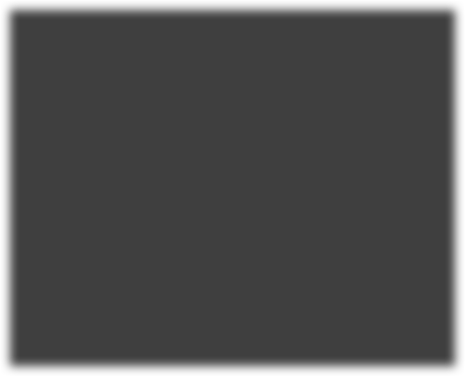
Les routeurs destinés aux privés sont dotés d’un serveur HTTP qui permet de les administrer depuis un navigateur. On tape leur adresse IP — par exemple 192.168.1.1 — dans la barre d’adresse et la fenêtre de connexion s’aﬀiche (image page suivante).

Les autres routeurs s’administrent comme les switches : ils contiennent un système d’exploitation avec lequel on dialogue au moyen d’un programme comme HyperTerminal ou Minicom. Physiquement, on passe également par une liaison Console.



Sur les nœuds de communication des réseaux nationaux, on

utilise des équipements beaucoup plus lourds, par exemple les routeurs Cisco de la série 7600 17 :



Les fonctions de routage sont assurées par un logiciel. Il est donc possible d’utiliser un ordinateur normal comme routeur. Les entreprises qui agissent ainsi utilisent généralement une machine Linux ou BSD dotée de programmes open source de routage et de pare-feu. Il existe une trentaine de distributions Linux

conçues expressément pour cela.

17 VISVIVA, Wikimedia, [http://commons.wikimedia.org/wiki/File:Cisco7600seriesrouter.jpg,](http://commons.wikimedia.org/wiki/File%3ACisco7600seriesrouter.jpg) 10 mars 2008.

**Le paramétrage d'un routeur sans fil**

Le paramétrage d'une liaison sans fil est plus compliqué que celui d'une liaison filaire. Voici une liste des champs à remplir. Certains sont obligatoires (le nom du réseau et la clé de chiﬀrement) et les autres sont généralement facultatifs (auquel cas ils sont découverts automatiquement par le logiciel de paramétrage).

**Nom** Nom du réseau.

**SSID** Synonyme de nom du réseau.

**ESSID** Synonyme de nom du réseau.

**Adresse** Adresse MAC ou adresse IP (cela dépend du contexte). Il s'agit soit de celle de la machine sur laquelle on est, soit de celle du routeur (cela dépend aussi du contexte).

**Adresse physique** Adresse MAC. Il s'agit soit de celle de la machine sur laquelle on est, soit de celle du routeur (cela dépend du contexte).

**BSSID** Adresse MAC du routeur.

En général, on ne doit indiquer manuellement la BSSID que si le routeur a été paramétré pour masquer sa SSID.

**CM MAC** Synonyme de BSSID lorsqu'il s'agit d'un routeur relié au câble de la télévision et non d'un routeur Ethernet.

**RF MAC** Synonyme de CM MAC. **CABLE** Synonyme de CM MAC. **CMAC** Synonyme de CM MAC. **HFC MAC** Synonyme de CM MAC. **WEP** Clé de chiﬀrement WEP.

**WPA** / **WPA2** Clé de chiﬀrement WPA / WPA2.

**MTU** Taille maximale autorisée des paquets (MTU signifie maximum transmission unit).

Ce paramètre est généralement optionnel. Sinon, choisir 1500.

Remarque : SSID signifie service set identification (identification de l'ensemble de services), ESSID extended service set identification et BSSID basic service set identification.

**Comment trouver le nom du réseau (la SSID) ?**

Quand on scanne l'environnement pour voir quels réseaux sans fils sont accessibles, les SSID sont les noms qui s'aﬀfichent dans la liste des réseaux.

Cette liste s'aﬀiche si on clique sur l'icône Réseaux. Sous Windows, cette icône se trouve dans la zone de notification au coin en bas à droite de l'écran. Sous Mac OS, elle est au coin en haut à droite de l'écran.

Sous Linux, cela dépend de l'interface graphique utilisée, mais l'icône se trouve généralement soit au coin en bas à droite, soit au coin en haut à droite de l'écran. On peut utiliser la commande

netsh wlan show network

On trouve souvent aussi la SSID sur une étiquette collée sous le routeur.

Sous Mac OS, il existe airport, un programme de service qui permet de gérer les réseaux sans fil, mais il se trouve à un endroit très peu pratique :

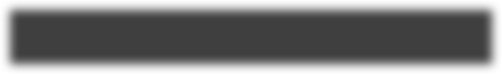
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources

Une solution consiste à créer un lien symbolique (une sorte de raccourci) à un endroit où airport aurait pu être mis plus utilement, par exemple /usr/sbin. Pour cela, taper la commande suivante sur une seule ligne en respectant bien les espaces :

sudo ln -s /System/Library/PrivateFrameworks/Apple80211.framework/Versions

/Current/Resources/airport /usr/sbin/airport

Il n'y a pas d'espace entre Versions et /Current/Resources/airport (voir ci-dessous).



Ensuite, on tape :

airport -s

pour lancer le programme.

Le répertoire 18 où se trouve airport ne fait pas partie de ceux que le système d'exploitation parcourt quand on lui demande de lancer un programme. Cela explique qu'il faut créer un lien dans l'un de ces répertoires, dont /usr/bin fait partie (on dit qu'il est « dans le path ») 19 .

Sous Linux, les programmes iwconfig et iwspy ont en gros la même fonction qu'airport. Sous Windows, c'est netsh. La commande :

netsh wlan ?

aﬀiche la liste des commandes possibles. La commande :

netsh wlan show networks mode=bssid

aﬀiche les réseaux sans fil disponibles. La commande :

netsh wlan reportissues

consigne les événements relatifs à la connexion sans fil dans le répertoire C:\Windows\tracing\wireless.

18 Apple appelle les répertoires « dossiers », mais le terme correct est répertoire.

19 Pour aﬀicher la liste des répertoires que le système d'exploitation parcourt quand on lui demande de lancer un programme, taper la commande echo $PATH sous Unix ou Linux et la commande path tout court sous Windows.

**Comment trouver l'adresse MAC de l'ordinateur ?**

Sous Windows, pour connaître l'adresse MAC de l'ordinateur sur lequel on est, on tape la commande :

ipconfig /all

Sous Unix et Linux, on tape :

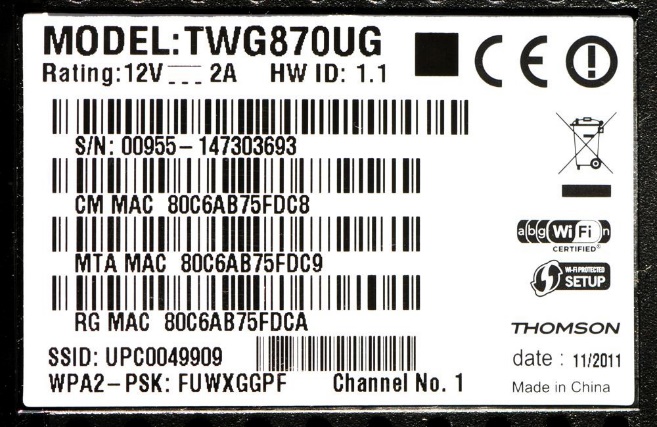
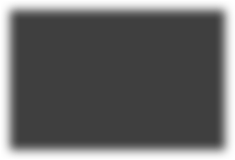
ifconfig -a

La ligne intitulée ethernet, mac ou physical address indique l'adresse MAC sous la forme de douze chiﬀres en base 16. Ils sont généralement groupés par deux. Exemple : D4:A9:20:1D:08:FD.

**Comment trouver l'adresse MAC du routeur (la BSSID) ?**

En règle générale, on trouve la BSSID sur une étiquette collée sous le routeur ou dans la docu-mentation technique que le fournisseur d'accès a envoyé avec le routeur.

L'image ci-contre montre une étiquette de routeur.



Le S/N (serial number) est le numéro de série du routeur. La BSSID est appelée CM MAC (cable modem medium

access control address). Il s'agit de 80:C6:AB:75:FD:C8 (les lettres sont en réalité des chiﬀres ; c'est un nombre en base 16).

La MTA MAC (multimedia terminal adapter medium access control address) concerne la VoIP (voice over IP), la téléphonie qui passe par le réseau informatique plutôt que par le réseau téléphonique.

En général, la RG MAC (residential gateway medium access control address) est sans importance (le cas échéant, la documentation technique spécifie ce qu'il faut en faire).

La SSID est le nom du réseau.

La WPA2–PSK (wi-fi protected access pre-shared key) est la clé de chiﬀrement. Elle est sensible à la casse

(les majuscules et les minuscules sont des lettres diﬀérentes).

On peut aussi trouver la BSSID au moyen de l'interface de commande. Sous Windows et Unix (mais pas

Linux), on tape la commande

arp -a

Sous Linux, on se connecte en mode administrateur et on tape la commande

iwlist scanning

Sous Mac OS et les distributions de la famille Debian (Debian, Ubuntu, Mint, Mepis, Damn Small Linux, etc.), le mode administrateur est activé par le préfixe sudo. On tape la commande

sudo iwlist scanning

Sudo (superuser do) signifie « je tape cette commande en tant qu'administrateur ».

**4. Le modèle OSI de l'ISO**

Le modèle OSI (Open Systems Interconnection) a été créé par l’ISO (International Organization for Standardization) il y a une trentaine d'années. Il fait l’objet d'une norme qui s'appelle 7498-1:1994 à l'ISO et X.200 à l'ITU (International Telecommunication Union).

C’est uniquement une **référence**, un texte abstrait destiné à fournir un cadre conceptuel pour les ingénieurs en télécoms et les informaticiens qui travaillent dans les réseaux.

Autrement dit, ce n’est pas un standard de communications, c’est seulement un moyen de mieux se comprendre.

Il définit sept couches. Chacune correspond à une famille de fonctions de communication :

**7. Application** (application layer) interface avec les programmes locaux (système d’exploitation, utilitaires et applications).

**6. Présentation** (presentation) transformations des données.

**5. Session** (session) gestion du dialogue dans le temps (ouverture du dialogue, déroulement, fin).

**4. Transport** (transport) gestion du dialogue dans l’espace, vérification que le programme destinataire reçoit bien les données envoyées par le programme expéditeur.

**3. Réseau** (network) gestion de l’adressage et du choix du chemin (routing).

**2. Liaison** (data link) type de réseau.

**1. Physique** (physical) définition des caractéristiques réelles de la transmission (type de prise, type de câble, voltage, etc.).

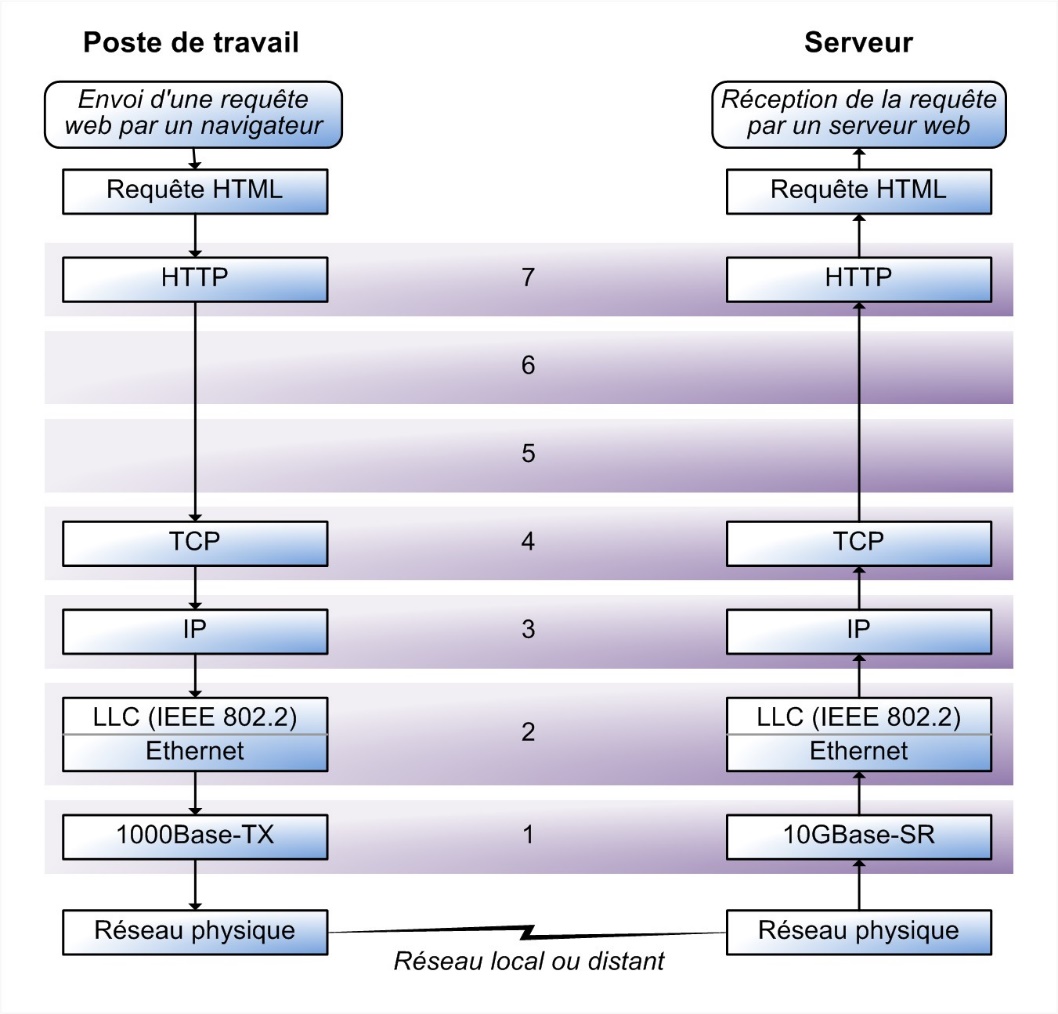
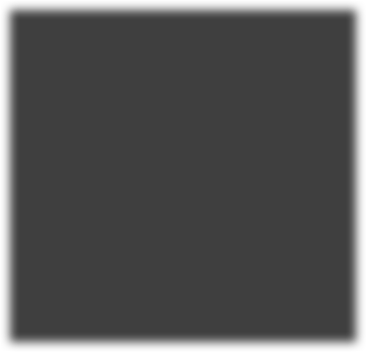
Le nom de la couche Physique est trompeur dans la mesure où il ne s’agit pas de la couche physique (matériel de réseau), mais de la couche qui décrit la couche physique. Les équipements et les câbles se situent en dehors du modèle OSI.

Le même problème se pose avec la couche Application, qui ne concerne pas les applications, mais les inter- faces avec les applications.

On appelle parfois couche « 8 » la couche qui contient les programmes locaux et couche « 0 » celle du réseau physique.

Un paquet de données transféré par un programme expéditeur à un programme destinataire passe (méta- phoriquement) par ces couches. Au départ, il traverse les couches 7 à 1 de l’ordinateur expéditeur, et, à l’arrivée, il traverse les couches 1 à 7 de l’ordinateur destinataire. Quand il passe par un système intermé- diaire, il monte jusqu’en haut des fonctions de ce système, est traité, puis redescend jusqu’en bas.

Voici un exemple avec le trajet d'une requête web :



La distance entre le poste de travail et le serveur du schéma ci-dessus peut être aussi bien de 2 mètres que de 20'000 kilomètres.

Une unité de données porte des noms diﬀérents selon la couche OSI concernée :

• au niveau 1, c'est une **suite de bits**,

• au niveau 2 une **trame** (frame),

• au niveau 3 un **paquet** (packet),

• au niveau 4 un **segment**,

• au-dessus, ce sont des **données** (data).

**Les services de chaque couche**

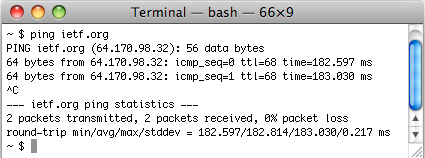
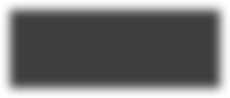
Dans le modèle OSI, la couche 5 est à peine utilisée et la 6 ne comprend généralement que MIME, le protocole de messagerie électronique qui permet de transmettre tous types de messages.

Sans MIME, on ne pourrait échanger que des messages ASCII, sans caractères accentués.

|  |  |  |
| --- | --- | --- |
| **Couche** | **Principaux services** | **Protocoles** |
| **7. Application** | Messagerie électronique, web, transfert de fichiers, accès à distance, systèmes de fichiers distribués, téléphonie sur IP, émulation de terminal, etc. | HTTP, SMTP, POP3, FTP, telnet, NFS, VoIP, BitTorrent, DNS, DHCP |
| **6. Présentation** | Format des données, chiﬀrement | MIME |
| **5. Session** | Gestion du dialogue entre les applications |  |
| **4. Transport** | Contrôle que les données parviennent bien à leur destinataire | TCP, UDP |
| **3. Réseau** | Adressage et gestion de l’itinéraire suivi par les données | IP, IPsec, ICMP, BGP |
| **2. Liaison** | Sous-couche LLC : gestion du déplacement des données (LLC  signifie Logical Link Control)  Sous-couche MAC : gestion de l’accès des données au réseau physique (MAC signifie Media Access Control) | 802.3 (Ethernet), 802.11 (Wi-Fi) |
| **1. Physique** | Définition du matériel : cuivre, fibre ou sans-fil, débit, nombre de fils, fonction de chaque fil, forme des prises, etc. | 1000Base-T et autres normes Ethernet phy- siques, liaison sérielle, etc. |

Le modèle OSI a une utilité pratique : quand on a un problème avec le réseau, il est plus facile de le diag- nostiquer et de le résoudre si on suit la logique des couches.

Par exemple, on peut commencer par vérifier la couche 3 en allant dans l'interface de commande et en faisant un ping sur un URL distant (exemple : ping ietf.org). Si on obtient le message « n packets transmitted, n packets received,



0% packet loss », c'est que tout va bien à ce niveau et que le problème se situe plus haut.

Si on a « 100% packet loss », c'est au contraire que le problème se situe plus bas et on peut vérifier que la LED qui se trouve à côté de la prise réseau de l'ordinateur et celle du switch sont bien allumées, ce qui indique que la liaison est bonne (couche 2). On peut ensuite faire un ping localhost ou un ping 127.0.0.1 (ce sont des synonymes) pour tester si la configuration du réseau sur le poste est OK. Si ce n'est pas le cas, le diagnostic est fait et il ne reste plus qu'à reconfigurer la connexion du système avec le réseau 20.

**Le modèle Internet**

Il existe un modèle concurrent : le **modèle Internet** ou **modèle TCP-IP**, qui a été créé par l’IETF (Internet

Engineering Task Force).

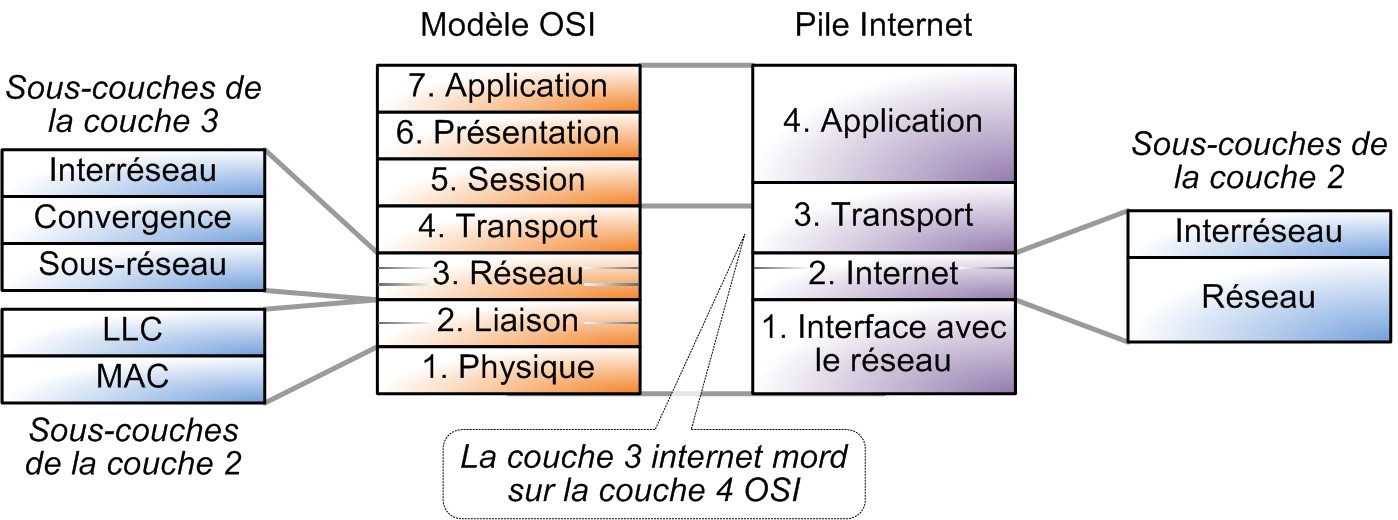
Il est décrit dans la RFC 1122, qui date de 1989 (l’expression de RFC, Request For Comment, désigne les normes édictées par l’IETF).

20 Dans Windows, c'est la section Réseau et Internet du Panneau de configuration. Dans Mac OS, c'est Internet et réseau dans les

Préférences Système. Avec Linux, cela varie de cas en cas.

Contrairement au modèle OSI, il est très peu cité comme référence théorique, mais, en pratique, c'est le modèle universel.

Il ne comprend que quatre couches. On peut les faire correspondre aux sept couches de l’ISO, mais de manière imparfaite :



**Protocoles de la couche Application**

Pour le programme qui utilise un service de communication, la couche 7 est la seule visible. Elle comprend des dizaines de protocoles.

**HTTP** (HyperText Transfer Protocol) est le protocole du web. Il réunit deux applications :

• un **client HTTP**, c’est-à-dire un navigateur (Firefox, Opera, Safari, Internet Explorer, etc.) ;

• un **serveur HTTP**, qui abrite le site et le met à la disposition des clients. Apache est le plus connu.

**SMTP** (Simple Message Transfer Protocol) gère le transport de messages électroniques quand ils sont constitués de texte sans accents. **MIME** (Multipurpose Internet Mail Extensions) le complète en couche 6 (Présentation) pour les échanges de texte avec accents ainsi que pour les fichiers non textuels

(images, sons, etc.). On parle de messagerie SMTP-MIME.

**Le serveur HTTP**

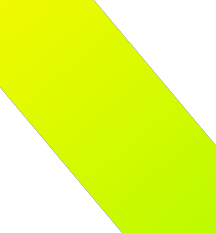
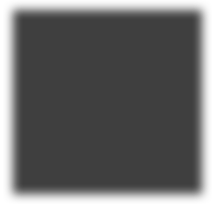
Il s'emploie pour plusieurs applications :

‒ serveur Internet (web),

‒ serveur intranet,

‒ serveur extranet.

Il est de plus en plus utilisé pour abriter des **applications web** (applications aux- quelles on accède depuis un navigateur). Elles sont créées au moyen d'outils appelés web frameworks comme **RoR** (Ruby on Rails, [h tt p://rubyonrails.org ,](http://rubyonrails.org/) h tt p:// www.railsfrance.org) ou **Django** (https:// www.djangoproject.com).



**POP3** (Post Oﬀice Protocol version 3) permet de relever les messages entreposés dans une boîte aux lettres par SMTP et de les copier ou de les transférer sur l’ordinateur sur lequel on travaille. **IMAP** (Internet Message Access Protocol) est similaire, mais il oﬀre plus de possibilités.

**DNS** (Domain Name System) gère la correspondance entre un nom de domaine et une adresse IP. C’est grâce à lui qu’on peut taper « [www.un.org](http://www.un.org/) » dans la barre d’adresse d’un navigateur et arriver sur le site des Nations Unies (United Nations). Sinon, il faudrait taper « 157.150.195.10 », ce qui n’est pas facile à retenir.

**FTP** (File Transfer Protocol) gère le transfert de fichiers. C’est lui qu’on emploie quand on copie un site sur un serveur web depuis l’ordinateur sur lequel on travaille.

**Telnet** (teletype ou telecommunication ou terminal network) est un protocole qu’on utilise pour ouvrir une session sur un ordinateur distant. Il s’emploie beaucoup pour administrer un serveur distant, mais il est de plus en plus remplacé par **SSH** (Secure Shell), qui est un telnet sécurisé.

**VoIP** (Voice over IP) gère la téléphonie sur le réseau informatique. Skype, Live Messenger et Yahoo Mes- senger sont des exemples de programmes VoIP.

**NFS** (Network File System) est un protocole qui permet d’accéder à des fichiers qui se trouvent sur une machine distante. L’application les manipule comme s’ils se trouvaient sur le disque dur local.

**La base commune : TCP-IP**

Tous ces protocoles fonctionnent sur TCP-IP ou UDP-IP.

**IP** (Internet Protocol) gère l’adressage des paquets. C’est l’équivalent du système postal.

**TCP** (Transmission Control Protocol) est un protocole d’un niveau plus élevé. Il vérifie que le destinataire et l’expéditeur sont bien en communication et que les paquets sont délivrés dans le bon ordre. Sauf exception, c’est TCP qui s’utilise avec les protocoles applicatifs qu’on a passés en revue ici (web, messa- gerie électronique, transfert de fichiers, etc.)

**UDP** (User Datagram Protocol) fonctionne aussi sur IP, mais il ne vérifie pas que le destinataire et l’expé- diteur sont bien en communication, ce qui veut dire qu’une erreur de transmission peut se produire sans qu’il s’en rende compte. Par contre, il est plus léger et plus rapide que TCP.

UDP s’emploie beaucoup, mais seulement quand une erreur ne prête pas à conséquence. Par exemple, si des routeurs s’envoient régulièrement des message pour mettre à jour les adresses des réseaux, c'est UDP qui s'utilise parce qu'il génère beaucoup moins de trafic que TCP.

**ARP**

Deux protocoles sont également importants : ARP et RARP. Ils se situent à l'interface entre la couche 3 et la couche 2.

**ARP** (Address Resolution Protocol) met en correspondance une adresse IP version 4 (couche 3) avec une adresse MAC (couche 2) 21 .

Avec les adresses IP version 6, ARP est remplacé par NDP (Neighbour Discovery Protocol).

Les nœuds qui se trouvent sur un réseau Ethernet ont besoin d'ARP pour fonctionner. Le problème est qu'ils ont une adresse IP mais que le protocole Ethernet, lui, travaille avec les adresses MAC. Quand un ordinateur X veut communiquer avec un ordinateur Y dont il ne connaît pas l'adresse MAC, il est donc obligé d'envoyer à tous les nœuds du réseau une demande d'information (« quelle est l'adresse MAC du nœud dont l'adresse IP est a.b.c.d ? ») et d'attendre la réponse de Y avant de pouvoir commencer à

dialoguer avec lui.

21 Les adresses IP s'écrivent le plus souvent en base dix, mais les adresses MAC, elles, sont presque toujours exprimées en base seize, d'où les lettres (A = 10, B = 11, C = 12, D = 13, E = 14 et F = 15). Exemple d'adresse IP : 192.168.1.10. Exemple d'adresse MAC :

49:B2:32:6C:FF:D1.

**BGP-4**

**BGP-4** (Border Gateway Protocol) est un protocole moins connu mais tout aussi important que TCP, UDP et IP : il est le maître de l’Internet. Tous les messages qui transitent par l’Internet sont acheminés par BGP-4. C'est la collaboration entre BGP-4 et les autres protocoles qui permet aux communications de fonctionner aussi bien entre les continents qu'entre les quartiers d'une ville.

Par exemple, si un poste de travail utilise les protocoles Ethernet, IP, TCP et HTTP pour faire sortir une requête web, BGP-4 entrera en jeu pendant le voyage du message sur l’Internet. À l’arrivée du paquet de données, ce sera de nouveau HTTP, TCP, IP et Ethernet qui entreront en jeu.

**5. Les systèmes intermédiaires**

Un réseau local se compose de deux grandes catégories de systèmes :

1° les **systèmes terminaux**, qu'on appelle ainsi parce qu'ils se trouvent à l'extrémité des câbles ou des ondes; ce sont les postes de travail, les serveurs, les imprimantes, etc.

2° les **systèmes intermédiaires**, qui occupent une position… intermédiaire, ce qui veut dire que les câbles ou les ondes les traversent et vont plus loin. Ce sont les points d'accès, les switches, les routeurs, les concentrateurs, etc.

Ls réseaux locaux réunissent des systèmes terminaux et des systèmes intermédiaires. Par contre, les réseaux téléinformatiques se composent presque uniquement de systèmes intermédiaires.

Les routeurs des PME sont géné- ralement des appareils de petite taille. Certains se posent sur une surface et ils ont typiquement la



taille d'un dictionnaire. D'autres  sont conçus pour être installés

dans un rack 19 pouces standard et ont généralement une hauteur

normalisée de 1 **U** (1,75 pouce, soit 4,45 centimètres).

Ceux des réseaux nationaux et internationaux sont plus gros, plus puissants et plus chers que ceux des réseaux locaux. Un gros routeur peut occuper un rack 42 U tout entier avec un débit dépassant un 1 Tbps (térabit par seconde). Le débit est appelé switching capacity (capacité de commutation).

Ce type de matériel sert à gérer le trafic qui passe par le réseau des câbles optiques terrestres et intercontinentaux. Ces câbles font transiter la plupart des paquets de données de l’Internet et des commu- nications téléphoniques internationales.

Entre l’Europe et les États-Unis, le flux global est de l’ordre de 20 térabits par seconde, et, entre les États- Unis et l’Extrême-Orient, de 10 térabits.

L’importance du trafic étant proportionnel à la richesse et au dynamisme économique de chaque région, le trafic qui augmente le plus actuellement est celui avec la Chine.

**Les fonctions des systèmes intermédiaires**

Les systèmes intermédiaires se présentent généralement sous la forme d'équipements matériels dotés d’un logiciel.

Ils rassemblent souvent plusieurs fonctions. Il y a six fonctions essentielles :



1° le **répéteur** (repeater) ;

2° le **concentrateur** ou hub 22 ;

3° le **pont** ou bridge ;

4° le **commutateur** ou switch ;

5° le **routeur** ;

6° la **passerelle** ou gateway 23 .

**Les fonctions du répéteur**

Le **répéteur** est un équipement passif qui amplifie et régénère le signal transmis. Il concerne le niveau 1

OSI (Physique). Il est essentiel pour le bon fonctionnement de tous les réseaux, mais, dans les LAN, il a disparu en tant qu’appareil. Il est intégré en tant que fonction dans les switches et les routeurs.

Dans les WAN, en revanche, il est omniprésent. Par exemple, les câbles sous-marins sont dotés de dizaines de répéteurs alimentés électriquement par les deux stations terrestres qui se trouvent à chaque bout du câble. Ils sont généralement distants de 40 à 120 kilomètres. La longueur maximale d'un câble est d'en- viron 13'000 kilomètres.

Le répéteur fonctionne de manière transparente par rapport aux protocoles des niveaux supérieurs, ce qui veut dire qu’il retransmet tels quels les trains de bits qu'il reçoit.

**Les fonctions du hub**

Le **hub** est un dispositif passif d'interconnexion qui se trouve au centre des réseaux en étoile. Il relie entre eux les nœuds situés sur les branches de l’étoile.

Un message reçu par un hub est retransmis à tous les nœuds. Cela provoque des problèmes de performances si le trafic est trop élevé ou si un utilisateur prend trop de bande passante (par exemple, s'il lance une grosse impression). C'est pourquoi il a pratiquement disparu.

Comme le répéteur, le hub fonctionne de manière transparente par rapport aux protocoles des niveaux supérieurs et il se contente de retransmettre les données sans rien y changer. Il concerne le niveau 1 OSI.

**Les fonctions du point d'accès**

Le **point d'accès**, ou AP (access point), WAP (wireless access point), ou encore transceiver, est un appareil d'interconnexion qui se trouve au centre d’un groupe de travail sans fil. Il joue le même rôle qu’un hub,

22 Attention, le terme français de concentrateur peut aussi désigner un appareil de télécommunication, appelé concentrator en anglais, qui n’a rien à voir avec le hub. Il sert à grouper plusieurs signaux sur une seule voie de transmission.

23 Attention, le terme de passerelle ou de gateway est souvent utilisé dans le sens de « routeur ».

mais dans un réseau sans fil. Plusieurs points d'accès peuvent être reliés ensemble par un câblage Ethernet pour former un maillage.

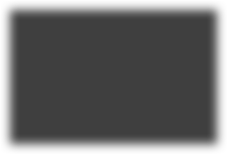
Un réseau à ondes s’appelle un **WLAN** (Wireless LAN). Aujourd'hui, tous les WLAN utilisent la même famille de normes : **IEEE 802.11** 24 .

Un point d'accès fonctionne de manière partagée. Cela provoque des problèmes de performances si le trafic est trop élevé ou si un utilisateur prend trop de bande passante (par exemple, s'il lance une grosse tâche d’impression). Une solution consiste à ajouter des points d'accès, de façon à diminuer le nombre d'utilisateurs par point d'accès.

Un avantage important des réseaux sans fil est qu’un utilisateur mobile qui se déplace d'une salle à l'autre ne perd pas le réseau. Une fonction appelée roaming (comme pour les téléphones cellulaires) permet au réseau de le suivre.

Un point d'accès peut être doté de fonctions de routage qui lui permettent, par exemple, de relier les utilisateurs à l'Internet. Techniquement, cela transforme le point d'accès en un WAP-routeur (mais ce terme n’est pas employé).

