A

Les réseaux IP

Objectif

Cette annexe en forme de petit chapitre a pour but de présenter les réseaux IP, leur configuration et les principaux protocoles qui les régissent. Elle est destinée aux lecteurs qui ne seraient pas familiarisés avec les réseaux IP, l'ARP, l'ICMP, le DHCP, le NAT, le DNS, le TCP et l'UDP et l'IGMP. Pour les autres, une piqûre de rappel ne peut pas faire de mal !

A.1 L'ORIGINE D'IP

L'*Internet Protocol* est issu des recherches menées par le département de Défense américain pendant la guerre froide, dans les années 1960, mais il n'a été standardisé qu'en 1982. Son but était de permettre l'émergence de réseaux maillés, donc décentralisés, de telle sorte qu'un unique missile nucléaire russe ne puisse pas paralyser l'ensemble des télécommunications aux États-Unis. Une multitude de réseaux différents sont interconnectés par des passerelles (les routeurs), ce qui permet à un paquet d'emprunter plusieurs chemins différents pour atteindre sa destination. Aujourd'hui, c'est fort heureusement pour des motifs bien plus agréables qu'on utilise IP : en effet, le réseau des réseau, Internet, repose sur lui.

A.2 LES ROUTEURS

Alors que le commutateur (ainsi que le pont) fonctionne au niveau de la couche 2 (les couches LLC et MAC), le routeur fonctionne sur la couche 3 (IP).

Voyons ce que cela signifie concrètement. Le commutateur lit l'en-tête des paquets Wi-Fi et Ethernet, en particulier les adresses MAC de destination et de source, et agit en conséquence. On dit pour cette raison qu'il s'agit d'un équipement « actif », contrairement à un concentrateur (*hub*) qui ne fait que répéter « passivement » ce qu'il reçoit, sans chercher à l'interpréter. En règle général, un commutateur ne modifie pas le paquet avant de le retransmettre sur un segment du réseau (sauf avec le MAC Masquerading, que nous avons vu au chapitre 2).

Un routeur va plus loin que le commutateur : il extrait le paquet IP de la trame Ethernet ou Wi-Fi, et utilise l'en-tête du paquet IP pour décider quoi en faire, c'est-à-dire essentiellement vers quelle interface réseau le retransmettre. Il laisse en général le paquet IP intact (à moins qu'il ne fasse du NAT, comme nous le verrons plus loin), mais pour réémettre le paquet IP sur le réseau voisin, il génère un nouveau paquet Ethernet ou Wi-Fi (éventuellement plusieurs) : le paquet IP est « encapsulé » (c'est-à-dire empaqueté) dans une trame de couche 2 contenant l'adresse MAC de la station courante comme source et celle du relais suivant comme destination, ainsi que le type 2048 (0x0800 en notation hexadécimale) pour indiquer que le protocole transporté est IP. Quand un paquet IP est bien encapsulé dans un ou plusieurs paquets Wi-Fi, il peut enfin être envoyé à travers les ondes.

A.3 L'ADRESSAGE IP

Chaque station possède une adresse IP[1], composée de 4 octets (notés au format décimal et séparés par des points, comme par exemple 192.168.12.34), unique sur l'ensemble des réseaux interconnectés. Elle est composée de deux parties, plus ou moins longues : la première représente le réseau auquel la station appartient, et la seconde représente l'identifiant de la station au sein de ce réseau. Ainsi, toutes les adresses IP des stations appartenant à un même réseau commencent par les mêmes bits. Par exemple, les 16 premiers bits (2 octets) peuvent être identiques : 192.168.10.5, 192.168.20.7, 192.168.30.4, etc. Ce réseau est alors noté de la façon suivante : 192.168.0.0 / 16. Une autre notation consiste à préciser le « masque réseau », c'est-à-dire les 4 octets dont les bits correspondant à l'adresse du réseau sont égaux à 1 et les autres à 0. Dans notre exemple, les 16 premiers bits sont égaux à 1 et les autres à 0 : on obtient 255.255.0.0.

1. Une station peut avoir plusieurs adresses IP. Dans ce cas, n'importe laquelle de ces adresses permet d'atteindre la station. Toutefois, une adresse IP ne doit être attribuée qu'à une seule station.

