5. PRINCIPES FONDAMENTAUX D'UN RÉSEAU

5.1. LE PROTOCOLE TCP/IP

Le principe fondamental de l'Internet a été de créer un mode de transmission par paquet remplaçant les modes en continu utilisés jusque−là pour la transmission de données. Chaque fichier transmit sur Internet est segmenté en paquets de données autonomes pouvant être transmis indépendamment les uns des autres. Pour que cela fonctionne, chaque paquet de données doit contenir des informations de pilotage telles que l'adresse de l'ordinateur émetteur et l'adresse de l'ordinateur récepteur.

Le protocole de communication permettant de transmettre des données sur Internet est le protocole **TCP/IP**. TCP/IP n'est en fait pas un mais deux protocoles, l'un étant superposé sur l'autre.

Le protocole de premier niveau, **IP** (Internet Protocol) s'occupe du routage des informations entre l'expéditeur et le destinataire : il accomplit sa tâche en divisant les informations en paquets (de 1 500 octets) et leur adjoint une adresse de provenance et de destination (exactement comme une enveloppe envoyée par la poste).

TCP (Transport Control Protocol) s'appuie sur IP pour gérer le transfert des données entre l'expéditeur et le destinataire. TCP fournit également les mécanismes permettant d'établir les connections, de vérifier l'arrivée dans le bon ordre des données, de gérer des données perdues, les erreurs et de récupérer des données concernées.

Lors de la transmission de données sous forme de paquet, IP ne vérifiant en aucune manière que le paquet est bien arrivée, TCP exige que le destinataire envoi un accusé de réception ou ACK (Acknowledged). De ce fait, l'hôte expéditeur peut se trouver devant trois situations différentes :

- lorsque le destinataire reçoit un paquet, et si celui−ci est le paquet attendu, il répond par le message ACK ;
- si la somme de contrôle indique une erreur ou si le numéro d'ordre est incorrect, le destinataire envoie un message NAK (Not Acknowledged) ;
- si le destinataire ne répond rien, TCP décide que soit le paquet, soit la réponse s'est perdu et renvoie de ce fait le paquet concerné.

A noter que outre les données, TCP envoie également des informations lors de l'établissement de la connexion et lors de son interruption.

Précisons également que TCP n'est pas le seul protocole utilisant IP : TCP/IP comprend également UDP (Unigram Data Protocol). Il s'agit d'un protocole sans connexion et sans garantie utilisé pour des transmissions de faible importance (comme la vidéo ou le son sur Internet).

5.2. LE MODÈLE RÉSEAU TCP/IP

TCP/IP ne constitue que deux couches dans un ensemble de protocoles allant de la base (matériel) vers le sommet (application). Le **modèle réseau TCP/IP** ressemble au modèle réseau ISO/OSI à 7 couches (couche physique, couche liaison, couche réseau, couche transport, couche session, couche présentation et couche application).

TCP/IP est une hiérarchie réseau à quatre niveaux superposés au matériel :

4	Protocoles d'application	SMTP (Sendmail), HTTP (Apache), telnet, ftp, rlogin, DNS, etc..
3	Protocoles de transport	TCP, UDP, ICMP
2	Protocoles de réseau (Internet)	IP
1	Protocoles d'accès au réseau (liaison de données)	Ethernet, ISDN, SLIP, PPP, etc..

Matériel	Câbles, lignes téléphoniques, etc..