Il peut aussi comprendre un switch, ce qui en fait un WAP-switch (mais ce terme n’est pas employé non plus), ou un switch et un routeur.



Beaucoup d'équipements utilisés par les particuliers, les micro-entreprises et les micro-sites d’entreprises intègrent les trois fonctions. Sur l'exemple ci-contre, on voit tout à droite l'antenne noire du sans-fil (fonction de point d'accès), les quatre prises Ethernet grises et jaunes en bas (fonction de switch) et, là où il y a le câble violet, la prise du WAN (fonction de routeur).

Le point d'accès concerne le niveau 2 OSI, sauf s'il comprend un routeur, auquel cas il concerne les niveaux

2 et 3.

**Les fonctions du pont**

Le **pont** a pour double fonction de filtrer les messages et de relier deux segments de réseaux locaux qui sont diﬀérents aux niveaux 1 et 2 OSI, mais en général semblables aux niveaux supérieurs. Par exemple, il faut un pont entre un réseau 100BaseT et un 1000BaseF. Il concerne le niveau 2 OSI.

Aujourd'hui, la fonction de pont est assurée par le switch. De fait, un switch est un « multipont », c’est-à- dire un pont à connexions multiples. En somme, un switch à huit ports est un ensemble formé de huit

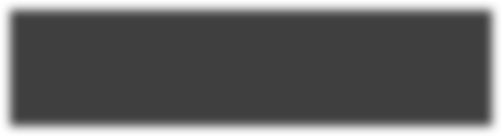
ponts et d'un hub.

24 Le Wi-Fi met en œuvre des techniques qui dérivent du système de radioguidage des torpilles que les États-Unis utilisaient pendant la deuxième guerre mondiale. Chose extraordinaire, ce système a été inventé par une femme, Hedy Lamarr (1914-2000), qui était connue à l'époque non pour ses qualités scientifiques mais pour ses rôles, disons, osés au cinéma dans des films comme Extase (1933) ou le Démon de la chair (1946).

**Les fonctions du switch**

Le **switch** ou **commutateur** est un appareil d'interconnexion situés au centre des étoiles. Il s'emploie notamment sur les réseaux Ethernet, ATM et Token Ring.

Contrairement au hub, il filtre les messages, ce qui veut dire qu'il ne les transmet qu'à leurs destinataires. Il comprend typiquement de 4 à 48 prises appelées ports. Les modèles les plus répandus en entreprise comprennent 12, 16 ou 24 ports. Ci-dessous, voici un Cisco Catalyst 3100 à 24 ports :



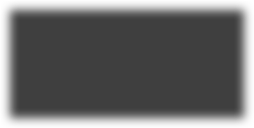
Pour être en mesure d'atteindre uniquement le destinataire, le switch construit automatiquement une table de commutation qui fait correspondre chaque adresse de noeud à un numéro de port.

Si c’est un switch à câblage métallique (prise RJ-45), il est très souvent trinorme : 10, 100 et 1000Base-T. S’il est à fibre optique, il gère souvent soit le 100Base-F et le 1 GE, soit le 100, le 1 GE et le 10 GE. Certains switches comprennent des ports RJ-45 et des ports pour la fibre optique.

Un switch multinorme est capable de détecter automatiquement à quelle vitesse il reçoit les données. C’est l’**autosensing**.

Avec les switches d’aujourd’hui, tous les ports peuvent être actifs en même temps sans que cela provoque un bouchon. On dit que le switch a une **matrice non bloquante**. Pour cela, il faut que son débit interne soit au moins égal à la somme de tous les débits d'entrée et de sortie.

Un switch d’entrée de gamme est non configurable. Pour le mettre en fonction, il suﬀit de le relier à la prise électrique 230V et de presser sur la touche on.



Les autres modèles sont configurables. On les paramètre en général depuis un poste de travail, soit par commandes, soit par l'intermédiaire d'un navigateur Internet (ce qui implique que le switch est doté d’un serveur HT TP). Une méthode classique consiste à brancher un ordinateur portatif à la prise Console du switch, qui est souvent une

prise sérielle mâle (voir image ci-contre), et à

l'administrer en direct. L'intérêt de cette méthode est qu'on passe par un câble sériel qui relie directement l'ordinateur au switch — on ne passe pas par le réseau. On peut donc administrer le switch même si le réseau est en panne (administration out-of-band).

Un switch comprend toujours des fonctions de niveau 1 et 2 OSI, mais il peut intégrer des fonctions supplémentaires de niveau 3 ou plus, jusqu’au niveau 7.

Un switch de niveau 2 travaille avec les adresses MAC des nœuds. Ces adresses sont attachées aux cartes de réseau et donc fixes.

La notion de qualité de service ou **QoS** (quality of service) s'applique à la gestion de la priorité de certaines données sur les autres. Par exemple, les échanges en interactif doivent avoir la priorité sur le trafic batch.

La gestion des priorités est possible au niveau 2 OSI, avec la norme IEEE **802.1p**, ainsi qu’au niveau 3 en tant que fonction ajoutée au protocole IP version 4 ou que fonction incluse dans IP version 6.

La norme 802.1p définit huit niveaux de service appelés User priority (la deuxième colonne indique la valeur en binaire de chaque niveau) :

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 000 | Best Eﬀort | Pas de garantie de délai, « faire de son mieux ». |
| 1 | 001 | Background | Tâches d'arrière-fond. |
| 2 | 010 | Spare | Standard, interactif normal. |
| 3 | 011 | Excellent Load | Trafic critique (business-critical). |
| 4 | 100 | Controlled Load | Multimédia. |
| 5 | 101 | Video | Voix et multimédia, délai maximum 0,1 seconde. |
| 6 | 110 | Voice | Voix et multimédia, délai maximum 0,01 seconde. |
| 7 | 111 | Network Control | Trafic réservé à la commande du réseau. |

Ces huit valeurs sont indiquée dans le champ user\_priority, qui fait trois bits, et qui fait partie de l'en-tête des trames (des paquets de données transmis de niveau 2 OSI).

Cette prioritisation du trafic est importante pour certaines applications :

• téléphonie sur IP (VoIP) ;

• téléconférence ;

• applications en temps réel pour l'industrie ou le secteur militaire ;

• émulation de protocole de réseau.

On peut gérer les types de trafic plus finement en utilisant des switches de niveau 7, mais ces équipements sont complexes et coûteux et les entreprises qui les emploient sont rares. Ce matériel intéresse principalement les multinationales et les entreprises très informatisées, par exemple les fournisseurs de services Internet.

La plupart des switches de groupes de travail sont de niveau 2. Ce type d'équipement est simple à installer. C'est parmi les switches de niveau 2 qu'on trouve ceux qui ne se configurent pas.

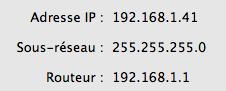
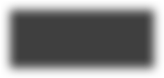
**Les fonctions du switch de niveau 3**

Un **switch de niveau 3** travaille avec les adresses IP et les adresses MAC. C'est ce qui le diﬀérencie au premier chef du switch de niveau 2, qui ne reconnaît, lui, que les adresses MAC.

En réalité, c'est un switch de niveau 1 + 2 + 3 : il comprend toutes les fonctions d'un switch de niveau 1 et

2 et il y ajoute des fonctions de routage (niveau 3).

Les adresses IP sont configurables par l’administrateur. Elles permettent de segmenter le réseau en **sous-réseaux** (**subnets**). Ainsi, l'adminis- trateur peut structurer hiérarchiquement les adresses IP de manière à modéliser la structure de l'organisation.



La plupart des switches centraux des PME sont de niveau 3.

Si un message est envoyé en **broadcast** (diﬀusion à tous les nœuds), seules les machines du sous-réseau le reçoivent. On dit que le sous-réseau forme un domaine de diﬀusion.

Les sous-réseaux ont deux avantages :

• on évite les problèmes de performances dus aux broadcasts eﬀectués sur de grands réseaux;

• on peut bâtir un système de sécurité d'accès sur les sous-réseaux.

De la même manière qu'il existe le protocole 802.1p pour le niveau 2 OSI, il existe aussi un mécanisme de qualité de service pour le niveau 3: **DiﬀServ** (diﬀerentiated services). Il est implanté dans l'en-tête de chaque paquet IP (IPv4 et IPv6).

**Les fonctions du MLS**

Un **MLS** (multilayer switch) ou commutateur multiniveau est un switch de niveau 4 ou plus. Il couvre souvent la plage 1 + 2 + 3 + 4 + 7 OSI (les couches 5 et 6 sont sans intérêt pour la commutation). Il comprend toutes les fonctions des couches 1, 2 et 3 et y ajoute des fonctions plus évoluées comme le choix d'un itinéraire selon le type d'un message. Le critère est fréquemment le port utilisé. On parle de **content switching** (commutation de contenu) ou d'**application switching** (commutation applicative). Cette méthode permet de gérer l'acheminement des messages sur le réseau d'une manière plus fine qu'avec les adresses MAC ou les adresses IP et de mettre en place une répartition de la charge (load balancing).

Les MLS s'emploient souvent avec les **server farms** (groupes de serveurs). On donne au groupe une adresse IP unique appelée **VIP** (virtual IP address) stockée dans le MLS qui donne accès aux serveurs. Le MLS est seul à savoir que, derrière cette adresse virtuelle unique, il y a plusieurs adresses réelles, qui sont appelées **RIP** (real IP addresses). C'est donc une méthode de virtualisation.

Elle est très pratique quand on a besoin de hautes performances tout en se contentant de petits serveurs peu onéreux. Actuellement, un serveur « normal » oﬀre un débit réel qui plafonne à un à deux gigabits par seconde. Le recours au MLS permet d'aller beaucoup plus haut. Avec ce mécanisme, les serveurs répondent comme s'il s'agissait d'une seule grosse machine. Même si un serveur tombe en panne, les utilisateurs ne remarquent souvent rien : le MLS marque sa RIP comme invalide et continue de travailler avec les autres.

L'administrateur du réseau paramètre la méthode de répartition dans le MLS. Il a normalement le choix entre plusieurs possibilités. En voici quelques unes :

• Manège (round-robin) : les requêtes sont envoyées à chaque RIP l'un après l'autre ;

• Manège corrigé : les requêtes sont envoyées à chaque RIP l'un après l'autre, mais on spécifie par exemple que le serveur 1 doit recevoir deux fois plus de requêtes que le serveur 2 ;

• Moindre nombre de sessions (least connections) : la requête est envoyé au serveur qui a le moins de sessions ouvertes.

Des trois méthodes, la meilleure est bien entendu la dernière parce que c'est celle qui tient le mieux compte de la diﬀérence de puissance des serveurs.

Les MLS sont très pratiques si on a des trafics à diﬀérencier ou des ressources à virtualiser. Par contre, ils coûtent cher et — surtout — ils nécessitent de bonnes compétences dans le domaine du paramétrage, de l'optimisation des performances et de la gestion des problèmes de trafic.

**Les VLAN**

Un **VLAN** (virtual LAN) est un réseau logique qui segmente un réseau réel. Cela permet de créer plusieurs domaines de diﬀusion dans le réseau local. Un message envoyé à tous les nœuds (broadcast) n'est transmis qu'à ceux du sous-réseau concerné.

|  |  |
| --- | --- |
| **Avantages du VLAN** | **Inconvénients** |
| Permet de définir des groupes de machines (en plus des groupes d’utilisateurs définis dans le système d’exploitation du serveur).  Diminue le trafic en segmentant les broadcasts. Normalisé (IEEE 802.1q).  Peut être mis en œuvre au niveau 2 ou 3 OSI. | Doit être administré (travail supplémentaire). Ajoute une couche de complexité. |

**En résumé**

Chaque type de switch convient à un niveau du réseau de l’entreprise :

• **groupe de travail** ou **access level** : switches de niveau 2 ;

• **département** ou **distribution level** : switches de niveau 3 ;

• **entreprise** ou **core level** : switches de niveau 3 ou plus.

Pour le groupe de travail, on parle d’access level parce que le poste de travail sert à accéder au réseau et aux ressources des serveurs.

Le distribution level est le niveau dans lequel les données venant d’un serveur central sont aiguillées vers le bon groupe de travail.

Le core level est le cœur du réseau, la partie qui concerne l’ensemble de l’entreprise.

|  |  |  |
| --- | --- | --- |
|  | **Avantages** | **Inconvénients** |
| **Hub** | Très simple à mettre en place.  Permet de surveiller aisément le trafic. | Domaine partagé (collisions).  Débit proportionnel au nombre de nœuds. Non configurable. |
| **Switch de niveau 2 non configurable** | Très simple à mettre en place.  Bien adapté aux groupes de travail. Très peu coûteux.  Pas de collisions possibles et pas de baisse du débit quand on ajoute des nœuds. | Fonctions limitées.  Inadapté aux réseaux de plus de quelques dizaines de postes.  Non configurable. |
| **Switch de niveau 2 configurable** | Configurable (VLAN, QoS, etc.).  Bien adapté aux grands groupes de travail. Peu coûteux.  Pas de collisions possibles et pas de baisse du débit quand on ajoute des nœuds. | Nécessite d’être configuré.  Ne gère pas les fonctions de niveau 3. Inadapté au routage interne (cas où il existe plusieurs chemins possibles d’un point A à un point B). |
| **Switch de niveau 3**  (en réalité : de niveau 2 et 3) | Configurable (routage interne, sous-réseaux, VLAN, QoS, etc.).  Bien adapté à la partie centrale des réseaux  (niveau distribution et niveau entreprise).  Pas de collisions et pas de baisse du débit quand on ajoute des nœuds. | Nécessite d’être configuré. Assez coûteux. |
| **MLS (Multilayer Switch)** | Très configurable.  Bien adapté au niveau entreprise. Commutation des messages selon leur contenu.  Répartition de la charge.  Pas de collisions possibles et pas de baisse du débit quand on ajoute des nœuds. | La configuration est complexe. Coûteux. |

**Les fonctions du routeur**

Un routeur a pour fonction de relier deux réseaux. À l’opposé du switch, qui est au centre du réseau, le routeur est à la périphérie. C’est la porte avec le monde extérieur. Il peut se présenter sous deux formes :

1° un équipement matériel et logiciel ;

2° un simple logiciel (il se trouve alors dans un ordinateur normal, souvent une machine Linux ou BSD). Les modèles pour entreprises contiennent au moins trois interfaces :

• une avec l’intérieur (Ethernet, 802.11),

• une avec l’extérieur (DSL, MPLS, etc.),

• une avec la console d’administration (elle permet de gérer le routeur en out-of-band).

Les routeurs pour TPE (très petites entreprises) et personnes privées ne disposent généralement pas d'une prise console, mais ils intègrent souvent un switch et un point d'accès sans fil. Microsoft leur donne le nom bizarre de passerelles résidentielles (residential gateways).

Deux réseaux reliés par un routeur forment un interréseau (internetwork). Le plus grand de tous est l’Internet. En fait, c’est même un interréseau de réseaux.

Le routeur travaille au niveau 3 du modèle OSI. Il est doté d'un système d'exploitation et il est plus « intel- ligent » que le switch de niveau 3, mais il est aussi plus lent.

Les routeurs d’aujourd’hui intègrent souvent des fonctions supplémentaires, notamment la protection contre les tentatives d'intrusion.

**Les fonctions de la passerelle**

Une passerelle (gateway) est un logiciel dont la fonction est de relier deux systèmes informatiques. Elle agit aux niveaux élevés du modèle OSI. Par exemple, c’est la passerelle qui traduit des données ISO-8859 en UTF-8 et réciproquement. En somme, c’est essentiellement un pont entre deux systèmes d'exploitation. Le plus souvent, c’est un logiciel installé sur un serveur.

Attention, le routeur est souvent appelé gateway alors que ce sont des systèmes complètement diﬀérents : le routeur gère des adresses IP et des itinéraires alors que la passerelle s'occupe de l’interfaçage des flux de données entre deux systèmes informatiques — par exemple, entre des machines sous Windows et d'autres sous Linux.

**Le routage interne**

Si le niveau access se compose presque toujours de simples étoiles, les niveaux distribution et core sont très souvent architecturés en **maillage** : on double ou on triple les systèmes intermédiaires centraux ainsi que les chemins entre eux et ceux entre les serveurs centraux et les systèmes intermédiaires centraux. Cette **redondance** apporte plus de sécurité et — à condition qu’on ait paramétré les switches en ce sens — un débit multiplié.

Toutefois, le fait qu’il y ait plusieurs chemins possibles entre deux points implique forcément un choix entre ces chemins. Si on installe le matériel et qu’on ne paramètre pas les switches pour opérer ce choix, c’est la pagaille : le trafic explose (on parle de bridge loop ou de switching loop), provoquant une tempête de diﬀusion ou **broadcast storm** : si un message est envoyé « à tout le monde », tous les switches l’envoient à tous leurs voisins, ce qui aboutit à une explosion du trafic.

Il existe deux moyens d'éviter cela : le Spanning Tree et les protocoles de routage interne.

**Le STP**

Le **STP** (spanning tree protocol) est un système de routage sur réseau local qui travaille au niveau 2 OSI. Il crée une représentation du réseau en arbre, et, s'il existe plusieurs chemins possibles vers un nœud, il

choisit l'un de ces chemins comme chemin actif et ferme les autres. En cas de changement dans le réseau, il recalcule l'arborescence et choisit un nouveau chemin unique vers chaque nœud.

Le fonctionnement du Spanning Tree est simple. Le protocole élit un switch central appelé root bridge et calcule la longueur du chemin (port's cost) entre cet élément central et chacun des autres noeuds. Le meilleur chemin est utilisé pour la transmission (mode forwarding), tandis que les autres sont écartés (mode blocking).

Tout changement dans le réseau rend nécessaire un recalcul des chemins puisqu’on doit passer d’un état stable à un autre état stable, avec certains chemins qui passent du mode forwarding au mode blocking ou réciproquement. Cela prend plusieurs secondes ; on parle de convergence time.

Le STP s’y prend en deux phases. La première, appelée mode listening, consiste à contrôler qu'il n'existe pas deux itinéraires vers le même noeud qui se trouveraient en mode forwarding. La seconde est le mode learning, qui correspond à la phase de reconstruction de la table de commutation du switch.

**Les IGP**

Les **IGP** (Interior Gateway Protocols) sont les protocoles de routage qui permettent d'acheminer des paquets sur un réseau d'entreprise. Ce réseau peut être un LAN (l’entreprise est sur un seul site) ou un WAN (l’entreprise est sur plusieurs sites).

**RIP** (Routing Information Protocol) est le plus simple. La version utilisée est la 2 (la 1 est obsolète). Chaque switch de niveau 3 et chaque routeur gère dans une table les itinéraires vers tous les nœuds connus. Toutes les 30 secondes, le contenu de la table est transmise par broadcast à tous les nœuds du réseau (y compris les postes de travail, les imprimantes, etc.). Les switches de niveau 3 et les routeurs qui sont ses voisins font ensuite de même, ce qui aboutit au bout d'un certain temps à une situation où tous les switches de niveau 3 et tous les routeurs partagent la même connaissance du réseau. C'est la **network convergence**.

**IGRP** (Interior Gateway Routing Protocol) a été créé par Cisco, qui est le principal fabricant de routeurs. C’est un RIP amélioré mais il ne s’utilise plus, remplacé par EIGRP.

**EIGRP** (Enhanced IGRP) est aussi propre à Cisco. Il se caractérise par la facilité avec laquelle il se met en place et par son eﬀicacité. Son fonctionnement se base sur le distance-vector routing, c’est-à-dire sur le nombre de sauts d’un point à un autre. Il dialogue avec les routeurs et les switches de niveau 3 qui sont ses voisins et non avec tous.

C’est un bon choix si on a un réseau de petite ou moyenne taille dont tous les systèmes intermédiaires de niveau 3 sont faits par Cisco.

C’est aussi un bon choix si on gère un gros réseau, mais à condition de savoir le configurer correctement et d’accepter d'utiliser un système propre à Cisco.

Si on n’est pas à l’aise avec les subtilités du paramétrage de réseau, toutefois, il vaut mieux demander à un consultant externe de le faire. Comme a dit Bill Barns, « there is a diﬀerence between making something foolproof and reducing the number of fools ».

**OSPF** (Open Shortest Path First) est un IGP où toute modification dans la topologie du réseau est aussitôt transmise à tous les routeurs et les switches de niveau 3. De plus, on peut diviser un réseau en sous- réseaux et assigner un coût à chaque chemin, ce qu’EIGRP ne sait pas faire.

Il est plus lourd à mettre en place et à gérer qu’EIGRP, ce qui est un défaut mais aussi une qualité : la mise en place d’OSPF réclame une bonne analyse préalable, ce qui tend à améliorer la qualité du système.

OSPF est normalisé, ce qui veut dire qu’on peut l’utiliser avec le matériel de tous les fabricants de routeurs et de switches de niveau 3. Même si on ne travaille qu'avec du matériel Cisco aujourd’hui, on ne sait jamais ce qui peut arriver dans deux ou trois ans.

**IS-IS** (Intermediate System to Intermediate System) est assez similaire à OSPF. Il est apprécié sur les grands réseaux parce que sa conception le rend un peu plus simple qu'OSPF mais au moins aussi puissant.

En résumé :

• RIP II est le meilleur choix sur un petit réseau, mais EIGRP, OSPF et IS-IS sont préférables sur un réseau de taille moyenne et indispensables sur un réseau de grande taille.

• Sur un grand réseau, RIP est inutilisable.

• EIGRP, OSPF et IS-IS sont techniquement équivalents (sauf dans des cas particuliers) mais il vaut mieux éviter EIGRP parce qu'il n'est pas normalisé.

• Qu’on utilise EIGRP, OSPF ou IS-IS, on aura un bon résultat si l’administrateur du réseau est compétent, et aucun d’eux ne donnera satisfaction s’il ne l'est pas. En pratique, le meilleur protocole est celui que l’administrateur du réseau maîtrise le mieux.

|  |  |  |
| --- | --- | --- |
|  | **Avantages** | **Inconvénients** |
| **STP** | Fonctionne au niveau 2 OSI (pas besoin de switches de niveau 3).  Coexiste sans problèmes avec un IGP. Il agit alors comme une roue de secours. | Pas d’amélioration des performances. |
| **RIP II** | Très facile à configurer et à gérer. Bien adapté aux petits réseaux. | Transmet les tables de routage à tous les nœuds, cela toutes les 30 secondes, ce qui est inutile s’il n’y a pas de changement et trop long s’il y a un changement.  Inadapté aux réseaux de moyenne ou grande taille. |
| **IGRP** | RIP amélioré. | Propre à Cisco. Obsolète. |
| **EIGRP** | Très facile à configurer si on utilise les valeurs par défaut.  Facile à gérer.  Bien adapté aux réseaux de petite ou moyenne taille.  Bien adapté aux grands réseaux à condition d’être bien configuré. | Propre à Cisco.  Presque trop facile à mettre en place : la configuration par défaut peut se révéler mal adaptée au fil du temps. |

|  |  |  |
| --- | --- | --- |
| **OSPF** | Très configurable.  Permet la division du réseau en sous-réseaux. Bien adapté aux réseaux de moyenne et grande taille.  Normalisé. | Plus complexe qu'IEGRP.  Inadapté à un petit réseau (mais, si l’adminis- trateur le connaît bien, rien n’empêche de l’utiliser). |
| **IS-IS** | Unpeu plus simple qu'OSPF. Plus résistant aux attaques.  Bien adapté à un très grand réseau. Normalisé. | Un peu moins riche en fonctions qu'OSPF. Inadapté à un petit réseau (mais, si l’adminis- trateur le connaît bien, rien n’empêche de l’utiliser). |

**Les EGP**

Les **EGP** (Exterior Gateway Protocols) sont les protocoles de routage qui permettent d'acheminer des paquets entre les entreprise et autres organisations. Ils concernent toujours les WAN.

**BGP4** (Border Gateway Protocol) est le seul EGP utilisé aujourd’hui. C’est lui qui gère l’acheminement des paquets sur les routeurs nationaux et internationaux. Par exemple, quand on envoie une requête à un serveur web situé aux États-Unis, les données sont acheminées d’un routeur à l’autre au moyen de BGP4.

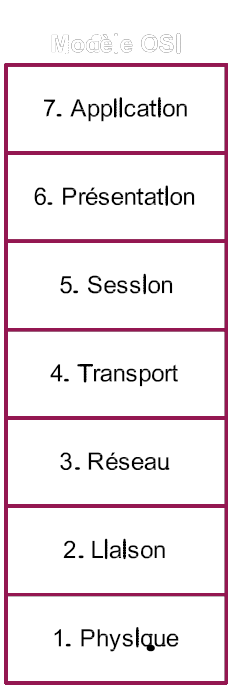
Les trois protocoles essentiels de l'Internet sont IP, TCP et BGP4.

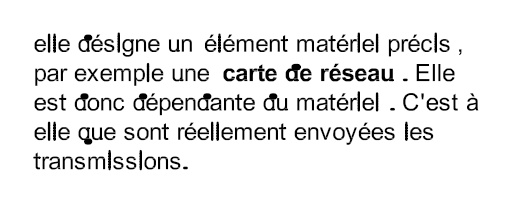
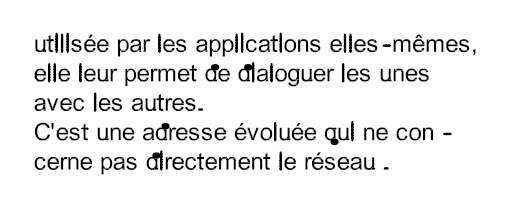
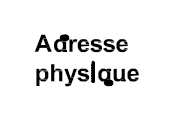
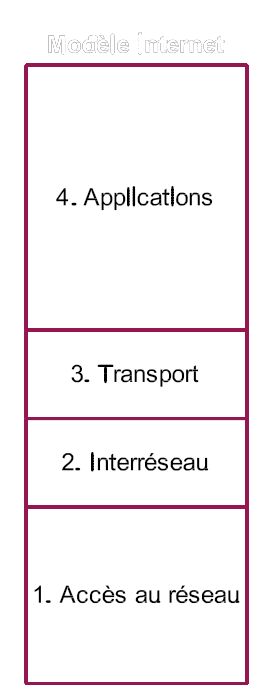
**6. L'adressage IP**

Le mécanisme de l’**adressage** est fondamental dans les réseaux. Sans lui, les machines qui les constituent ne pourraient pas s’identifier et se contacter les unes les autres, ce qui veut dire qu’aucun réseau ne pourrait exister.

Actuellement, un système d’adressage est standard dans le monde entier : l’adressage **IP** (Internet Protocol). Le terme Internet ne désignant pas l’Internet en particulier, mais n’importe quel internetwork (réseau de réseaux) en général.

Les machines que l’on peut joindre par leur adresse IP s’appellent des **hôtes** (hosts). Ce terme s’applique à toute entité dotée d’une ou plusieurs adresses de réseau. Les serveurs, les postes de travail, les imprimantes de réseau, les routeurs, les téléphones IP (Voice over IP) et beaucoup de switches sont des hôtes.

Dans le modèle TCP-IP, il y a un adressage au niveau applicatif, TCP, IP et physique.



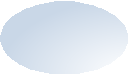
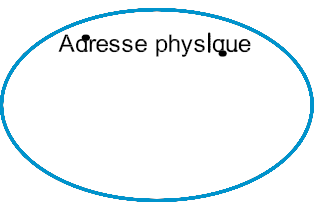
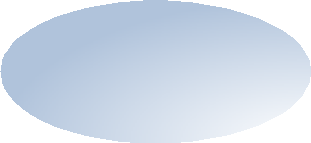
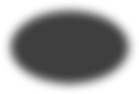
|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |
|  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |

L'ensemble formé d'un port TCP ou UDP et d'une adresse IP s'appelle un **socket**.

Quand une adresse physique concerne un hôte de réseau 802.2 (c’est-à-dire un réseau Ethernet, Token

Ring, FDDI, etc.), c’est une **adresse MAC**. Quand elle concerne un hôte Ethernet, c’est une **adresse**

**Ethernet**. Autrement dit, l’adresse Ethernet est un cas particulier d’adresse MAC et une adresse MAC un cas particulier d’adresse physique (voir le schéma ci-contre).



Une remarque juridique : aux États-Unis, les adresses IP sont publiques, ce qui veut dire, par exemple, qu’un organisme d’État a le droit de les inter- cepter. En Europe, en revanche, les adresses IP sont des données à caractère personnel, c’est-à-dire des informations « concernant une personne phy- sique identifiée ou identifiable » (Directive 95/46/CE du 24 octobre 1995, art. 2 let. a), informations soumises à « la protection des libertés et droits

fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel » (art. 1).

**Adresses IP v4 publiques et privées**

Une **adresse IP publique** (aussi appelée registered address ou Internet address) identifie un réseau de manière unique dans le monde entier, et elle est visible partout dans le monde. Par exemple, si on tape

209.85.135.147 dans la fenêtre de l’adresse à rechercher dans un navigateur, on obtient la version française

de Google.

Les adresses publiques sont attribuées par une organisation oﬀicielle, l’**IANA** (Internet Assigned Numbers Authority), qui dépend de l’**ICANN** (Internet Corporation for Assigned Names and Numbers), elle-même sous contrat avec le Département du commerce des États-Unis. Autrement dit, c'est le gouvernement des États-Unis qui gère l’adressage public de l’ensemble des systèmes informatiques du monde.

Une **adresse IP privée** identifie un hôte à l’intérieur d’un réseau. Elle est choisie librement par l’adminis- trateur du réseau parmi les plages d’adresses privées prédéfinies par l’IANA (norme RFC 1918 ) :

• de 10.0.0.0 à 10.255.255.255 ;

• de 172.16.0.0 à 172.32.255.255 ;

• de 192.168.0.0 à 192.168.255.255.

Contrairement à une adresse publique, une adresse privée est invisible de l’extérieur et ne peut pas être acheminée sur l’Internet ou tout autre réseau national ou international. Il est donc nécessaire d’activer un mécanisme de traduction d’adresses entre le réseau interne et le monde extérieur.

Une adresse publique ne peut ni se situer dans les plages privées ni commencer par 0 ou 127, ces débuts d’adresse étant respectivement réservés au chemin par défaut (default route) et aux tests sur l’hôte local (loopback). Il existe encore d’autres plages réservées.

Pour trouver l'adresse publique de notre routeur (celle qui est visible depuis l'extérieur), on peut utiliser un site comme ipillion.com. Il permet aussi de se renseigner sur une autre adresse.

**Les deux parties d'une adresse IP v4**

Une adresse IP v4 se compose de deux parties. La première identifie le **réseau** et elle s’appelle **network number** ou **network prefix** ; elle est fixe. La seconde identifie l’hôte et s’appelle **host number** ; selon le

choix de l’administrateur du réseau, elle peut être fixe ou dynamique. Dans le second cas, un logiciel attribue automatiquement une adresse à chaque hôte du réseau. C'est le **DHCP** (Dynamic Host Configu- ration Protocol).

Par définition, tous les hôtes d’un réseau partagent le même network prefix et chacun d’eux a un host number diﬀérent.

**Le CIDR**

En septembre 1981, quand la norme IP est apparue, les concepteurs du système ont décidé de créer un système d’adressage par classes (classful addressing). On a trois classes : la A, la B et la C. Chacune occupe une partie bien précise de l’espace d’adressage ; par exemple, une adresse dont le premier octet est plus petit que 127 est forcément une adresse de classe A.

La taille du réseau se reconnaît aux premiers bits de l’adresse. Par exemple, l’adresse d’un réseau «/24»

commence par les bits 110 et donc par les chiﬀres 192 (**11000000** en binaire) à 223 (**11011111**).

|  |  |  |  |
| --- | --- | --- | --- |
| **Classe** | **Début adresse, binaire** | **Début adresse, décimal** | **Partie réseau (R)**  **et**  **partie interne (hôte, h)** |
| **A (/8)** | **0** | **1** à **126** | RRRRRRRR.hhhhhhhh.hhhhhhhh.hhhhhhhh |
| **B (/16)** | **10** | **128** à **191** | RRRRRRRR.RRRRRRRR.hhhhhhhh.hhhhhhhh |
| **C (/24)** | **110** | **192** à **223** | RRRRRRRR.RRRRRRRR.RRRRRRRR.hhhhhhhh |
| **D** | **1110** | **224** à **239** | Réservé au multicasting |
| **E** | **1111** | **240** à **255** | Réservé aux expérimentations |

Par exemple, l’adresse 192.11.240.10 appartient à la classe C ; le réseau est le 192.11.240 et l’hôte le 10.

Aujourd’hui, on préfère employer la notation **CIDR** (Classless InterDomain Routing, normes RFC 1518 et

1519). Le network prefix est indiqué sous la forme /N (slash N), où N est le nombre de bits occupé par le network prefix. Ainsi, la classe A est désignée par «/8» et la classe B par «/16».

Si tous les chiﬀres binaires de la partie interne sont à zéro, l’adresse désigne le réseau. S’ils sont tous à un, l’adresse indique la diﬀusion (broadcast), c’est-à-dire un message adressé à tous les hôtes d’un réseau. Exemple :

• l’adresse 192.11.240.0 désigne le réseau 192.11.240 (dont la plage va de 192.11.240.0 à

192.11.240.255) ;

• l’adresse 192.11.240.255 désigne le broadcast du réseau 192.11.240.0.

Si le dernier chiﬀre est 1, il s’agit fréquemment du **routeur** (gateway), c’est-à-dire de l’équipement qui sert de porte entre le réseau et le reste du monde. Ainsi, l’adresse 192.11.240.1 désigne souvent (mais pas forcément) le routeur du réseau 192.11.240.0.

