Chapitre 8

Le routage

Nous avons vu au cours des chapitres précédents que l'acheminement des messages à travers un ou plusieurs réseaux nécessitait des connaissances sur le réseau et l'état de ses liaisons. Les équipements spécifiques, les routeurs, organisent cet acheminement. Ils utilisent pour cela des algorithmes classiques de recherche du meilleur chemin dans un graphe. Nous verrons que pour la mise en œuvre dans un grand réseau, il faut prévoir d'échanger entre ces routeurs des informations de contrôle dont le but est de construire pour chacun une table de routage. Cette table donne, pour chaque destination, la route à emprunter ainsi que son coût. Nous abordons les deux grandes familles d'algorithmes de routage et les protocoles associés pour véhiculer les informations entre les routeurs.

1 Objectifs du routage

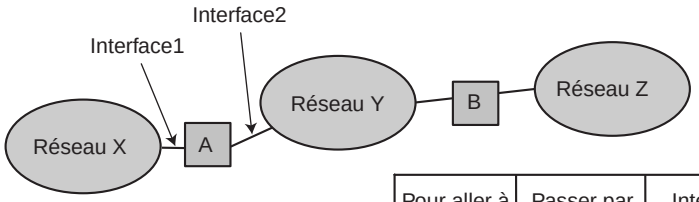
Le but d'un protocole de routage est très simple : fournir l'information nécessaire pour effectuer un routage, c'est-à-dire la détermination d'un chemin à travers le réseau entre une machine émettrice et une machine réceptrice, toutes deux identifiées par leur adresse. Les protocoles de routage établissent des règles d'échange entre routeurs pour mettre à jour leurs tables selon des critères de coût comme, par exemple, la distance, l'état de la liaison, le débit. Ils améliorent ainsi l'efficacité du routage. La diversité des réseaux et de leurs services fait du routage un élément clé de leur bon fonctionnement. Il y a de très nombreux problèmes à résoudre. L'un des problèmes fondamentaux à éviter réside dans les boucles de routage (le message peut « tourner en rond » dans le réseau et ne jamais atteindre son destinataire). L'autre apparaît lorsqu'il y a une panne dans le réseau et qu'il faut optimiser le calcul des nouvelles routes : une fois la panne détectée, il faut transmettre l'information sur l'événement le plus rapidement possible pour que les différents routeurs recalculent par où faire passer leurs messages en contournant la liaison en panne.

Le premier protocole de routage sur Internet fut RIP (*Routing Information Protocol*). On lui préfère aujourd'hui une version plus élaborée, OSPF (*Open Shortest Path First*). Le premier s'appuie sur un algorithme de la famille *à vecteurs de distance*. Le second utilise un algorithmes de la famille *à état des liens*. Dans les deux cas, les algorithmes de base sont issus de la théorie des graphes (Bellman[1]-Ford, pour RIP, et Dijkstra[2], pour OSPF). La difficulté est de les mettre en œuvre dans des environnements réels avec efficacité, tout en minimisant la consommation des ressources réseau.

Les tables de routage s'accroissent au fur et à mesure de la taille du réseau. Cela augmente l'espace mémoire nécessaire dans les routeurs et les ressources processeur. D'autre part, cela contribue à diminuer les performances du réseau, puisque celui-ci doit propager un important trafic entre les routeurs eux-mêmes. On découpe alors le réseau en sous-ensembles régionaux. À l'intérieur d'une région, les tables de routage contiennent une entrée par routeur (voir figure 8.1). De cette façon, l'interconnexion de réseaux différents est aisée. Une hiérarchisation à plusieurs niveaux peut s'envisager pour les très gros réseaux, même si la distance parcourue entre régions n'est pas globalement optimale.

Figure 8.1

Un routeur A et sa table de routage.