Exemple :

Dans une communication typique entre un serveur web et un client, les différentes couches ressembleraient à cela :

Du coté serveur, relié à un réseau Ethernet :

- niveau 4 : HTTP (Apache)
- niveau 3 : TCP
- niveau 2 : IP
- niveau 1 : Ethernet

Du coté du client, connecté à Internet par modem :

- niveau 4 : HTTP (Netscape)
- niveau 3 : TCP
- niveau 2 : IP
- niveau 1 : PPP (Point−To−Point Protocol) imbriqué sur la connexion série afin de franchir l'étape entre IP et le matériel)

5.3. ADRESSES IP ET CLASSES DE RÉSEAUX

5.3.1. Le futur IPv6

Selon la norme IPv4, une adresse est codée sur 32 bits (soient 4 octets), ce qui permettrait théoriquement d'attribuer 232 adresses. Du fait de la répartition en réseaux de classe A,B et C, le nombre d'adresses possibles est largement inférieur au nombre théorique et il existe aujourd'hui un risque de pénurie d'adresse IP.

La norme IPv6 consiste à utiliser 128 bits pour coder les adresses (soient 16 octets). Cette norme a été adoptée en 1995 après quatre années de discussions dans différentes assemblées et groupes de travail.

La compatibilité avec la norme IPv4 a été préservé afin de permettre une phase de transition suffisante pour le passage de IPv4 vers IPv6. A noter que les versions récentes de Linux prennent déjà en compte la norme IPv6.

5.3.2. Classes de réseaux

Pour que l'acheminement des données fonctionne sur un réseau TCP/IP (Intranet ou Internet), chaque ordinateur doit posséder **une adresse IP unique**. Si en plus, l'ordinateur doit communiquer sur Internet, son adresse IP doit également être unique.

Selon la norme en vigueur actuellement (**IPv4**), une adresse IP est codé sur 32 bits répartis en quatre octets : par exemple 192.168.20.101 (la valeur d'un octet variant de 0 à 255).

L'ensemble des adresses IP est divisé en régions, à l'intérieur desquelles coexistent plusieurs classes de réseaux. Internet considère que les adresses IP à l'intérieur d'une classe de réseau font partie du même réseau : Internet n'attend qu'un point d'entrée, ce que nous appelons une **passerelle**, pour pouvoir router des paquets aux hôtes de ce réseau.

L'espace adresse IP est réparti entre des régions de réseaux de classe A, B et C :

- les réseaux de classe A, en nombre très limité, possèdent une adresse dont le premier nombre est compris entre 1 et 126. Seul ce premier nombre est fixe. Un réseau de classe A peut posséder 16 777 214 hôtes ;

- les réseaux de classe B, possèdent une adresse dont le premier nombre est compris entre 128 et 191. Les deux premiers nombres sont fixes. Il peut ainsi exister 16 382 réseaux de classe B possédant chacun jusqu'à 65 534 hôtes ;

- les réseaux de classe C, possèdent une adresse dont le premier nombre est compris entre 192 et 223. Les trois premiers nombres sont fixes. Il peut ainsi exister plus de 2 millions de réseaux de classe C possédant chacun un maximum de 254 hôtes.

5.3.3. Masque de réseau et routage

Un masque de réseau est un nombre logiquement ajouté (à l'aide de l'opérateur booléen AND) à une adresse IP afin d'obtenir l'adresse réseau.

Exemple :

	198	4	211	127	Adresse IP
	255	255	255	0	Masque de réseau de classe C
donne	198	4	211	0	Adresse de réseau

Le masque de réseau définit les adresses d'une plage adresse IP considérés comme étant directement connectés, c'est à dire appartenant au même segment de réseau. Des adresses différentes − obtenues par addition avec le masque de réseau − sont considérées comme appartenant à un réseau externe, et doivent utiliser les passerelles et les routeurs pour communiquer.

Exemple : considérons les 3 hôtes suivants : hôte 1 d'adresse 192.168.1.1, hôte 2 d'adresse 192.168.1.2 et hôte 3 d'adresse 192.168.2.1

En définissant un masque de réseau de 255.255.255.0 pour tous les hôtes, les hôtes 1 et 2 sont considérés comme appartenant au même réseau : si l'hôte 1 envoie un paquet à l'hôte 2, TCP/IP tentera de l'envoyer directement. En revanche, l'hôte 1 ne peut envoyer de données directement à l'hôte 3 car le masque considère que 192.168.1 et 192.168.2 sont deux réseaux différents : il enverra donc le paquet vers une passerelle. Il en résulte que tout hôte possède l'adresse IP d'au moins une passerelle afin de pouvoir expédier les paquets qu'il ne peut transmettre lui−même.