La première adresse IP d'un réseau est réservée pour représenter le réseau lui-même : il s'agit de 192.168.0.0 dans notre exemple. Cette adresse n'est en principe pas utilisée dans les paquets mais plutôt pour la configuration des matériels (dans les tables de routage, par exemple, comme nous le verrons). La dernière adresse IP d'un réseau est réservée pour pouvoir envoyer un paquet à toutes les stations du réseau et de ses éventuels sous-réseaux : c'est l'adresse de « broadcast direct ». Dans notre exemple, il s'agit de 192.168.255.255. Par exemple, si le réseau est constitué de trois sous-réseaux, 192.168.10.0 / 24, 192.168.20.0 / 24 et 192.168.30.0 / 24, alors un paquet envoyé à 192.168.255.255 atteindra toutes les stations de tous ces sous-réseaux. On peut également envoyer un paquet en broadcast en l'adressant à 255.255.255.255 qui est l'adresse de « broadcast limité ». Dans ce cas, le paquet ne sera envoyé qu'aux stations du réseau local, et non aux stations des autres sous-réseaux voisins.

A.4 CONFIGURATION IP D'UNE STATION ET DHCP

En général, une station est configurée de façon assez simple : on lui donne son adresse IP, son masque réseau, et enfin, dans ce réseau, l'adresse d'une « passerelle par défaut » par laquelle tout le trafic destiné à des stations extérieures au réseau local devra passer. Voici un exemple de configuration :

- Adresse IP : 192.168.1.37 ;
- Masque réseau : 255.255.255.0 ;
- Passerelle par défaut = 192.168.1.254.

Lorsque la configuration IP est fixée manuellement, on parle de configuration « statique ». Inversement, la configuration IP peut être obtenue automatiquement grâce au protocole *Dynamic Host Configuration Protocol* (DHCP) : si la station est configurée en « client DHCP », alors dès qu'elle est connectée au réseau (c'est-à-dire au moment de l'association dans le cas d'une station Wi-Fi), elle peut émettre une requête DHCP sur le réseau local (en *broadcast*) afin de réclamer sa configuration IP. Si un serveur DHCP se trouve sur le réseau local, alors il peut renvoyer à la station tous les paramètres IP dont elle a besoin. Ceci permet de simplifier considérablement la configuration réseau des stations : une fois un serveur DHCP configuré sur le réseau, il suffit de brancher les stations !

Le serveur DHCP peut éventuellement utiliser l'adresse MAC de la station (ou bien un identifiant qu'elle doit fournir dans la requête DHCP) afin d'attribuer systématiquement la même configuration IP à une station donnée. Ceci permet d'éviter qu'à chaque nouvelle connexion, une station obtienne une adresse IP différente.

A.5 LE DNS

Travailler avec des adresses IP n'est pas toujours très pratique pour un être humain, car ces adresses n'ont pas un format très lisible. Il existe heureusement un mécanisme appelé le *Domain Name System* (DNS) qui permet d'associer un « nom de domaine » à une adresse IP : exactement comme les pages blanches qui associent un numéro de téléphone à un nom. Lorsque vous tapez une adresse dans votre navigateur Web, mettons `www.wi-fiplanet.com`, votre navigateur commence par contacter un serveur DNS pour savoir à quelle adresse IP correspond ce nom de domaine (par exemple 63.236.18.119). Afin de ne pas perdre trop de temps en consultations DNS, le résultat des requêtes est conservé en mémoire tampon (*cache*) pendant un certain temps. Les logiciels réseau sont en général capables d'effectuer cette « résolution » de nom de domaine, et ils acceptent donc indifféremment les adresses IP ou les noms de domaine. La seule contrainte est qu'il faut configurer la station en lui donnant l'adresse IP d'un serveur DNS (ou de plusieurs, en cas d'échec sur le premier). Heureusement, les serveurs DNS peuvent être inclus dans la configuration renvoyée par le serveur DHCP, ce qui facilite la configuration des stations sur un réseau local.

