

Première partie : l'Internet

Introduction :

Né aux US pendant la guerre froide
Décentralisé, fonctionnant grâce à des normes claires.
Les soucis actuels autour de la gestion des rootservers.

Internet : petite révision

On commet souvent des abus de langage, qui peuvent révéler une certaine méconnaissance de ce qu'est Internet. Qui n'a jamais entendu dire "je surfe sur Internet" ?

Internet, comme nous le disions plus haut est **un ensemble de protocoles**, pour autant d'applications.

Si on veut synthétiser rapidement, le Net se compose, entre autres :

Activité > Protocole

- * Du **Web**, "l'interface graphique" qui permet d'afficher des informations sous la forme de pages HTML grâce au HTTP.
- * Du **Mail**, avec les protocoles que l'on connaît : IMAP, POP, SMTP, etc.
- * Du **chat**, comme l'IRC, pour Internet Relay Chat, qui permet de discuter en temps réel avec des personnes
- * Du **FTP**, pour File Transfer Protocol, qui permet de transférer des fichiers d'un client à un serveur, d'un ordinateur à un autre.
- * De **Usenet**, pour "Users' Network", qui permet les newsgroups.
- * Des protocoles de connexions et d'interrogations à distance; comme **Telnet**, **SSH**, etc.

Tout cela est normé (le W3C par exemple pour le web) ou les RFC pour de nombreux protocoles.

PRATIQUE : LE SITE DU W3C, LE SITE RFC EDITOR

Voilà un bref résumé de toute ce qu'on peut trouver sur Internet, et voilà pourquoi monter un serveur chez soi ne consiste pas seulement à installer un serveur Web de type Apache. Si vous souhaitez offrir une gamme complète de services à vos utilisateurs ou si vous préférez être indépendant pour le plus grand nombre d'applications, il va vous falloir trouver un outil pour chacun de ces éléments.

Le protocole TCP/IP : simple et indispensable

Début des années 60, contexte de guerre froide, le **DARPA** (l'agence du ministère de la Défense américain, chargée des projets de recherche militaire) commence à travailler sur la mise en réseau à grande échelle d'ordinateurs. Depuis le DARPA a mis au point le GPS et travaille, entre autres, à la mise sur pied de véhicules capables de circuler sans intervention humaine sur des dizaines de km.

60-70 : premières connexions de machines distantes, évolution des protocoles

72 : Invention du mail (courrier électronique)

78 : TCP/IP (Transmission Control Protocol), par Vinton Cerf et Robert Kahn

Cyclades : en France un projet similaire nommé Cyclades évoluait. Robert Kahn expliquera que certains concepts du projet Cyclades furent récupérés pour le réseau Arnapet

83 : Norme pour tout l'ARPAnet

89 : naissance du web au CERN en Suisse, par Tim Berners-Lee

HISTORIQUE DETAILLE

Le protocole **TCP/IP** est clairement indispensable au bon fonctionnement d'Internet. On pourrait presque dire qu'il est Internet.

En fait, le protocole TCP/IP se compose de deux protocoles, le Transmission Control Protocol et l'Internet Protocol. **Le TCP est détaillé dans un document en 1974 et introduit en 1977**, pour prendre la suite du protocole NCP (pour Network Control Protocol), qui n'était pas assez performant. Nommons ses célèbres inventeurs, **Vinton Cerf et Robert Kahn**. **En 1978**, un an après l'introduction de TCP, apparaît IP, qui lui est ajouté. **Ce double protocole devait être simple, robuste et tourner sur toutes les plates-formes (différents systèmes d'exploitation et différents matériels).**

Avec la connexion d'autres réseaux à l'**ARPAnet**, qui était réservé à l'usage militaire et scientifique dans le courant des années 70, il a fallu qu'un protocole prenne le dessus et soit adopté comme référence. **C'est en 1983 que le TCP/IP devient officiellement le protocole d'Internet**. Tous les sites connectés à l'ARPAnet, ancêtre d'Internet, ont dû passer à ce protocole, non sans quelques heurts.