**Les sous-réseaux IP v4**

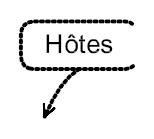
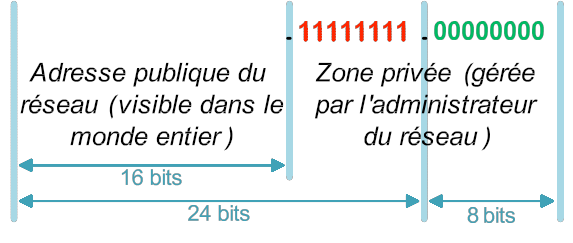
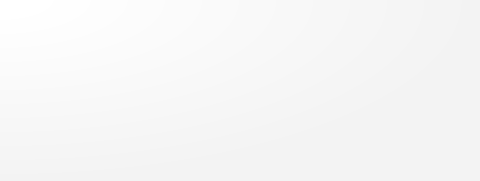
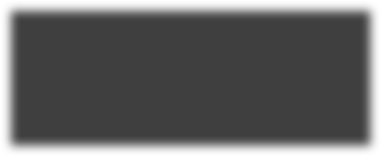
À l’intérieur d’un réseau, on peut mettre en place des **sous-réseaux** (subnets). On identifie la frontière avec la partie qui recense les hôtes au moyen d’un **masque de sous-réseau** (subnet mask). Les masques

correspondants aux réseaux /8, /16 et /24 sont les suivants :

|  |  |  |
| --- | --- | --- |
| **CIDR** | **Masque binaire** | **Masque décimal** |
| **/8** | **11111111.00000000.00000000.00000000** | **255.0.0.0** |
| **/16** | **11111111.11111111.00000000.00000000** | **255.255.0.0** |
| **/24** | **11111111.11111111.11111111.00000000** | **255.255.255.0** |

Avec le subnetting, on a donc un adressage en trois parties : le network prefix, le subnet number et le host number.

Par exemple, si l’administrateur du réseau 148.196.0.0/16 souhaite utiliser tout le troisième octet pour le subnetting, il va spécifier le masque 255.255.255.0 pour les adresses. Les deux premiers octets étant forcément utilisés pour le masque du réseau (une adresse commençant par 148 se situe dans la plage des réseaux de classe B), cet administrateur pourra définir 254 sous-réseaux formés de 254 hôtes au maximum. En binaire, cela donne 11111111.11111111.11111111.00000000.



Si cinq sous-réseaux lui suﬀisent, il va spécifier le masque 255.255.224.0, ce qui lui donnera au maximum 8 sous-réseaux et 8’190 hôtes par sous-réseau. En binaire, le masque est le suivant :

11111111.11111111.11100000.00000000 (224 vaut 11100000 en binaire).

Il existe des programmes de calcul de masques IP, par exemple Advanced IP Address Calculator (http:// [www.radmin.com/products/utilities/ipcalculator.php),](http://www.radmin.com/products/utilities/ipcalculator.php)) ainsi que des sites de calcul en ligne, par exemple <http://www.t1shopper.com/tools/calculate/ip-subnet>et [http://www.subnet-calculator.com.](http://www.subnet-calculator.com/)

Le subnetting est utile pour les performances : il y a moins de trafic global puisque la portée d’un broad- cast est le sous-réseau) et les tables des switches sont plus légères puisqu'elles ne comportent pas les adresses des hôtes des autres sous-réseaux.

Il sert aussi la sécurité : aux niveaux 1 et 2 OSI, les sous-réseaux ne se voient pas. Pour pouvoir circuler de l’un à l’autre, un message doit passer par le niveau 3, qui est matérialisé par un switch de niveau 3 ou un routeur, ce qui permet un filtrage et un contrôle du trafic plus fins que le 2.

**Le subnetting d'un réseau /8**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CIDR** | **Masque** | **Nbre de bits** | **Nbre de sous-réseaux** | **Nombre d’hôtes** |
| /10 | **255.192.0.0** | 2 | 2 | 4'194’302 |
| /11 | **255.224.0.0** | 3 | 6 | 2'097’150 |
| /12 | **255.240.0.0** | 4 | 14 | 1'048’574 |
| /13 | **255.248.0.0** | 5 | 30 | 524’286 |
| /14 | **255.252.0.0** | 6 | 62 | 262’142 |
| /15 | **255.254.0.0** | 7 | 126 | 131’070 |
| /16 | **255.255.0.0** | 8 | 254 | 65’534 |
| /17 | **255.255.128.0** | 9 | 510 | 32’766 |
| /18 | **255.255.192.0** | 10 | 1’022 | 16’382 |
| /19 | **255.255.224.0** | 11 | 2’046 | 8’190 |
| /20 | **255.255.240.0** | 12 | 4’094 | 4’094 |
| /21 | **255.255.248.0** | 13 | 8’190 | 2’046 |
| /22 | **255.255.252.0** | 14 | 16’382 | 1’022 |
| /23 | **255.255.254.0** | 15 | 32’766 | 510 |
| /24 | **255.255.255.0** | 16 | 65’534 | 254 |
| /25 | **255.255.255.192** | 17 | 131’070 | 126 |
| /26 | **255.255.255.192** | 18 | 262’142 | 62 |
| /27 | **255.255.255.224** | 19 | 524’286 | 30 |
| /28 | **255.255.255.240** | 20 | 1'048’574 | 14 |
| /29 | **255.255.255.248** | 21 | 2'097’150 | 6 |
| /30 | **255.255.255.252** | 22 | 4'194’302 | 2 |

**Le subnetting d'un réseau /16**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CIDR** | **Masque** | **Nbre de bits** | **Nbre de sous-réseaux** | **Nombre d’hôtes** |
| /18 | **255.255.192.0** | 2 | 2 | 16’382 |
| /19 | **255.255.224.0** | 3 | 6 | 8’190 |
| /20 | **255.255.240.0** | 4 | 14 | 4’094 |
| /21 | **255.255.248.0** | 5 | 30 | 2’046 |
| /22 | **255.255.252.0** | 6 | 62 | 1’022 |
| /23 | **255.255.254.0** | 7 | 126 | 510 |
| /24 | **255.255.255.0** | 8 | 254 | 254 |
| /25 | **255.255.255.192** | 9 | 510 | 126 |
| /26 | **255.255.255.192** | 10 | 1’022 | 62 |
| /27 | **255.255.255.224** | 11 | 2’046 | 30 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| /28 | **255.255.255.240** | 12 | 4’094 | 14 |
| /29 | **255.255.255.248** | 13 | 8’190 | 6 |
| /30 | **255.255.255.252** | 14 | 16’382 | 2 |

**Le subnetting d'un réseau /24**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CIDR** | **Masque** | **Nbre de bits** | **Nbre de sous-réseaux** | **Nombre d’hôtes** |
| /26 | **255.255.255.192** | 2 | 2 | 62 |
| /27 | **255.255.255.224** | 3 | 6 | 30 |
| /28 | **255.255.255.240** | 4 | 14 | 14 |
| /29 | **255.255.255.248** | 5 | 30 | 6 |
| /30 | **255.255.255.252** | 6 | 62 | 2 |

**Le VLSM**

Les sous-réseaux ont souvent tous la même taille, mais on peut aussi créer des sous-réseaux de tailles diﬀérentes. C’est le **VLSM** (Variable Length Subnet Masks). Par exemple, si on a 254 hôtes en tout, on peut faire un groupe de 126 hôtes et deux groupes de 62.

**IP v6**

Le 6 mai 2012, deux événements se sont passés en même temps : on a fêté le Diamond Jubilee de la reine d'Angleterre (60 ans de règne) et de nombreuses parties de l'Internet sont passées d'IP version 4 à IP version 6 ou **IPv6**. Personne ne s'en rendu compte à l'exception des techniciens qui surveillaient la tran- sition en faisant des vœux pour que tout se passe bien, et le passage s'est eﬀectivement passé sans en- combre. Depuis cette date, on accède à Google ou Facebook en passant par TCP-IPv6.

Le premier avantage d'IPv6 est le très grand nombre d'adresses possibles : 2128 possibilités, soit 3,4・1038. En chiﬀres, cela donne 340'282'366'920'938'463'463'374'607'431'768'211'456.

On représente généralement une adresse IPv6 par huit nombres de quatre chiﬀres en base seize. Voici un exemple :

2d43:77ff:0000:c9c6:00c4:573:0a11:62d4

Les zéros qui se trouvent en début d'un groupe de quatre chiﬀres peuvent être sous-entendus. L'adresse ci- dessus peut donc aussi être écrite comme ceci :

2d43:77ff::c9c6:c4:573:a11:62d4

L'adresse de loopback (l'équivalent de 127.0.0.1) est une suite de 31 zéros suivis d'un 1 terminal :

0000:0000:0000:0000:0000:0000:0000:0001

Elle peut s'abréger :

::1

Rappel : il s'agit d'hexadécimal, pas de binaire.

Comme une adresse IPv4, une adresse IPv6 se compose d'une **partie réseau** et d'une **partie hôte**, et optionnel- lement d'une **partie sous-réseau**.

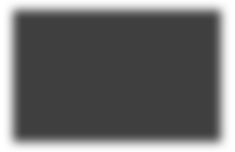
Contrairement aux adresses IPv4, par contre, la partie réseau et la partie hôte ont en principe une taille fixe : 64 bits chacune. On peut donc avoir 264 réseaux et 264 hôtes

(et sous-réseaux éventuels).

Le passage à IPv6 pose de graves problèmes de sécurité :

• Certains pare-feu, programmes de détection d'intrusion et autres équipements de sécurité fonctionnent seulement en IPv4.

• C e u x q u i s o n t b i s t a n d a r d n e s o n t probablement pas encore eﬀicaces en IPv6 puisque la sécurité IPv6 ne sera testable que quand ce standard se popularisera.



Pour noter les sous-réseaux, on emploie la notation **CIDR** comme en IPv4.

Grâce à leur nombre, les adresses IPv6 rendent inutiles le mécanisme de NAT (Network Address Translation) : tous les hôtes IPv6 ont leur propre adresse publique. Cela pose évidemment un gros problème de confidentialité. Pour pallier à ce problème, un mécanisme de génération d'adresse éphémère d'hôte est utilisé, mais ce n'est qu'un palliatif, puisque l'adresse du réseau reste, elle, fixe. Autrement dit, si un seul hôte se trouve dans un réseau donné, le changement d'adresse est de la poudre aux yeux.

IPv6 contient une logique qui permet aux hôtes de s'autoconfigurer pour le réseau.

Les réseau x i nfo rmat i q u es 58 h tt p // www jaqu et .o rg, mai 2111 5

**7. FTP**

FTP (file transfer protocol) est une norme et un logiciel :

1° Un protocole normalisé de transfert de fichiers très utilisé dans les principaux environnements infor- matiques actuels : Unix, Linux, Windows, etc.

Il fait l’objet des normes RFC 959, 1579, 2228, 2428 et 3659 de l’IETF (Internet Engineering Task Force).

2° Tout programme de communication conforme au protocole FTP.

C’est ce second sens qui nous intéresse. L'essentiel sur FTP :

• C'est la solution universelle de transfert de fichiers. Il peut s'employer sur tout réseau TCP-IP.

• Le transfert intervient entre un client et un serveur (logiciel).

• FTP est né dans le monde Unix et Linux et il en a la logique d'utilisation. En particulier, les noms et la syntaxe des commandes se conforment aux règles de Unix et Linux.

Une version simplifiée de FTP est incluse dans Firefox, Internet Explorer et les autres navigateurs. Quand on importe des fichiers (download) 25 depuis l’Internet, c’est généralement FTP qui fait le travail sans qu’on le sache. Toutefois, ce FTP est rudimentaire et il ne convient pas si on veut télécharger de nombreux fichiers. Pour cela, on emploie un programme FTP spécialisé comme FileZilla. C’est généralement ce qu’on fait si on gère un site web.

Le logiciel FTP existe sur presque toutes les plates-formes informatiques. La magie de FTP, c’est qu’on peut transférer de manière transparente un fichier entre Windows, Unix et Linux (ou z/OS, ou n’importe quel autre environnement). On ne sait même pas si l’autre machine fonctionne sous le même système d’exploitation que la machine locale, et on n’a pas besoin de le savoir.

Attention, cela signifie juste que le fichier sera transmis sans problèmes. Sera-t-il compris, c’est une autre aﬀaire. Par exemple, un ordinateur sous z/OS n’a aucune idée de la structure d’un fichier Word ou Excel, et un PC sous Windows ne peut rien faire d’un fichier créé sous z/OS par DB2.

Les opérations permises par FTP sont notamment le transfert d’un ou plusieurs fichiers, la reprise automatique du transfert s’il a été accidentellement interrompu, la mise en file d’attente des fichiers prêts à être transférés (queuing), la programmation d’un transfert à une heure donnée, la modification des droits d’accès sur les fichiers, l’eﬀacement de fichiers, la synchronisation de fichiers et la programmation de lots de tâches (batch scripting).

Par définition, c’est le logiciel client qui initie l’échange, en passant par le port 21, avec le logiciel serveur, qui se trouve presque toujours sur un ordinateur distant. Le logiciel serveur s’appelle l’hôte (host).

25 En français, le download s’appelle « télédéchargement » et l’upload « téléchargement », mais la majorité des gens utilisent le terme de téléchargement à l’envers et n’emploient pas du tout celui de télédéchargement.

La suite dépend du mode adopté. En mode passif, le serveur ouvre un port choisi au hasard et le client utilise ce port pour transmettre les données. En mode actif, c’est le client qui ouvre un port choisi au hasard et qui demande au serveur de lui envoyer les données sur ce port. Il faut éviter le mode actif parce que les pare-feu l’acceptent mal.

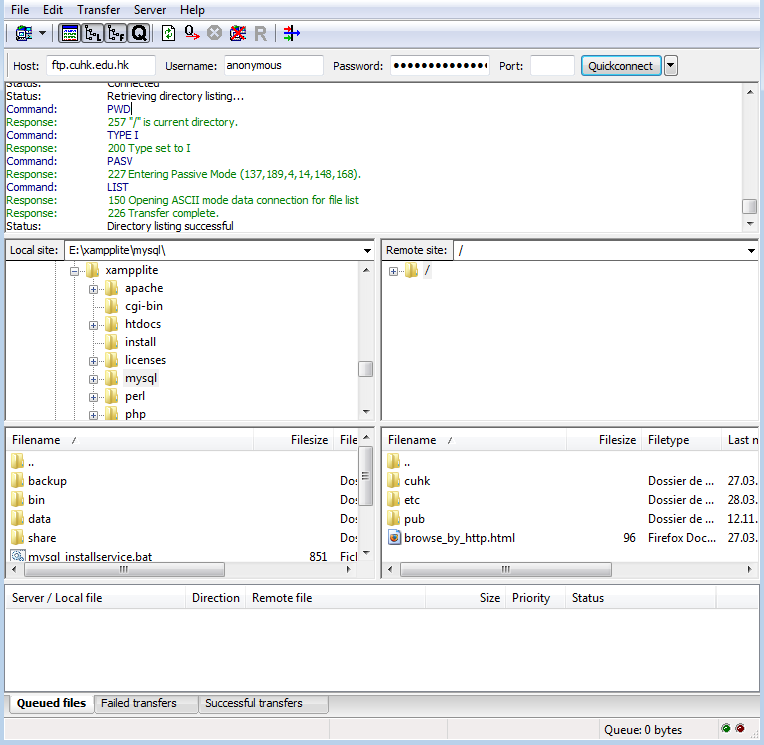
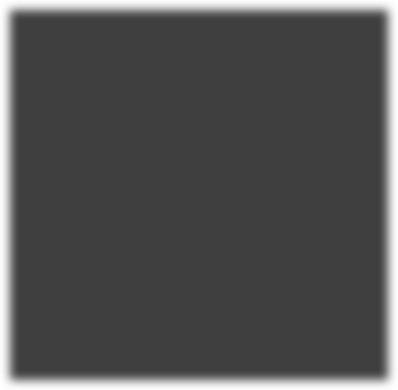
**Filezilla**

FTP est un standard ouvert, ce qui veut dire que n’importe qui peut créer un logiciel FTP. Il existe plusieurs dizaines de clients, certains payants, d’autres gratuits. FileZilla est très populaire, gratuit et open source (http://filezilla-project.org). C’est celui qui est présenté ici.

Il existe aussi des dizaines de serveurs FTP. La plupart sont conçus pour Windows et/ou le monde Unix et

Linux. En open source, il y a FileZilla Server (http://filezilla-project.org).

Voici l’écran de FileZilla Client :

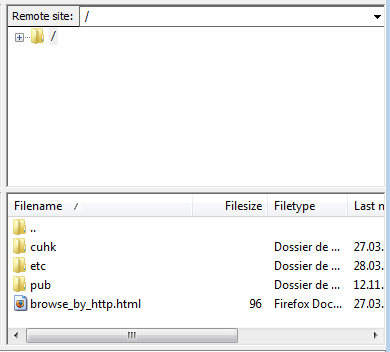
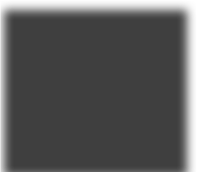
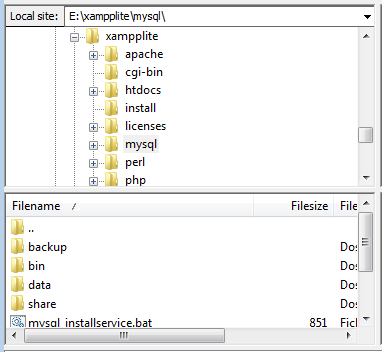
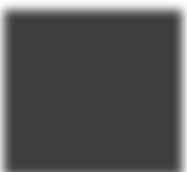


Les écrans de la plupart des clients FTP ont en gros la même structure, avec, à gauche, le répertoire où l’on se situe localement (appelé local site par FileZilla), et, à droite, l’endroit où le serveur nous accueille

(remote site). Le programme aﬀiche également le journal des requêtes du client et des réponses du serveur

(en haut) ainsi que des statistiques sur les transferts (en bas).

**Le site local Le site distant**



Pour transférer des fichiers, il suﬀit de sélectionner les fichiers ou les répertoires qu’on veut télécharger dans la zone Local site puis de les faire glisser avec la souris dans la zone Remote site ou de cliquer sur la commande Upload (on y accède en cliquant avec le bouton droit sur les fichiers sélectionnés). Dans d’autres clients FTP, on peut aussi cliquer sur une flèche aﬀichée dans la zone de séparation entre le site local et le site distant.

Attention, les fichiers sont automatiquement copiés dans le répertoire courant du site distant. Avant de lancer le transfert, il faut donc se rendre dans le bon répertoire cible.

L’inverse est aussi possible : on peut sélectionner des éléments dans le site distant et les télédé-charger sur le site local au moyen de la commande Download.

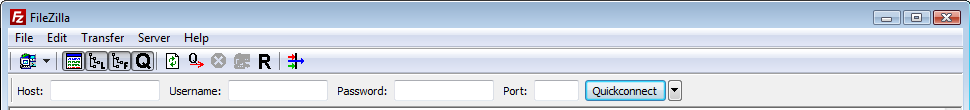
Pour lancer une connexion, il y a deux cas de figure.

1° **FTP anonyme** : on se connecte à un site FTP à accès public. Dans ce cas, on n’a pas besoin de donner un nom et un mot de passe, il suﬀit d’indiquer l’adresse de la machine où se trouve le serveur FTP. Par exemple, on se connecte au site FTP public de l’université du Texas en tapant ftp.utexas.edu dans la barre Quickconnect. Les autres champs se remplissent automatiquement : le nom d’utilisateur est anonymous, le port a la valeur 21 et le mot de passe prend une valeur quelconque (normalement, on est censé indiquer son adresse d’e-mail).



2° **FTP « normal »** : on se connecte à un site à accès protégé par nom et mot de passe. Dans ce cas, il faut indiquer l’adresse de la machine, le nom d’utilisateur et le mot de passe. On peut le faire dans la barre Quickconnect, mais les informations données de cette manière ne seront pas enregistrées, ou créer une connexion qui va être sauvegardée.

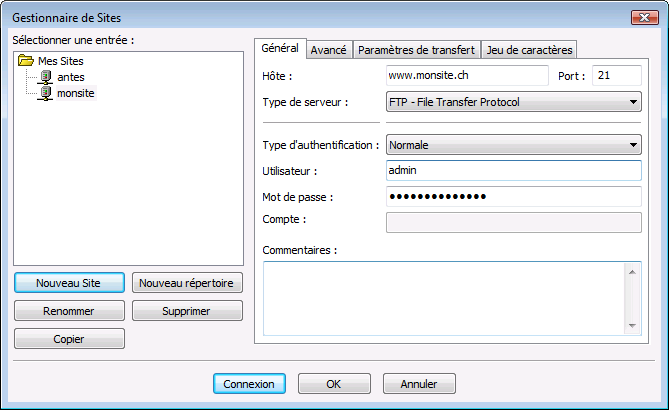
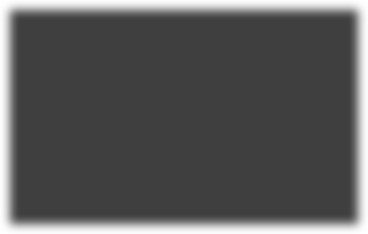
Pour cela, on clique sur l’icône tout à gauche qui représente un ordinateur :



Cela ouvre une fenêtre appelée Site Manager qui permet d’enregistrer les sites FTP qu’on fréquente régulièrement. C’est, en gros, l’équivalent des marque-pages de Firefox.

**Le site manager**

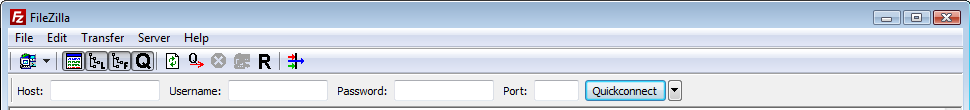
La fenêtre suivante s’aﬀiche :



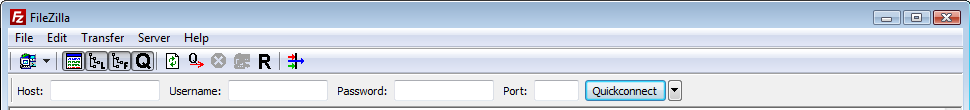
Si on sélectionne Mes Sites en haut à gauche, le bouton Nouveau Site devient actif. En cliquant dessus, on peut créer un nouveau site. L’Hôte est le serveur distant (par exemple : www.monsite.ch), le port est 21 (sauf exception), le Type de serveur FTP - File Transfer Protocol et le Type d’authentification Normale (ou Anonyme si c’est un accès anonyme). L’Utilisateur est le nom d’utilisateur et le Mot de passe le mot de passe. Ces deux informations ont été données auparavant par l’administrateur du site distant (sauf si c’est un accès anonyme).

Une fois ces informations remplies, on clique sur OK pour les enregistrer, Annuler pour annuler les modifications ou Connexion pour les enregistrer et lancer directement la connexion.

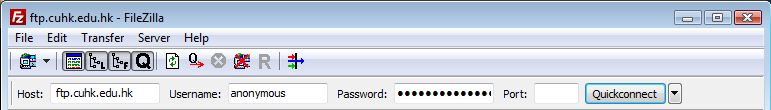
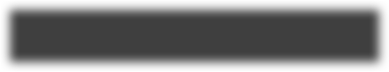
Dorénavant, un clic sur la flèche à droite de l’icône de l’ordinateur aﬀiche la liste des sites enregistrés et un clic sur le nom désiré lance la connexion.



Une icône utile est le R. Elle permet de se reconnecter au dernier serveur en un seul clic. Le raccourci de clavier Ctrl-R a le même eﬀet.



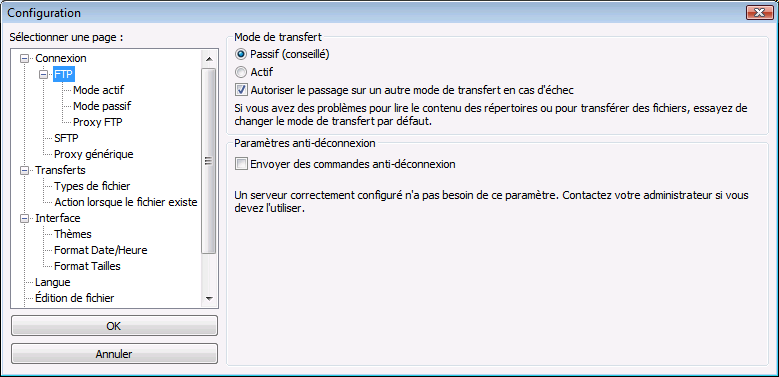
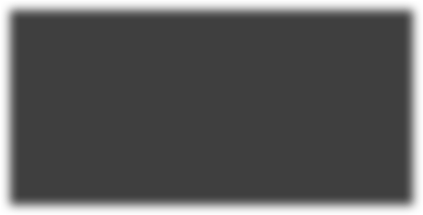
Pour arrêter l’opération en cours, on fait Ctrl-C. Pour fermer la connexion, on fait Ctrl-D ou on clique sur l’icône située à gauche du R.



Si le programme d’administration du site distant est cPanel, le répertoire qui tient lieu de répertoire racine sur le serveur distant est normalement public\_html (c’est le cas classique si le serveur fonctionne sous Linux). Si c’est Plesk, c’est httpdocs (sous Windows) ou parfois www ou html tout court.

**Les problèmes classiques**

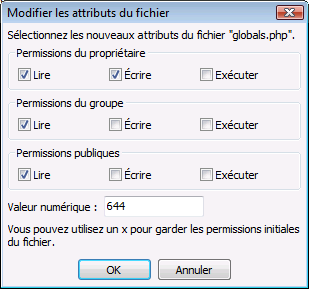
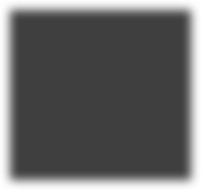
**Pare-feu** – Si on a un problème de fonctionnement, c’est souvent un problème de pare-feu. Aller dans le menu Édition → Configuration et vérifier sous FTP que le mode passif est activé et la case Autoriser le passage sur un autre mode de transfert en cas d’échec est cochée.



Permissions d’accès – Un autre problème classique est un choix inadapté des permissions d’accès sur les fichiers du site distant.

Un clic droit sur un nom de fichier ou de répertoire du site distant donne accès au menu contextuel, dont la dernière ligne est la commande Attributs du fichier.

Il y a trois possibilités : lire, écrire et exécuter, qui se donnent à trois communautés d’utilisateurs : le pro- priétaire du fichier ou du répertoire, le groupe auquel le propriétaire appartient et l’ensemble des utili- sateurs (Permissions publiques).



Dans le cas d’un site, l'administrateur doit souvent avoir les droits de lecture, écriture et exécution sur les fichiers et réper- toires du site pour que tout fonctionne correctement.

**Racine** – Dans le cas d’un site web, les fichiers doivent être placés au bon endroit : public\_html, httpdocs ou autre.

**Noms de fichiers** – Contrairement à Windows, les systèmes d'exploitation du monde Unix et Linux ne confondent pas les majuscules et les minuscules. Par exemple, le fichier configu- ration.php et le fichier Configuration.php sont deux fichiers diﬀérents. Or on a souvent des problèmes de fonctionnement avec Linux si on y transfère des fichiers Windows dont le nom comporte des majuscules.

Par précaution, il faut donc utiliser uniquement des minuscules dans tous les noms de fichiers.

**Une ouverture de session**

Voici un exemple d’ouverture de session :

Status: Resolving IP-Address for FTP.cuhk.edu.hk

Status: Connecting to 137.189.4.14:21…

Status: Connection established, waiting for welcome message…

Response: 220-For anonymous FTP users, please use 'anonymous' as the login name and your

Response: e-mail address as the password. Response: 220 \*\*\*Welcome to CUHK FTP Server\*\*\* Command: USER anonymous

Response: 331 Anonymous login ok, send your complete email address as your password.

Command: PASS \*\*\*\*\*\*\*\*\*\*\*\*\*\*

Response: 230-Welcome to the Chinese University FTP server FTP.cuhk.edu.hk. You are user

Response: number 363 out of a possible total of 800 users. For beginners, login as Response: "FTP", and give your eaddr (e.g. s123456@mailserv.cuhk.edu.hk) as password. Response:

Response: Comments? Pls email to [FTPadmin@FTP.cuhk.edu.hk.](mailto:FTPadmin@FTP.cuhk.edu.hk) Response: 230 Anonymous access granted, restrictions apply. Command: SYST

Response: 215 UNIX Type: L8

Command: FEAT Response: 211-Features: Response: MDTM

Response: REST STREAM Response: SIZE

Response: 211 End

Status: Connected

Status: Retrieving directory listing… Command: CWD /

Response: 250 CWD command successful

Command: PWD

Response: 257 "/" is current directory. Command: TYPE I

Response: 200 Type set to I

Command: PASV

Response: 227 Entering Passive Mode (137,189,4,14,215,6). Command: LIST

Response: 150 Opening ASCII mode data connection for file list

Response: 226 Transfer complete. Status: Directory listing successful

Les trois premières lignes rendent compte de la connexion. Ensuite commence le dialogue entre le serveur distant et le client local.

Le serveur : « service prêt pour le nouvel utilisateur » (c’est ce que veut dire le nombre 220) et annonce que l’utilisateur doit utiliser le nom d’utilisateur anonymous et son adresse de messagerie comme mot de passe.

Le client répond avec la commande USER (nom d’utilisateur) et le paramètre anonymous. Le serveur : « nom d’utilisateur OK, mot de passe demandé » (c’est le nombre 331).

Le client répond avec la commande PASS (mot de passe) et son adresse de messagerie. Le serveur : « utilisateur connecté, continuer » (c’est le nombre 230).

… et ainsi de suite.

La liste complète des codes et de leur signification se trouve dans la RFC 959. Il y en a cinq catégories :

• 1⁇ : réponse préliminaire positive ;

• 2⁇ : réponse positive indiquant que la dernière commande s’est terminée avec succès ;

• 3⁇ : réponse intermédiaire positive. Une autre commande doit être envoyée ;

• 4⁇ : réponse négative non définitive. L’action demandée n’a pas été eﬀectuée mais elle peut être tentée à nouveau ;

• 5⁇ : réponse négative définitive.

**Commandes principales**

Il existe une bonne trentaine de commandes, mais elles ne s’emploient pas toutes. Voici une liste des plus importantes :

ABOR interrompre le transfert

BYE ou QUIT ou ! terminer la connexion et quitter FTP

CDUP se déplacer dans le répertoire père sur le serveur distant

CWD changer de répertoire sur le serveur distant

DELE eﬀacer le fichier ou le répertoire spécifié sur le serveur distant

HELP aide sur les commandes

LIST ou LS ou DIR aﬀicher le contenu du répertoire courant sur le serveur distant

MGET récupérer plusieurs fichiers ou répertoires

MKD créer un répertoire

MODE spécifier le mode de transfert

MPUT envoyer plusieurs fichiers ou répertoires

NLST envoyer au client le contenu d’un répertoire situé sur le serveur

PASS donner un mot de passe (cette commande suit forcément la commande USER) PORT indiquer le port sur lequel le client attend une requête de connexion

PWD aﬀicher le nom du répertoire courant sur le serveur distant

RETR ou GET télédécharger un fichier ou un répertoire (download) RMD eﬀacer un répertoire

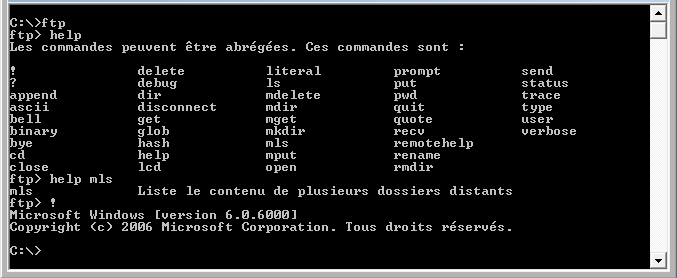
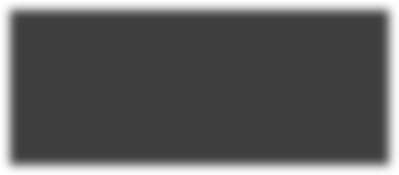
SEND ou PUT télécharger un fichier (upload)

STOR charger un fichier ou un répertoire sur le serveur distant en écrasant le fichier ou le répertoire existant s’il existe

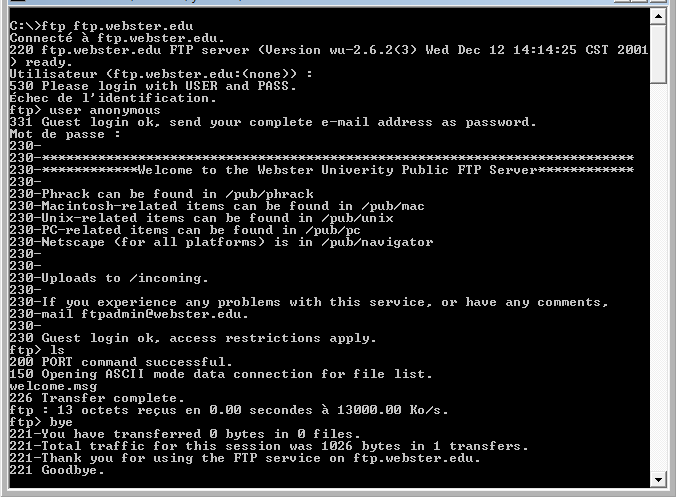
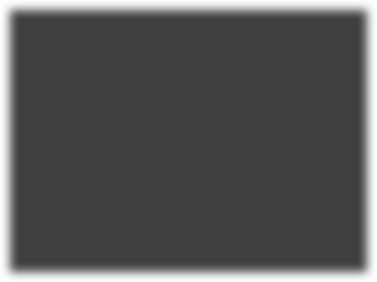
TYPE définir le type de transfert par rapport au type de fichier (texte ou binaire)

USER donner le nom de l’utilisateur

Voici la liste des commandes FTP disponibles dans Windows (l’invite ftp> indique qu’on est dans FTP). La commande help nom\_commande donne une brève description de la commande spécifiée.