A.6 LES RÈGLES DE ROUTAGE

À partir de sa configuration, chaque station déduit des règles de routage. Ainsi pour l'exemple précédent, les règles suivantes sont déduites : si un paquet est adressé à une adresse IP située entre 192.168.1.1 et 192.168.1.254, il faut chercher sur le réseau local l'adresse MAC de la station possédant cette adresse IP (voir paragraphes suivants) et lui envoyer directement le paquet. Si le paquet est adressé à l'IP 192.168.1.255, il faut le retransmettre sur l'ensemble du réseau local (*broadcast*). Pour toutes les autres IP, il faut transmettre le paquet à la passerelle située à l'adresse 192.168.1.254 qui se chargera de faire suivre le paquet.

En outre, d'autres règles de routage peuvent être rajoutées manuellement. Par exemple : « pour atteindre le réseau 10.15.0.0 / 16, passer par la passerelle 192.168.1.1 ».

Enfin, certains routeurs mettent en œuvre des protocoles de routage tels que *Routing Information Protocol* (RIP) qui permettent aux différents routeurs d'un réseau de s'échanger leurs informations de routage. RIP permet de simplifier la configuration de chaque routeur, mais aussi de réagir correctement si une route n'est plus disponible (même 2 ou 3 « sauts » plus loin).

Un routeur étant connecté à plusieurs réseaux distincts au travers de plusieurs ports, il possède une configuration IP complète pour chaque port, en particulier une adresse IP et un masque réseau. Chaque règle de routage doit préciser le port qu'il faut emprunter.

Enfin, il peut arriver que plusieurs passerelles permettent d'atteindre le même réseau. Il est alors nécessaire de définir un coût, appelé la « métrique », pour chaque règle de routage. Lorsque plusieurs routes sont possibles, celle dont le coût est le plus faible est prioritaire.

Une règle de routage se résume donc en général de la façon suivante :

Adresse du réseau de destination	Masque du réseau de destination	Adresse de la passerelle	Interface à emprunter	Métrique

Dans notre exemple précédent, nous aurions la table de routage suivante :

192.168.1.0	255.255.255.0	192.168.1.254	Port WLAN	0
10.15.0.0	255.255.0.0	192.168.1.1	Port WLAN	0
0.0.0.0 (par défaut)	0.0.0.0	192.168.1.254	Port WLAN	0

Imaginons un routeur Wi-Fi servant de passerelle avec un réseau filaire. La configuration suivante serait envisageable :

10.1.0.0	255.255.0.0	10.1.0.1	Port WLAN	0
10.2.0.0	255.255.0.0	10.2.0.1	Port LAN	0
0.0.0.0 (par défaut)	0.0.0.0	10.2.0.1	Port LAN	0

Si un paquet est envoyé, par exemple, à l'adresse 213.91.4.193, alors seule la troisième règle est satisfaisante, donc le paquet est envoyé vers la passerelle située à l'adresse 10.2.0.1 sur le port LAN. En revanche, si un paquet est envoyé à l'adresse 10.1.5.3, alors la première et la troisième règle semblent toutes deux satisfaisantes. On pourrait penser que le choix se fera en fonction de la métrique. Néanmoins, lorsqu'on a le choix entre un réseau et ses sous-réseaux, le sous-réseau a la priorité. Ainsi, la première règle sera choisie, et le paquet sera émis sur le port WLAN. Si l'on avait eu une règle de routage concernant le réseau 10.1.5.0 / 255.255.255.0, par exemple, alors elle aurait eu la priorité, quelle que soit sa métrique, car il s'agit d'un sous-réseau du réseau 10.1.0.0 / 255.255.0.0.

A.7 L'ARP

Avant qu'un paquet IP puisse être envoyé à la passerelle suivante (ou bien directement à la station finale si celle-ci se trouve sur le réseau local), il est nécessaire de trouver l'adresse MAC de cette passerelle (ou de la station finale), afin de pouvoir encapsuler le paquet IP dans un paquet Wi-Fi valable. Chaque station doit donc être capable de trouver, pour une adresse IP donnée, l'adresse MAC correspondante.