Pour aller à	Passer par	Interface
X	–	1
Y	–	2
Z	B	2

Le réseau Internet est ainsi organisé comme une collection de « systèmes autonomes », et une seule autorité administre en général chacun d'entre eux. On appelle système autonome, ou SA, un ensemble de réseaux interconnectés partageant la même

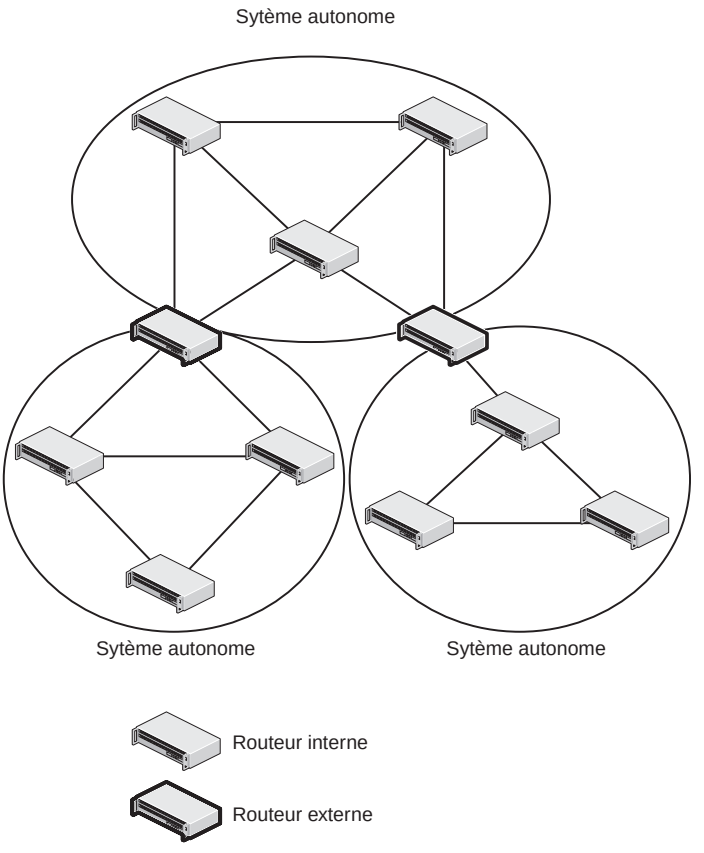
1. Richard Bellman (1920-1984), mathématicien américain, connu pour la programmation dynamique.
2. Edsger Dijkstra (1930-2002), chercheur hollandais, l'un des plus influents dans le domaine de l'informatique, récompensé par le prix ACM Turing.

stratégie de routage : tous les routeurs internes à un système autonome respectent le même protocole de routage régi par une autorité administrative (un département responsable spécifique comme un fournisseur d'accès ou toute autre organisation) [voir figure 8.2].

On désigne comme protocole *interne* aux routeurs, le protocole de routage ou IGP (*Interior Gateway Protocol*) utilisé à l'intérieur d'un système autonome. Par opposition, un protocole *externe* appelé EGP (*Exterior Gateway Protocol*) transfère les informations de routage entre les différents systèmes autonomes.

Figure 8.2

Systèmes autonomes et protocoles de routage internes et externes.



2 Principaux protocoles de routage

Nous décrivons succinctement dans cette section les protocoles de routage internes RIP et OSPF puis le protocole externe BGP.

2.1 RIP (*Routing Information Protocol*)

On a conçu RIP (*Routing Information Protocol*) pour fonctionner en tant que protocole interne dans des systèmes autonomes de taille modérée. Sa première version fut standardisée en 1988 (RFC 1058). La RFC 1723 propose des améliorations depuis 1994. RIP recherche le plus court chemin selon un critère de coût simple : le nombre de routeurs traversés. Cela revient à affecter un coût unitaire à la traversée de chaque routeur. RIP appartient à la famille des protocoles à vecteurs de distance, puisqu'il calcule la distance, en nombre de routeurs traversés, entre origine et destination.

Principe de fonctionnement

Le protocole est limité aux réseaux dont le plus long chemin (qu'on appelle couramment *le diamètre* du réseau) implique quinze routeurs au maximum. Il est mal adapté au traitement des boucles dans les chemins et utilise des mesures du coût des chemins (ou *métriques*) fixes pour comparer les routes alternatives. Les situations où les routes doivent être choisies en fonction de paramètres mesurés en temps réel comme un délai, une fiabilité ou une charge, se prêtent mal à ce type de traitement.