Quel est l'intérêt de ce système ?

En divisant l'espace adresse en réseaux logiques, trouver un hôte particulier devient une tâche facile. Pas besoin de connaître tous les hôtes de l'Internet car il suffit de disposer d'une liste de passerelles et de sélectionner celle constituant l'étape logique suivant la route. La passerelle suit la même procédure à l'aide de sa propre liste de passerelles et ainsi de suite, jusqu'à ce que le paquet atteigne la passerelle finale et sa destination.

5.3.4. Adresses IP particulières

Il existe des adresses IP appelées adresses de diffusion permettant la réception de données sur l'ensemble des hôtes d'un réseau. Nous ne traiterons pas ici ces adresses particulières.

Certaines adresses sont réservées à un usage personnel. Elles ne sont pas routées sur l'Internet et ne peuvent pas générer de problèmes quand vous les réutilisez. Leurs intervalles sont :

Classe	Masque de réseau	Adresses réseau
A	255.0.0.0	10.0.0.0

B	255.255.0.0	172.16.0.0 à 172.31.0.0
C	255.255.255.0	192.168.0.0 à 192.168.255.0

Quelle adresse choisir pour configurer un réseau local ? Cela n'a pas vraiment d'importance mais il est recommandé d'utiliser pour un même réseau, des nombres consécutifs.

Par exemple, si vous avez deux ordinateurs connectés via Ethernet et vous avez besoin maintenant de deux adresses à assigner aux deux cartes réseau, vous pouvez utiliser simplement 192.168.0.1 et 192.168.0.2

A noter également que l'adresse 127 de réseau de classe A est universellement réservée à la boucle locale du réseau, ce qui permet de tester les fonctionnalités de l'interface réseau de son propre ordinateur (c'est pour cela que l'on retrouve systématiquement la ligne `127.0.0.1 localhost` dans le fichier `/etc/hosts`).

5.3.5. Le concept des ports

Lorsqu'un client contacte un serveur, c'est le plus souvent en vue d'utiliser un service précis, courrier électronique ou FTP par exemple. Afin de différencier ces services, TCP dispose du concept de port qui permet à même interface réseau de fournir plusieurs services différents.

Le port standard pour le protocole HTTP correspond au port 80. Tout service ou protocole réseau standard possède un port associé auquel se connectent les clients pour y accéder : qu'il s'agisse d'HTTP, de FTP, de telnet ou de tout autre standard. La liste des ports standards est défini dans le fichier `/etc/services`. Voici ci−après une liste provenant du fichier `/etc/services` : Les ports `http` (80) et `https` (443) sont les plus répandus. Il est possible de préciser un port particulier dans l'URL d'un navigateur : il suffit de placer " :" ainsi que le numéro de port après l'adresse web. Exemple : `http://localhost:10000` pour accéder à WebMin.

`inetd` (Internet Daemon) est le service chargé d'écouter les différents port. Lorsque `inetd` reçoit une requête sur un port dont il a la charge d'écouter, il exécute le service associé (contrairement à Apache qui s'exécute indépendamment).

5.4. NOMS LOGIQUES ET DNS

5.4.1. Adresses IP et noms logiques d'ordinateurs

Etant donné qu'il est difficile de mémoriser les adresses IP des différents ordinateurs au sein d'un réseau, il est fort pratique d'associer à chaque adresse IP un nom logique. La définition des correspondances entre les noms des machines et les adresses IP se trouve dans le fichier `/etc/hosts`.
Ce fichier doit être présent sur toutes les machines du réseau. Si un ordinateur est ajouté ou retiré du réseau, le fichier `/etc/hosts` doit être modifié en conséquence sur toutes les machines du réseau. Ce type d'administration n'est donc possible que si le réseau ne dépasse pas une certaine taille.