Ceci est mis en œuvre grâce à l'*Address Resolution Protocol* (ARP). Chaque station conserve en mémoire une table d'association entre adresses IP et adresses MAC. Celle-ci peut éventuellement être configurée manuellement, mais en général elle est constituée automatiquement. Lorsqu'une station a besoin de connaître l'adresse MAC correspondant à une adresse IP donnée, elle commence par consulter sa table ARP. Si l'adresse IP recherchée ne s'y trouve pas, la station émet alors une requête ARP sur le réseau local (en *broadcast*). Cette requête demande en substance : « que la station possédant l'adresse IP *a.b.c.d* se manifeste et me renvoie son adresse MAC ». Dès que la réponse revient, la nouvelle association est rajoutée à la table ARP.

En général, une association est automatiquement retirée de la table si elle n'est pas utilisée pendant quelques minutes. Consulter la table ARP est une méthode pour savoir quelles stations sont actuellement actives sur le réseau.

A.8 LES ADRESSES PUBLIQUES

Pour pouvoir communiquer avec le reste du monde sur Internet, une station doit avoir une adresse IP unique, qu'on appelle adresse IP « publique ». Afin de garantir cette unicité, un organisme appelé l'*Internet Network Information Center* (InterNIC) a été mis en place pour attribuer les adresses IP. Dans la pratique, il attribue des groupes d'adresses à des organismes tiers qui ont le droit (ou non) de les redistribuer à d'autres. Depuis 1993, des organismes distincts gèrent l'adressage pour l'Europe (RIPE), l'Asie (APNIC), le Canada (CA*net), le Brésil (RNP), etc.

Par exemple, un fournisseur d'accès à internet (FAI) français peut faire une demande auprès de l'organisme RIPE pour obtenir un groupe d'adresses (par exemple, 213.91.0.0 / 20, soit 4 096 adresses). Par la suite, lorsqu'un client se connecte à Internet au travers de ce FAI, il peut obtenir l'une de ces adresses IP publiques (par DHCP, par exemple). Le FAI possède souvent beaucoup plus de clients que d'adresses IP publiques : il compte alors sur le fait que ses clients ne se connectent pas tous en même temps. Le résultat est que l'adresse IP du client

peut varier d'une connexion à l'autre : on parle d'*adresse IP dynamique*. Certains FAI proposent en option un adressage IP statique (en général pour les offres professionnelles, plus coûteuses) : ils réservent alors une adresse IP (ou plusieurs) pour le client, et lui attribuent toujours la même. Ceci permet au client d'héberger des serveurs qui seront joignables depuis Internet, en tout temps, au travers de la même adresse IP publique.

Malheureusement, les adresses IP n'ont que 4 octets, ce qui n'offre « que » 4 milliards de possibilités environ. En outre, ces adresses sont attribuées par groupes, et ce partitionnement implique forcément des pertes : ainsi dans notre exemple, si le FAI ne compte que 500 clients connectés à un moment donné (en moyenne) alors près de 3 600 adresses sont inutilisées, donc gâchées. Les adresses ont été regroupées en cinq grandes classes :

- A = 0.0.0.0 / 1, divisé en subnets de 0.0.0.0 / 8 à 127.0.0.0 / 8 ;
- B = 128.0.0.0 / 2, divisé en subnets de 128.0.0.0 / 16 à 191.255.0.0 / 16 ;
- C = 192.0.0.0 / 3, divisé en subnets de 192.0.0.0 / 24 à 223.255.0.0 / 24 ;
- D = 224.0.0.0 / 4, réservé pour le multicast (voir paragraphes suivants).
- E = 240.0.0.0 / 4, réservé pour un usage futur.

Au début de l'Internet, des groupes d'adresses énormes ont été attribués un peu à la va-vite, essentiellement à de grosses sociétés ou organismes (en général américains). Par exemple, les sociétés Hewlett-Packard, Bell, Ford, Xerox, Apple, et bien d'autres ont toutes des groupes d'adresses de classes A !

Il existe maintenant une véritable pénurie d'adresses IP (surtout à l'extérieur des USA), ce qui signifie qu'une société n'utilise en général pas des adresses publiques pour l'adressage des stations de son réseau.