Pour bien aider à faire la différence entre Internet et Web, précisons que le système hypertextuel, inventé par **Tim Berners-Lee n'a fait sa première apparition qu'en 1989**, avec des premiers pas de développement qui s'étalent sur les années 90 et 91, soit 15 ans après les débuts du TCP/IP.

TCP/IP, comment ça marche ?

On a dit que le TCP/IP est composé de deux protocoles. Si on se réfère au modèle OSI (pour Open Systems Interconnection, qui découpe les systèmes de réseau en sept couches), on découvre que TCP et IP sont des protocoles de couches différentes.

Au sein de cette architecture OSI, le protocole TCP est **un layer 4. TCP veille au transfert de données entre les différents éléments de la session**. Afin d'arriver à ses fins, TCP utilise IP, d'où leur union.

IP est un protocole de couche, de layer 3. **IP sert au routage des données**, à savoir qu'il ouvre la voie aux paquets de bits jusqu'à l'utilisateur final en passant par les nœuds de commutations, ces points du réseau espacé entre l'émetteur et le récepteur, ou par des passerelles. **IP est de fait un protocole qui ne nécessite pas qu'une connexion continue soit établie entre les deux points.**

Résumons, les données sont découpées en paquets par TCP, qui les confie à IP pour le transport. Ces paquets contiennent entre autres l'adresse de l'expéditeur et du destinataire. IP se charge de l'envoi. Celui-ci passe par des nœuds, des gateways, qui l'expédient vers d'autres jusqu'à ce que le tout arrive à destination. Toutefois, le protocole IP ne fait pas attention à l'ordre d'arrivée. C'est alors au tour de TCP de tout mettre dans le bon ordre.

Les adresses IP

Les adresses IP sont extrêmement importantes dans le monde d'Internet. Chacune d'entre elles identifie un ordinateur unique pendant un certain temps, un bail. Ce bail est reconductible automatiquement. Dans la plupart des cas, une adresse IP = une machine. Dès que vous connectez une machine à Internet, elle doit avoir sa propre adresse IP. Son attribution se fait de différente façon. Toutefois dans la plupart des cas, cette adresse vous est accordée par votre FAI après tirage au hasard au sein d'un ensemble d'adresses disponibles.

IPv4 et IPv6

Actuellement la version la plus répandue du protocole IP est la version 4 (IPv4). Elle a été développée au début de l'année **1983**. Toutefois, une nouvelle version prend de plus en plus d'importance, l'IPv6, dont le déploiement a commencé le **14 juillet 1999** (preuve que le bogue de l'an 2000 n'inquiétait pas tant que ça). Cette version 6 offre des adresses IP plus longues, ce qui permet de fournir un plus grand nombre d'adresse IP, donc de satisfaire une plus grande demande. L'IPv6 est compatible avec l'IPv4.

Une adresse IP (version 4) est composée de quatre chiffres ou nombres séparés par des points. Par exemple 169.85.86.31. Ceci est un IP version 4, donc de 32 bits. Les IP créées par la version 6 sont de 128 bits. Elles sont notées sous forme hexadécimale, comme par exemple : 1075:0:0:0:7:620:212C:457A.

Les adresses IP sont actuellement réparties en quatre classes. Les classes A, B, C et D. La première pouvant comporter 16 millions d'adresses sur 126 réseaux, la classe B supportent 64.000 hôtes sur 16.000 réseaux, la classe C 254 hôtes sur 2 millions de réseaux, et la classe D propose des adresses multicast. Notons qu'une classe E existe, mais qu'elle reste expérimentale (champ décimal : 240 à 254).

L'adoption de l'IPv6 est très importante dans un contexte de "connexion permanente". S'il y a de plus en plus de personnes connectés, avec de plus en plus de matériels connectés, notamment à cause de la domotique, il faut trouver un moyen de nommer tout le monde. L'IPv6 le permet.

Attribution des adresses IP

Pour éviter que le réseau devienne une totale anarchie avec des centaines d'ordinateurs ayant la même adresse IP, celles-ci sont attribués par une instance centrale, l'**Internet Assigned Numbers and Authority (IANA)**.