En fait, les programmes FTP comme FileZilla ou CuteFTP ne sont que des interfaces graphiques qui se greﬀent par-dessus le logiciel FTP inclus dans le système d’exploitation qu’on utilise. On peut parfai- tement travailler « en direct », depuis l’interface de commandes de Windows :



**FTP et les pare-feu**

Les programmes FTP déplaisent aux pare-feu parce qu’ils ouvrent des ports choisis au hasard. Or les pare- feu se chargent justement de bloquer les ports inutilisés pour éviter de laisser des portes grandes ouvertes aux intrus. La seule solution consiste à utiliser un pare-feu qui « comprend » le protocole FTP et qui est capable de diﬀérencier un échange de données FTP normal et une tentative d’intrusion, et à le paramétrer en ce sens — mais cela prend du temps et n’est pas tout simple.

Comme le mode actif pose plus de problèmes aux pare-feu que le mode passif, il faut préférer le second. En fait, on n’a souvent pas le choix : sur beaucoup de sites, le mode actif ne fonctionne tout simplement pas parce que le pare-feu prend le flux FTP entrant pour une connexion et le bloque.

N.B. : ce problème concerne les entreprises dont le pare-feu est un dispositif indépendant installé à l’entrée du réseau. Il ne concerne pas la plupart des particuliers et des très petites entreprises, dont le pare-feu se présente généralement sous la forme d’un logiciel installé sur le poste de travail. Ce type de pare-feu réagit en demandant à l’utilisateur s’il autorise ou non le transfert. Il suﬀit de répondre aﬀirmativement.

**La confidentialité**

FTP a été créé avant que les problèmes de sécurité ne polluent les échanges informatiques si bien que le protocole n’oﬀre aucun dispositif de sécurité intrinsèque. En particulier, il transmet les mots de passe en clair. C’est d’autant plus ennuyeux qu’on a tendance à utiliser partout les mêmes mots de passe, ce qui veut dire qu’un pirate qui intercepte un mot de passe FTP obtient souvent l’accès à d’autres systèmes.

On peut cependant sécuriser les échanges FTP en les plaçant à l’intérieur de paquets IPsec ou en utilisant une autre solution de transfert de fichiers. Un exemple est SSH (secure shell), aussi appelé SFTP (SSH FTP), ce qui provoque une confusion avec… SFTP (simple file transfer protocol), une version simplifiée de FTP. SSH n’a rien à voir avec FTP, mais il peut s’employer pour transférer des fichiers de manière sécurisée.

Une autre solution consiste à utiliser FTPS (file transfer protocol over secure sockets Layer), qui s’appuyait sur SSL (d’où le S dans FTPS), mais qui utilise maintenant le successeur de SSL 26 : TLS (transport layer security).

Pour simplifier ce fouillis, disons que FTPS est une extension sécurisée de FTP alors que SSH est un protocole de conception diﬀérente qui va bien au-delà du transfert de fichiers. Il permet notamment d’exécuter des commandes à distante. Par défaut, un utilisateur qui se connecte par SSH peut donc faire beaucoup plus de choses (et donc de dégâts) qu’une personne qui emploie FTPS, et il est diﬀicile de

« désarmer » SSH. Il vaut donc mieux utiliser FTPS, d’autant que beaucoup de machines sur lesquelles

tourne un serveur FTP ont été dotées de FTPS. SSH est moins répandu.

En revanche, si l’utilisateur doit non seulement transférer des fichiers mais aussi eﬀectuer des tâches d’administration de serveur, il faut choisir SSH.

26 TLS 1.0 est SSL 3.1.

**8. Commandes de réseau**

Les commandes sont indispensables aux administrateurs de réseaux, qui n'ont ni le temps ni l'envie d'aller dans l'interface graphique de chacune des machines qu'ils ont à gérer, mais elles sont aussi très utiles aux autres informaticiens.

Pour travailler avec des commandes, il faut se rendre dans l'**interface de commandes** ou **CLI** (Command

Language Interface) ou encore **shell**. Sous Windows, il y a deux possibilités :

• Démarrer → Tous les programmes → Accessoires → Invite de commande ;

• Démarrer → Exécuter puis taper cmd.exe (si cette fonction est absente, l'activer en faisant un clic droit sur l'icône du menu Démarrer, aller dans Propriétés → Menu Démarrer → Personnaliser et cocher la ligne Commande Exécuter.

Sous Mac OS, c'est :

• *Finder* → *Applications* → *Utilitaires* → *Terminal.app*.

Sous Linux, le chemin des menus varie d'une interface graphique à l'autre :

• Gnome : Applications → Accessoires → Terminal ;

• KDE : Outils → Konsole ;

Mais le plus rapide consiste à cliquer sur l'icône d'un écran noir sur la barre des tâches — si cette icône existe. On peut aussi taper Alt-Ctrl-F1 (pour revenir, c'est Alt-Ctrl-F7) ou faire un clic droit sur le fond de l'écran et sélectionner Ouvrir un terminal dans le menu qui apparaît.

**Quand une commande ne passe pas**

Si une commande ne semble pas fonctionner, vérifier en premier lieu qu'on l'a tapée correctement. Les principales causes de problèmes sont :

• un espace là où il ne fallait pas en mettre ;

• un espace manquant ;

• une faute de syntaxe, par exemple une majuscule au lieu d'une minuscule ;

• une erreur d'environnement (exemple : ifconfig ou ipconfig).

La commande ifconfig existe dans tous les systèmes d'exploitation, à l'exception de Windows, où elle est remplacée par ipconfig.

Dans le monde Unix (Linux, BSD, Mac OS, etc.), les options se présentent le plus souvent sous la forme de lettres précédées d'un tiret alors que Windows utilise — normalement — le slash. Ainsi, la commande Unix

ifconfig -a se traduit sous Windows par ipconfig /all. Par contre, la commande Windows netstat utilise des tirets comme dans le monde Unix.

En ce qui concerne l'espace, se souvenir que ce n'est pas un caractère normal mais un **caractère de com- mande** : il sert de séparateur entre les paramètres des commandes. Il ne devrait donc jamais être utilisé à l'intérieur d'un nom.

La combinaison de touches **Ctrl-C** est importante : elle permet d'arrêter une commande en cours d'exécution et de retourner à l'invite de commande (c'est le caractère ASCII n°3, End of text, aussi appelé Break).

**ping**

La commande **ping** est peut-être la plus utile de toutes. Elle sert à tester la connectivité avec le réseau de l'ordinateur ou à vérifier si une machine distante est accessible.

Quand on ne parvient pas à se connecter au réseau, voici les trois commandes à utiliser (dans cet ordre) :

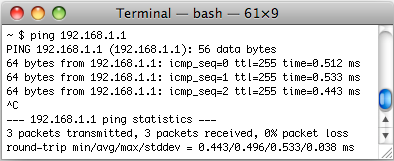
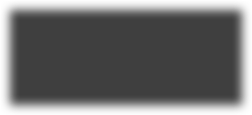
**ping 127.0.0.1**! ! ← la configuration du réseau de mon ordinateur est-elle OK ?

**ping 192.168.1.1**!! ← le réseau local est-il OK ?

**ping 88.221.62.198**! ← le réseau distant est-il OK ?

L'adresse 127.0.0.1 est par définition celle de l'interface de réseau de l'ordinateur sur lequel on tape la commande (au lieu de ping 127.0.0.1, on peut taper ping localhost, c'est un synonyme).

En tapant la première commande, on demande à l'interface si elle est bien en état de marche. Si on obtient une réponse, c'est que tout va bien (la réponse est du genre « 4 packets transmitted, 4 packets received, 0% packet loss »).



Dans la deuxième commande, il faut remplacer l'adresse 192.168.1.1 par celle du routeur (qui est souvent 192.168.1.1 dans les réseaux de petite taille).

Pour connaître cette adresse, on peut utiliser la commande traceroute (tracert sous Windows), qui aﬀiche la liste des routeurs par lesquels le paquet de

données passe entre la machine qu'on utilise et une machine cible quelconque. Ici, c'est le routeur de

l'IEEE ([http://www.ieee.org/portal/site),](http://www.ieee.org/portal/site)) qui a l'adresse 88.221.62.198. Le premier routeur de la liste est le nôtre.



Dans la troisième commande, n'importe quelle adresse distante fait l'aﬀaire. Ce qui importe, c'est de voir si on a accès au monde

extérieur. Attention, toutefois, certains routeurs sont paramétrés pour ignorer les requêtes ping, cela pour des raisons de sécurité. Un insuccès ne signifie donc pas forcément qu'il y a un problème.

La commande ping existe dans tous les systèmes d'exploitation usuels (Windows, Linux, Mac OS, Solaris, HP-UX, z/OS, etc.). Elle utilise le protocole ICMP, qui concerne la couche 3 OSI.

**traceroute**

La commande **traceroute** (Linux, Mac OS, BSD, Solaris, HP-UX, z/OS, etc.) ou **tracert** (Windows) sert à suivre l'itinéraire entre l'hôte source et un hôte distant.

En cas de ralentissement du trafic, elle sert à voir à quel endroit se situe le problème. Il est particulièrement utile de savoir si c'est sur le réseau local ou sur le WAN puisque, dans le premier cas, on peut prendre des mesures pour résoudre le problème. Dans l'exemple qu'on a vu plus haut, il a fallu 0,592 milliseconde pour atteindre le routeur, ce qui veut dire que tout va bien.

Comme ping, traceroute utilise le protocole ICMP.

**ifconfig**

La commande **ifconfig** (Linux, Mac OS, BSD, Solaris, HP-UX, z/OS, etc.) ou **ipconfig** (Windows)

s'emploie pour aﬀicher et modifier la configuration de l'interface du réseau.

Pour être précis, ipconfig (Windows) ne permet que de voir les informations. Par contre, ifconfig (Unix) permet aussi de les modifier. En conséquence, c'est une commande beaucoup plus utile dans le monde Unix.

Sous Windows, la commande **getmac** aﬀiche la ou les adresses MAC de l'ordinateur.

**host**

La commande **host** aﬀiche les informations de base sur un URL (Uniform Resource Locator), c'est-à-dire sur un nom de ressource comme [http://www.ieee.org.](http://www.ieee.org/)

Comme les commandes précédentes, elle accepte les adresses IP comme les URL. Par exemple, la commande host 88.221.62.198 est synonyme de host [www.ieee.org.](http://www.ieee.org/)

Le type n'est pas toujours http. Il y a aussi ftp, https, etc. Par exemple, l'URL ftp://cdimage.ubun-tu.com/

cdimage donne accès aux images ISO des versions d'Ubuntu. Elle n'existe pas sous Windows.

**dig**

La commande **dig** est similaire à host, mais elle est beaucoup plus riche en options. Elle est très pratique pour diagnostiquer un problème de DNS (Domain Name System).

Elle succède à nslookup, qui est obsolète. Elle n'existe pas sous Windows.

**netstat**

La commande **netstat** aﬀiche les connexions avec l'extérieur.

Elle s'emploie pour diagnostiquer un problème de communication. Par exemple, si la connexion avec l'Internet ralentit fortement, netstat peut permettre de voir où se situe le goulet d'étranglement.

Cette commande peut aussi servir à démasquer un programme malveillant (pour autant qu'il ne truque pas l'aﬀichage de netstat). Si on est un néophyte, il vaut mieux fermer tous les autres programmes pour éviter d'avoir à trier le bon grain de l'ivraie dans une longue liste de connexions.

**finger**

La commande **finger** aﬀiche les utilisateurs de la machine spécifiée ainsi qu'un certain nombre d'infor- mations sur eux. Elle est donc très utilisée par les pirates.

**telnet et ssh**

Les commandes **telnet** et **ssh** permettent de se connecter à une machine distante et d'utiliser toutes les commandes normales. En réalité, ce ne sont pas des commandes, mais des environnements d'exécution dans lesquels on tape des commandes (open, set, quit, etc.).

Si on sort du réseau local, il vaut mieux éviter telnet parce que la connexion n'est pas sécurisée.

Avec la majorité des distributions Linux et Mac OS, ssh est inclus et prêt à l'emploi (il s'agit d'OpenSSH, http://www.openssh.org). Avec Windows, il faut installer un logiciel tiers comme PuTTY (client) et freeSSHd (serveur).

**ftp**

Pour transférer des fichiers, on utilise généralement **ftp** (File Transfer Protocol). Il s'utilise pour l'upload

comme pour le download.

Comme telnet et ssh, c'est un environnement d'exécution dans lequel on tape des commandes (user, pass,

cwd, pwd, get, type, ls, quit, etc.). Comme dans le cas de telnet et ssh, ce sont des commandes Unix.

Il existe des frontaux graphiques qui isolent l'utilisateur des commandes ftp (Filezilla est un exemple), mais, si on connaît le mode par commandes, on peut transférer des fichiers sur n'importe quel ordinateur. Sinon, on doit d'abord installer le logiciel graphique dont on a l'habitude, pour autant qu'il existe sur la plate-forme concernée.

**net view, net share**

La commande **net view** permet d'aﬀicher la liste des serveurs du réseau et celle des partages. Par exemple, net view /domain donne la liste de tous les partages du domaine. La commande **NET SHARE** permet de gérer les partages.

Elles n'existent que sous Windows.

**net use**

La commande **net use** permet de se connecter à un partage. Par exemple, net use n: \\ser-veur1\share /p:yes

joint le partage spécifié sous le nom de N: et rend le lien persistant (p). Elle n'existe que sous Windows.

**net user, net accounts, net group**

Les commandes **net user** et **net group** permettent de gérer les comptes et les groupes d'utilisateurs.

**Net accounts** permet de gérer certains paramètres des comptes. Ainsi, net accounts /minpwlen:9 /domain

interdit les mots de passe de moins de 9 caractères.

Elles n'existent que sous Windows, mais la commande useradd permet d'ajouter un utilisateur sous Linux. Il y a aussi les commandes users, who et w qui permettent d'aﬀicher des informations sur les utilisateurs sous Linux et Mac OS.

**Automatiser les commandes**

Beaucoup de commandes d'administration sont utiles si elles s'exécutent tous les soir, ou à chaque fois qu'un utilisateur se connecte ou se déconnecte. Cela nécessite l'emploi de **daemons** ou « génies » (mais c'est le mot « démon » qui s'emploie par confusion entre les mots anglais demon et daemon).

Les daemons sont des services, c'est-à-dire des programmes qui tournent en arrière-fond, sans inter- vention de l'utilisateur, et se réveillent à intervalle régulier ou à la suite d'un événement pour accomplir une tâche donnée.

Sous Windows, la commande **schtasks** (schedule tasks) sert à cela.

Dans la famille Unix et Linux, on peut utiliser **cron** (chronograph). Les données utilisées par cron pour savoir quand s'activer se trouvent dans la table **crontab** (cron table).

Sous Mac OS et FreeBSD, **launchd** (launch daemon) est préférable à cron.

**Une remarque juridique**

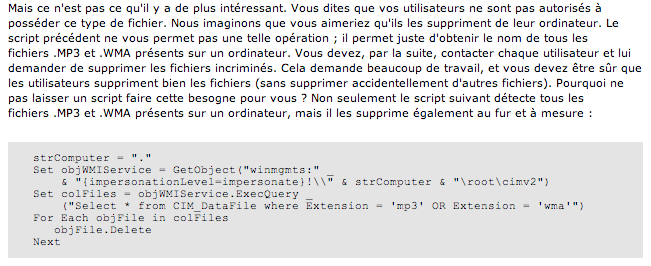
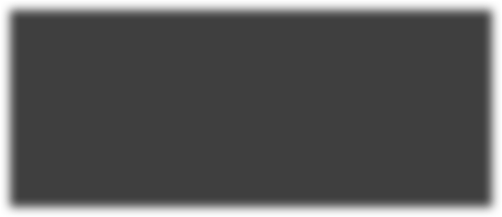
En matière de commandes et de scripts, il y a ce que la technique permet et il y a ce que le droit autorise. Par exemple, en Europe, le salarié a droit au respect de sa vie privée et donc au secret de sa correspon- dance privée, y compris sur son lieu de travail.

À Paris, la Cour de cassation a jugé le 2 octobre 2001 dans l'aﬀaire Nikon que le salarié a droit à la confi- dentialité de ses messages personnels 27 :

le salarié a droit, même au temps et au lieu de travail, au respect de sa vie privée ; celle-ci implique en parti- culier le secret de ses correspondances ; l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié ou reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.

Ce droit est manifeste si le champ Objet du message comprend un mot comme « personnel » ou « privé », mais il est également protégé par toute autre expression de nature personnelle, par exemple « ci-joint la vidéo de l'anniversaire de Junior » 28 .

Le problème est que les auteurs des scripts d'administration de système qu'on trouve sur le web ne con- naissent souvent pas le droit. Ainsi, un administrateur nommé AK demande à Microsoft comment il peut savoir si ses utilisateurs possèdent certains fichiers, par exemple des MP3 ou des WMA. Voici un extrait de la réponse 29 :



Si on fait cela, on est doublement dans l'illégalité. En Europe, on n'a ni le droit de rechercher des fichiers privés sur les volumes des utilisateurs, ni de les détruire.

27 Bulletin, 2001, V, n°291, p. 233.

28 Pour plus d'informations, voir le site de la CNIL et notamment le document <http://www.cnil.fr/les-themes/travail/fiche->pratique/article/le-controle-de-lutilisation-dinternet-et-de-la-messagerie/.

29 Source : [http://technet.microsoft.com/fr-fr/library/ﬀ952783.aspx.](http://technet.microsoft.com/fr-fr/library/%EF%AC%80952783.aspx)

Aux États-Unis, en revanche, le droit à la vie privée est minimal, et cela pose un problème en Europe parce que certaines filiales européennes de firmes américaines adoptent la politique que leur direction générale a décidée. Si, par exemple, une charte informatique avertit les employés que leurs messages électroniques sont archivés à long terme et peuvent être contrôlés à tout moment, l'obligation légale d'informer les employés à l'avance est respectée, mais cette façon de faire peut contrevenir à certaines dispositions du droit du travail. Par exemple, en France, le code du travail impose explicitement le respect du principe de proportionnalité en cas de restrictions des libertés individuelles (art. L 120-2).

Le droit international protège la vie privée, mais dans des termes peu solides. Le Pacte international relatif aux droits civils et politiques interdit les immixtions dans la vie privée et la correspondance, mais seu- lement si elles sont « arbitraires ou illégales » (art. 17 § 1). Cela veut dire qu'il suﬀit que le parlement adopte une loi qui autorise les employeurs à espionner leurs employés pour que ces immixtions deviennent ipso facto légales. Il ne reste alors que la protection contre l'arbitraire, mais, à cause de la séparation des pouvoirs, beaucoup de juges hésiteront à déclarer arbitraire une loi qui a été adoptée valablement par le pouvoir législatif.

On a eu un exemple réel de légalisation d'actes criminels quand le président Bush fils a légalisé la torture 30, avec l'appui du juge Scalia, doyen de la Cour suprême des États-Unis 31 .

30 « Legalizing Torture », The Washington Post, 9 juin 2004, p. A20.

En 2014, un rapport de 6'000 pages du Select Committee on Intelligence du Sénat américain a montré que ces actes étaient non seulement illégaux et immoraux, mais peut-être même nuisibles à la sécurité : leurs victimes ont souvent raconté n'importe quoi juste pour interrompre les mauvais traitements et les enquêteurs ont perdu énormément de temps à suivre de fausses pistes. Ce temps aurait été mieux employé à travailler sur de vraies menaces.

31 « "La torture pas anticonstitutionnelle", dit le doyen de la Cour suprême US », RTS Info, <http://www.rts.ch/info/monde/6378744->la-torture-pas-anticonstitutionnelle-dit-le-doyen-de-la-cour-supreme-us.html, 12 décembre 2014.

Les réseau x i nfo rmat i q u es 76 h tt p // www jaqu et .o rg, mai 21115

**9. La sécurité du réseau local**

Depuis que les réseaux d’entreprises sont reliés au monde extérieur par une liaison informatique, on assiste à des tentatives d’intrusion par des personnes malveillantes.

Grâce aux logiciels robots qui scannent l'Internet à l'aveugle, chaque entreprise est l'objet de plusieurs milliers d'attaques par jour.

**L'essentiel en bref**

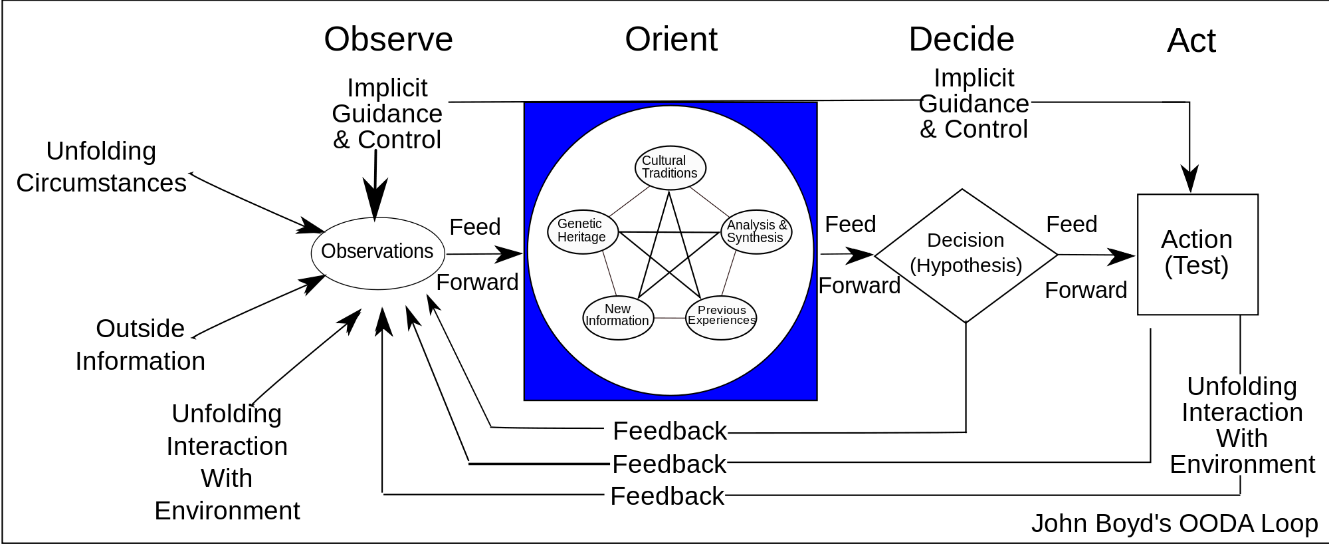
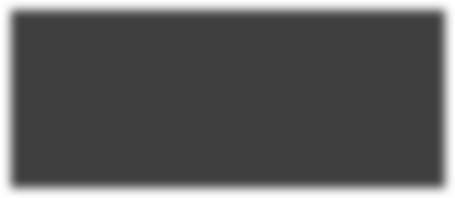
Aucun système matériel et logiciel de sécurité n'est eﬀicace s'il n'est pas le résultat d'une **politique de sécurité** bien conçue et bien mise en œuvre.

Il faut penser au principe du **KISS** (Keep It Simple, Stupid!, « Fais au plus simple, idiot ! »). Un système de sécurité qu'on maîtrise mal est un système de sécurité qui risque de présenter des failles indétectées.

**La boucle de Boyd**

En sécurité, la boucle de Deming (planifier → faire → vérifier → agir) n'est pas suﬀisamment rapide. À la place, on peut utiliser la **boucle de Boyd**, qui été conçue par le colonel américain John Boyd pour les opérations militaires, mais qui s'applique bien à la sécurité des réseaux. On l'appelle aussi boucle OODA

(observer → s'orienter → décider → agir) 32 .



32 Wikipedia, [http://en.wikipedia.org/wiki/OODA\_loop,](http://en.wikipedia.org/wiki/OODA_loop) 27 mars 2012.

La boucle de Boyd peut être rapide si la phase d'orientation l'est elle-même. Quand on se fait attaquer par le réseau, il peut arriver que l'action doive être prise dans les minutes qui suivent l'alerte.

Il n'y a pas de durée minimale alors que la boucle de Deming est bien adaptée à un cycle variant entre quelques mois et un an.

**Moyens techniques**

Les principaux moyens techniques de sécurité des réseaux sont les pare-feu (firewalls), les NIDS (Network Intrusion Detection Systems), les systèmes AAA (Authentification, Authorization, Accounting) et les pro- grammes anti-malware.

Le **pare-feu** est un logiciel de sécurité qui se trouve soit dans son propre boîtier (firewall appliance), soit dans un autre système intermédiaire (souvent un routeur), soit dans un ordinateur (généralement Linux ou BSD).

Le but du pare-feu est d'autoriser seulement le trafic légitime et de bloquer les paquets frauduleux. Le blocage concerne les paquets suivants :

• ceux dont l'adresse IP n'est pas acceptée (niveau 3 OSI) ;

• ceux qui ne font pas partie d'une session légitime (niveaux 4 et 5) ;

• ceux qui n'emploient pas un protocole prévu, qui tentent de passer par un port anormal ou qui manifestent un autre comportement équivoque (niveaux 5 et 7).

Le tri peut se faire de deux manières : sur **liste noire** (tous les paquets sont acceptés sauf ceux qui pro- viennent d'une source qui est dans la liste) ou sur **liste blanche** (tous les paquets sont refusés sauf ceux qui proviennent d'une source qui est dans la liste).

Un pare-feu peut être installé dans un **proxy**. Un proxy est un ordinateur qui masque le réseau interne et agit comme s'il était la machine destinatrice alors qu'il n'est qu'un relais.

Le **NIDS** est un logiciel qui analyse le trafic entrant et sortant pour tenter de repérer les activités malveillantes. Il journalise les activités suspectes et envoie un message d'avertissement à la personne qui administre le réseau ou au logiciel d'administration du réseau s'il découvre un problème. Il se trouve à l'entrée du réseau et éventuellement à d'autres endroits du réseau.

Il est complété par des HIDS (Host-based Intrusion Detection Systems), qui sont, eux, sur des serveurs.

Le NIDS est diﬀérent du pare-feu. Si un paquet suspect est repéré par un pare-feu, il est rejeté en silence et il n'entre pas dans le LAN. L'action du pare-feu est préventive. Le NIDS, lui, est curatif. Il se trouve dans le réseau. S'il repère un paquet, cela signifie que le pare-feu ne l'a pas décelé et qu'il l'a laissé entrer dans le LAN..

Le serveur **AAA** est un logiciel qui assure l'authentification de l'expéditeur d'un paquet, gère ses permissions d'accès à la ressource destinataire et journalise les événements (date et heure de la demande d'accès, identité de l'expéditeur, identité du destinataire, etc.). **Radius** est un exemple.

On peut installer une **DMZ** (DeMilitarized Zone) entre le WAN et le LAN. Cette protection est la meilleure, mais aussi la plus coûteuse. Elle sert à mettre dans une zone tampon les ressources visibles de l'extérieur.

Une DMZ n'a pas de sens si aucune ressource ne doit être visible de l'extérieur. Dans une petite entreprise, le serveur de messagerie et le site web sont tous deux chez un ISP (Internet Services Provider). C'est chez l'ISP qu'il faudra mettre une DMZ en place, pas dans l'entreprise en question.

**Les types de malware**

Le **logiciel malveillan**t ou malware se compose de deux familles de programmes : ceux qui se trans- mettent (contamination) et ceux qui se camouflent quelque part sur le système.

1° Le logiciel transmis par **infection** :

• Le **virus**. Il infecte un fichier. Il se transmet à d'autres fichiers quand on ouvre celui qui est corrompu. Le virus implique donc une action de l'utilisateur.

• Le **ver** (worm). Il est indépendant (pas inclus dans un fichier). Il se transmet automatiquement sans intervention de l'utilisateur.

2° Le logiciel qui se **dissimule** (et qui ne se déplace pas) :

• Le **cheval de Troie** (trojan). C'est du code malveillant qui fait partie intégrante d'un programme apparemment anodin.

• La **porte dérobée** (backdoor). C'est un moyen dissimulé d'entrer dans un programme. C'est souvent un nom d'utilisateur et un mot de passe inscrits « en dur » dans

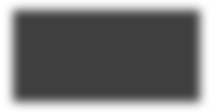
le logiciel.

La situation dans le monde Windows est catastrophique :

• En 2011, on a passé la barre des dix millions de signatures de malware.

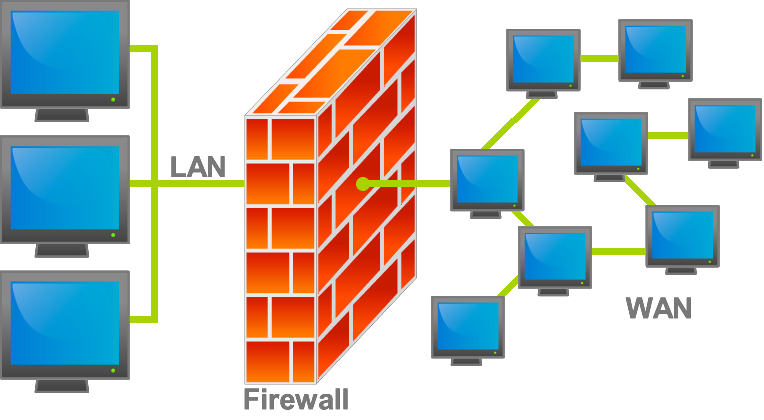
• La moitié des ordinateurs Windows du monde sont infectés par du malware.

• Le **rootkit**. Il modifie le système d'exploitation pour se rendre invisible, ce qui le rend diﬀicile à découvrir et à supprimer.



• Tout **programme indépendant** à but malveillant. Il ne se dissimule souvent que dans la mesure où on ne sait pas quel est son nom et le répertoire où il se trouve.

Des mélanges sont possibles : un ver peut transporter un virus, un cheval de Troie générer un rootkit, etc. Par exemple, Stuxnet se compose d'un ver fonctionnant sous Windows qui sert de véhicule et d'un pro- gramme malveillant qui s'attaque spécifiquement à des contrôleurs industriels Siemens. Ce programme n'est pas capable de se déplacer, il a besoin du ver pour cela.

Actuellement, Windows est le seul système d'exploitation attaqué par tous ces types de malware. Par contre, tous les systèmes d'exploitation peuvent être victimes du malware qui se dissimule puisque tout utilisateur qui a les permissions nécessaires pour installer un logiciel peut installer un logiciel qui contient un cheval de Troie.

Pour empêcher ces tentatives d’aboutir, il est nécessaire de mettre en place une **barrière** devant le réseau. Son rôle consiste à filtrer les paquets de données qui entrent, mais aussi ceux qui sortent (confidentialité).

Cette barrière est le pare-feu. On le place entre le réseau local et le réseau distant (illustration ci-contre) 33.

33 PEDROZO, Pedro, [http://en.wikipedia.org/wiki/File:Firewall.png,](http://en.wikipedia.org/wiki/File%3AFirewall.png) Wikipedia, 24 mai 2014.

l'entreprise, qu'on appelle le **système autonome** (**AS**, autonomous system). La frontière est souvent appelée WAN edge.

**Le pare-feu**

Le **pare-feu** (firewall) est un logiciel de sécurité qui peut fonctionner sur divers types d’équipements :

1. un poste de travail ou un serveur, auquel cas il protège seulement cet ordinateur ;

2. un routeur, auquel cas il protège tout le réseau interne ;

3. un dispositif physique indépendant appelé firewall appliance, auquel cas il protège également tout le réseau interne ;

4. un ordinateur normal tenant lieu de firewall appliance. Il s’agit généralement d’un système Linux ou BSD dit « militarisé » (hardened). Il est configuré pour laisser le moins possible de failles et tous les composants du système d’exploitation qui ne servent pas à la sécurité en sont retirés. Il sert uni- quement de pare-feu.

Les entreprises utilisent le plus souvent les solutions 1 et 2, ou 1 et 3, ou 1, 2 et 3.

Le coût d’une firewall appliance varie typiquement entre 100 et 2'000 euros, mais les grandes entreprises mettent en place une architecture de sécurité intégrée dont le coût peut s’exprimer en centaines de milliers d'euros ou en millions.

Physiquement, une firewall appliance ressemble en général à une lame de rack ordinaire, comme cet équi- pement de LinuxAppliance.net 34 :

Chez Cisco, les pare-feu peuvent être intégrés comme des modules aux routeurs et même aux switches, ou se placer dans des firewall appliances appelées ASA 35 .

Les pare-feu opèrent à plusieurs niveaux :

1° Le filtrage de paquets (packet filtering, niveau 3 OSI)

analyse et autorise — ou non — l'entrée de chaque paquet de données transmis. Il travaille avec les adresses IP. Il est indépendant des applications.