A.9 ADRESSES PRIVÉES ET NAT

Pour permettre aux réseaux locaux d'utiliser IP malgré la pénurie d'adresses IP publiques, un certain nombre d'adresses ont été réservées pour un usage local :

- 10.0.0.0 / 8 : de 10.0.0.0 à 10.255.255.255 (soit 16 777 216 adresses, classe A) ;
- 127.0.0.0 / 8 : de 127.0.0.0 à 127.255.255.255 (comme ci-dessus) ;
- 172.16.0.0 / 12 : de 172.16.0.0 à 172.31.255.255 (1 048 576 adresses, classe B) ;
- 192.168.0.0 / 16 : de 192.168.0.0 à 192.168.255.255 (65 536 adresses, classe C).

Le réseau local peut lui-même être partitionné en plusieurs sous-réseaux, par exemple 10.1.0.0 / 16 et 10.2.0.0 / 16. Par ailleurs, les adresses 127.0.0.0 / 8 sont réservées à l'interface *loopback*, c'est-à-dire pour qu'une station s'envoie un paquet à elle-même (en général l'adresse 127.0.0.1 est utilisée).

Bien entendu, si un paquet est émis directement sur Internet avec pour origine l'une de ces adresses privées, le destinataire recevra peut être le paquet, mais il ne saura pas où le renvoyer !

Pour résoudre ce problème, un mécanisme appelé la translation d'adresse ou *Network Adresse Translation* (NAT) est mis en œuvre par la passerelle entre le réseau local et Internet. Cette passerelle est la seule à devoir posséder une adresse IP publique (par exemple, 62.212.111.76), alors que toutes les stations du réseau local peuvent avoir des adresses IP privées. Ce mécanisme ressemble au *MAC Masquerading* décrit dans le chapitre 4, mais il se déroule au niveau de la couche IP. Lorsqu'un paquet part d'une station du réseau local (par exemple 10.1.0.32) vers Internet (par exemple 213.91.4.193), la passerelle située à l'interface entre le réseau local et l'Internet modifie le paquet sortant en remplaçant l'adresse IP source (10.1.0.32) par sa propre adresse IP publique (62.212.111.76) : c'est le *Source NAT* (SNAT). De cette façon, le destinataire aura une adresse IP publique valide à qui renvoyer sa réponse. Lorsque la réponse parvient à la passerelle, celle-ci modifie l'adresse de destination du paquet (62.212.111.76) en la remplaçant par l'adresse IP de la station qui était à l'origine de la requête (10.1.0.32) : c'est le *Destination NAT* (DNAT). Ce mécanisme, géré automatiquement par la passerelle, est parfois appelé le « NAT dynamique ».

Outre le fait qu'il permet à plusieurs stations de partager une même connexion à Internet, ce mécanisme sécurise en partie le réseau local : en effet, si un paquet provient d'Internet et n'est la réponse à aucune requête émise par une station locale, alors la passerelle le rejettera. Toutefois, afin de permettre à certains services locaux d'être accessible à partir d'Internet (serveur Web, service de voix sur IP…), la plupart des passerelles permettent de définir des règles de NAT manuellement : par exemple, on peut décider que tout le trafic de voix sur IP (VoIP) sera redirigé vers une station locale donnée. C'est ce qu'on appelle le « NAT statique ».

Malheureusement, le NAT est loin d'être idéal. On peut le voir comme une béquille pour pallier à la pénurie d'adresses sur Internet. Il présente plusieurs inconvénients :

- Le fait de devoir analyser et modifier les paquets prend du temps, ce qui ralentit légèrement les communications.
- Dans certains protocoles de haut niveau, par exemple le *streaming* audio ou vidéo ou certains jeux en réseau, une requête émise peut entraîner des

réponses multiples, simultanées ou non, éventuellement de nature différente et provenant même parfois de plusieurs serveurs distincts ! La passerelle doit alors être capable de comprendre que toutes ces réponses variées correspondent bien à telle ou telle requête, afin d'être capable de les acheminer vers la bonne station. Pour cela, il est nécessaire que la passerelle « reconnaisse » le protocole de haut niveau utilisé. De nouveaux protocoles étant définis tous les jours, la passerelle doit être régulièrement mise à jour pour savoir gérer le NAT pour tous les protocoles qu'on utilise.