Un routeur RIP calcule des chemins pour différentes destinations, lesquelles sont spécifiées par leurs adresses IP, c'est-à-dire qu'une entrée dans la table peut représenter soit un réseau, soit un sous-réseau ou encore un nœud isolé. RIP ne spécifie pas le type de l'adresse : les routeurs découvrent la nature du destinataire en analysant les adresses transmises.

Les routeurs RIP sont *actifs* ou *passifs*. Actifs, ils transmettent et reçoivent les routes : ils diffusent leurs informations aux autres routeurs. Passifs, ils ne font qu'attendre la réception des informations. En fonction de celles-ci, ils calculent leurs tables de routage mais ne partagent pas les résultats de leurs calculs avec d'autres routeurs.

Le routeur RIP actif permet aux autres routeurs de mettre à jour leurs tables de routage toutes les 30 secondes. Si un routeur ne reçoit aucune mise à jour d'un autre routeur dans un délai de 180 secondes, il marque les routes desservies par ce dernier comme inutilisables. S'il n'y a aucune mise à jour après 240 secondes, le protocole RIP supprime toutes les entrées correspondant au routeur qui ne répond pas. Chaque diffusion RIP contient des paires adresses IP/nombre de routeurs à traverser (ou nombre de *sauts*). Comme le nombre de sauts est la seule mesure utilisée par le protocole, RIP ne garantit pas que le chemin sélectionné soit le plus rapide : un chemin court mais embouteillé peut être un mauvais choix par rapport à un chemin plus long mais totalement dégagé.

Lorsqu'un événement dans le réseau provoque un changement dans la table de routage d'un routeur actif, celui-ci envoie un message de mise à jour à ses voisins. Si cet événement a un impact sur les voisins, ceux-ci propagent l'information. On utilise une temporisation afin de stabiliser l'état du réseau et garantir que tous les messages de mise à jour ont été pris en compte avant de renvoyer une nouvelle mise à jour.

Variantes et améliorations

Des variantes procurent des améliorations au fonctionnement du protocole. Au lieu de diffuser le même message sur toutes les liaisons qui les relient, les routeurs composent des versions différentes de leurs informations, pour tenir compte des destinations atteintes *via* chaque liaison. Par exemple, si un routeur *A* envoie, *via B*, les messages à destination de *X*, c'est inutile pour *B* d'essayer d'atteindre *X via A*. Deux variantes sont possibles :

- Les routeurs ne donnent pas les informations sur les destinations atteintes à travers la liaison. Cette stratégie, dite « horizon partagé » (*Split-Horizon*), est la plus simple à implanter.
- Les routeurs indiquent dans leurs messages toutes les destinations possibles mais ils affectent une distance infinie pour celles situées en aval de ce nœud. Cette variante, dite « horizon partagé avec retour empoisonné » (*Split-Horizon with Poison-Reverse*), élimine immédiatement toute boucle de longueur 2.

Malgré ces améliorations, on ne supprime pas entièrement les risques de boucles.

Exemple

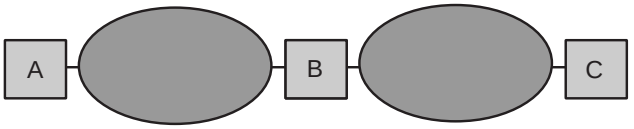
Soit un ensemble de trois routeurs *A*, *B*, *C*, illustrés à la figure 8.3, avec les tables de routage suivantes :

routage(A) = [(A, 0, –) ; (B, 1, B) ; (C, 2, B)].
routage(B) = [(A, 1, A) ; (B, 0, –) ; (C, 1, C)].
routage(C) = [(A, 2, B) ; (B, 1, B) ; (C, 0, –)].