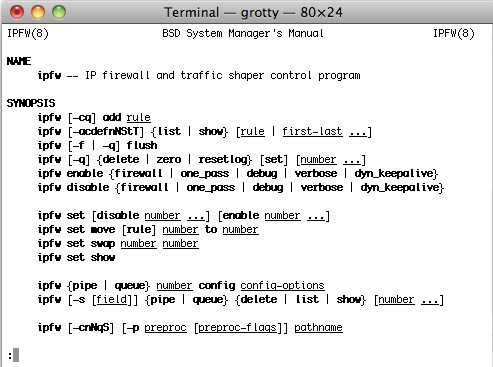
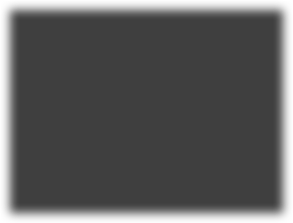
2° L’inspection à état (stateful inspection) analyse le trafic entrant à partir du trafic sortant, ce qui permet de n’autoriser le passage que s’il y a correspondance entre les deux.

Ce service est lié aux sessions (niveau 5 OSI) et concerne le trafic TCP. Pour le filtrage du trafic UDP, le travail se fait en mode sans état (stateless).

34 Source : LinuxAppliance.net, <http://www.linuxappliance.net/firewall/pfsense-firewall-solutions/strongbochs-p100-pfsense->appliance, 24 mai 2014.

35 Présentation de ces systèmes : <http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation->firewalls/data\_sheet\_c78-701659.html.

ipchains.



3° Le filtrage au niveau de la couche Application (niveau 7 OSI) travaille sur les requêtes de connexion des programmes en exécution. Il est com- plémentaire du filtrage sur les ports.

Exemples : SELinux, AppArmor, Grse- curity.

4° Le rôle d’intermédiaire local (proxy), de relais entre le réseau interne et le réseau externe. Le proxy est spécifique à une application.

Les pare-feu comprennent généralement un logiciel de prévention d'intrusion ou **IPS** (Intrusion Detection System).

Fondamentalement, le paramétrage d’un pare-feu se fonde sur deux mécanismes :

• autoriser certains flux de paquets (allow) ;

• bloquer d’autres flux (deny).

On peut opter entre deux politiques de contrôle d’accès : « tout autoriser sauf… » ou « tout refuser sauf… ». Dans le premier cas, c’est le principe de la **liste noire**, et, dans le second, c’est celui de la **liste blanche**. La seconde méthode est évidemment beaucoup plus sûre que la première, mais elle est aussi beaucoup plus bloquante.

Parmi les principaux critères de filtrage utilisés par les pare-feu, il y a :

• l’adresse IP (source et destinataire) ;

• le nom de domaine ;

• le port (source et destinataire) ;

• le protocole (IP, TCP, FTP, HTTP, Telnet, etc.).

Un pare-feu n'est eﬀicace que s'il est bien configuré.



Les principaux dangers dont un pare-feu peut protéger un réseau d’entreprise sont :

• la connexion à distance (remote login) ;

• l’intrusion par une porte dérobée (backdoor) ;

• l’attaque indirecte (zombie), où notre système informatique est utilisé comme intermédiaire pour l’attaque d’un autre système ;

• l’exploitation d’un bug (système d’exploitation, SGBD, application, etc.) ;

• les vers et les chevaux de Troie (mais seulement dans une certaine mesure).

Aujourd'hui, les produits intégrés sont répandus, avec un couplage des fonctions de pare-feu, d'IPS, d'antivirus, etc. L’erreur humaine reste toutefois non couverte (exemple : oublier de désactiver les services inutilisés d’un serveur).

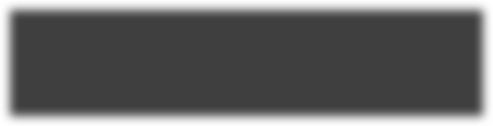
dispositif gratuit bien configuré est plus eﬀicace qu’un dispositif coûteux mal configuré.

Si une entreprise travaille sur plusieurs sites, on peut mettre un pare-feu sur chaque site ou bien un seul pour toute l’entreprise. La première solution coûte moins cher en frais de communication entre sites, mais il existe autant de portes vers l’extérieur qu’il y a de sites.

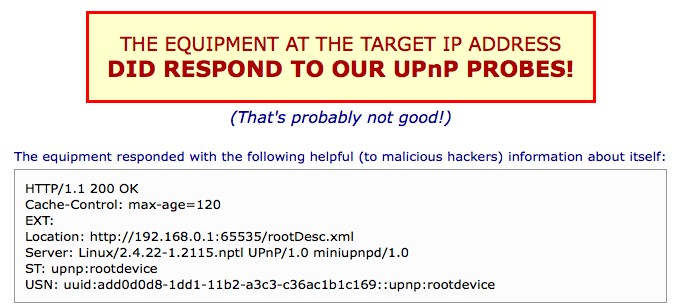
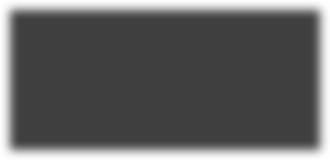
La seconde solution est plus sûre puisqu’il y a une seule porte à surveiller, mais elle nécessite la mise en place d’un système sécurisé de communication entre les sites, par exemple un VPN (Virtual Private Network), qui doit assurer le cryptage et l’authentification des transmissions, au moyen, par exemple, du protocole TLS (Transport Layer Security) ou IPsec (IP security) 36 .

Sur l’Internet, il existe des moyens de vérifier si la sécurité d’un réseau est bonne ou non. Un exemple est

Shields Up (http://www.grc.com). Si tout se passe bien, la fenêtre suivante s'aﬀiche :



Si, en revanche, le système est mal protégé, la fenêtre suivante s'aﬀiche :



Ce genre d'outils est utile pour avoir une idée de la situation, mais, pour un contrôle de sécurité solide, il faut demander un audit à une société spécialisée.

36 TLS est la version 3.1 de SSL (Secure Sockets Layer), raison pour laquelle TLS est parfois appelé SSL, ce qui n’est pas très intelligent : si un logiciel de sécurité est déclaré « SSL », on ne sait pas si cela veut dire qu’il est obsolète parce qu’il est basé sur SSL — sous-entendu SSL 2.0 — ou si cela signifie que tout va bien parce qu’il est basé sur SSL

— sous-entendu SSL 3.1, c’est-à-dire TLS.

**La DMZ**

Bien entendu, plus un pare-feu est configuré de manière restrictive, mieux il protège le réseau, mais plus il gêne la communication avec le monde extérieur. Or une entreprise veut généralement que certaines de ses ressources soient librement accessibles par tout un chacun — le site web, la messagerie — alors que les autres ressources doivent rester invisibles de l’extérieur, notamment la base de données de l’entreprise. Comment gérer ces diﬀérences ? La réponse consiste à créer une zone intermédiaire entre le réseau interne et l’Internet, et d’y placer les serveurs qui doivent être visibles de l’extérieur. C’est le rôle de la **DMZ** (Demilitarized Zone).

De la solution la moins chère à la plus eﬀicace, il peut s’agir de :

1. un répertoire sur un ordinateur ;

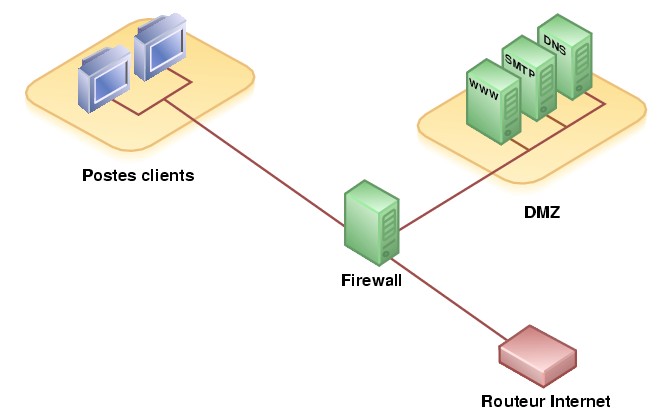
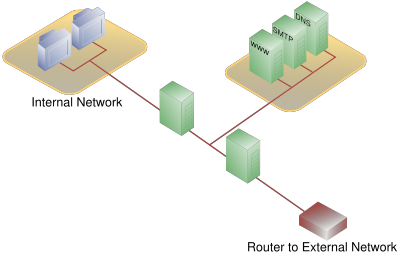
2. un serveur sur lequel le pare-feu dérive les messages entrants ; on parle de **bastion** (bastion host)

parce qu’il est configuré pour résister à d’éventuelles attaques ;

3. un bastion placé entre le pare-feu qui commande l’entrée sur le réseau (external ou front-end firewall)

et un second pare-feu qui sépare la DMZ du réseau interne (internal ou back-end firewall) ;

4. tout un sous-réseau placé entre le pare-feu externe et le pare-feu interne. Voici à gauche la solution 2 et à droite la solution 4 37 :



La solution 1 est à éviter dans toute la mesure du possible parce que le répertoire tampon se trouve dans le réseau interne. Les moyens de sécurité du système d’exploitation sont donc le seul rempart contre un assaillant.

La solution 2 oﬀre une bonne sécurité. Le pare-feu gère trois zones : l’extérieur, la DMZ et l’intérieur. C’est simple, peu coûteux et eﬀicace, mais, si un pirate parvient à casser les protections du pare-feu, il peut accéder librement à tout le réseau interne.

La solution 3 coûte plus cher, mais elle est très sûre parce qu’elle permet de mettre en place un pare-feu interne de marque diﬀérente du pare-feu externe, ce qui impose à un assaillant éventuel de connaître les deux environnements (par exemple, Cisco et Check Point).

La solution 4 est une variation de la 3. Elle permet de mieux structurer la DMZ, de tenir un trafic plus important et de moduler plus finement les moyens de protection.

Pour autant que les systèmes aient été paramétrés correctement, les pirates « normaux » sont arrêtés par une barrière de type 3 ou 4. Les professionnels peuvent passer au travers, mais ils ne sont pas nombreux.

37 « DMZ (computing) », [http://en.wikipedia.org/wiki/DMZ\_(computing),](http://en.wikipedia.org/wiki/DMZ_(computing)) Wikipedia, 2011.

De manière générale, tous les serveurs accessibles depuis l’extérieur doivent être placés dans la DMZ :

1. le relais (proxy) de messagerie (le vrai serveur de messagerie reste invisible, caché dans le réseau interne ; ce proxy est en réalité avant tout un reverse-proxy : il sert de relais aux requêtes venues de

l’extérieur ) ;

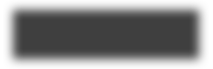
2. le serveur DNS ;

3. le serveur d’authentification ;

4. le serveur ftp ;

On trouve souvent des informations utiles sur les groupes spécialisés en sécurité, par exemple comp.security.unix

5. le serveur qui sert de relais entre les postes de travail et le web (ce proxy est important parce que, dans beaucoup de pays d’Europe, l’employeur est juridiquement responsable de ce que font les employés sur le web) ;



6. le serveur d’e-commerce (il sert de reverse proxy) ;

7. le serveur web (ce cas est relativement rare ; en général, ce serveur se trouve chez le fournisseur d’accès à l’Internet) ;

8. le pot de miel (honey pot), un faux serveur destiné à piéger un assaillant éventuel.

Seules les grandes entreprises mettent en place un pot de miel car l’entretien d’une telle machine coûte cher.

**Pour conclure**

Pour assurer une bonne sécurité du réseau, deux choses sont particulièrement importantes :

1° **Agir avec compétence**. Se tenir au courant des questions de sécurité, maintenir une politique et une pratique de sécurité solides et suivre la boucle de Boyd (observer → s'orienter → décider → agir) ou une autre méthode agile. La politique de sécurité doit évoluer en permanence : la sécurité est un processus sans fin.

Parmi les actions les plus importantes, il y a former les utilisateurs, eﬀectuer immédiatement toutes les mises à jour de sécurité, avoir une infrastructure de sécurité eﬀicace, connaître les ressources à protéger, donner aux comptes des utilisateurs et aux programmes les permis-sions les plus basses possibles, chiﬀrer les informations sensibles (surtout sur le cloud et les notebooks), faire les sauvegardes, tester régulièrement la restauration des données, savoir quoi faire en cas de sinistre.

2° **Éduquer les utilisateurs**. Il arrive souvent que les utilisateurs connaissent mal la sécurité et manquent de prudence.

Pour un criminel, trouver le moyen de donner une clé USB ou un CD à un dirigeant de banque, c'est la garantie d'avoir accès à toute la banque si les mesures de sécurité ne sont pas particulièrement solides. Aucun utilisateur ne doit ignorer les risques principaux :

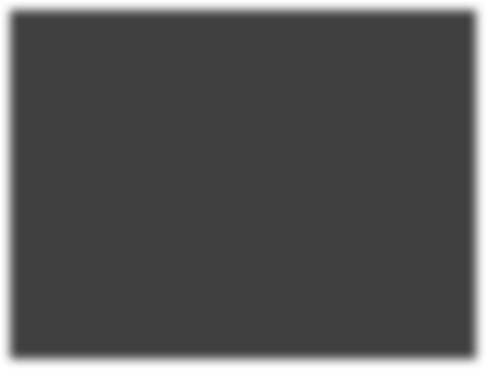
• ne pas donner des informations confidentielles en réponse à un message électronique dont on n'est pas sûr ;

• ne pas charger des fichiers depuis un site dont on n'est pas sûr ou se rendre sur un site non sûr.

Cliquer sur « Mise à jour Java » peut suﬀir à contaminer un ordinateur.

Utiliser pour le web un système d'exploitation sécurisé est un moyen de minimiser les risques. **LPS**, le

Linux créé aux États-Unis par l'Air Force Research Laboratory, est un exemple :

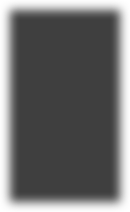


Les réseaux sociaux comme Facebook ou Twitter sont particulièrement dangereux. Il vaut mieux ne pas les fréquenter depuis un poste de travail d'entreprise.

Les réseau x i nfo rmat i q u es 86 h tt p // www jaqu et .o rg, mai 21115

**10. Les réseaux téléinformatiques**

Les **réseaux téléinformatiques** ou **WAN** (wide-area networks) sont les réseaux qui traversent le domaine public. Jusqu'à récemment, ils nécessitaient une autorisation de la part de l’État 38 ,



mais cela n'est plus toujours le cas aujourd'hui.

Jusqu’en 1991 en France et en Belgique, et jusqu'en 1998 en Suisse, c’étaient respectivement les P&T, la RTT et les PTT qui étaient chargées des télécommu- nications.

Ces dernières années, la libéralisation et la privatisation des services ont souvent abouti à une situation où les entreprises privées ont le droit d’exploiter des câbles sans rien payer à l’État, et on assiste à une érosion du pouvoir de l’État en matière de télécommunications.

L'organisme international de régulation est une agence des Nations unies, l'**ITU**

(International Telecommunication Union, [http://www.itu.int/fr/Pages/default.aspx).](http://www.itu.int/fr/Pages/default.aspx))

Un réseau téléinformatique traverse deux zones : la boucle locale et le réseau national et international de télécommunications.

**La boucle locale**

C’est surtout la **boucle locale** qui est intéressante parce que les câbles nationaux et internationaux regardent la sécurité nationale et on ne sait même pas par où ils passent. Le secret qui les entoure s'explique par le fait que, en cas de guerre, ils sont une cible privilégiée, et que le terrorisme est également devenu une menace.

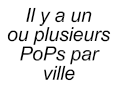
La boucle locale est aussi appelée **dernier kilomètre**, **last mile** ou **subscriber line**. Elle relie un site d'entreprise ou le domicile d'un particulier au PoP le plus proche. Un **PoP** (point of presence, point de présence) est un point d’accès au réseau national et international de télécommunications. Quand un PoP appartient à une société de télécommunication, on parle aussi de **CO** (central oﬀice).

Concrètement, un PoP est un local où se trouvent des équipements de télécommunications et des câblages qui vont, d’un côté, vers les entreprises et les domiciles privés des environs, et, de l’autre côté, vers le réseau national. Le matériel de la boucle locale forme la partie visible du système de télécommunication.

La boucle locale a longtemps été le terrain exclusif des anciens opérateurs publics et elle est toujours dominée par les entreprises héritières de ces opérateurs, c’est-à-dire Orange, Belgacom, Swisscom, etc.

38 Tout État détient normalement six pouvoirs : la monnaie, les impôts, l’armée, la police, les aﬀaires étrangères et les communications. Les WAN concernent ce dernier pouvoir.

Les câbles ont pour la plupart été posés avant la privatisation. Les nouvelles entreprises de télécommuni- cations doivent donc les louer puisqu'il serait économiquement absurde que chaque société de télécoms pose son propre câble jusqu’aux bâtiments des clients finals.



Dans les zones rurales, les anciens opérateurs publics conservent souvent un monopole de fait, mais il y a de nouveaux arrivants dans les grandes agglomérations. Ces sociétés ont des origines diverses :

• les télécommunications,

• la télévision par câble,

• l'électricité, avec un système appelé PLC (power-line communication, courants porteurs en ligne) où les données de télécommunications sont transportées sur le réseau 230 volts.

Les équipements de télécommunications qui se trouvent sur le site de l’entreprise utilisatrice et qui lui appartiennent portent le nom de **CPE** (customer premises equipement, équipements situés sur le site du client). La distance entre le CPE et le PoP varie entre une centaine de mètres et quelques kilomètres.

Dans les pays riches, la boucle locale passe généralement par des fibres optiques, mais les ondes se répandent de plus en plus. Dans beaucoup de pays pauvres, tout passe par le sans-fil. Avec la 4G, quelques centaines de mâts d'antennes peuvent couvrir tout un pays alors qu'il faudrait installer des milliers de kilomètres de fibres, ce qui impliquerait des années de travail pour creuser les tranchées, ce qui représenterait une dépense de plusieurs milliards. Ce choix s'explique aussi par le fait que les ondes sont nécessaires pour accéder au réseau depuis les nouveaux moyens de communication (tablettes, smartphones, etc.).

En filaire, la connexion est généralement **permanente**, ce qui veut dire qu'elle reste active 24 heures sur

24, 7 jours sur 7.

Dans beaucoup de pays, le coût des télécommunications est encore élevé, et le débit y reste donc souvent bas. Cela n'est pas une bonne idée du point de vue de l'économie nationale. En Extrême-Orient et en Scandinavie, les débits sur la boucle locale sont plutôt de 100 Mbps ou plus. Dans ces pays, des télécom- munications bon marché et à haut débit sont considérées comme une priorité nationale parce qu’ils contribuent à alimenter le moteur de la croissance économique.

**Le réseau national et international**

Le réseau national et international de télécommunications se compose de liaisons à haut débit qui forment un vaste maillage de câbles optiques.

Il existe un certain nombre de débits standard en Europe, au Japon et aux États-Unis pour ces liaisons. Ils forment le T-carrier system aux États-Unis et le **E-carrier system** en Europe et dans le reste du monde, à

l'exception du Canada et du Japon.

|  |  |  |
| --- | --- | --- |
| **États-Unis** | **Japon** | **Europe** |
| 64 kbps (T0, DS0) | 64 kbps | 64 kbps (E0) |
| 1,544 Mbps (T1, DS1) | 1,544 Mbps | 2,048 Mbps (E1) |
| 6,312 Mbps (T2, DS2) | 6,312 ou 7,768 Mbps | 8,448 Mbps (E2) |
| 44,736 Mbps (T3, DS3) | 32,064 Mbps | 34,368 Mbps (E3) |
| 274,176 Mbps (T4, DS4) | 97,728 Mbps | 139,264 Mbps (E4) |
| 400,352 Mbps (T5, DS5) | 565,148 Mbps | 565,148 Mbps (E5) |

On parle indiﬀéremment de liaison T1 ou de liaison DS1. Plus précisément, les noms DS0, DS1, etc., désignent les données transmises alors que les noms T0, T1, etc., désignent les circuits sur lesquels ces données sont transmises, mais, en pratique, on emploie les deux séries de termes comme s’ils étaients synonymes.

Ces protocoles concernent le niveau 1 du modèle OSI. Une autre série de normes de même niveau est **SDH** (synchronous digital hierarchy), avec les spécifications STM-0, STM-1, STM-4, STM-16, STM-64 et STM-256, qui vont de 52 Mbps à 40 Gbps. Les normes SDH s'emploient notamment pour transporter du trafic E1 et E3.

Au niveau 2 du modèle OSI, les liaisons nationales et internationales s'eﬀectuent de plus en plus sur des liaisons Ethernet à longue distance. Un exemple est EoS (Ethernet over SDH).

**La vision « contrat »**

Pour un client, ce n'est pas simple de louer des services de télécommunication en tant que tels parce que c'est un sujet très technique. Il est plus simple de payer une solution globale, c'est-à-dire un ensemble de prestations faisant l'objet d'un contrat :

• débit garanti (par exemple, 10 Mbps) ;

• disponibilité garantie (par exemple, 99,9%) ;

• services additionnels (par exemple, la sécurité).

Les aspects techniques sont alors l'aﬀaire de l'opérateur de télécommunication choisi. L'entreprise cliente ne s'en occupe pas : pour elle, peu importe comment les messages sont transmis, ce qui importe, c'est le **niveau de service** et la **qualité de service**, qui font souvent l'objet d'un **SLA** (service level agreement).

Le SLA prévoit souvent des pénalités en cas d'interruption de fonctionnement (downtime) au-delà de la limite prévue, par exemple 99,5% ou 99,7% de temps de fonctionnement (uptime).

Un SLA peut comprendre des dizaines de pages de dispositions, ce qui est un problème. Plus ils sont longs, plus ils sont complexes et plus l'opérateur de télécommunications peut se réfugier derrière les exceptions aux règles pour tenter d'échapper à ses obligations.

**La connexion sur la boucle locale**

Parmi les moyens de se connecter à un WAN sur la boucle locale, deux sont non permanents (dial-up) :

• le **RTC** (réseau téléphonique commuté analogique) ;

• l'**ISDN** (integrated services digital network), en français RNIS (réseau numérique à intégration de services).

Le réseau analogique est souvent surnommé POTS (plain old telephone system, ce qu'on peut traduire par

« le bon vieux système téléphonique »).

|  |  |  |
| --- | --- | --- |
|  | **Débit** | **Commentaire** |
| **POTS** | Très bas  (20 à 40 kbps) | Très lent, surtout à l’établissement de la connexion. Mauvaise solution dans la plupart des cas. |
| **ISDN** | Très bas  (60 kbps) | Lent mais intrinsèquement très sûr et disponible même si le réseau informatique est en panne puisque c'est une liaison out-of-band. |

Les autres solutions sont permanentes. La plupart passent par l’**Internet**. C’est le cas de CATV, Power

Line et DSL.

|  |  |  |
| --- | --- | --- |
|  | **Débit** | **Commentaire** |
| **CATV** | Bas à moyen | Le medium est le câble de la télévision. La connexion est partagée avec les autres abonnés du quartier, ce qui pose des problèmes de sécurité et de performances. Le CATV est à réserver aux particuliers. Pour les entreprises, c'est une mauvaise solution parce que la qualité de service n'est pas garantie. |
| **Power**  **Line** | Bas à moyen | Le medium est le câblage électrique, ce qui est pratique, mais la con- nexion est partagée. |
| **ADSL** | Bas | Le medium est le câble téléphonique existant. Le trafic ADSL et le trafic téléphonique se partagent la ligne.  Contrairement à ce que son nom indique (asymmetric digital subscriber line), ADSL peut être symétrique. |
| **SDSL** | Bas | Le medium est un câble téléphonique dédié. Contrairement à ADSL, SDSL (symmetric digital subscriber line) ne partage pas le câble avec le service de voix. La portée maximale est d’environ 3 km.  Le coût est forfaitaire et peu élevé, et la qualité de service meilleure que celle d’ADSL. Cela fait de SDSL une solution bien adaptée aux petites entreprises ou aux petites filiales qui n'ont pas besoin d'un débit élevé et qui souhaitent une qualité de service plus élevée qu'avec ADSL. |

|  |  |  |
| --- | --- | --- |
| **VDSL** | Bas à moyen | Avec VDSL (Very High Speed Digital Subscriber Line), le medium est un câble téléphonique existant. C'est le successeur d'ADSL. |
|  | | La qualité de service n’est pas parfaite, mais le coût de la ligne est forfaitaire et très bas. Cela fait de VDSL une bonne solution pour les petites entreprises ou les petites filiales de grandes entreprises pour |
| autant qu'elles n'aient pas besoin d'un débit élevé et que la qualité de service ne soit pas une priorité. |

Attention, la notion de portée maximale ne concerne que la boucle locale. Par exemple, une liaison ADSL peut relier un site à Paris avec un site à Shangaï. C'est la distance entre un site et son PoP qui ne peut pas dépasser quelques kilomètres. La liaison entre les PoP peut, elle, être aussi longue qu'on veut.

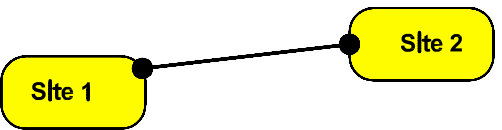
D’autres solutions ne passent pas par l'Internet. La plus ancienne est la **ligne louée** (leased line, dedicated line). Le client gère les équipements terminaux, qu’on appelle CSU (channel service units) ou DSU (data

service units).

|  |  |  |
| --- | --- | --- |
|  | **Débit** | **Commentaire** |
| **Ligne louée** | Très bas  à très élevé | Le medium est un câble optique dédié qui relie deux sites en point-à- point. Les deux extrémités de la ligne sont reliées en permanence. À l’intérieur d’une boucle locale, la liaison est souvent physique. Au-delà, elle est généralement virtuelle.  Contrairement aux solutions qui passent par l’Internet, la sécurité intrinsèque est excellente. Les performances sont garanties (bande passante et temps de latence). Par contre, le prix, forfaitaire, est élevé. |

Le principal inconvénient des lignes louées est le fait qu’elles nécessitent une liaison **point-à-point**, c'est-

à-dire une liaison pour chaque paire de sites. Exemple :



Une ligne louée est parfois un simple câble. Rien n’empêche donc une entreprise de faire installer des lignes louées, puis de mettre elle-même en place les protocoles qui lui conviennent le mieux, mais cela nécessite des compétences internes de haut niveau.

Cette solution ne convient pas aux entreprises qui sont déployées sur de nombreux sites — grandes banques, assurances, chaînes de supermarchés, etc. — parce qu’il faudrait mettre en place des dizaines ou des centaines de liaisons. La gestion de tous ces équipements terminaux serait un cauchemar et le coût serait prohibitif. Quand il y a beaucoup de sites à relier, on utilise donc un réseau **multipoint**, qui ne nécessite qu'un routeur sur chaque site. Ainsi, sur le site 1 du schéma ci-dessus, on n'aurait pas besoin de trois équipements terminaux (un pour chaque ligne), mais d'un seul.

Une solution très utilisée est **MPLS** (multiprotocol label switching), mais, dans certains pays, on rencontre parfois ATM (asynchronous transfer mode) ou encore Frame Relay, l'ancien standard des WAN multipoint.

|  |  |  |
| --- | --- | --- |
|  | **Débit** | **Commentaire** |
| **ATM** | Élevé à très élevé | ATM est un réseau multipoint qui reste utilisé par les sociétés de télécommunications, mais qui n’est plus oﬀert aux clients finals que dans certains pays. |
| **Frame**  **Relay** | Bas à moyen | Le Frame Relay (« relais de trame ») est également un réseau multipoint. Il est en voie de disparition. |
| **MPLS** | Bas à très élevé | MPLS est un réseau multipoint et multiservice qui peut véhiculer toutes sortes de trafics, avec des débits diﬀérents pour chaque site.  Il est compatible avec IPv4 et IPv6.  Les performances sont garanties et la sécurité très bonne. Par contre, le prix est élevé.  C’est la meilleure solution pour les liaisons entre sites où la qualité est primordiale. |

MPLS est, actuellement, la solution standard pour les liaisons entre sites d’une entreprise. Elle coûte cher, mais l'opérateur se charge de tout.

Une autre solution est bâtie sur Ethernet, ce qui est pratique puisque les réseaux Ethernet sont très répandus, bon marché et compatibles avec presque tous les matériels et les logiciels informatiques. Pour les diﬀérencier des standards Ethernets habituels, qui concernent les réseaux locaux, on parle de **Long**

**Haul Ethernet** (« Ethernet à longue distance »).

|  |  |  |
| --- | --- | --- |
|  | **Débit** | **Commentaire** |
| **Ethernet pur** | Élevé à très élevé | Ce standard circule sur des fibres noires.  Il s’emploie principalement dans les MAN, et on parle alors de **Metro**  **Ethernet**. C’est le moins cher. |
| **Ethernet sur**  **SDH** | Bas à très élevé | Ce standard est véhiculé par le standard SDH. |
| **Ethernet sur**  **MPLS** | Bas à très élevé | Cette solution utilise MPLS comme véhicule des trames Ethernet. C’est la plus coûteuse mais aussi la plus souple. Elle est bien adaptée aux réseaux complexes. |

Le Long Haul Ethernet établit un **LAN virtuel unique** qui couvre l’ensemble des sites de l’organisation. Les routeurs sont inutiles, remplacés par des switches Ethernet de niveau 3.

On peut mettre en place un système de VLAN (VLAN stacking).

**L'essentiel en bref**

CATV est à éviter. C'est une solution à réserver aux particuliers.

DSL et Power Line sont des solutions bon marché mais le débit est peu élevé et la qualité de service ne fait normalement pas l'objet d'un SLA. C'est le règne du **best eﬀort** (l'opérateur se contente de promettre de faire de son mieux). S'il y a des problèmes, l'utilisateur n'a qu'une solution : mettre fin à son contrat dans le délai prévu et espérer qu'il sera mieux servi chez un autre opérateur.

Ces solutions font passer le trafic par l'Internet et oﬀrent donc trois services en un : les liaisons entre sites (LAN-to-LAN), la messagerie et le web. Elles coûtent en général entre 50 et 200 euros par mois et par site. C'est cinq à dix fois moins cher que les autres solutions. Par contre, le fait qu'elles empruntent les chemins de l'Internet implique qu'il faut mettre en place des moyens de sécurité.

Les autres solutions se basent sur un SLA et la liaison fonctionne pratiquement sans interruption. En cas de problème, des techniciens réagissent rapidement, mais ces avantages se payent en termes financiers.

Les lignes louées sont fiables et ne coûtent pas cher si on n'a qu'un petit nombre de sites à relier et qu'ils sont géographiquement proches les uns des autres. Sinon, il vaut mieux choisir MPLS.

MPLS coûte moins cher que les lignes louées dès qu'il y a plus de trois ou quatre sites ou que les distances dépassent quelques dizaines de kilomètres, et cette solution oﬀre en gros les mêmes avantages en matière de qualité de service. Comme les lignes louées, les réseaux MPLS sont généralement accompagnés d'un

SLA.

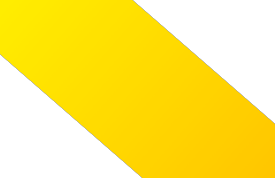
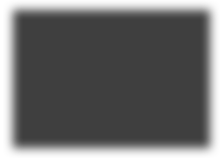
Avec les lignes louées, ATM, Frame Relay et MPLS, le coût dépend du nombre de sites, des débits, des distances et du niveau de service, mais, toutes choses égales par ailleurs, il est toujours beaucoup plus élevé qu'avec DSL.

Les lignes louées ne passent pas par l'Internet, ce qui oﬀre l'avantage d'une excellente sécurité mais cela oblige l'entreprise utilisatrice à avoir en plus sur chaque site une liaison DSL pour accéder à l'Internet (web et messagerie

électronique).

Une banque ou une autre entreprise pour laquelle l'informatique est vitale n'a pas le choix : elle doit opter pour une solution à haute qualité de service comme MPLS.

En revanche, une PME qui n'échange pas beaucoup de données entre ses sites et qui n'est pas trop gênée par une interruption épisodique des communications de quelques minutes peut se contenter de DSL.



Actuellement, MPLS est la solution la plus universelle : elle permet à la fois un accès à l'Internet (web et messagerie) et une liaison entre sites avec un débit diﬀérent pour chaque site, et elle peut véhiculer tous les types de trafic (données, voix, etc.). Son principal inconvénient est son prix.

Les réseaux Long Haul Ethernet sont intéressants parce qu'ils transforment les ensembles de LAN réunis par un WAN en un seul LAN virtuel et qu'ils oﬀrent un bon rapport débit/prix. Du point de vue de l'administration de réseau, on a un seul réseau. Par contre, un problème de réseau peut se propager partout alors qu'une solution classique empêche souvent un dysfonctionnement de rayonner hors du site touché.

L'Ethernet à longue distance n'est disponible que dans certaines zones, principalement les grandes agglomérations.

Les très grandes entreprises dépensent des millions d'euros chaque année pour leurs télécommunications et elle emploient un mix de solutions — par exemple, une ligne louée entre leurs datacentres et Long Haul Ethernet ou MPLS dans les autres cas.