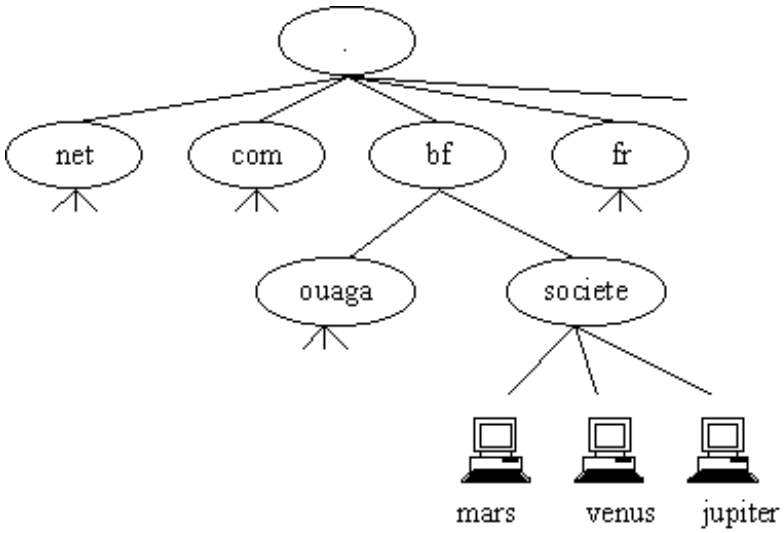
5.4.2. DNS − Domain Name Service

La méthode de mise en correspondance des noms d'ordinateurs et des adresses IP décrite précédemment a été la seule méthode employée sur l'Internet jusqu'en 1984. Jusqu'à cette date, toutes les adresses et noms d'ordinateurs étaient centralisés et gérés aux Etats−Unis par le NIC (Network Information Centre) sous la forme d'un fichier hosts.txt. Face à l'accroissement rapide de l'Internet, cette méthode s'est avérée rapidement impraticable, d'où l'introduction d'un nouveau mode d'adressage des ordinateurs : le DNS (Domain Name Service).

Organisation et structure de DNS :

Le DNS organise les noms d'ordinateurs selon une hiérarchie de domaines semblable à celle du système de fichier Linux. Partant d'une racine commune (domain racine), le service se stratifie en plusieurs couches depuis la couche

supérieur contenant les domaines principaux, vers les couches inférieures divisées en sous−domaines.



Exemple de structure de domaine

Par domaine, on entend une collection d'ordinateurs regroupés selon des critères géographiques ou organisationnels. Ce type de structure permet de satisfaire facilement la contrainte d'unicité des noms d'ordinateurs. On obtient le nom complet d'un ordinateur en commençant par le nom de la machine dans le cadre de son sous−domaine particulier et en suivant le chemin qui remonte vers le niveau supérieur de la hiérarchie (TLD ou Top Level Domain) ; le symbole de séparation entre les différents niveaux étant le point.

L'administration des noms de domaine génériques est effectué par le NIC (http://www.internic.net). L'administration des noms de domaines géographiques a été transférée aux différents pays. En principe, le nombre de sous−domaines placés en dessous de la couche des domaines de second niveau n'est pas limité.

Fonctionnement du DNS :

Avec cette structure, on obtient une gestion décentralisée et délocalisée des domaines. Chaque serveur de nom local gère les données pertinentes de tous les ordinateurs relevant de son domaine de compétence et est en mesure de répondre aux demandes en provenance de l'Internet concernant son domaine.