Le triplet (*X*, *distance*, *Y*) signifie « pour aller à *X*, passer par *Y*, le chemin est de longueur *distance* ».
Si la liaison entre *B* et *C* tombe en panne, la table de *B* devient routage(*B*) = [(*A*, 1, *A*) ; (*B*, 0, –) ; (*C*, 16, *C*)]. En effet, 16 est considéré comme une destination inaccessible puisque le plus long chemin est de longueur 15. Quand *A* envoie sa table à *B*, celui-ci constate que *A* connaît une route de longueur 2 pour aller à *C*. Il met à jour sa propre table qui devient : (*B*) = [(*A*, 1, *A*) ; (*B*, 0, –) ; (*C*, 3, *A*)]. Cela crée une boucle puisque, pour aller à *C*, le routeur *A* envoie les messages vers *B* et le routeur *B* les renvoie vers *A*…

Figure 8.3

Trois routeurs et une boucle potentielle.



La nouvelle version RIPv2 fonctionne sur le même principe. Ce protocole véhicule simplement des informations supplémentaires, comme une étiquette qui fait la distinction entre les routes internes apprises nativement par RIP et les routes externes apprises par un autre protocole de routage. Il transporte de même le masque de sous-réseau qui permet d'affiner les routes avec la connaissance des sous-réseaux ou de l'*agrégation des adresses*[3]. Ces informations allègent la taille des tables de routage et participent à une meilleure efficacité du routage.

Remarque

Du point de vue de l'architecture en couches, le routage RIP est une application ; il utilise UDP comme protocole de transport avec le numéro de port 520. Un routeur RIP est donc une machine avec une architecture complète de protocoles, y compris Transport et Application.

D'autres fonctionnalités ont été proposées pour améliorer le fonctionnement du routage. On a cherché, par exemple, des moyens de rompre la *synchronisation* (les routeurs se mettent tous à diffuser leurs informations au même moment, et provoquent une rafale de trafic qui peut être insupportable). Puisque RIP utilise le protocole de transport UDP, on a imaginé des moyens d'acquitter de manière sûre la mise à jour, mais aussi de supporter plusieurs métriques, de rompre les boucles… Finalement, on a retenu une autre solution dans Internet : celle d'utiliser les protocoles à état des liens comme OSPF, considérés comme supérieurs aux protocoles à vecteurs de distance et que nous présentons à la section suivante.

2.2 OSPF (*Open Shortest Path First*)

L'algorithme SPF (*Shortest Path First*) calcule le plus court chemin vers toutes les destinations de la zone ou du système autonome, en partant du routeur où s'effectue le calcul (à partir de sa base de données topologiques). Il utilise un algorithme conçu par Dijkstra et calcule le plus court chemin, selon un critère de coût où interviennent de multiples paramètres : l'état des liens, l'encombrement du réseau et des mémoires des routeurs intermédiaires.

3. Cette expression désigne le regroupement du plus grand nombre de bits communs à deux ou plusieurs adresses IP. Par exemple, les adresses réseau : `195.67.65.0` et `195.67.127.0` ont leurs 17 premiers bits en commun. Pour un routeur donné, si le chemin pour atteindre les deux réseaux passe par le même routeur suivant, sa table de routage ne contiendra qu'une seule entrée pour les deux réseaux.