L'IANA attribue donc un certain champ d'adresses IP à un **Regional Internet Registry** (les régions sont l'Europe, l'Asie/Australie/Pacifique, l'Amérique Latine et les Caraïbes, l'Afrique et l'Amérique du Nord). A leur tour, les RIR distribue gratuitement, les adresses IP étant un bien public, un certain nombre de blocs d'adresses IP de différentes classes aux Local Internet Registry.

Adresse IP dynamique ou statique ?

Vous savez que ce sont les FAI qui donnent une adresse IP à votre machine lorsque vous vous connectez. Votre ordinateur alors fait une requête et les serveurs du fournisseur d'accès. Vous savez également qu'il y a plusieurs classes d'adresses IP. Mais il existe une autre différence entre les adresses IP, et cette différence provient de la manière dont vous êtes connecté.

Si vous êtes connecté à Internet via l'ADSL ou le câble, il y a de fortes chances pour que votre adresse IP soit toujours la même, dans ce cas, on dit qu'elle est fixe ou statique. Rien de plus simple. On vous donne une adresse IP avec un bail renouvelé automatiquement.

Notez que si vous utilisez le câble, il arrive qu'en débranchant votre modem pendant un long moment, votre adresse IP soit attribuée à un autre modem, dans ce cas, votre adresse IP change. Certains fournisseurs d'accès à Internet via des services DSL permettent que vous gardiez la même adresse IP. Vous pouvez ainsi plus facilement monter un serveur chez vous. Nous verrons plus loin pourquoi.

Si vous vous connectez via un modem RTC, c'est-à-dire en utilisant votre ligne téléphonique normale, votre adresse IP, sauf chance extraordinaire, sera toujours différente, attribuée à la volée par votre FAI. Dans ce cas, votre adresse IP est valide le temps d'une connexion. On dit qu'elle est dynamique ou flottante.

Quelque soit "l'état" de votre adresse IP, elle vous est attribué de la même manière, grâce au même protocole. Dans cette famille de protocole les plus connus sont NAT, BOOTP et surtout **DHCP**.

NAT, pour **Network Address Translation**, traduit l'adresse IP connu dans un réseau en une autre adresse connue dans un autre réseau. Evidemment **le premier réseau est un réseau interne et le deuxième est le réseau externe**. Ce protocole permet de faire que plusieurs adresses IP internes correspondent à une ou plusieurs adresses IP externes. Cette solution est appréciée des entreprises puisqu'elle permet d'authentifier chaque packets de données, chaque requête passant par ce protocole. Il n'est pas utilisé par les FAI pour satisfaire votre demande. BOOTP, pour Bootstrap Protocol, est un protocole qui donne automatiquement une adresse IP à un utilisateur du réseau, les fonctions réseaux du système d'exploitation sont également mises à jour sans manipulation. BOOTP utilise un système de bail pour l'attribution temporaire des adresses, choisies au sein d'un "pool". Il existe toutefois un protocole plus avancé, le DHCP.

DHCP, pour **Dynamic Host Configuration Protocol**, automatise la gestion et l'attribution des adresses IP au sein d'un réseau utilisant le protocole TCP/IP. Ainsi, vous n'avez pas besoin d'entrer manuellement l'adresse IP de votre machine. Une telle manière de travailler peut convenir pour un tout petit réseau, mais est rapidement lassante.

Par exemple, admettons qu'un FAI a à sa disposition 150 adresses IP. C'est un exemple peu probable bien sûr. Le serveur DHCP veillera à ce que les 150 adresses IP soient correctement distribuées et une seule fois, tant que la première adresse est utilisée, elle ne sera pas refournie.

DHCP fonctionne sur le principe de bail d'une durée déterminée. Une adresse IP = un ordinateur = une période déterminée de temps. Mais il est également capable d'attribuer des adresses IP statiques, pour les serveurs notamment.

DNS : le lien entre l'IP et le nom de domaine

Service essentiel de l'Internet assurant la conversion des noms de domaine (e.g. www.linux-france.org) en adresse IP (e.g. 212.208.53.35). L'intérêt essentiel est de disposer de noms de machines plus faciles à mémoriser.