**Le sans-fil sur la boucle locale**

Il existe plusieurs protocoles pour la communication sans fil (wireless). Ils peuvent tous s’utiliser pour la téléinformatique.

|  |  |  |
| --- | --- | --- |
|  | **Débit** | **Commentaire** |
| **GSM** | Extrêmement bas | GSM (global system for mobile communications) est le protocole de base pour les téléphones cellulaires. C'est la « 2 G », la deuxième génération de téléphonie cellulaire. |
| **GPRS** | Très bas | GPRS (general packet radio service) est une extension de GSM pour la transmission de paquets de données. Il est compatible avec IP. |
| **EDGE** | Bas | EDGE (enhanced data rates for GSM evolution) est une extension de  GSM-GPRS. On parle de 2,5 G. |
| **UMTS** | Moyen | UMTS (universal mobile telecommunications system) est la 3 G. |
| **WLL** | Élevé | Il existe plusieurs systèmes WLL (wireless local loop), mais le plus répandu est le standard 802.11 (wi-fi), qui s’emploie dans le LAN et la boucle locale. Sa portée est typiquement d’une centaine de mètres, mais elle peut atteindre plusieurs kilomètres, voire plus (on parle de long range wi-fi). Le débit diminue avec la distance.  WLL s’emploie notamment pour l’accès à l'Internet et comme moyen d’accès à un hot spot, c'est-à-dire un point d’accès public à l'Internet. |
| **WiMAX** | Élevé | WiMAX (worldwide interoperability for microwave access) est aussi appelé Wireless MAN. Il fait l'objet des normes IEEE 802.16.  Il s'emploie pour accéder à la boucle locale. Sa portée peut atteindre des dizaines de kilomètres, mais le débit diminue avec la distance. |
| **LTE** | Élevé | LTE (long term evolution) dérive d'UMTS. Cette norme transmet les données. Pour la voix, il faut y ajouter la norme complémentaire VoLTE (voice over LTE). C'est la 3,9 G. |
| **LTE-Advanced** | Très élevé | Réseau 4 G. Il a fait ses débuts en 2013. |
| **Satellite** | Très bas à moyen | Coûteux et sensible aux aléas de la météo, le satellite s’emploie peu en téléinformatique. Il est utile dans les régions où il n’existe pas d’autre moyen de communication. |

Les hot spots se trouvent sur les places des villes, les hôtels, les restaurants, les gares, les aéroports, etc.

**Sans-fil et sécurité**

Par définition, le sans-fil pose des problèmes de sécurité puisque n’importe qui peut potentiellement capter une onde. Il suﬀit de se trouver suﬀisamment près de l’émission et de lancer un logiciel qui scanne les ondes.

La sécurité de la connexion peut être assurée par des moyens de chiﬀrement et d'authentification comme WEP (Wired Equivalent Privacy) ou **WPA** (Wireless Protected Access). La sécurité oﬀerte par WEP est faible, et on peut le casser aisément avec un outil comme Aircrack-ng (http://www.aircrack-ng.org).

On peut aussi utiliser un serveur d’authentification comme **RADIUS** (Remote Authentication Dial-in User Service) ou un tunnel chiﬀré et authentifié (**VPN**, Virtual Private Network). Concrètement, ce sont des logiciels. Les serveurs RADIUS sont des solutions lourdes mais riches en fonctions.

Attention : l’exploitant d’un réseau sans fil qui ne prend pas les mesures de sécurité nécessaires pour se protéger sera le premier suspect en cas d’enquête pénale sur un délit commis depuis son réseau. Dans certains pays, il peut même être accusé de complicité passive.

Les réseau x i nfo rmat i q u es 96 h tt p // www jaqu et .o rg, mai 2111 5

**11. L'Internet**

Avec l'Internet, on est passé d'une logique où les systèmes informatiques des entreprises étaient des environnements isolés, sans communication avec le monde, à une logique où ils baignent dans le paysage informatique global. Toute une série de services inter-entreprises se sont développés :

• le B2B (business to business),

• le B2C (business to consumer),

• l'e-mail,

• le web,

• le stockage de données (IaaS),

• la sauvegarde en ligne,

• les applications web (PaaS),

• le cloud, notamment le SaaS,

Une application web (PaaS) appartient à une entreprise bien précise. Ses utilisateurs sont les employés de cette entreprise. Ils y accèdent au moyen d'un navigateur.

Une application en SaaS appartient à un ISP (Internet services provider). Toute entreprise qui le désire peut ouvrir un compte et l'utiliser. On y accède au moyen d'un navi- gateur. Google Docs est un exemple.

• les communications smartphones ⟷ serveurs, tablettes ⟷ serveurs, etc.

L'Internet véhicule aussi beaucoup de trafic intra-entreprise, principalement de la messagerie et des données transmises entre sites (le mot « site » étant à prendre dans le sens de lieu géographique, pas de site web). C'est le LAN-to-LAN, ensemble des liaisons entre réseaux locaux d'une seule et même entreprise.

**L'infrastructure de l'Internet**

Physiquement, les fibres optiques de l'Internet forment un maillage de câbles nationaux et internationaux. Il y a des centaines de milliers d'itinéraires possibles sur ce maillage mondial.

Du point de vue des acteurs concernés, l'Internet est hiérarchique.

Au niveau le plus bas, il y a les **utilisateurs**, c'est-à-dire les clients finals. Ce sont les entreprises mais aussi les particuliers qui ont une liaison avec l'Internet.

Les clients finals se connectent à un ou plusieurs **ISP** (Internet services providers). Pour des raisons de sécu- rité (redondance), une grande entreprise a généralement un contrat auprès de plusieurs ISP.

Chaque ISP gère un ou plusieurs **AS** (autonomous systems). Il a la maîtrise de son réseau : il en choisit notamment la topologie, les débits, les routeurs et les protocoles IGP (par exemple OSPF ou IS-IS).

Les **telcos** (les sociétés de télécommunications) gèrent également leur propres AS.

Il y a deux catégories d'opérateurs d'interconnexion : ceux qui s'occupent de transporter les données, mais aussi de raccorder les clients finals à leur réseau, et ceux qui ne s'occupent que de transport de données.

Aujourd'hui, l'Internet se compose de plusieurs dizaines de milliers d'AS (30'000 en 2009, 50'000 en 2015). Les plus grands AS réunissent plusieurs dizaines de millions d'adresses IP, les plus petits une seule.

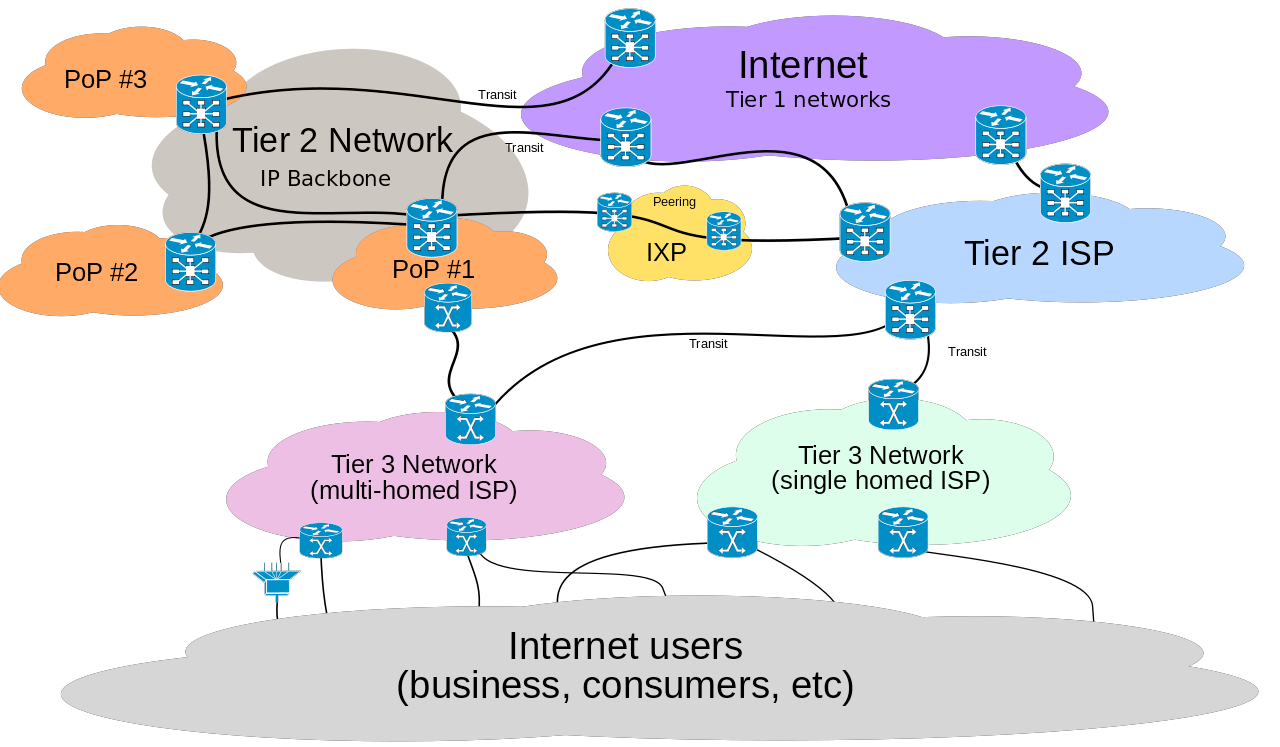
Les grands opérateurs mondiaux sont dits de niveau 1 (tier 1). Ils peuvent accéder à l'ensemble des réseaux de l'Internet, dans le monde entier. Ils ont des accords d'échange (peering) : en règle générale, les services qu'il s'oﬀrent entre eux sont gratuits.

Les opérateurs d'importance moyenne sont dits de niveau 2 (tier 2). Ils sont régionaux et dépendent des opérateurs de niveau 1 pour le transit de leurs données. Ce service leur est facturé par les opérateurs de niveau 1, mais les services entre opérateurs de niveau 2 font souvent l'objet d'accords de peering, auquel cas ils sont gratuits.

Les petits opérateurs sont dits de niveau 3 (tier 3). Ils n'oﬀrent pas de service de transit et dépendent des opérateurs de niveau 2 pour le transit de leurs données. Ce service leur est facturé.

Les plus petits opérateurs de niveau 3 ne sont connectés qu'à un seul opérateur de niveau 2. Les autres sont multihomed, connectés à plusieurs opérateurs.

Voici un schéma qui montre comment cela se présente 39 :



Les AS sont reliés entre eux par de gros routeurs installés dans des points d'échange appelés **IXP**, **IX**, **GIX**

ou **NIX** (Internet exchange points ; le G est pour global, le N pour neutral). Ces sigles sont synonymes.

Les IXP se composent de switches Ethernet de type MLS (multilevel switches) qui fonctionnent généra- lement à 10 Gbps. Grâce à eux, les AS voisins s'échangent directement les données, ce qui diminue le coût des échanges, augmente la vitesse des liaisons et économise de la bande passante. Il y en a deux en Belgique, trois en Suisse et une vingtaine en France.

Le routage est eﬀectué par **BGP4**, sauf si la connexion relie un opérateur de niveau 3 à un seul opérateur de niveau 2, puisqu'il n'y a alors qu'un seul chemin possible. C'est avec les opérateurs de niveau 3 multihomed et les opérateurs de niveau 1 et 2 que BGP4 est nécessaire.

39 LUDOVIC.FERRE, [http://en.wikipedia.org/wiki/File:Internet\_Connectivity\_Distribution\_%26\_Core.svg,](http://en.wikipedia.org/wiki/File%3AInternet_Connectivity_Distribution_%26_Core.svg) Wikipedia, 16 avril 2010.

Les tables de routage BGP4 sont beaucoup plus grandes que les tables des routeurs qui s'occupe du routage interne dans les entreprises des utilisateurs. Elles comprennent plusieurs centaines de milliers d'adresses IP v4 et IP v6. Le cap du demi-million a été dépassé en 2014.

Globalement, l'Internet repose sur cinq protocoles :

• **Ethernet** est l'ensemble de normes qui sont devenues récemment les protocoles de bas niveau dominants de l'Internet.

• **IP** fournit les services d'acheminement et d'adressage des paquets.

• **TCP** assure l'établissement de la connexion, son déroulement et sa fin et vérifie que tout se passe bien.

• **UDP** s'utilise à la place de TCP pour les tâches qui concerne le fonctionnement du réseau. UDP est plus léger et donc plus rapide que TCP, mais il ne vérifie pas que tout se passe bien (on peut comparer UDP au courrier postal normal et TCP au courrier recommandé).

• **BGP4** gère les choix d'itinéraires entre AS. Alors qu'IP ne « voit » pas plus loin que ses voisins, BGP4 a une vue d'ensemble de l'Internet.

Contrairement à IP, qui est partout, BGP4 ne se trouve que sur les grands routeurs de l'Internet, ceux des IXP.

Le web a été inventé en 1989 par Tim Berners-Lee, un scientifique du CERN de Genève, qui est aussi l'auteur du protocole HTTP, du langage HTML et du navigateur. L'Internet existait déjà sous le nom d'ARPANET. Le premier site web a été mis en ligne au CERN le 6 août 1991 avec l'adresse info.cern.ch. Il fonctionnait sur un serveur Next doté du système d'exploitation Nextstep, l'ancêtre de Mac OS X.

**APNIC, ARIN et autres RIR**

L'Internet est organisé en bureaux d'enregistrement Internet régionaux ou RIR (regional Internet registries), ce qui a été traduit en mauvais français par registres Internet régionaux.

Il y en a cinq : l'AfriNIC (African Network Information Centre), l'APNIC (Asia Pacific Network Information Centre), l'ARIN (American Registry for Internet Numbers), le LACNIC (Latin America and Caribbean Network Information Centre) et le RIPE NCC (Réseaux IP Européens, Network Coordination Centre) 40.

Près de la moitié des utilisateurs de l'Internet sont en région APNIC, avec en premier lieu la Chine, puis l'Inde, le Japon et l'Indonésie.

L'organisation qui supervise l'Internet est l'**ICANN** (Internet Corporation for Assigned Names and Numbers). Elle dépend du Département du commerce du gouvernement des États-Unis.

L'Internet étant un réseau mondial et une ressource dont l'accès libre est susceptible de devenir bientôt un droit fondamental, il serait logique que l'ICANN devienne une institution spécialisée des Nations Unies au sens du chapitre IX de la Charte 41 . L'Internet appartiendrait ainsi à la communauté internationale dans

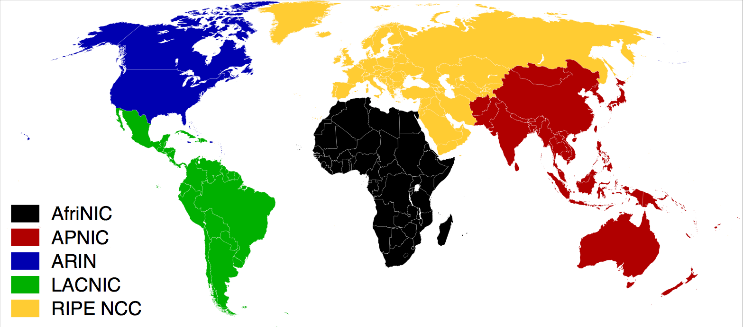
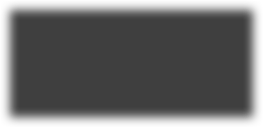
son ensemble. C'est ainsi que la France demande « une meilleure prise en compte des recommandations

40 Wikipedia, [http://en.wikipedia.org/wiki/Regional\_Internet\_registry#/media/File:Regional\_Internet\_Registries\_world\_map.svg,](http://en.wikipedia.org/wiki/Regional_Internet_registry%23/media/File%3ARegional_Internet_Registries_world_map.svg) 28 janvier

2009.

41 Charte des Nations Unies, [http://www.un.org/fr/documents/charter/.](http://www.un.org/fr/documents/charter/)

des États dans la gestion de l’internet, afin d’élaborer un modèle de gouvernance qui soit davantage trans- parent et inclusif » 42 , mais les Américains ne



veulent pas céder.

Le département de l'ICANN qui gère les adresses IP est l'**IANA** (Internet Assigned Numbers Autho- rity).

L'IANA délègue ce travail aux RIR dans le cadre de la norme RFC-7020 43 .

À leur tour, les RIR distribuent leurs ressources à

leurs clients, qui sont les ISP (Internet services providers) comme Orange (qui a succédé à France Télécom), Belgacom, Swisscom, etc.

La sécurité de l'Internet fait l'objet d'une surveillance par des dizaines d'organisations réparties dans le monde entier. En France, c'est le CERT-FR (http://www.cert.ssi.gouv.fr), en Belgique le BELNET CERT (https://cert.belnet.be) et en Suisse le Swisscom CSIRT.

Sur le web, on trouve des statistiques sur l'Internet (exemple : <http://www.internetsociety.org/internet/what->internet/facts-and-figures) et le trafic mondial (exemple : [http://thyme.apnic.net/current/data-summary).](http://thyme.apnic.net/current/data-summary))

**Aspects légaux**

Qu'est-ce que les entreprises et les particuliers ont le droit de faire sur le web et qu'est-ce qui est interdit, c'est un point devenu très important aujourd'hui sachant que la plupart des entreprises ont un site web.

Une question préalable est la détermination de la **compétence** avec les problèmes de conflits de juri- diction et de conflits de lois qui vont avec.

Par exemple, le contenu d'un site web pronazi sera peut-être toléré aux États-Unis au nom de la liberté d'opinion (premier amendement de la Constitution) et interdit en France au nom de la loi sur la liberté de la presse (art. 24) 44 :

Ceux qui […] auront provoqué à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appar- tenance à une ethnie, une nation, une race ou une religion déterminée, seront punis d'un an d'empri- sonnement et de 45 000 euros d'amende ou de l'une de ces deux peines seulement.

En Belgique, le cadre légal est plus compliqué : sont concernées la loi antiracisme du 30 juillet 1981 (art.

20s), la loi antidiscrimination du 10 mai 2007 et la loi contre le négationnisme du 23 mars 1995. Les règles

sont similaires à celles de la France.

42 « Gouvernance de l'Internet - Décision du conseil d'administration de l'ICANN (27 mars 2014), » <http://www.diplomatie.gouv.fr/> fr/politique-etrangere-de-la-france/diplomatie-numerique/evenements-22750/article/gouvernance-de-l-internet-decision, Ministère des Aﬀaires étrangères, accès le 12 mars 2015.

43 RFC-7020, [http://tools.ietf.org/html/rfc7020.](http://tools.ietf.org/html/rfc7020)

44 Loi du 29 juillet 1881 sur la liberté de la presse, [http://www.legifrance.gouv.fr/aﬀichTexte.do?cidTexte=JORFTEXT000000877119,](http://www.legifrance.gouv.fr/a%EF%AC%80ichTexte.do?cidTexte=JORFTEXT000000877119) version consolidée au 16 mars 2015.

En Suisse, le code pénal interdit le déni d'un crime contre l'humanité, l'incitation à la haine ou à la discrimination ethnique, raciale ou religieuse, ainsi que la propagation d'une idéologie ou les manifes- tations publiques de tout type (paroles, écrits, images, gestes, etc.) qui relèvent d'une discrimination (art.

261 bis).

C'est une question de balance d'intérêts : qu'est-ce qui est le plus important, la liberté d'opinion ou la lutte contre le racisme ? Aux États-Unis, les tribunaux privilégient la liberté d'opinion alors que, en France, en Belgique et en Suisse, c'est la lutte contre le racisme qui l'emporte. À titre personnel, je préfère la vision américaine parce que le seul résultat de la peur du gendarme est de cacher le problème (les racistes sont toujours là, simplement ils font plus attention à ce qu'ils disent en public).

La priorité donnée par les tribunaux des États-Unis à la liberté d'expression repose sur le premier amen- dement de la Constitution :

Le Congrès ne fera aucune loi […] pour limiter la liberté d'expression ou de la presse (Congress shall make no law […] abridging the freedom of speech, or of the press) […].

Cette disposition est toutefois interprétée aujourd'hui d'une manière très créative. D'un côté, la protection a été considérablement étendue en y soumettant non seulement le Congrès, mais aussi le pouvoir exécutif et judiciaire fédéral ainsi que le législatif, l'exécutif et le judiciaire des cinquante États de l'Union. De l'autre côté, des restrictions y ont été apportées dans bon nombre de lois, notamment au nom de la sécu- rité nationale.

Au niveau international, cette norme a une limite fixée par le Pacte international relatif aux droits civils et politiques, que les États-Unis ont ratifié en 1992 (art. 20 al. 2) :

Tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence est interdit par la loi.

Normalement, la liberté d'expression est la norme générale et l'interdiction de l'appel à la haine l'exception, et l'exception prévaut (principe lex specialis derogat legi generali), mais le premier amendement est très respecté aux États-Unis. Sachant qu'un site web hébergé aux États-Unis est soumis à la législation américaine (compétence territoriale), il suﬀit donc à un pronazi européen de déménager aux États-Unis et d'y héberger son site web pour diminuer considérablement les risques d'être condamné pour ce qu'il publie.

Les **conflits de juridiction** concernent les compétences de l'État et sont étroitement liés à la question de la souveraineté. Il y a essentiellement deux dimensions à considérer :

• la compétence territoriale, qui s'exerce sur toute personne qui se trouve sur le territoire national (si un

Français se trouve en Belgique, il doit respecter les lois en vigueur en Belgique) ;

• la compétence personnelle, qui s'exerce sur les citoyens de l'État concerné où qu'ils se trouvent, que ce soit sur le territoire national, à l'étranger ou dans un espace international comme la haute mer.

Les **conflit de lois** sont liés aux conflits de juridiction. Quelle législation faut-il appliquer quand une aﬀaire concerne le citoyen d'un pays A (lex patriae) domicilié dans un pays B (lex domicilii), et que cette aﬀaire s'est passée dans un pays C (lex loci) tout en concernant une propriété qui se trouve dans un pays D (lex situs) ? La réponse n'est pas évidente et elle dépend notamment des décisions prises au fil du temps par les tribunaux des pays concernés.

Pour prendre un cas concret, si un cybercriminel est de nationalité française, belge ou suisse (lex patriae), il a intérêt, par exemple, à habiter en Chypre du Nord (lex domicilii), à installer ses serveurs en Trans- nistrie (lex situs) et à limiter ses activités à d'autres pays (lex loci).

Aux États-Unis, le principe de base est de considérer que la cause doit être entendue dans le lieu qui présente le « lien le plus significatif » (most significant relationship) avec l'aﬀaire.

En Europe, il suﬀit en général qu'un site web soit accessible dans le pays pour que les tribunaux de ce pays se déclarent compétents. Les cybercriminels ont donc intérêt à habiter dans un pays dont les tribunaux ont une politique d'entraide internationale limitée, comme en Chypre du Nord.

En dehors de ces problèmes de conflits de compétence, les points importants sont :

• le droit à l'image ;

• le droit d'auteur.

**Le droit à l'image**

Le **droit à l'image** prévoit que chacun est propriétaire de son image. Il a donc le droit exclusif d'autoriser ou d'interdir l'utilisation publique de son image.

Par exemple, on ne peut pas publier sur un site web une photo où une personne est reconnaissable sans avoir préalablement obtenu son accord. Cet accord peut être oral ou même tacite, mais il est plus prudent de prévoir une formule d'autorisation (release form).

Les sites sociaux comme Facebook fourmillent donc certainement de photos illégales. Ils contiennent des millions d'images de fêtes familiales, de soirées entre amis et de sorties d'entreprises dont la majorité n'ont probablement jamais donné lieu à des demandes d'autorisation.

Par contre, on peut, par exemple, mettre dans un album de photo personnel une photo où une personne est reconnaissable parce que c'est un usage privé et non un usage public.

Cela pose le problème de la limite : un site web accessible à tous est clairement public et un album de photos clairement privé, mais qu'en est-il de Flickr, par exemple, où on peut rendre une photo publique ou visible par les amis seulement ? Dans ce dernier cas, on a a priori aﬀaire à un cadre privé, qui ne nécessite donc pas d'autorisation, mais il ne faudrait pas non plus que le nombre des amis soit si élevé que cela transforme le cadre apparemment privé en cadre public de fait.

Les personnages publics constituent un cas particulier. Si le président de la République fait un discours devant la mairie, on peut le prendre en photo et publier les images. Par exemple, le site web d'une entre- prise de la ville pourra mentionner l'événement et mettre une photo sur son site web. Il n'y a pas d'autori- sation à demander parce que le président est venu en tant que personnage public et le **droit à l'infor- mation** prime dans ce cas sur le droit à l'image.

Par contre, si le président de la République vient incognito en ville et qu'on le photographie en catimini, il n'est plus dans la peau d'un personnage public et il faudrait obtenir son autorisation pour publier l'image.

D'autre part, les journaux et les sites web d'information mettent beaucoup d'images en ligne avec, par exemple, l'équipe de football locale. Comme avec les personnages publics, on s'intéresse au caractère

public ou privé de la photo. Le droit à l'image n'est pas absolu : la question est de mettre en balance le droit à l'image et le droit à l'information.

**Le droit d'auteur**

Le **droit d'auteur** est l'ensemble des droits dont dispose l'auteur d'une image sur son œuvre. Il se crée automatiquement. À l'instant même où une photo est prise, son auteur est protégé par le droit d'auteur.

La Convention de Berne pour la protection des œuvres littéraires et artistiques est le texte international fondamental pour le droit d'auteur 45 . Elle protège « toutes les productions du domaine littéraire, scienti- fique et artistique, quel qu’en soit le mode ou la forme d’expression, telles que: les livres, brochures et autres écrits; les conférences, allocutions, sermons et autres œuvres de même nature; les œuvres drama- tiques ou dramatico-musicales; les œuvres chorégraphiques et les pantomimes; les compositions musicales avec ou sans paroles; les œuvres cinématographiques, auxquelles sont assimilées les œuvres exprimées par un procédé analogue à la cinématographie; les œuvres de dessin, de peinture, d’architecture, de sculpture, de gravure, de lithographie; les œuvres photographiques, auxquelles sont assimilées les œuvres exprimées par un procédé analogue à la photographie; les œuvres des arts appliqués; les illustrations, les cartes géo- graphiques; les plans, croquis et ouvrages plastiques relatifs à la géographie, à la topographie, à l’architec- ture ou aux sciences » (art. 2 al. 1). Les sites web font partie de ces œuvres protégées. On n'a par con- séquent pas le droit de copier le design d'un site pour en créer un autre.

La durée minimale de protection est de 50 ans après la mort de l'auteur mais certains pays allongent cette durée (70 ans en France, en Belgique et en Suisse). Passé ce délai, l'œuvre entre dans le domaine public.

En règle générale, les œuvres créées par un employé donnent le droit exclusif à son employeur de les exploiter alors que les œuvres créées dans un autre contexte sont la propriété de leur auteur.

Par exemple, si l'employé d'une entreprise de photographie fait des photos de mariage, ses images seront exploitées économiquement par son entreprise. Par contre, si un photographe indépendant intervient en renfort, il restera le propriétaire de ses images sauf si le contrat entre ce photographe et l'entreprise qui a fait appel à lui en dispose autrement.

L'auteur a le droit exclusif d'autoriser ou d'interdir l'utilisation de son œuvre en dehors d'un cadre privé. Par exemple, aucune photo ne peut être mise sur un site web sans son accord (ou, le cas échéant, celui de son employeur).

Le fait que l'usage privé est autorisé signifie, par exemple, qu'on est libre d'employer au domicile comme fond d'écran une photo trouvée sur le web.

Si on la met sur le poste de travail de l'entreprise, par contre, ce n'est plus un usage privé puisque des étrangers peuvent la voir (usage privé veut dire usage en famille et avec les amis).

Une autre exception est la citation : on n'a pas le droit de réutiliser le texte d'une page de site, mais on a le droit de citer quelques phrases à condition de préciser la source et l'auteur (les notes de bas de page de ce

texte sont des références de ce type).

45 Convention de Berne pour la protection des œuvres littéraires et artistiques du 9 septembre 1886, <http://www.wipo.int/treaties/fr/>

text.jsp?file\_id=283699, modifiée le 28 septembre 1979.

Dans beaucoup de pays, les textes oﬀiciels d’ordre législatif, administratif ou judiciaire ne sont pas protégés par le droit d'auteur (Convention de Berne, art. 2 al. 4) et les nouvelles du jour ou les faits divers qui ont le caractère de simples informations de presse ne le sont pas non plus (art. 2 al. 8).

Une dernière question est importante : quand a-t-on besoin d'une autorisation pour faire une photo ? Dans un **endroit public**, on fait ce qu'on veut à deux conditions :

1° Personne n'est reconnaissable sur l'image (problème du droit à l'image).

2° L'image ne représente pas une œuvre (problème du droit d'auteur).

Les milliers de gens qui photographient chaque jour le Centre Pompidou se mettent en contravention avec la loi puisque c'est une œuvre due aux architectes Piano, Rogers et Franchini. Les deux premiers sont toujours vivants et leurs œuvres n'entreront sans doute pas dans le domaine public avant les années 2090.

En revanche, on a le droit de prendre une photo de son conjoint avec le Centre Pompidon en arrière-fond et de publier cette photo (sous réserve de l'accord du conjoint). De même, on peut photographier un bus londonien et mettre l'image sur un site web sans demander l'autorisation des entreprises dont la publicité est aﬀichée sur le bus.

Un **endroit privé** appartient, lui, à une personne privée (entreprise ou particulier). Contrairement à ce qu'on croit souvent, un supermarché, un restaurant, une salle de spectacle ou un hall de gare sont des endroits privés puisqu'ils appartiennent à des entreprises. Dans ce cas, on a aﬀaire, pour être précis, à une **propriété privée à accès public**.

Dans le cas des endroits privés, il y a trois conditions :

1° Personne n'est reconnaissable sur l'image.

2° L'image ne représente pas une œuvre.

3° Le propriétaire des lieux a donné son accord.

Par exemple, il y a sur ma galerie Flickr environ 300 photos prises dans des propriétés appartenant au National Trust ([https://w](http://www.flickr.com/photos/pierre_et_nelly/sets/72)ww.flick[r.com/photos/pierre\_et\_nelly/sets/72](http://www.flickr.com/photos/pierre_et_nelly/sets/72)

157632838529304). Cela n'est possible que parce que le

National Trust accepte — à bien plaire — que les visiteurs

Le **copyright** est l'équivalent du droit d'auteur

dans les pays de common law (le Royaume-Uni et ses anciennes colonies).

Comme l'indique son nom, il est axé sur la pro- tection non de l'auteur mais de l'œuvre (le copy right est le droit de copier l'œuvre). Cela change fondamentalement la perspective, d'où pas mal de diﬀicultés quand une procédure judiciaire est à cheval sur les deux mondes.

mettent leurs images sur les réseaux sociaux. Cette tolérance s'explique sans doute par le fait que ces images ont pour résultat de donner envie à d'autres gens de visiter ces propriétés et qu'il ne s'agit pas d'une activité commerciale.

Par contre, il ne serait pas possible de vendre l'une de ces photos sans demander d'abord l'accord du National Trust et il faudrait sans doute leur verser une certaine somme en tant que propriétaires de l'endroit photographié.

**Un droit fondamental**

Depuis le début du siècle, il est question de faire un droit fondamental de l'**accès à l'Internet** (ou, plus précisément, de l'accès aux informations stockées et échangées sur l'Internet).

En 2003, l'Assemblée générale des Nations Unies a approuvé dans sa résolution 56/183 la tenue à Genève d'un sommet mondial sur la société de l'information, dont la déclaration de principes finale a déterminé que la liberté d'opinion et la liberté d'expression impliquent la possibilité de participer à la société de l'in- formation 46 :

4. Nous réaﬀirmons qu’à titre de fondement essentiel de la société de l'information et comme l’énonce l'article 19 de la Déclaration universelle des droits de l'homme, tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considération de frontière, les informations et les idées par quelque moyen d'expression que ce soit. La communication est un processus social fondamental, un besoin essentiel de l'être humain et la base de toute organisation sociale. Elle est le pivot de la société de l'information. Toute personne, où que ce soit dans le monde, devrait avoir la possibilité de participer à la société de l'information et nul ne devrait être privé des avantages qu'elle oﬀre.

En 2009, le Conseil constitutionnel français a approuvé cette déclaration 47 :

La liberté de communication et d'expression, énoncée à l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789, fait l'objet d'une constante jurisprudence protectrice par le Conseil constitutionnel (voir dernièrement décision n °2009-577 DC du 3 mars 2009). Cette liberté implique aujourd'hui, eu égard au développement généralisé d'internet et à son importance pour la participation à la vie démocratique et à l'expression des idées et des opinions, la liberté d'accéder à ces services de communication au public en ligne.

En 2011, c'était le tour du Conseil des droits de l'homme des Nations Unies 48 :

67. Contrairement à tout autre média, l'Internet permet aux individus de chercher, de recevoir et de partager instantanément et à peu de frais toutes sortes d'informations au-delà des frontières nationales. En augmentant la capacité des individus à jouir de leur droit à la liberté d'opinion et d'expression, lequel facilite l'exercice d'autres droits de l'homme, l'Internet stimule le développement économique, social et politique, et contribue au progrès de l'humanité dans son ensemble. […]

68. Le Rapporteur spécial souligne qu'il faut imposer le moins de restrictions possible à la circulation des informations sur l'Internet, sauf cas exceptionnels prévus par le droit international des droits de l'homme. Il insiste par ailleurs sur le fait que la pleine garantie du droit à la liberté d'expression doit être la norme, que toute restriction doit être exceptionnelle et que ce principe ne doit jamais être inversé. […]

79. Le Rapporteur spécial demande à tous les États de veiller à ce que l'accès à l'Internet soit maintenu en permanence, y compris pendant les périodes de troubles politiques. […]

85. Étant donné que l'Internet est devenu un outil indispensable pour assurer l’exercice d’un large éventail des droits de l'homme, combattre les inégalités et accélérer le développement et le progrès humain, la garantie de l'accès universel à l'Internet devrait être une priorité pour tous les États.

En 2014, l'Assemblée parlementaire du Conseil de l'Europe a fait des recommandations dans le même sens 49 :

46 « Construire la société de l'information : un défi mondial pour le nouveau millénaire », Sommet mondial sur la société de l'information, Document WSIS-03/GENEVA/DOC/4-F, [http://www.itu.int/dms\_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004‼PDF-](http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004%E2%80%BCPDF-) F.pdf, 12 mai 2004.