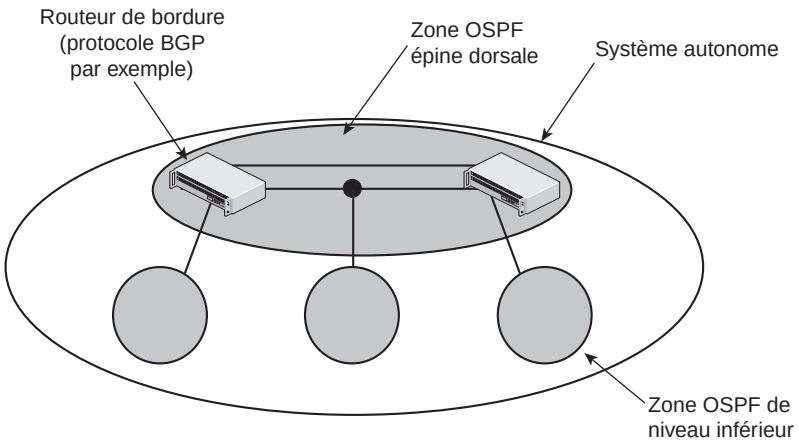
Principe de fonctionnement

Le calcul du plus court chemin est effectué de manière indépendante par tous les routeurs internes d'un système autonome SA. Grâce à cet algorithme, un routeur peut connaître le prochain routeur qui transmettra le message : il trouve les plus courts chemins (en termes de coût) d'un point à un autre, pour que le message arrive de manière optimale à son destinataire, puis il effectue la mise à jour de sa table de routage. Chaque mise à jour de la base de données entraîne celle de la table de routage. Il y a, comme précédemment, communication entre les routeurs. Celle-ci est régie par le protocole OSPF.

Ce protocole définit les règles et les formats de messages entre routeurs OSPF internes à un système autonome. Il a la particularité de s'appuyer directement sur IP (et non sur UDP comme le protocole RIP). C'est une nette amélioration, car le routage devient un traitement interne à la couche réseau et n'est plus considéré comme une application. De plus, le fonctionnement d'OSPF est optimisé si le SA est découpé en zones ; OSPF prévoit un découpage avec une hiérarchie à deux niveaux de zones. La zone de niveau le plus élevé est l'*épine dorsale* (ou *backbone zone*). Elle interconnecte les « routeurs de bordure » (*edge routers*). À l'intérieur de chaque zone du second niveau, les routeurs ne connaissent – et ne diffusent – que des informations internes à leur zone. Un routeur de bordure dans chaque zone assure le lien avec l'épine dorsale, comme le montre la figure 8.4.

Figure 8.4

Hiérarchie d'organisation des zones OSPF.



Messages du protocole OSPF

On distingue cinq messages OSPF : *hello*, *description de base de données*, *requête d'état de lien*, *mise à jour d'état de lien*, *acquittement d'état de lien*. Ils transportent des informations sur l'état des liaisons du SA et servent à déterminer une fonction de coût plus efficace que dans RIP.

Un routeur OSPF émet des messages hello à intervalles réguliers (environ toutes les dix secondes), sur chacune de ses interfaces. Ces messages établissent les relations d'adjacence[4] avec les routeurs directement liés à l'émetteur de ces messages. Les routeurs qui les ont reçus vérifient que les chemins restent disponibles.

Sur un réseau possédant au moins deux routeurs, on élit un *routeur désigné*, c'est-à-dire le responsable qui échange avec les routeurs des réseaux voisins. Il s'occupe de la distribution des messages de mise à jour d'état de lien. Son choix se fait sur la base de la plus petite

4. Dans la théorie des graphes, deux nœuds sont adjacents s'ils sont directement reliés. Ici, la notion d'adjacence est légèrement différente, puisqu'elle ajoute une règle supplémentaire : le routeur désigné est adjacent à tous les autres. C'est l'efficacité qui prévaut : dans un réseau local, il est inutile que tous les routeurs participent au routage. Seul l'un entre eux est le routeur désigné, tous les autres lui sont adjacents.

adresse IP parmi les routeurs susceptibles d'assumer ce rôle. Deux routeurs *R1* et *R2* établissent une relation d'adjacence si et seulement s'ils sont reliés par un lien direct ou si l'un d'entre eux est routeur désigné. Lorsqu'une nouvelle adjacence s'établit entre deux routeurs, ils synchronisent leurs bases de données d'état des liens par le message description de base de données.