- Lorsque les paquets sont cryptés au niveau de la couche 3 (en particulier avec IPSec) le fait de modifier le paquet peut rendre le paquet invalide. Ainsi, il n'est pas rare qu'il soit impossible de se connecter à un serveur VPN sur Internet à partir d'un réseau local.
- Certains serveurs VPN (ou autres) refusent même complètement que plusieurs clients se connectent à partir de la même adresse IP.

A.10 AUTRES FONCTIONS D'IP

En plus du routage entre réseaux et sous-réseaux, le protocole IP offre quelques fonctions supplémentaires, en particulier :

- Un contrôle d'erreur (assez sommaire), mis en œuvre dans l'en-tête de chaque paquet par une somme de contrôle calculée en fonction du contenu de l'en-tête.
- La capacité d'éviter les boucles infinies grâce à un nombre (8 bits) situé dans l'en-tête des paquets : le « temps à vivre » ou *Time To Live* (TTL). Ce TTL est décrémenté à chaque fois que le paquet passe par une passerelle. Lorsque le compteur arrive à zéro, le paquet est éliminé.
- La possibilité de distinguer le type de service (*Type of Service*,ToS) requis pour chaque paquet, par exemple pour mettre en œuvre des priorités différentes entre le trafic multimédia et le reste. Le champ ToS (8 bits) est malheureusement assez peu utilisé sur Internet, mais rien ne vous empêche d'en tirer profit au sein de votre réseau.
- La fragmentation des paquets si leur taille dépasse la taille maximale autorisée pour ce réseau : le *Maximum Transfer Unit* (MTU). Le MTU dépend du type de réseau sous-jacent. Lorsque le réseau sous-jacent est de type Ethernet, le MTU est par défaut de 1 500 octets car c'est la quantité maximale de données qui puisse être contenue par un paquet Ethernet. Bien entendu, la couche IP s'occupe de rassembler les paquets fragmentés à l'arrivée pour obtenir le paquet IP initial.

A.11 ICMP

Le protocole IP ne garantit pas qu'un paquet arrivera à destination. Aucun mécanisme de tentatives multiples n'est mis en œuvre à ce niveau. Toutefois, des protocoles de couches supérieures, tels que le *Transport Control Protocol* (TCP) peuvent mettre en œuvre des mécanismes assurant l'arrivée des paquets. En outre, il existe un protocole très lié au protocole IP, et dont le rôle est d'offrir un minimum de fonctions de contrôle pour assister le protocole IP : c'est l'ICMP.

L'*Internet Control Message Protocol* (ICMP) est un protocole transporté par des paquets IP, et qui sert à fournir un contrôle des communications IP entre les stations :

- En cas d'erreur, par exemple lorsque le compteur TTL arrive à zéro, lorsque la destination n'est pas joignable ou encore si le paquet est corrompu, alors un paquet ICMP peut être renvoyé par la passerelle vers la station source, pour l'informer de l'échec. Si le paquet ICMP lui-même ne parvient pas à destination, aucun nouveau paquet ICMP n'est envoyé, afin d'éviter un effet « boule de neige ». Il s'agit donc, à l'instar du protocole IP, d'un mécanisme sans garantie. Les anglophones appellent ça le *best effort*, c'est-à-dire le « meilleur effort », sous-entendu « sans garantie de résultat ».
- En outre, si une partie du réseau devient congestionnée, des paquets ICMP peuvent être échangés par les passerelles pour que des routes différentes soient empruntées.
- Enfin, les paquets ICMP peuvent être utilisés à des fins d'analyse du réseau, en particulier grâce aux paquets *ping*. Lorsqu'une station reçoit un ping (qui signifie à peu près « y a-t-il quelqu'un ? »), elle est censée répondre positivement. On peut ainsi savoir si une station est active ou non. En envoyant des ping successifs avec un TTL égal à 1, puis 2, puis 3, etc., on obtient des ICMP d'échec provenant des différentes passerelles par lesquelles les paquets passent pour arriver à destination. C'est ce qu'on appelle le mécanisme de « traceroute ».