47 « Communiqué de presse - 2009-580 DC », Conseil constitutionnel, <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/>francais/les-decisions/acces-par-date/decisions-depuis-1959/2009/2009-580-dc/communique-de-presse.45951.html, décision n°2009-580 du 10 juin 2009.

48 « Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue », Conseil des droits de l'homme, Réf. A/HRC/17/27, [http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/132/02/PDF/G1113202.pdf,](http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/132/02/PDF/G1113202.pdf) 16 mai 2011.

49 « Le droit d'accès à internet », Assemblée parlementaire du Conseil de l'Europe, résolution 1987, <http://assembly.coe.int/nw/xml/>XRef/Xref-XML2HTML-FR.asp?fileid=20870&lang=FR, 9 avril 2014.

5. […] l’Assemblée recommande aux États membres du Conseil de l’Europe de garantir le droit d’accès à internet sur la base des principes suivants :

5.1. chacun doit jouir du droit d’accès à internet en tant que condition essentielle à l’exercice des droits en vertu de la Convention européenne des droits de l’homme ;

5.2. le droit d’accès à internet inclut celui d’avoir accès à des informations ou des idées, ainsi que d’en recevoir et d’en communiquer via internet, sans qu’il puisse y avoir ingérence d’autorités publiques et sans considération de frontière, sous réserve seulement des restrictions prévues par l'article 10 de la Convention européenne des droits de l'homme ; compte tenu de l’importance d’internet pour les sociétés démocratiques, toute restriction de ce type devrait faire l’objet d’une définition claire et rigoureuse ; […]

5.4. comme l’accès à internet est également essentiel pour l’exercice d’autres droits de l’homme, tels que le droit à la liberté de réunion et le droit au respect de la vie privée et familiale, les Etats membres devraient reconnaître le droit fondamental à l’accès à internet dans la loi et la pratique ; […].

Les déclarations et les recommandations ne sont que cela : des déclarations et des recommandations. Ce ne sont ni des traités ni des décisions, ce qui veut dire qu'elles ont très peu de force en droit international. Mais le principe du libre accès à l'Internet s'appuie sur une disposition du Pacte international relatif aux droits civils et politiques. Étant conventionnelle, elle est juridiquement obligatoire : « Toute personne a droit à la liberté d'expression ; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix. » (art. 19 par. 2). À l'exception de la Chine et de Cuba, pratiquement tous les pays du monde sont parties de ce traité.

Aux États-Unis, le gouvernement a décidé de préserver la **neutralité de l'Internet**, c'est-à-dire de garantir que toutes les données soient traitées de la même manière par les ISP. Concrètement, cela veut dire, par exemple, que les ISP n'ont pas le droit de donner plus de bande passante aux demandes d'accès à certains sites. Contrairement à ce qu'on lit parfois, cela ne veut pas dire que le gouvernement américain a fait de l'accès à l'Internet un droit fondamental 50 . Deux choses tout à fait diﬀérentes sont à distinguer :

• Le principe de la neutralité de l'Internet interdit aux ISP de manipuler les vitesses d'accès et de privi- légier ainsi certains types de trafic ou certains clients. C'est une histoire de tuyaux.

• Le principe du droit d'accès en tant que droit fondamental interdit aux États d'espionner les inter- nautes (droit à la vie privée) ou de les empêcher de lire ou de publier certaines informations (liberté de pensée, d'opinion et d'expression). C'est une histoire de contenus.

Le droit à la vie privée est garanti par l'article 17 du Pacte international relatif aux droits civils et poli- tiques, la liberté de pensée par l'article 18 et la liberté d'opinion et d'expression par l'article 19 51 .

Le respect de ces libertés n'interdit évidemment pas à un juge d'ordonner la surveillance d'une personne ou l'interdiction d'un site, mais c'est dans le cadre d'une enquête légale. Le droit à la vie privée est subor- donné aux nécessités de la justice et la liberté d'opinion à l'interdiction de l'incitation à la haine, de la pédopornographie, etc.

Les limitations mises aux libertés fondamentales ne sont censées être justifiées que par des raisons elles aussi fondamentales, mais ce n'est pas toujours le cas. Au Texas, un nommé Gregory Lee Johnson a été

50 Julien DUPONT-CALBO, « Les États-Unis érigent Internet en droit fondamental », Les Échos, 27 février 2015.

51 Pacte international relatif aux droits civils et politiques du 16 décembre 1966, <http://www.ohchr.org/FR/ProfessionalInterest/Pages/>CCPR.aspx, entré en vigueur le 23 mars 1976.

jugé en 1988 pour avoir brûlé un drapeau national pour protester contre la polique du président Reagan. Il a dû aller jusqu'à la Cour suprême des États-Unis pour que les juges lui donnent raison de justesse, par 5 voix contre 4, au nom de la liberté d'opinion (premier amendement) 52 . Il y a aussi Estelle Grisword, con- damnée en 1964 au Connecticut pour avoir conseillé à des couples mariés d'utiliser des contraceptifs. Elle aussi a dû s'adresser à la Cour suprême des États-Unis pour que les juges lui donnent raison par 7 voix contre 2 au nom du respect de la vie privée, en s'appuyant sur le premier, le neuvième et le quatorzième amendement 53 (la cour n'a pas pu faire référence au Pacte international sur les droits civils et politiques

puisque que les États-Unis n'ont ratifié ce traité qu'en 1992).

52 Texas v. Johnson, 491 U.S. 397 (1989), [http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=491&invol=397,](http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&amp;vol=491&amp;invol=397) 21 juin 1989.

53 Griswold v. Connecticut, 381 U.S. 479 (1965), [http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=CASE&court=US&vol=381&](http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=CASE&amp;court=US&amp;vol=381)

page=479, 7 juin 1965.

Les r éseau x informat i ques 1118 http // www jaquet.org, mai 21115

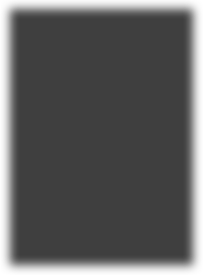
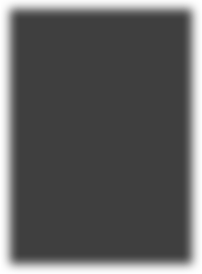
**12. Le DNS**

Le **DNS** (Domain Name System) est le système de mise en correspondance des adresses IP et des noms

Internet. Ces noms s'appellent des **URL** (Uniform Resource Locators).

On pourrait s'en passer. Il suﬀirait de taper les adresses au lieu des URL. On arriverait au même endroit :

Mais ce serait peu pratique. D'une part, les êtres humaines retiennent beaucoup plus facilement les noms que les chiﬀres, et nous serions obligés d'avoir un bottin des adresses IP comme nous avons un bottin du téléphone. D'autre part, cela empêcherait les changements. Grâce au DNS, l'adresse IP des Nations unies peut changer tous les jours ; on ne s'en rendra même pas compte pourvu que son nom ne change pas.



Ce qu'il faut bien voir, c'est que les équipements informatiques (ordinateurs, routeurs, etc.) ne savent manipuler que les adresses IP. Le DNS est un service destiné uniquement aux êtres humains. Le téléphone fonctionne de la même manière : le bottin téléphonique met en correspondance des numéros de téléphone avec des noms et adresses de personnes, mais le système téléphonique lui-même ne gère que des numéros de téléphone.

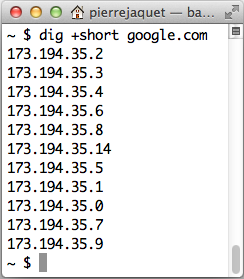
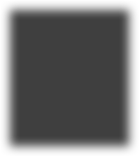
|  |  |  |
| --- | --- | --- |
|  | **Bottin téléphonique** | **DNS** |
| Mise en correspondance | Nom et adresse ⟷ Numéro de tél. | Nom Internet ⟷ Adresse IP |
| Transmission des messages | Par les numéros de téléphone seuls | Par les adresses IP seules |

**L'infrastructure DNS**

Le **DNS** (Domain Name System) est mis en œuvre par des programmes appelés **serveurs DNS** ou **serveurs de noms** (name servers). Leur tâche est de gérer la mise en correspondance des adresses IP et des noms Internet. Ils travaillent en client–serveur.

Le trafic DNS passe par le port UDP 53.

Pour savoir à quelle ou quelles adresses IP correspond une URL, on peut utiliser la commande **dig** (domain information groper). Exemple (image ci-contre) :



**dig +short google.com**

Les serveurs DNS forment une arborescence qui correspond à celle des noms. La racine est représentée par un point, d'où la notation « .com », « .fr », etc.

Un domaine de premier niveau s'appelle un **TLD** (Top Level Domain). Il y a deux types de TLD, ceux qui concernent un pays, comme « .fr », qui sont les **ccTLD** (country code TLDs), et ceux qui sont transversaux, comme « .com » ou « .org », qui sont les **gTLD** (generic TLDs). Les sous-arborescences sont appelées **zones**.

Au sommet, il y a 13 **root servers** (serveurs racines). Ces logiciels fonctionnent sur des ordinateurs situées dans plus de cent datacentres éparpillés dans le monde.

Cette redondance a pour but d'améliorer les performances et surtout la fiabilité. La panne d'un ordinateur n'entraîne aucune conséquence, à part une légère baisse des performances dans la zone géographique con- cernée.

Leur rôle se limite à répondre aux requêtes demandant l'adresse du serveur responsable d'un TLD donné

(par exemple « .fr »).

Ils sont gérés par des États et de grands fournisseurs d'accès.

Le nombre de requêtes envoyées chaque jour aux root servers se chiﬀre en dizaines de milliards, mais ces serveurs sont conçus pour absorber une quantité encore plus grande de requêtes, l'idée étant de rendre inopérantes les attaques DDoS (Distributed Denial of Service) 54 .

Les **primary servers** (serveurs primaires) sont les serveurs responsables de tel ou tel TLD. Par exemple, il y a un serveur chargé de gérer tous les URL commençant par « .fr ».

Sous ces serveurs, les **secondary servers** (serveurs secondaires) gèrent des zones à l'intérieur d'un TLD. Par exemple, les fournisseurs d'accès comme Orange, Belgacom ou Swisscom ont leurs propres serveurs DNS secondaires.

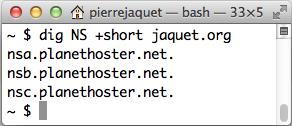
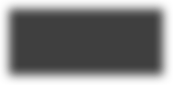
En bas de la hiérarchie, il y a les **serveurs locaux**. Ils ont pour rôle de gérer le service de noms à l'in- térieur de chaque entreprise.

54 Le DDoS (Distributed Denial of Service) consiste à inonder un serveur de requêtes pour ralentir fortement son fonctionnement ou le faire crasher.

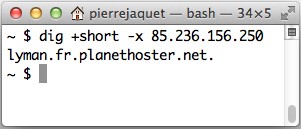
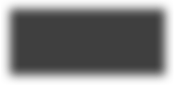
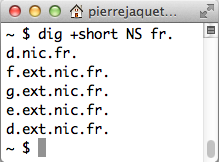
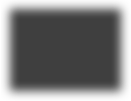
Pour savoir quels sont les serveurs de noms primaires associés à une URL, on peut utiliser dig avec l'option

NS (image ci-dessous à gauche), et on peut faire pareil avec un TLD (image ci-dessous au milieu).

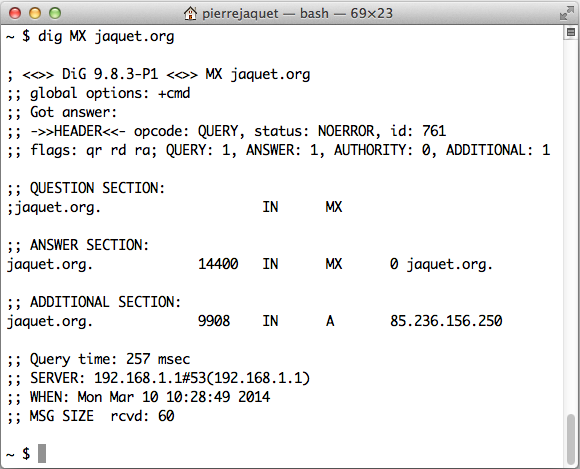
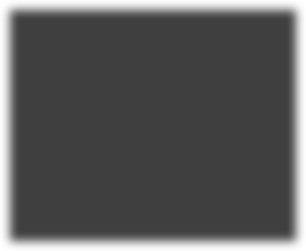
Pour connaître l'URL d'un ordinateur dont on connaît l'adresse IP, c'est l'option x (ci-dessous à droite).



Pour savoir quel est le serveur de messagerie responsable pour un domaine, on emploie l'option MX. Le serveur est indiqué dans Answer section (image ci-dessous).



Un domaine est trouvé en lisant son nom de droite à gauche.



Par exemple, le site de la City de Londres s'appelle [www.cityoflondon.gov.uk.](http://www.cityoflondon.gov.uk/) Si on tape cette adresse, le navigateur va de- mander à un serveur racine de lui donner l'adresse du serveur principal chargé du TLD « .uk ». Le serveur racine va la lui donner. Le navigateur va alors interroger le serveur principal, qui va le diriger vers le serveur responsable de « gov », lequel va lui indiquer l'adresse du serveur nommé « www ».

La syntaxe se présente ainsi :

**Sous-domaine.domaine.TLD**

Soit dit entre parenthèses, on n'a souvent plus besoin de donner l'indication du sous-domaine « www » parce que les serveurs DNS considèrent de plus en plus que c'est une valeur par défaut. C'est pareil pour le préfixe http, sauf que ce n'est pas le serveur DNS, mais le navigateur qui s'en occupe. Exemple : cityoflon- don.gov.uk = [http://www.cityoflondon.gov.uk.](http://www.cityoflondon.gov.uk/)

Le DNS est un système récursif : il fonctionne en cascade, sauf au niveau des serveurs racines.

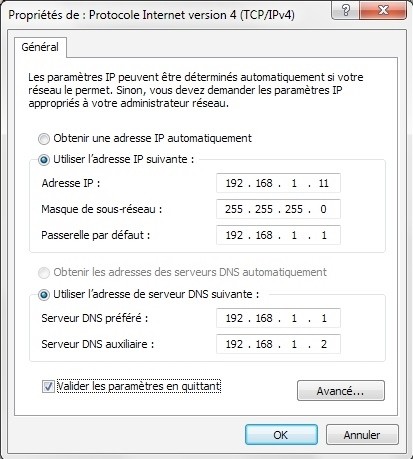
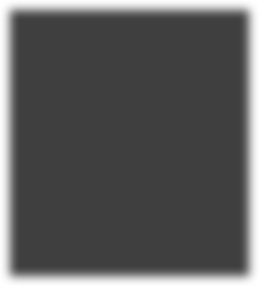
Pour améliorer les performances, un système de caching est utilisé. Par exemple, si l'employé Paul a tapé [www.cityoflondon.gov.uk](http://www.cityoflondon.gov.uk/) il y a cinq minutes, sa collègue Virginie y accèdera directement parce que le serveur DNS de leur entreprise aura gardé en mémoire l'adresse IP du serveur [www.cityoflondon.gov.uk.](http://www.cityoflondon.gov.uk/) On peut configurer le délai après lequel l'adresse est jetée.

Les clients DNS les plus communs sont les navigateurs web.

Un client DNS s'appelle aussi un DNS resolver, ce qui peut se traduire par « programme chargé de résoudre les correspondances entre adresses IP et noms URL ».

**Le DNS sur l'hôte**

Pour que le DNS fonctionne, chaque hôte (chaque ordinateur) doit connaître l'adresse de son serveur DNS local.



Sous Windows, cette adresse se trouve dans les Propriétés du protocole Internet. On y va par le Panneau de configuration → Centre réseau et partage → Aﬀicher les connexions réseau. Sur la fenêtre qui s'aﬀiche, on sélectionne la connexion à configurer (par exemple Connexion au réseau local), on fait un clic droit, on choisit Propriétés

→ Protocole Internet version 4 → Propriétés et

c'est la ligne Serveur DNS préféré (image ci- contre).

Sous Linux, le chemin dépend de la distribution. Le serveur DNS est souvent appelé name server.

Sous Mac OS, c'est Préférences système →

Réseau, ligne Serveur DNS (image ci-dessous).

Dans une petite entreprise, un petit site de grand groupe ou au domicile d'un particulier, le serveur DNS se trouve en général sur le routeur (lequel est appelé



« passerelle par défaut » par Windows et « routeur » par Mac OS).

Dans une moyenne ou grande entreprise, il se trouve habituellement sur un serveur, un routeur ou un pare-feu.

**Un exemple de requête DNS**

Qu'on clique sur un lien ou qu'on tape un URL dans la barre d'adresse d'un navigateur, le processus est le même. Voici un exemple simplifié avec [www.jaquet.org.](http://www.jaquet.org/)

1° Le navigateur demande au système d'exploitation d'envoyer la requête suivante au serveur DNS

local : « quelle est l'adresse IP qui correspond à l'URL [www.jaquet.org](http://www.jaquet.org/) ? ».

2° Le système d'exploitation consulte sa configuration de réseau pour connaître l'adresse IP du serveur

DNS local. C'est par exemple 192.168.1.1.

3° Le système d'exploitation envoie à l'adresse 192.168.1.1 (au serveur DNS local) la requête de l'étape 1.

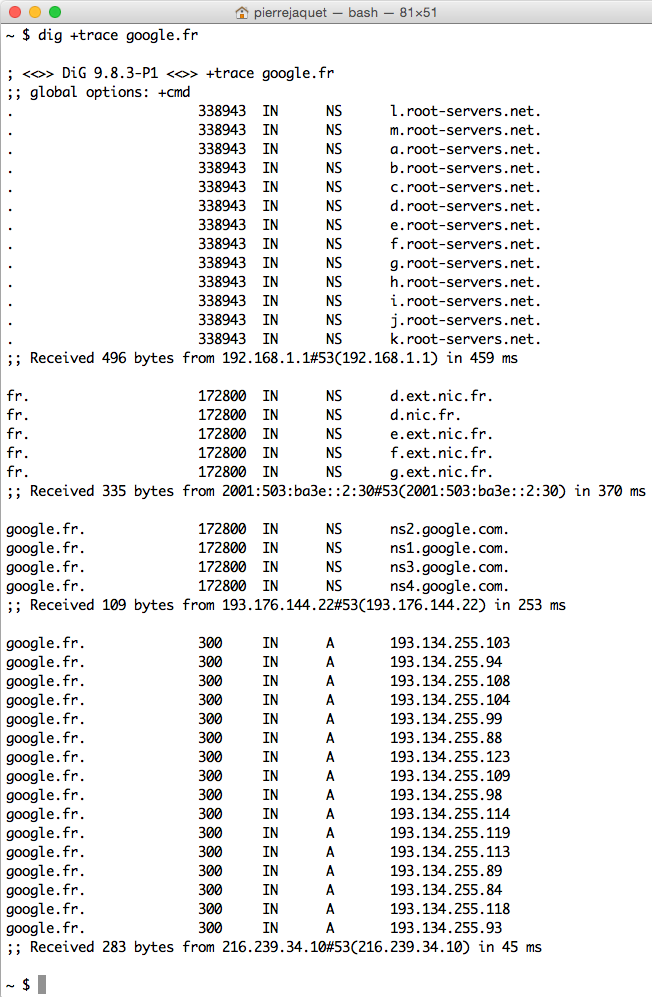
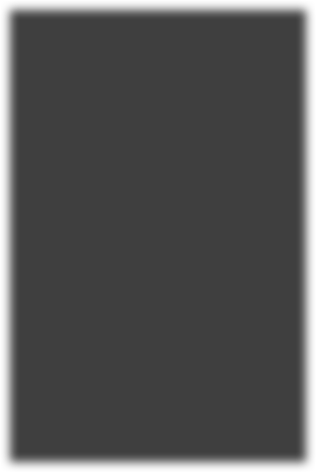
4° Le serveur DNS local envoie à l'un des 13 serveurs DNS racines la requête suivante : « quelle est l'adresse IP d'un serveur DNS qui peut me donner l'adresse IP correspondant à [www.jaquet.org](http://www.jaquet.org/) ? »

5° Le serveur racine répond au serveur DNS local en lui donnant l'adresse d'un serveur DNS qui peut répondre à cette question.

6° Le serveur DNS local envoie à ce serveur la requête : « quelle est l'adresse IP qui correspond à l'URL [www.jaquet.org](http://www.jaquet.org/) ? ». Cette adresse correspond à la page web par défaut du serveur [www.jaquet.org,](http://www.jaquet.org/) mais on peut aussi être plus précis et demander par exemple la page <http://jaquet.org/pdfs/mac_os_>premiers\_pas.pdf.

7° Le serveur DNS dont le serveur racine a donné l'adresse répond au serveur DNS local en lui indiquant l'adresse IP en question : [www.jaquet.org](http://www.jaquet.org/) = 85.236.156.250.

8° Le serveur DNS local place cette réponse dans son cache. De cette façon, si l'un des ordinateurs du réseau local demande à accéder à [www.jaquet.org](http://www.jaquet.org/) dans quelques minutes ou quelques heures, l'infor- mation sera directement dispo-



nible.

9° En parallèle, il retransmet l'in- formation au système d'exploita- tion de l'ordinateur d'où la requête est partie.

10° À son tour, le système d'ex- ploitation la transmet au navi- gateur. Cela permet à ce dernier d'envoyer la requête de l'utili- sateur à l'adresse 85.36.156.250.

C'est seulement à partir de cette dixième étape que la communi- cation entre le navigateur et le serveur HTTP désiré va pouvoir commencer.

Pour reprendre la comparaison avec le téléphone, les 9 pre- mières étapes ne servent qu'à trouver le destinataire. Faire son numéro sur le téléphone, c'est déjà l'étape 10.

On peut suivre le chemin suivi par une requête DNS en utilisant l'option trace de la commande dig (image ci- contre).

Le DNS est très lourd : la majorité des messages transmis sur l'Internet concernent ce service.

**BIND**

Le serveur DNS le plus utilisé est BIND (Berkeley Internet Name Domain). Il est open source et gratuit. Il s'emploie sur pratiquement tous les ordinateurs Unix et Linux dotés d'un serveur DNS.

Il réunit trois composants :

• Un serveur DNS. C'est lui qui gère les requêtes DNS (voir l'exemple donné plus haut). Il constitue le composant essentiel du système. Toute entreprise peut fournir des services DNS en l'installant sur un ordinateur.

• Une bibliothèque appelée DNS resolver library. Elle peut être employée par tout programmeur qui veut inclure des services DNS dans son application.

• Des outils de test qui permettent de contrôler que le dialogue entre un client et un serveur DNS s'effectue correctement.

Étant donné que les protocoles DNS sont bien définis, un client DNS peut fonctionner, par exemple, sur un ordinateur Windows et dialoguer avec un serveur qui se trouve sur une machine Unix.

**13. Services Internet**

À cause de l'importance de l'Internet dans l'informatique d'aujourd'hui, toute une palette de services s'est développée, surtout depuis le début des années 2000. Ces services sont destinés aux entreprises et aux particuliers.

**Fourniture d'accès**

Le service le plus important est évidemment l'accès à l'Internet puisque tous les autres services en dépendent. Ce service concerne des contenus (des informations) ; il ne porte pas sur les télécommuni- cations (les moyens de transmission).

Les fournisseurs sont principalement les entreprises de télécommunications (telcos), mais certaines sociétés d'électricité ou de télévision par câble sont aussi présentes sur ce marché.

Les liaisons utilisée sont généralement :

• une liaison DSL ;

• une liaison dédiée, généralement sous la forme d'une fibre optique ;

• un réseau d'entreprise, par exemple MPLS ou Ethernet à longue distance ;

• une connexion sans fil de type Wi-Fi 55 , 4G ou éventuellement satellite.

Les fournisseurs d'accès peuvent être des opérateurs de niveau 1, 2 ou 3 (voir chapitre précédent). Ils ont leur propre PoP (point of presence) ou sont sous contrat avec une telco qui en possède.

Beaucoup d'entre eux offrent en plus de l'accès des services comme la messagerie et l'hébergement de sites web, ce qui en fait des ISP (Internet services providers).

**Messagerie**

La messagerie électronique est également importante. Il y a cinquante ans, il n'existait que deux manières de contacter une personne à distance : le courrier postal et le téléphone. La messagerie a complété ces deux méthodes en combinant certains de leurs avantages, notamment l'instantanéité du téléphone, et, pour le courrier, le caractère écrit et la possibilité d'inclure des pièces jointes.

L'hébergement de messagerie réunit plusieurs services, notamment :

• la mise à disposition d'un serveur de messagerie (c'est un logiciel, pas un ordinateur) ;

• la maintenance de ce serveur ;

55 Rappel : il y a deux sortes de réseaux sans fil, ceux qui sont internes à l'entreprise (LAN) et ceux qui concernent la boucle locale (MAN et WAN). Quand un employé se trouve dans les locaux de son entreprise et qu'il se connecte au serveur, c'est le LAN qui est concerné. Quand cet employé se trouve dans une gare ou un hôtel et qu'il utilise le Wi-Fi de cette gare ou de cet hôtel pour se connecter au réseau de son entreprise, c'est le WAN.

• la gestion de la sécurité (pare-feu, logiciel antispam, etc.).

Le logiciel antispam est particulièrement important sachant que la majorité des messages qui s'échangent sur l'Internet sont des spams et que le spam coûte des dizaines de milliards de dollars chaque année en temps perdu, en gaspillage de ressources informatiques, en messages valides filtrés par erreur (faux positifs), en développement de programmes antispam et en frais de défense.

Le serveur gère la réception, le stockage et l'envoi des messages.

Il y a plusieurs catégories de fournisseurs de services de messagerie :

1° Des sociétés oﬀrent gratuitement leurs services, comme Gmail. Cette solution s'adresse aux parti- culiers mais aussi aux entreprises pour des adresses « jetables » (des adresses qu'on donne à n'importe qui et qu'on annule si elles sont l'objet de trop de spams).

2° Les fournisseurs d'accès incluent souvent une adresse de messagerie avec le service d'accès. Cette solution s'emploie de moins en moins.

3° Des sociétés spécialisées oﬀrent un service de messagerie payant (premium e-mail). Cette solution est aussi en déclin.

4° Les hébergeurs de sites web oﬀrent généralement un service de messagerie lié au site. C'est la solution utilisée par la plupart des entreprises.

Les principaux protocoles utilisés sont POP, SMTP et IMAP. Avec POP, les messages doivent être transférés sur le poste de travail pour être lus, alors qu'IMAP stocke les messages sur le serveur.

Parmi les principaux serveurs de messagerie, il y a Exim, Postfix et Sendmail. Ils fonctionnent généra- lement sur des machines Linux.

**Hébergement de sites web**

Pratiquement toutes les entreprises ont un site web. Au minimum, c'est une vitrine qui permet à l'entre- prise d'être trouvée par une personne qui recherche sur le web les entreprises actives à un certain endroit dans un certain domaine d'activité.

L'hébergement de sites web consiste à oﬀrir aux clients une plate-forme sur laquelle ils placent leur site. On y accède depuis l'Internet, ce qui donne une présence mondiale à tous les sites web.

En général, cette plate-forme réunit les éléments suivants :

• un espace sur un serveur virtuel (tous les fournisseurs emploient la virtualisation de serveurs dans leurs datacentres) ;

• un programme d'administration, par exemple cPanel ou Plesk ;

• le logiciel nécessaire pour créer le site (LAMP : Linux, Apache, MySQL et PHP-Perl-Python) 56 ;

• le logiciel assurant le fonctionnement de certains CMS (Wordpress, Joomla, Drupal, etc.) ;

56 Il existe une version de LAMP pour Windows (WAMP) et une pour Mac OS (MAMP), mais les hébergeurs utilisent Linux parce que c'est le système d'exploitation qui oﬀre le meilleur rapport performances-prix dans le domaine de l'Internet. Les grandes entreprises de l'Internet possèdent des centaines de milliers d'ordinateurs. Si ces machines fonctionnaient sous Windows, elles coûteraient des millions de dollars par année en licences et les frais pour assurer leur sécurité seraient très élevés.

• le logiciel pour la compatibilité avec certains environnements de développement d'applications web

(RoR, Django, Grails, etc.).

Les sites web peuvent aller d'une simple page statique écrite en HTML à un système complet de com- merce en ligne comme Amazon ou eBay.

**Synchronisation de données**

Le service de **file-syncing** (synchronisation de données) a pour but de maintenir l'intégrité des données réparties sur diﬀérents systèmes. Par exemple, il s'agit d'éviter la situation où un serveur stocke l'ancien numéro de téléphone d'une personne alors qu'un smartphone contient son nouveau numéro de téléphone.

Beaucoup d'utilisateurs utilisent ce service pour gérer leurs mots de passe, mais il faut faire attention à la sécurité. Il existe des programmes qui chiﬀrent les données avant de les télécharger sur les serveurs de synchronisation. Boxcryptor est un exemple.

Le service s'appuie sur quatre éléments :

• un espace de stockage sur un serveur virtuel ;

• chez l'utilisateur, un programme de synchronisation client sur chacun des ordinateurs concernés

(postes de travail, smartphones, tablettes, etc.) ;

• un programme de synchronisation serveur chez le fournisseur de service ;

• une base de données qui stocke les informations qui asssurent la coordination des versions des fichiers.

Dropbox est un exemple de fournisseur de services de synchronisation de données. Le stockage n'est pas assuré par Dropbox mais par AWS (Amazon Web Services).

Le logiciel est écrit en Python, ce qui a permis à des informaticiens de créer des add-ons (des programmes qui oﬀrent des fonctions complémentaires).

**Sauvegarde en ligne**

Beaucoup de gens confondent la synchronisation de données avec la sauvegarde, mais ce sont deux services tout à fait diﬀérents : la synchronisation assure la cohérence de données existant à plusieurs endroits au moyen d'un programme de synchronisation alors que la sauvegarde assure la sécurité des données existant à un endroit en les copiant au moyen d'un programme de sauvegarde.

Avec le file-syncing, on évite d'avoir des données discordantes. Avec la sauvegarde, on évite de perdre des données.

Le service de sauvegarde s'appuie sur trois éléments :

• un espace de stockage sur un serveur virtuel ;

• un programme de sauvegarde client sur l'ordinateur dont les données sont à copier ;

• un programme de sauvegarde serveur chez le fournisseur de service.

Backblaze et Crashplan sont des exemples de fournisseurs de service de sauvegarde en ligne.

**IaaS**

Les services d'IaaS (infrastructure as a service) concernent soit des serveurs physiques, soit des serveurs virtuels, soit les deux (réels et virtuels). La première possibilité est largement obsolète compte tenu du fait que la virtualisation de serveurs oﬀre de nombreux avantages (coût d'exploitation plus bas, disponibilité plus élevée, capacité élastique, meilleure séparation des applications, durée de vie des applications plus longue, séparation TEST-PROD plus simple, meilleure compacité, consommation électrique moindre, récu- pération sur sinistre beaucoup plus simple).

Les services oﬀerts peuvent être de divers types :

• Colocation (colocation ou housing). Le client achète le serveur et le logiciel, gère le système et l'utilise.

Le fournisseur se contente de fournir l'infrastructure (l'espace dans le datacentre, la sécurité physique, la climatisation, etc.). La capacité est fixe et la facturation est forfaitaire.

• Dédié (dedicated hosting). Le fournisseur possède le serveur et le gère (maintenance, sécurité, sauve- gardes, etc.). Le client installe le système d'exploitation et les applications et utilise le système. La capa- cité est fixe et la facturation est forfaitaire.

• Dédié et géré (managed dedicated hosting). Le fournisseur possède le serveur et le gère (maintenance, sécurité, sauvegardes, etc.) et c'est aussi lui qui installe le système d'exploitation et les applications, qui s'occupe des patches de sécurité et qui assure la sécurité (pare-feu et détection d'intrusions). Le client se contente d'utiliser le système. Il ne dispose souvent pas de permissions d'accès de type root. La capacité est fixe et la facturation est forfaitaire.

• À la demande (on-demand cloud hosting) ou en temps partagé (time-sharing). Comme en dédié, le fournisseur possède le serveur et le gère, le client installe le système d'exploitation et les applications et utilise le système. Par contre, le service est facturé selon l'utilisation et la capacité peut être augmentée ou diminuée selon les besoins immédiats.

Avec la colocation, le client doit avoir les mêmes compétences en administration de systèmes que si son système informatique se trouvait dans ses locaux. Le principal avantage de cette solution est de partager les coûts élevés liés à un datacentre.

Les solutions dédiées déchargent le client d'une partie du travail d'administration de systèmes. On a besoin de moins de compétences qu'avec la colocation, mais on a aussi moins de liberté.

Le cloud hosting est la solution la plus souple.

AWS (Amazon Web Services) et Rackspace sont des exemples de fournisseur de services IaaS.

**PaaS**

Les services de PaaS (platform as a service) consistent à fournir un environnement d'exécution. Dans ce modèle, l'entreprise utilisatrice écrit ses propres applications en employant les outils proposés par un fournisseur de services PaaS, puis elle les héberge chez lui. Elle y accède par un simple navigateur. Cela permet à l'entreprise utilisatrice d'avoir un système informatique minimal formé uniquement de postes de travail et d'un routeur.

Un fournisseur de services PaaS n'oﬀre souvent pas de services IaaS. Il les délègue à une entreprise spécialisée comme AWS.