Il est très important de protéger la base de données contre des erreurs (accidentelles ou dues à la malveillance), pour garantir la cohérence des calculs de chemins. Pour cela, on a prévu plusieurs précautions : acquittement, transmission sécurisée et temporisation des messages sur chaque liaison. Le message *acquittement d'état de lien* accuse réception d'une mise à jour : le routeur qui a envoyé ses indications de coût vers ses voisins sait que le message est bien parvenu. La transmission des messages de *description de base de données* est sécurisée : chaque enregistrement est protégé par un total de contrôle et tous les messages sont authentifiés. Cela évite d'éventuels messages qui contiendraient des informations erronées (éventuellement malveillantes, afin de détourner le trafic dans le réseau, par exemple). Enfin, on associe une temporisation à tout enregistrement : l'information contenue dans l'entrée de la table de routage sera supprimée si elle n'a pas été rafraîchie récemment : on préfère n'avoir aucune information momentanément plutôt qu'une information ancienne et inutilisable. Quand un routeur constate qu'une ou plusieurs des entrées de sa base de données sont périmées, il envoie une *requête d'état de lien* aux routeurs voisins pour faire la mise à jour des données.

OSPF est aujourd'hui le protocole interne le plus utilisé dans Internet. La qualité des informations transportées et la sécurité associée sont ses principaux atouts. Le fait que le routage reste interne à la couche réseau est un élément d'efficacité supplémentaire.

2.3 BGP (*Border Gateway Protocol*)

BGP est le protocole de routage interdomaine utilisé actuellement partout dans le monde. Conçu pour échanger des informations de routage entre systèmes autonomes, il est défini dans les RFC 1771 et 1774. Pour BGP, les différents réseaux sont organisés en SA, reliés par une ou plusieurs liaisons. Au sein d'un SA, le routage est calculé avec l'un des protocoles précédents (RIP ou OSPF). BGP intervient lorsque la route doit emprunter plusieurs SA.

Dans un système autonome, il y a un ou plusieurs routeurs de bordure qui dialoguent avec le ou les routeurs de bordure des SA voisins. Lorsqu'il n'y a qu'un seul routeur de bordure, le SA est vu comme un cul-de-sac : il ne peut pas être un SA de transit pour des messages sur l'interconnexion. Il est alors ignoré de BGP. Quand il y en a plusieurs, le SA est un SA de transit : des messages sur l'interconnexion peuvent y entrer par l'un des routeurs de bordure et ressortir par l'autre. Il faut toutefois ajouter que certains SA interdisent le transit interne (pour des raisons politiques ou commerciales, par exemple). Ils sont encore ignorés de BGP.

BGP ne prend donc en compte que les SA où le transit est autorisé (réseaux fédérateurs d'Internet, par exemple, ou réseaux d'opérateurs, moyennant des accords financiers). Les routeurs de bordure de ces SA sont appelés *routeurs BGP*. Ils calculent des routes avec un algorithme à vecteurs de distance. À la différence de RIP, ils mémorisent la totalité du chemin et non seulement le premier routeur du chemin. Ils échangent donc des informations complètes, ce qui est possible car le graphe BGP est de petite taille.

Les routeurs BGP communiquent par échange de messages transportés par des connexions TCP permanentes sur le port 179. Un routeur BGP est une machine dotée d'une architecture de communication complète, car le routage entre SA est considéré comme une application exigeant une grande fiabilité de communication.

2.4 Vecteurs de distance ou état des liens

Nous avons vu qu'il y avait deux familles d'algorithmes (à vecteurs de distance et à état des liens). La première calcule le meilleur chemin selon sa longueur (généralement exprimée en nombre de routeurs traversés). La seconde calcule le meilleur chemin selon une fonction de coût (le meilleur délai de traversée par exemple). Étudions quelques éléments d'analyse et de comparaison de ces deux familles : rapidité de convergence de l'algorithme, possibilités de métriques différentes, choix d'un chemin parmi plusieurs équivalents, utilisation de routes externes. On considère généralement qu'un protocole à état des liens offre plusieurs avantages par rapport à un protocole à vecteurs de distance.