A.12 IPv4 ET IPv6

Dans l'en-tête de chaque paquet IP, on trouve la version du protocole utilisé (4 bits) : actuellement la plus répandue est la version 4 (notée IPv4). La version 6 d'IP (IPv6) a été définie mais n'est pas encore très répandue. Elle apporte pourtant de nombreuses améliorations, en particulier :

- Des adresses IP de 16 octets (et non plus 4), ce qui permettra d'éliminer les problèmes de pénurie d'adresses que l'on observe actuellement : on peut calculer que même s'il y avait des milliards de milliards d'équipements connectés à Internet sur chaque mètre carré de la surface de la terre, chaque équipement pourrait avoir sa propre adresse IPv6. Bref, même en tenant compte du gâchis lors des partitionnements d'adresses, cela suffira pour longtemps.
- Les en-têtes ont été simplifiés, et la performance s'en trouve accrue.
- L'IPv6 définit un mécanisme d'attribution automatique des adresses dans un réseau local, ce qui devrait rendre le DHCP inutile et simplifier la configuration des réseaux.

La grande question actuelle est : si l'IPv6 a tant de qualités, quand va-t-on l'utiliser sur Internet ? Déjà, de nombreuses sociétés l'utilisent en interne (quelques opérateurs mobiles et FAI en particulier). Les principaux opérateurs sont en train de migrer vers l'IPv6. Windows et Linux le gèrent correctement. Toutefois, il manque encore une réelle volonté de la part de certains des opérateurs principaux d'effectuer ce changement (en particulier là où la pénurie d'adresse ne se fait pas encore sentir). En outre, il faudrait que l'ensemble des logiciels réseaux soit mis à jour pour comprendre l'IPv6 ! Bref, le plus probable est que des îlots de réseaux IPv6 vont s'étendre, en s'interconnectant au travers de l'IPv4, jusqu'à le remplacer complètement.

A.13 L'IGMP ET LE MULTICAST

Comme nous l'avons vu précédemment, les adresses de la classe D (224.0.0.0 / 4) sont réservées au trafic multicast. Le multicast permet de transférer des données de façon optimale à un groupe de stations : l'émetteur n'envoie qu'une seule copie des données, et les routeurs du réseau se chargent de fournir à chaque utilisateur du groupe sa propre copie des données. Pour cela, les stations doivent manifester auprès des routeurs leur volonté de rejoindre ou de quitter un groupe. C'est le but de l'*Internet Group Management Protocol* (IGMP) : pour rejoindre ou quitter un groupe, une station doit envoyer un paquet IGMP en broadcast IP limité (sur le réseau local). Les routeurs du réseau, s'ils savent gérer le multicast, écoutent ces paquets IGMP, et utilisent ensuite des protocoles variés (comme DVRMP ou PIM par exemple) pour se synchroniser avec les autres routeurs et optimiser la livraison des paquets, par exemple en bâtissant dynamiquement un arbre de livraison pour chaque groupe multicast présent sur le réseau. Si vous comptez faire beaucoup de vidéoconférences ou de VoIP, il est possible que de tels routeurs (et commutateurs) soient nécessaires.

Malheureusement, IPv4 considère le multicast comme une option. De ce fait, ce type de trafic ne passe pas bien sur Internet car rares sont les opérateurs qui le mettent en œuvre. Toutefois, certains opérateurs ont commencé à déployer des routeurs multicast, de sorte qu'une part grandissante d'Internet, appelée le MBone (ou *Multicast backBone*), autorise ce type de trafic. Aujourd'hui, l'accès au MBone est encore assez limité, mais il s'agit là encore d'une des révolutions annoncées du Web, car cela permettra d'ouvrir réellement les portes d'Internet à des applications telles que la téléphonie et la télévision numérique haute définition. Notons qu'avec IPv6, la gestion du multicast est obligatoire pour les routeurs : l'IPv6 apportera également le multicast.

A.14 L'UDP ET LE TCP

Pour finir sur ce résumé des réseaux IP, il faut mentionner les principaux protocoles utilisés au-dessus d'IP, sur la couche 4 (transport), à commencer par le *User Datagram Protocol* (UDP) et le *Transport Control Protocol* (TCP).