**SaaS**

Les services de SaaS (software as a service) consistent à fournir des applications en ligne. Exemples : Zoho

Oﬀice de Zoho et Gmail, Docs, Sheets et Drive de Google.

L'entreprise utilisatrice évite ainsi d'avoir à installer et faire la maintenance des applications sur les postes de travail ou les serveurs (modèles de virtualisation DaaS, Desktop as a service, ou AaaS, Application as a service).

Tout est externalisé : les applications, les données, les systèmes d'exploitation, les serveurs réels et virtuels, le stockage et le réseau. C'est une solution très intéressante pour les plus petites entreprises, qui n'ont généralement ni le temps, ni les compétences de gérer un parc informatique, mais il faut faire attention à la sécurité.

Ces applications appartiennent à la bureautique, mais un autre courant prend de l'importance : la location à tout client intéressé d'applications hébergées chez un fournisseur de services IaaS. Au lieu de créer une application que l'entreprise utilisatrice installe sur son serveur, l'éditeur la met à disposition sur le web.

**14. Les systèmes Cisco**

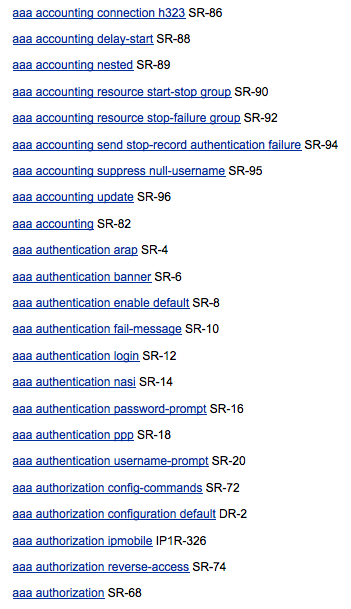
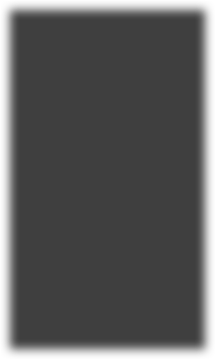
De la même manière que Windows règne sur le monde des postes de travail et de la bureautique et que Linux est le système d'exploitation des serveurs de l'Internet, il y deux environnements dominants dans les réseaux :

• Unix pour les équipements de télécommunications ;

• Cisco IOS pour les équipements de réseaux (switches, routeurs, etc.).

**Le système d'exploitation IOS**

Les routeurs, les pare-feu et la majorité des switches Cisco contiennent un système d’exploitation appelé **IOS** (Inter- network Operating System, à ne pas confondre avec iOS d'Apple). La version 15 est sortie en 2011.



Les routeurs à haute disponibilité contiennent, eux, un autre système d'exploitation appelé **IOS XR**. En interne, il est complètement diﬀérent de la lignée IOS tout court, mais son interface avec l'utilisateur est la même.

Le noyau d'IOS XR est QNX, un système d'exploitation Unix qui fonctionne en temps réel, ce qui veut dire qu'il travaille avec des délais impératifs.

Le système regroupe des fonctions de plusieurs types :

• télécommunications,

• routage (détermination des itinéraires),

• connexions interréseaux,

• commutation (switching),

• qualité de service ou QoS (Quality of Service),

• disponibilité (availability),

• sécurité (ACLs, VPN, AAA, pare-feu, etc.). Physiquement, IOS est stocké en mémoire flash.

Il comprend un langage de commandes très riche. L'image ci-contre ne montre que celles qui commencent par aaa 57 .

Seize niveaux de privilèges sont associés aux commandes, numérotés de 0 à 15.

57 [http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\_command\_summary09186a008020b3d8.html).](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_summary09186a008020b3d8.html))

On le met à jour depuis le site de Cisco. Ce service est payant ; les moyennes et grandes entreprises y souscrivent, mais les micro-entreprises s’en passent le plus souvent.

L’interface principale d’IOS avec l’utilisateur est une CLI (Command Language Interface), une interface par commandes. On peut y accéder de trois façons :

• par la console (c’est le seul moyen d’accès pour la configuration initiale) ;

• par telnet, via le réseau (que ce soit le LAN ou le WAN) ;

• par modem, via une liaison RAS ou VPN.

**Les outils de configuration**

Il existe trois manières de configurer un système Cisco.

Premièrement, on peut travailler par commandes (avec la CLI d'IOS). Il existe trois manières d’accéder au langage de commande :

• si le système n’a pas encore d’adresse IP, on utilise un programme d’**émulation de terminal** et on passe par la liaison console ;

• s’il est configuré et qu’au moins un de ses ports est doté d’une adresse IP, on peut passer par le réseau, avec deux possibilités :

- travailler en interactif avec **telnet** ou **ssh** ;

- travailler en batch avec **tftp** (trivial file transfer protocol) ; c’est un ftp simplifié ;

• si on passe par un modem, on utilise la prise auxiliaire AUX.

Il faut éviter telnet si on désire une connexion sécurisée. Tout est transmis en clair, y compris le mot de passe. Il vaut mieux utiliser **ssh** (secure shell), qui, lui, transmet des données chiﬀrées. Il oﬀre des fonctions similaires à rexec et rsh.

Tftp permet de transférer des fichiers via un réseau. Il sert notamment à copier un fichier de configuration d’un ordinateur vers un routeur ou réciproquement.

Deuxièmement, on peut configurer le système au moyen d’une interface graphique, mais les moyens d’administration oﬀerts sont souvent inférieurs en qualité et en quantité. Les CLI proposent généralement beaucoup plus d'options que les GUI, et elles permettent en outre d'automatiser les tâches (scripting).

Enfin, on peut passer par un logiciel d’administration de réseau comme Tivoli (<http://www-01.ibm.com/>software/tivoli), IT Performance Suite (<http://www8.hp.com/us/en/software/enterprise-software.html)>ou le logiciel open source gratuit Nagios (http://www.nagios.com).

**Les modes**

Le système d'exploitation IOS rassemble huit modes. C'est en somme comme s'il y avait huit interfaces de commandes diﬀérentes. La logique est la même qu'avec les deux modes de Unix et Linux (normal et root).

Le mode de base est le **user mode**. C'est de là qu'on part et qu'on peut aller dans le **privileged mode** puis dans des modes plus spécialisés. On se déplace de l'un à l'autre au moyen d'une commande spéci- fique. Par exemple, taper

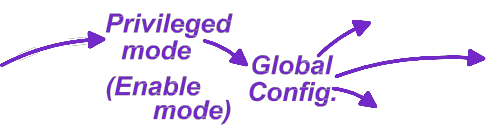
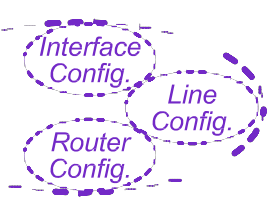
enable

permet de passer du user mode au mode privilégié. Un mot de passe est demandé. Chaque mode oﬀre un ensemble de fonctions spécifiques :

|  |  |
| --- | --- |
| **Mode** | **Utilisation** |
| Setup mode | Créer la configuration initiale (ce mode est optionnel) |
| User mode | Voir la configuration sans risque de la modifier par erreur |
| Privileged ou Enable mode | Administrer le système |
| Global configuration mode | Configurer le système |
| Line configuration mode | Configurer les lignes de terminal |
| Router configuration mode | Configurer les protocoles de routage |
| Interface configuration mode | Configurer les interfaces (réelles) du système |
| Subinterface configuration mode | Configurer les sous-interfaces (logicielles) du système |

Les modes sont imbriqués.

Le mode privilégié englobe cinq sous-modes (Global configuration, Interface configuration, Line configu- ration et Router configuration) et il joue en même temps le rôle de mode intermédiaire entre le user mode et le mode de configuration globale :



Les réseau x i nfo rmat i q u es 1 24 h tt p // www jaqu et .o rg, mai 2111 5

**15. La sécurité des réseaux**

Ces dernières années, la sécurité des réseaux a profondément changé. Avant, les attaques étaient parfois massives mais elles étaient le fait de malfaiteurs d'occasion ou de groupes de hackers. Aujourd'hui, on a souvent aﬀaire à des organisations criminelles et des gouvernements. Cinq d'entre eux sont particuliè- rement actifs : les États-Unis, le Royaume-Uni, Israël, la Russie et la Chine.

La criminalité informatique est devenue un véritable secteur d'activité économique. Par exemple, il existe un marché pour les **méthodes d'attaque** (exploits). Une bonne méthode d'attaque se vend très cher.

Selon le World Economic Forum, il y a deux principes de base 58 :

Tout équipement dont le comportement est défini par logiciel peut être contraint à faire des choses que ses créateurs n'avaient pas l'intention qu'il fasse.

Risque = vulnérabilité x

menace x conséquences.



Tout équipement relié de n'importe quelle manière à un réseau de n'importe quel type peut être infecté par une tierce partie. Beaucoup de ces infections n'ont pas encore été détectées.

De nombreux ordinateurs sont infectés par des chevaux de Troie et servent de relais pour des attaques de type **DDoS** (Distributed Denial of Service). L'attaque se passe en deux phases :

1° La préparation de l'attaque consiste à infecter des machines (les **zombies**) avec un cheval de Troie dormant. Le réseau des zombies est appelé **botnet** (robot network).

2° Le jour de l'attaque venu, le cheval de Troie dissimulé dans les ordinateurs du botnet reçoit de la part d'un serveur situé sur le web l'ordre d'adresser des rafales de paquets à un serveur cible, qui s'écroule sous la charge.

Le DDoS touche principalement les petites entreprises et les particuliers. Les grandes entreprises ont dans leurs équipes informatiques un personnel spécialisé en sécurité qui sait se défendre contre les attaques classiques.

Les réseaux des petites entreprises sont particulièrement visés pour plusieurs raisons :

• Elles ne gèrent souvent pas bien leur sécurité informatique.

• Elles manquent de moyens financiers pour bien gérer leur sécurité.

• Leurs serveurs fonctionnent sous Windows et ils sont souvent mal mis à jour, ce qui veut dire qu'ils présentent des failles bien connues (les criminels utilisent des robots pour scanner le web à la recherche des cibles mal protégées).

L'imprudence des petites entreprises est préoccupante : aux États-Unis, il semble que 80 à 90 % d'entre elles n'ont pas mis en place de procédures adéquates de protection des données, et on ne voit pas

pourquoi la situation serait meilleure en Europe. Selon Price Waterhouse Cooper, un sinistre de sécurité

58 World Economic Forum, Global Risks 2012, Genève, 2012, p. 27.

coûte généralement aux petites entreprises entre 100'000 et 170'00 euros. Le principal point à régler consiste à empêcher les employers de se balader sur des sites web douteux 59 .

Une mesure de sécurité eﬀicace et peu coûteuse est d'appliquer immédiatement les mises à jour de sécurité du système d'exploitation et des applications.

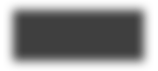
L'espionnage industriel est un problème particulièrement grave. Toutes les entreprises de pointe sont des cibles potentielles et le problème est bien plus répandu qu'on ne pourrait le croire. Rien que dans mon entourage proche, je connais deux cas. Dans la fabrique d'horlogerie où travaillait mon père, des secrets de fabrication ont été volés par des visiteurs lors d'une journée portes ouvertes. Dans l'entreprise infor- matique où travaillait mon ex-épouse, des secrets de fabrication ont été volés en récupérant des papiers

jetés dans la poubelle.

Même les circuits électroniques des équipements de réseaux peuvent contenir du malware. Dans certains cas, ce sont les fabricants qui sont en cause 60 , mais on a découvert aussi que la NSA intercepte des routeurs pour y implanter du malware dans des composants électroniques (en rem-

plaçant ou en ajoutant des composants) 61.

Ne pas corriger les failles connues est irresponsable du point de vue de la sécurité.



De manière générale, les nécessités de la sécurité sont sous-estimées, comme l'a montré une analyse datant de 2011 mais qui ne serait pas très diﬀérente si elle était conduite aujourd'hui 62 :

Une large majorité des applications Web (Web Apps) déployées pour le monde du SaaS (applications proposées en mode hébergé sous la forme d'un service) sont conçues sans prendre en compte les principaux critères de sécurité informatique. La tendance est mise en exergue par un récent rapport publié par le spécialiste du test logiciel Veracode.

58 % des 4'835 applications Web analysées par la société sur les 18 derniers mois n'ont manifestement fait l'objet d'aucun test ou audit sur le terrain de la sécurité informatique avant d'être postées sur une plate-forme de Cloud Computing. Plus grave, 66 % des applications SaaS développées par les acteurs de l'édition logicielle disposeraient d'un niveau de sécurité inacceptable, selon les critères de Veracode. Dans le domaine de la gestion de la relation client, 82 % des applications seraient dans ce cas, et pire

72 % des applications liées au domaine de la sécurité.

Selon une analyse eﬀectuée par Cenzic, 96 % des applications web testées ont des failles. Elles sont devenues une cible privilégiée parce qu'il est plus facile d'exploiter des failles applicatives que des failles du logiciel de base 63 .

À peu près 60 % des attaques sont financières, mais l'espionnage industriel en représente environ 25 % 64 . Aux États-Unis seuls, le nombre annuel de plaintes pour cybercrime a passé le cap de 300'000 en 2009,

mais le FBI pense que beaucoup de victimes ne portent pas plainte et que le nombre réel de cas est bien

59 Steve VIUKER, « Cybercrime and hacking are even bigger worries for small business owners », The Guardian, 21 janvier 2015.

60 John MARKOFF, « Old Trick Threatens the Newest Weapons », The New York Times, 26 octobre 2009.

61 Sean GALLAGHER, « Photos of an NSA "upgrade" factory show Cisco router getting implant », Ars Technica, 14 mai 2014.

62 « 58% des Web Apps ne font pas l'objet de test de sécurité », <http://www.journaldunet.com/developpeur/algo-methodes/la->securite-des-web-apps-mise-en-question-0411.shtml, Le Journal du Net, 26 avril 2011.

63 « Application Vulnerability Trends Report: 2014 », Cenzic, [http://www.cenzic.com,](http://www.cenzic.com/) 2014.

64 « 2014 Data Breach Investigations Report », Verizon, htt[p:w](http://www.verizonenterprise.com/)ww[.verizonenterprise.com,](http://www.verizonenterprise.com/) 2014.

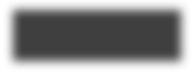
plus élevé que cela 65 . Chaque année, la situation empire un peu plus parce que la criminalité informatique est moins risquée que les activités classiques comme le trafic d'êtres humains ou de drogue.

Selon la Maison Blanche, la cybercriminalité coûte dans le monde

1'000 milliards de dollars par année. Une estimation de l'Interpol parle aussi de 1'000 milliards de dollars, mais pour l'Europe seule 66 . D'autres évaluations sont plus optimistes et parlent de

400 à 600 milliards pour le monde 67 .

Le coût global de la cybercriminalité représente 15 à 20 % de la valeur créée par l'économie de l'Internet.



Le point fondamental que les entreprises doivent garder à l'esprit est que les outils sont nécessaires mais loin d'être suﬀisants. C'est un personnel motivé et compétent en sécurité qui est essentiel.

**Le social engineering**

Les plus grands risques ne sont souvent pas liés à l'infrastructure de sécurité du réseau mais au facteur humain et au **social engineering** (exploitation des failles humaines).

Même les organismes qui devraient être les plus prudents se montrent souvent inconscients des risques. Par exemple, un ver-rootkit appelé Stuxnet a attaqué en 2009 des équipements nucléaires en Iran, endom- mageant gravement des centrifugeuses 68 . Comme les postes de travail fonctionnaient sous Windows, il a suﬀi qu'un collaborateur apporte avec lui une clé USB contenant Stuxnet et la connecte à son PC pour que le ver s'installe automatiquement grâce à la fonction autorun (auto-exécution) de Windows.

Comment se fait-il que les Iraniens utilisent Windows, le système d'exploitation qui est de loin le plus attaqué de tous, alors que leur programme nucléaire est la cible des États-Unis et d'Israël, au point que quatre experts nucléaires iraniens ont été assassinés 69 ? Il existe pourtant des moyens de sécuriser les systèmes d'exploitation Unix et Linux, alors que ce n'est pas possible avec Windows puisque le code n'est pas open source. Des projets comme TrustedBSD (Unix) et Selinux (Linux) ont donné lieu à des résultats qui ont été appliqués dans BSD, Mac OS et Linux. Attention, cela ne veut pas dire que Windows est moins sûr que Unix ou Linux (il est impossible de le savoir puisque Windows n'est pas open source, ce qui signifie que son code source est inaccessible). Le problème, c'est que des organismes comme la CIA ou la NSA peuvent implanter dans Windows tout le code malveillant qu'ils veulent, il restera invisible. Les dirigeants de Microsoft constituent le seul rempart contre ces agissements. Ont-ils les moyens de refuser, toute la question est là. C'est l'avantage essentiel de BSD et Linux en matière de sécurité : ils sont open source, ce qui veut dire qu'on peut en analyser le code source à la recherche de malware.

Stuxnet a mis à mal les installations nucléaires iraniennes en 2009. En 2010, un autre malware, Flame, a fait de même avec les installations nucléaires et pétrolières iraniennes. Comme Stuxnet, il visait les postes

65 Claudia BUCK, « California led nation in cybercrimes in 2011 », The Sacramento Bee, 13 mai 2012.

66 Misha GLENNY, « Cybercrime: is it out of control? », The Guardian, 21 septembre 2011 ; Daniella CHESLOW, « Interpol to Crack

Down on Cyber Crime », ABC News, 8 mai 2012.

67 Dune LAWRENCE, « The Global Cost of Cybercrime: More Than $400 Billion Per Year », Bloomberg, 9 juin 2014.

68 Stuxnet fait partie d'une attaque d'ensemble appelée « Olympic Games » et menée par le président George W. Bush junior et son successeur Barack Obama. Voir David E. SANGER, « Obama Order Sped Up Wave of Cyberattacks Against Iran », The New York Times, 1 juin 2012.

69 T. ERDBRINK et J. WARRICK, « Iranian scientist involved in nuclear program killed in Tehran bomb attack », The Washington Post,

11 janvier 2012.

de travail Windows. Il entrait sur les réseaux par l'intermédiaire de clés USB et il était basé sur un rootkit qui lui permettait de rester invisible si un antivirus eﬀectuait un scan du système. Il a apparemment été réalisé par la CIA et l'unité israélienne qui s'occupe de guerre électronique 70 .

Cette légèreté n'est pas propre aux Iraniens. En 2014, on a découvert un logiciel malveillant appelé Regin qui s'attaque également aux postes de travail Windows. Très modulaire, il rassemble plusieurs composants et existe en cinq formes successives. Il a notamment pris pour cibles des machines situées en Europe et au Moyen-Orient, y compris en Iran. Dans certains cas en tout cas, il s'introduit par une clé USB.

Les moyens d'attaquer un système sont nombreux. Durant la deuxième guerre contre l'Irak (2003), les militaires américains se sont aperçus que le logiciel Windows des drones Predators et Reapers était infecté par un virus qui s'est révélé diﬀicile à éradiquer 71. Le code malveillant était apparemment entré transporté par des programmes de jeu auxquels les pilotes jouaient pendant leur travail.

En 2009, le réseau électrique des États-Unis a été pris pour cible en attaquant des programmes fonctionnant sous Windows. Selon Fox News 72 :

Des espions ont piraté le réseau électrique US et ont laissé derrière eux des programmes informatiques qui leur permettraient de faire tomber le service, ce qui met en lumière des vulnérabilités potentiel- lement catastrophiques à des endroits clés de l'infrastructure nationale […].

Là aussi, les améliorations sont restées incertaines. Un an plus tard, le Scientific American écrivait 73 :

Le gouvernement fédéral a répertorié des dizaines de milliers de vulnérabilités dans le réseau de plus de 200'000 miles de lignes à haute tension, dans les milliers d'usines électriques et dans les millions de contrôleurs numériques.

Deux ans plus tard, il n'y avait pas de changement 74 :

[Comme le réseau à haute tension utilise Windows], les administrateurs de systèmes dans les centrales électriques ne peuvent pas mettre à jour le logiciel quand des bugs deviennent apparents. Les systèmes de gestion du réseau électrique ne peuvent pas être arrêtés trois heures par semaine pour la mainte- nance ; ils doivent fonctionner de manière continue.

De son côté, le New York Times a relevé qu'une bévue peut avoir des conséquences graves 75 :

Lors d'un briefing confidentiel, on a montré aux sénateurs comment un employé d'une entreprise électrique pouvait mettre en panne le réseau électrique de New York en cliquant sur le nom d'un fichier joint à un message électronique envoyé par un hacker, et comment une attaque menée durant une vague de chaleur pouvait avoir un impact en cascade qui mènerait à des morts et coûterait des milliards de

dollars à la nation.

70 E. NAKASHIMA, G. MILLER et J. TATE, « U.S., Israel developed Flame computer virus to slow Iranian nuclear eﬀorts, oﬀicials say »,

The Washington Post, 19 juin 2012.

71 James HIDER, « Mystery virus threatens US drones », The Times, 10 octobre 2011.

72 Jordan ROBERTSON et Eileen SULLIVAN, « AP source: Spies compromised US electric grid », <http://www.foxnews.com/wires/>

2009Apr08/0,4670,TECElectricGridHacking,00.html, Fox News, 8 avril 2009.

73 Melissa HATHAWAY, « Power Hackers: The U.S. Smart Grid Is Shaping Up to Be Dangerously Insecure », The Scientific American, octobre 2010.

74 David M. NICOL, « Hacking the Lights Out », The Scientific American, juillet 2011.

75 Michael S. SCHMIDT, « New Interest in Hacking as Threat to Security », The New York Times, 13 mars 2012.

Selon les prévisions de Richard A. Clarke, ancien conseiller de la Maison Blanche, une panne du réseau électrique des États-Unis pourrait causer plusieurs dizaines de milliers de morts 76 .

En 2009, Integral Energy, une société australienne qui gère une partie du réseau électrique national, a été attaquée par le virus W32.Virut.CF, qui s'attaque à Windows. La panne générale a été évitée grâce au fait que la gestion du réseau à haute tension s'eﬀectuait sous Unix (Solaris). Après cette alerte, Integral Energy a décidé de remplacer les postes de travail Windows par des machines Linux 77 .

**L'infestation**

Le malware s'infiltre par deux canaux principaux :

• le réseau, principalement la messagerie et le web ;

• les mémoires externes, notamment les clés USB, les disques durs et les cartes mémoires.

La majorité des mémoires externes sont formatées en FAT (File Allocation Table), qui était le système de fichiers de MS-DOS. C'est le cas de presque toutes les cartes SD, microSD et Compact Flash des smart- phones, des appareils de photo, des caméscopes, des GPS et des consoles de jeux.

C'est l'une des raisons qui expliquent que les systèmes Windows sont plus attaqués que les autres : le système de fichiers FAT est catastrophique du point de vue de la sécurité. Il constitue un moyen très simple d'infecter un système Windows.

Le problème est aggravé par la fonction autorun, une fonction stupide du point de vue de la sécurité, et qui n'existe que sur Windows et les Linux dotés d'une interface graphique qui comprend cette fonction (les serveurs ne sont donc pas concernés). Par exemple, un criminel qui vise une entreprise précise peut placer le malware qu'il a créé sur quelques clés USB et « semer » ces clés devant les portes. Si un employé de l'entreprise ramasse l'une de ces clés et la branche sur son poste de travail, l'autorun prend la main, accédant au système d'exploitation au moyen d'un des drivers installés par défaut, et le malware s'installe silencieusement sur le poste de travail de cet employé.

Un malware eﬀicace comprend trois fonctions :

• un mécanisme d'injection du code malveillant dans le système cible ;

• une fonction d'évasion qui a pour rôle d'empêcher le logiciel de sécurité de détecter sa présence ;

• une fonction de feinte pour le cas où le malware est détecté malgré tout. Cette fonction a pour rôle de faire croire au logiciel de sécurité qu'il a eﬀacé le malware alors qu'il n'en est rien.

**Les attaques par messagerie**

Les attaques par messagerie sont très courantes. Les plus classiques sont :

• le **scam** (ce terme anglais recouvre deux notions en français : l'abus de confiance et la fraude**)** ;

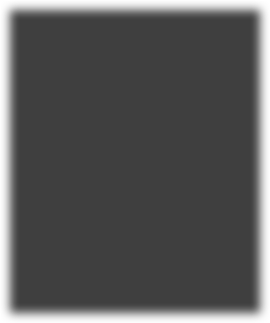
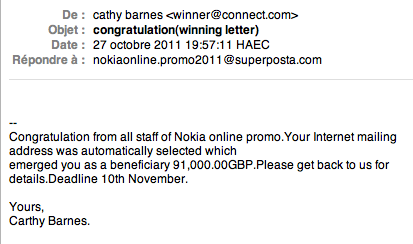
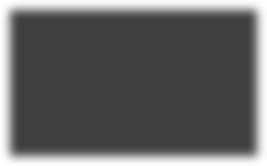
• le **cheval de Troie** (trojan).

76 Alex SPILLIUS, « Cyber attack 'could fell US within 15 minutes' », The Telegraph, 7 mai 2010.

77 Asher MOSES, « 'Sinister' Integral Energy virus outbreak a threat to power grid », The Sydney Morning Herald, 1 octobre 2009.

Un exemple classique de scam est l'annonce qu'on a gagné un prix (image ci-dessous).

Un autre cas répandu de scam est le **phishing** : la tentative de voler des données appartenant à une personne en essayant par exemple de lui faire mettre à jour son compte (image ci-dessous). Pour des raisons évidentes de sécurité, les entre- prises réelles ne font jamais ce genre de choses. Il est donc très facile de voir le piège : 100 % de ces messages sont des faux.

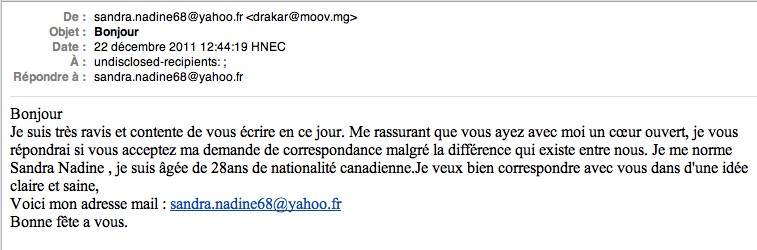
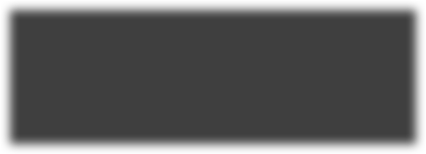


Un troisième cas classique, c'est une propo- sition de contact de la part d'une dame inconnue (romance scam).

Ces messages sont souvent destinés à des un- disclosed recipients, ce qui est louche en soi, et ils sont le plus souvent écrits en très mauvais français (image ci-dessous).

Il faut être particulièrement peu avisé pour tomber dans le piège des scams classiques. Par contre, il existe des scams beaucoup plus subtils qui s'appuient sur des données con- cernant la personne cible, données trouvées par exemple sur LinkedIn ou le site web de l'entreprise où on travaille. L'accroche est du genre « vous vous souvenez sûrement de moi, on travaillait ensemble dans les années 1990 chez France Télécoms ». Ces scams person- nalisés coûtent toutefois beaucoup plus cher que les scams habituels et ils sont donc ordi-

nairement adressés à des cibles particulièrement intéressantes comme les cadres supérieurs.



Le **cheval de Troie** est plus rare que le scam, mais c'est le danger numéro 1 de la messagerie. Tout down- load depuis un site douteux est potentiellement dangereux. Télécharger un programme gratuit sur l'In- ternet peut suﬀire à installer en même temps un cheval de Troie caché à l'intérieur du programme.

Il existe aussi des chevaux de Troie qui s'installent tout seuls, sans intervention de l'utilisateur. Ceux-là sont particulièrement dangereux parce qu'il suﬀit de se rendre sur un site infecté pour qu'ils entrent dans le système sans qu'on s'en aperçoive. C'est pourquoi il ne faut en aucun cas laisser Java activé sur les navi- gateurs qu'on utilise.

Un cheval de Troie est impossible à déceler, sauf si on désassemble le logiciel dans lequel il est dissimulé.

Le désassemblage consiste à passer le programme dans un traducteur qui convertit le code exécutable en langage d'assemblage au moyen d'un traducteur appelé disassembler. C'est le processus inverse de celui d'un assembleur. Il est même possible de recréer du code qui ressemble au C/C++, mais le résultat est seu- lement du pseudo-code ; il constitue une aide à la lecture, il n'est pas recompilable. Cette conversion est eﬀectuée par un décompilateur (decompiler).

Hopper (http://www.hopperapp.com) et Retargetable Decompiler (https://retdec.com) sont des exemples de désassembleurs-décompilateurs et Hex-Rays ([https://w](http://www.hex-rays.com/products/decompiler))ww.he[x-rays.com/pr](http://www.hex-rays.com/products/decompiler))o[ducts/decompiler](http://www.hex-rays.com/products/decompiler))) un exemple de décompilateur.

La lecture du code désassemblé ou décompilé réclame beaucoup de patience, car le code créé est peu lisible. Par exemple, les noms originaux des variables sont perdus au moment de l'assemblage et ils ne peuvent pas être retrouvés. Ils sont donc exprimés en chiﬀres : total, inc et fin deviennent var0001, var0002 et var0003.

De plus, le code occupe beaucoup de place. Par exemple, les cinq lignes d'un programme Hello world classique en langage C, une fois assemblées puis désassemblées avec Retargetable Decompiler, deviennent un pro- gramme en langage d'assemblage de plus de 1'600 lignes.

Par exemple, cela veut dire que, pour trouver un malware caché dans le code de Windows en désas- semblant le code, il faudrait planifier quelques milliers d'années de travail à plein temps pour analyser le résultat : à la louche, la version désassemblée de Windows représente deux ou trois milliards de lignes de code.

**L'injection SQL**

Un autre type d'attaque est l'**injection SQL**. Supposons qu'une application web demande le nom de la personne qui eﬀectue une commande.

Si le client tape :

Dupont

Le code SQL ressemblera par exemple à ceci :

SELECT \* FROM Clients WHERE Nom = '**Dupont**'

Supposons maintenant qu'un malfaiteur tape ce qui suit à la place du nom :

'; DELETE FROM Clients WHERE 1 OR Nom = '

Le code SQL sera alors :

SELECT \* FROM Clients WHERE Nom = '**'; DELETE FROM Clients WHERE 1 OR Nom = '**'

Le résultat est que la table Clients va être entièrement vidée.

Une authentification par mot de passe peut être brûlée par le même moyen. Supposons que l'application demande le nom et le mot de passe.

Si le client tape :

Dupont

1234

Le code SQL ressemblera à ceci :

SELECT \* FROM Clients WHERE Nom = '**Dupont**' AND Motdepasse = '**1234**'

Supposons maintenant qu'un malfaiteur tape :

Dupont'--

Le code SQL sera alors :

SELECT \* FROM Clients WHERE Nom = '**Dupont'--**' AND Motdepasse = ''

La fin de la ligne va être ignorée puisque les deux tirets disent à l'interpréteur que c'est le début d'un com- mentaire. L'entrée du malfaiteur va être acceptée sans mot de passe.

**L'administration de la sécurité du réseau**

Si l'installation du câblage et des systèmes intermédiaires est faite par une entreprise externe spécialisée dans ce travail, les **daily jobs** (la gestion au quotidien du réseau) sont, eux l'aﬀaire des informaticiens internes de l'entreprise. Même si personne parmi eux n'est spécialisé en réseaux, ils sont chargés des actions de premier niveau. C'est à eux de détecter les problèmes et de faire venir les spécialistes quand besoin est.

Il y a plusieurs éléments essentiels pour assurer une bonne gestion du réseau et de la sécurité :

• Agir immédiatement en cas de problème. La surveillance du réseau est une tâche permanente.

Les opérations des malfaiteurs durent généralement de quelques secondes à quelques heures, mais il arrive trop souvent qu'on ne découvre ce qui s'est passé que des mois plus tard.

• Les personnes qui agissent au premier niveau doivent savoir par quel canal avertir les personnes du deuxième niveau (**escalation**).

• Gérer les alertes sans se laisser décourager par les fausses alertes. Tous les messages d'alertes doivent être vérifiés et « quittancés ».

Si une fausse alerte se produit de façon répétée, paramétrer le logiciel de sécurité qui la génère pour que cela cesse.

• Comprendre l'infrastructure du réseau et le routing interne pour être en mesure d'interpréter correc- tement les flux de données.

• Être capable d'interpréter correctement les journaux d'événements et de découvrir ce qui ne va pas.

Beaucoup d'administrateurs de réseaux ne savent pas distinguer les éléments suspects dans le flot énorme du trafic normal.

• Le trafic doit être journalisé. C'est souvent en analysant des journaux d'événements qu'on s'aperçoit qu'une attaque a eu lieu.

• Avoir une documentation du réseau à jour. Elle est nécessaire pour savoir où se trouvent les systèmes intermédiaires (switches, routeurs, etc.), à quoi ils servent et comment ils sont connectés au reste du réseau.

Des applications appelées NMS (Network Monitoring Systems) permettent de gérer le réseau. Cacti, Nagios et OpenNMS sont open source et gratuits.

Il existe aussi des centaines d'applications plus spécialisées comme Nessus, Nmap ou Wireshark.

Ces logiciels sont très utiles pour autant qu'on sache les utiliser, les paramétrer et analyser leurs résultats. Dans les réseaux comme dans tous les domaines de l'informatique, il faut penser au principe du **KISS** (Keep It Simple, Stupid!).