Le DNS constitue une banque de données mondiale constitué d'un grand nombre de serveurs de noms de domaines. Un serveur de nom de domaine stocke les informations nécessaires relatives à tous les ordinateurs présent dans son domaine de compétence. Cette zone peut comprendre un ou plusieurs domaines. Dans chaque zone, deux serveurs de noms au moins doivent exister pour des raisons de fiabilité (informations accessibles par des voies redondantes).

Rappelons que l'adressage de chaque machine de l'Internet s'effectue exclusivement par l'intermédiaire de l'adresse IP. Lorsqu'une application (Netscape par exemple) veut prendre contact avec un ordinateur dont seul le nom DNS est connu, il est nécessaire de convertir au préalable le nom DNS en une adresse IP. Pour cela une requête est envoyé au serveurs de noms figurant dans le fichier de configuration. Concernant le fichier de configuration de résolution de noms de domaine, il existe deux stratégies différentes :

- la première possibilité consiste à adresser une requête directement à un serveur dont la compétence s'exerce sur les domaines principaux ;
- la seconde possibilité consiste à adresser la requête à un serveur de nom local qui à son tour, s'il ne peut satisfaire lui−même la requête, adresse celle−ci à un autre serveur de nom, etc.. la requête migre ainsi de la base vers le sommet.

La mise en oeuvre d'un serveur DNS sera traité ultérieurement.

5.5. OUTILS RÉSEAUX

Linux contient de nombreux de nombreux utilitaires permettant de faciliter l'administration d'un réseau.

ifconfig : utilitaire standard UNIX permettant d'obtenir des informations sur la configuration de l'interface réseau (carte Ethernet par exemple) : `$ ifconfig −a`
Servez−vous de `man ifconfig` pour connaître les options.

netstat : utilitaire de surveillance d'un réseau sous les systèmes UNIX.

ping : l'outil le plus simple et le plus pratique des outils réseaux. ping permet de vérifier si un nom d'hôte distant ou une adresse IP est accessible.

traceroute : utilitaire trés utile pour diagnostiquer des problèmes réseaux, en particulier si la commande ping ne réussit pas à atteindre le serveur distant. Il existe des traceroute graphiques permettant de visualiser le chemin parcouru par les données entre un client et un serveur.

5.6. CONFIGURATION D'UN RÉSEAU LOCAL SOUS LINUX

Interface réseau : l'interface réseau est représentée physiquement par votre carte réseau mais le terme interface réseau est aussi utilisé pour désigner un nom logiciel auquel assigner une adresse IP (eth0 par exemple). Une adresse IP est toujours assignée à une interface réseau, jamais à un ordinateur. La commande ifconfig sert à afficher la configuration des différentes interfaces réseau actives.

Adresses IP : référez vous au chapitre *Adresses IP particulières* pour décider quelle adresse utiliser pour votre réseau.

Fichiers de configuration :

`/etc/hosts` : ce fichier spécifie comment résoudre les noms des machines du réseau local (inutile de mettre en oeuvre un serveur DNS pour un petit réseau local). La syntaxe des lignes de ce fichier est :

```
     Adresse IP      Nom de l'hôte          Alias
Ex : 127.0.0.1       localhost
     192.168.0.1     sirius.mondomainesirius
```

`/etc/resolv.conf` : ce fichier spécifie où résoudre ce qui ne se trouve pas dans `/etc/hosts`. C'est dans ce fichier que vous devez spécifier les adresses IP des serveurs DNS utilisés pour accéder à Internet en suivant la syntaxe suivante : `nameserver 212.102.31.1`

`/etc/HOSTNAME` (ou `/etc/sysconfig/network` sur certaines distributions) : ce fichier configure le nom de la machine locale. Au démarrage du système, ce fichier est lu et son contenu est envoyé à la commande hostname. Vous pouvez utiliser la commande `hostname` pour changer le nom du serveur.

Exemple : `hostname sirius.mondomaine`

Autres fichiers de configuration du réseau : `/etc/hosts.allow` , `/etc/hosts.deny` et `/etc/hosts.equiv`.