L'ICANN (Organisme créé en 1998) est le principal organisme international chargé de la gestion des DNS.

*tranet

On connaît le réseau des réseaux, le grand **Internet**, accessible à tous, disponible en permanence. Mais les on parle moins souvent des **intranet** ou des **extranet**.

Intranet

Le premier est un réseau qui offre des services similaires à ceux qu'on trouve sur Internet, mais ils tournent sur un réseau qui n'est pas forcément connecté au Net. L'intranet est souvent utilisé par les entreprises pour rendre accessibles des informations, via un réseau TCP/IP interne, fermé. L'intranet est souvent constitué de plusieurs sous-réseaux, des **Wide Area Network** ou des **Local Area Network**. Plusieurs réseaux intranet peuvent être reliés grâce au "**tunnelling**", à savoir un accès crypté sur un réseau public.

Extranet

Pour leur part, les extranet sont assez similaires aux intranets. A la différence qu'ils sont ouverts sur Internet, mais à un public bien précis. La présence d'un extranet ne signifie pas qu'il n'y a pas un site Web accessible à tous. Généralement l'extranet est un bon moyen de fournir un contenu particulier à des personnes privilégiées. **Des personnes en déplacement**, des collaborateurs, des clients, à qui on donne des identifiants et mots de passe pour se connecter au travers d'un **firewall**.

Les articulations et défenses du réseau

Intéressons nous un peu à la topologie des réseaux, ceux des entreprises ou des particuliers. Tous fonctionnent ensemble grâce au TCP/IP.

- * **Ces réseaux sont connectés entre eux par des gateways**, qui les interconnectent. On les appelle aussi "protocol converter". Il peut s'agir d'un élément matériel ou logiciel qui fait le pont entre deux protocoles qui servent la même fonction, l'exemple le plus connu est celui du TCP et du TP4.
- * **Certains gateways sont des proxies** : des ordinateurs et des logiciels dont le but est de répondre aux requêtes de clients, généralement un navigateur, en allant chercher l'information désirée sur le net et en la renvoyant au demandeur. Les proxies sont des agents sécurisés qui se connectent à Internet pour le compte d'un client. Pour éviter certaines attaques ou certains désagréments, les proxies tournent souvent sur des machines équipées d'un firewall.
- * **Les firewalls ou pare-feux sont de plus en plus répandus**. Windows XP propose d'ailleurs un pare-feu intégré. Il est toutefois recommandé d'en installer un autre, plus performant. Le firewall est un gateway très sécurisé qui protège l'accès à un parc de machines à la sécurité plus relâchée. Dans la plupart des cas (pour des amateurs), la machine qui sert de pare-feu est une machine sacrifiée, sur laquelle on surveille tout ce qui se passe.
- * Quelquefois sécuriser l'entrée dans un réseau n'est pas suffisant, dans ce cas, il faut simplement sécuriser la connexion à distance. Pour cela, on utilise le **VPN**, pour Virtual Private Network. VPN ajoute une surcouche cryptée sur un des layers de protocole les plus bas (Cf. l'architecture OSI). Ainsi VPN utilise le réseau Internet et connecte deux points distants grâce à un réseau privé virtuel, bien moins coûteux qu'un réseau privé physique. Le cryptage est fourni par des logiciels particuliers, des logiciels de pare-feux ou encore par des routeurs spéciaux. Notons qu'il existe plusieurs niveaux de cryptage, sur différents layers (2 et 3 pour un cryptage complet empêchant toute lecture de headers et donc toute analyse du réseau ou sur les layers 3 et 4, au niveau des protocoles. Les en-têtes sont en clair dans ce dernier cas de figure.

La bataille autour de l'IANA

Internet Address Naming Authority. Organisme vérifiant l'unicité des adresses sur le réseau des réseaux.

Qu'est-ce qu'un rootserver ?