A.14.1 L'UDP

UDP ne fournit presque aucun service supplémentaire par rapport à IP :

- Une somme de contrôle permet d'avoir une certaine garantie qu'un paquet n'a pas été corrompu pendant son transport.
- Chaque paquet contient le « port » de destination (un nombre de 2 octets) : il permet d'identifier un service spécifique sur la machine distante (il n'a aucun rapport avec les ports physiques des routeurs et des commutateurs). Ainsi, une même machine peut héberger deux services UDP (par exemple deux serveurs RADIUS) configurés sur deux ports différents : par exemple les ports 1 812 et 1 813. De cette façon, une station pourra préciser, grâce au port, le service avec lequel elle souhaite communiquer. Bien qu'on puisse en principe utiliser n'importe quel port pour n'importe quel service, de nombreux ports ont été réservés pour des services particuliers. Par exemple, les ports UDP 1 812 et 1 813 sont réservés au protocole RADIUS.
- Chaque paquet contient également le port source, qui peut éventuellement être utilisé par le destinataire pour répondre à la requête.

C'est tout ! Le protocole UDP est un protocole non orienté « connexion », c'est-à-dire qu'il n'est pas nécessaire d'établir un lien entre deux stations avant de communiquer. Comme IP, rien ne garantit qu'un paquet UDP arrivera bien à

destination, et en outre, si l'on envoie plusieurs paquets, on ne peut même pas être sûr qu'ils arriveront dans le bon ordre ! En revanche, c'est un protocole très « léger », qui est bien adapté pour des échanges ponctuels (supervision de matériel par exemple) ou des échanges de données pour lesquels quelques pertes et imprécisions ne sont pas graves pourvu que le flux soit soutenu (*streaming* vidéo par exemple). En outre, il est possible d'envoyer des paquets UDP en broadcast ou en multicast, alors que le TCP est limité à l'unicast.

Les principaux protocoles basés sur UDP/IP sont : DHCP et DNS (voir paragraphes précédents), SNMP (supervision de stations) et RADIUS (authentification, autorisations et comptabilité). Ce dernier est détaillé dans le chapitre 10.

A.14.2Le TCP

Le *Transport Control Protocol* (TCP) est le protocole de transport le plus utilisé sur Internet. Il offre quelques services essentiels qu'IP ne fournit pas :

- Grâce à des échanges d'accusés de réception (ACK) et de renvoi automatique des paquets en cas de problèmes, le protocole TCP peut être considéré comme fiable du point de vue des couches supérieures.
- Le protocole TCP gère des connexions : avant de se communiquer des données, les deux stations doivent établir une connexion logique, appelée un *socket* (littéralement, une prise). Bien que dans la pratique les données soient toujours échangées par le biais de paquets, le protocole TCP donne l'illusion aux protocoles de couches supérieures que le flux de données est continu, en regroupant lui-même les données à transmettre en paquets et en les rassemblant à l'arrivée (éventuellement en les remettant dans le bon ordre). Ceci est particulièrement pratique lorsqu'il s'agit de transférer des fichiers, par exemple.
- TCP offre ainsi des connexions fiables et *full duplex*, c'est-à-dire que les deux stations peuvent envoyer et recevoir des données au travers du même socket TCP/IP.
- Comme UDP, un paquet TCP contient un port source et un port de destination. Une fois qu'un socket est établi, les ports source et destination sont fixés.
- Un mécanisme (optionnel) permet de détecter si un socket est rompu même lorsqu'il n'est pas utilisé par les couches supérieures, et d'en informer les couches supérieures.
- Comme si tout ceci n'était pas suffisant, TCP contrôle automatiquement le débit, pour l'optimiser en fonction de la bande passante et de la disponibilité de chaque station.

La liste des protocoles qui reposent sur TCP/IP est longue, mais voici les plus connus : *HyperText Transfer Protocol* (HTTP, navigation Web), *File Transfer Protocol* (FTP, transfert de fichiers), *Simple Mail Transfer Protocol* (SMTP, envoi d'emails), *Post Office Protocol* (POP, téléchargement d'emails), *Internet Message Access Protocol* (IMAP, gestion d'emails), *Network News Transport Protocol* (NNTP, gestion de groupes de discussions), etc.