Il existe 13 rootservers qui gèrent le trafic de l'Internet. Ce sont en fait de très grosses bases de données qui disposent d'enregistrements individuels pour tous les TLD du type .com, .net ou .org mais également pour les domaines géographiques.

Qui gère les rootservers gère l'ajout de nouveau TLD.

Qui gère les rootservers ?

Géré par l'IANA, une société de droit américain.

Où sont situés les rootservers ?

Les 13 serveurs ne sont pas tous situés aux USA. On les distingue par des lettres, de A à M. Le serveur M est géré par le projet WIDE à Tokyo, le serveur K est à Amsterdam, le F, I et J pointent en fait vers d'autres serveurs dans le monde (qq 80 sites dans 34 pays).

Pourquoi la polémique ?

Depuis juin 2005

Russie, Iran, Brésil, UE.

Proposent que l'IANA soit géré par un organisme du type ONU en lieu et place des Etats-Unis.

Si jamais on va au clash : deux sites pourraient exister pour la même adresse.

Les USA ne veulent pas de l'ONU.

De plus on ne peut pas confier la gestion de l'Internet à n'importe qui. Les USA ont assuré jusqu'à présent un développement harmonieux et ouvert de l'Internet. Le web, par exemple, a pu prendre son essor alors qu'il ne s'agissait pas d'une invention purement US. Des pays comme la Tunisie ou la Chine ne feraient pas de bons gestionnaires de l'Internet...

Comprendre les offres des FAI : principe de l'ADSL.

Ligne asymétrique.

Faut-il se dégrouper ?

Quelle importance à le débit ?

Comment établir une connexion ?

-> établir une connexion, les grandes étapes

Sites pratiques :

www.degrouptest.com

www.grenouille.com

Seconde partie : Installation Linux

Rappel : Linux est un système d'exploitation. Il ne fonctionne pas en même temps que Windows. Il utilise pleinement la machine. Il faut donc l'installer comme on installerait à nouveau Windows. Les deux systèmes peuvent cohabiter sur la même machine. La plus grande prudence est requise lors de l'installation si l'on manipule un disque dur sur lequel est déjà installé Windows.

Un LiveCD (un système qui se charge en mémoire) permet de tester sa machine et de découvrir Linux.

A - INSTALLATION

1 – Choisir une machine

Quel PC ?

Vérifier la compatibilité à l'aide d'un live CD, à l'aide d'un site web

2 – sauvegarder ses données

Quelles données sauvegarder ?

Quels outils pour les sauvegardes ?

Sur quels supports ?

Pratique : l'utilitaire de sauvegarde de Windows

3 – Acquérir les supports

Acheter une distrib

Acheter un CD gravé / acheter un magasin

Télécharger et graver une image ISO

Pratique : LinuxISO

4 – Lancer l'installation

Booter sur le CDRom (passage par le BIOS)

Les premières étapes de l'installation

(Si on utilise un liveCD on saute l'étape du partitionnement)

Ajout d'un support en ligne dans le cas d'une netinstall

Choix du niveau de sécurisation

Pratique : le BIOS (rôle et fonctionnement)

5 – Le partitionnement

MandrivaLinux : édition de la table des partitions, les différents cas de figure

Ubuntu : édition en mode texte

OpenSUSE : partitionnement automatique ou édition manuelle

Création d'une partition /boot, le concept du dossier / partition

6 – Choix des paquetages

Les différents types d'installation (modifier le choix des paquetages par défaut pour arriver à une conso d'espace disque convenable). Le concept des partitions.

Les différences entre les différents types d'installation.

Quels sont les paquetages que l'on peut supprimer ? Quels sont ceux que l'on doit conserver ?

Choix de l'interface graphique.

7 – Formatage des partitions / installation

8 – Le chargeur de démarrage

9 – Création des comptes utilisateurs

Rappel sur l'utilisateur root / sur les mots de passe

10 – Configuration de fin d'installation

Reboot et vérification du chargeur de démarrage

B – PREMIER BOOT

1 – Ouverture de la session

2 – Activation des mises à jour automatiques

Suse watcher, Mandriva Update

3 – Vérification des périphériques

4 – Connexion au réseau