- *Convergence rapide et sans boucle de l'algorithme.* Dans un algorithme à vecteurs de distance, le nombre d'itérations est proportionnel au nombre de routeurs. Dans le pire cas, il est égal au nombre de routeurs moins 1. Dans un algorithme à état des liens, la convergence s'établit en deux phases : transmission rapide des nouvelles informations puis calcul local du chemin. De plus, cette méthode évite les boucles, puisque tous les chemins calculés sont sains.
- *Métriques multiples.* Alors qu'il est difficile d'utiliser des métriques trop fines dans les algorithmes à vecteurs de distance, on peut supporter plusieurs métriques en parallèle, sans ralentir la convergence, dans les protocoles à état des liens. Cela provient du fait que la topologie est complètement connue pendant le calcul des chemins. On peut donc choisir la meilleure route en fonction de critères différents, en appliquant des métriques différentes. Les algorithmes à état des liens sont les premiers à offrir un routage en fonction de la qualité de service requise par l'utilisateur.
- *Chemins multiples.* Dans un protocole à vecteurs de distance, le choix d'un chemin parmi plusieurs se fait au hasard de la chronologie des échanges de messages. De plus, il n'est prévu qu'un seul routeur suivant dans la table de routage. Moyennant une légère modification de l'algorithme, les protocoles à état des liens peuvent tolérer des chemins multiples. On peut ainsi répartir le trafic entre plusieurs chemins équivalents en termes de coûts. L'équilibrage du trafic dans le réseau est une valeur ajoutée considérable, car elle contribue à la fluidité de la circulation des données et permet un réel contrôle de congestion.
- *Routes externes.* Les problèmes de routage que nous avons évoqués ne concernent que l'acheminement des données dans un réseau (considéré comme un ensemble homogène de stations et de routeurs). Une route externe est une route qui passe par d'autres zones ou d'autres réseaux que celui dans lequel on se trouve. Dans les grands réseaux – et plus encore dans Internet –, la connectivité se réalise à travers plusieurs points d'accès à différents réseaux de transit. Les éléments du choix des routes deviendraient trop complexes dans un protocole à vecteurs de distance : il faudrait prendre en compte plusieurs points d'accès, plusieurs prestataires de services, utiliser une route par défaut… Avec la possibilité d'utiliser des métriques multiples, les calculs de chemins intégrant des routes externes se font plus naturellement dans les protocoles à état des liens.

3 Routage et évolution des réseaux

Les services offerts dans les réseaux évoluent. La diffusion partielle ou totale des messages et certaines architectures comme les réseaux *peer-to-peer* posent des problèmes spécifiques. En outre, la présence d'utilisateurs mobiles est un nouveau défi pour le routage.

3.1 Diffusion

La diffusion générale (*broadcast*) suppose que le message est destiné à toutes les stations du réseau. La diffusion restreinte (*multicast*) suppose que le message est à transmettre à une liste de destinataires ou à un groupe d'utilisateurs, identifiés par une seule adresse dite *adresse de groupe*. On peut envisager plusieurs méthodes pour diffuser un même message à plusieurs destinataires : envoyer autant de messages que de destinataires, inonder le réseau avec des copies du message, calculer et gérer un arbre couvrant pour atteindre tous les destinataires.

- *Envoyer autant de messages que de destinataires.* Cette solution simpliste entraîne un gaspillage des ressources dans le réseau et nécessite le maintien d'une liste complète de tous les destinataires.
- *Inondation (envoi d'une copie du message sur chaque route).* Le nombre de messages et les ressources consommées sont excessifs… Il n'y a pas besoin de contrôler la liste des destinataires mais l'arrêt de l'inondation n'est pas un problème simple !
- *Routage multidestination.* Dès qu'un message arrive dans un routeur, ce dernier examine toutes les destinations pour déterminer les interfaces de sortie requises. Il génère autant de copies que nécessaire, en explicitant les destinataires concernés sur chaque interface. Après la traversée d'un certain nombre de routeurs, on se retrouve avec des messages qui n'ont plus qu'une seule destination.
- *Calcul d'un arbre couvrant par le premier routeur.* Cette méthode consiste à utiliser une variante de l'algorithme de *Spanning Tree* que nous avons vu lors du fonctionnement des ponts, au chapitre 5. Si le routeur connaît sur l'ensemble de ses liaisons celles qui font partie de l'arbre couvrant, il copie le message sur toutes les liaisons concernées (sauf celle d'où provient le message). Ce mécanisme est efficace mais il nécessite la connaissance de l'arbre couvrant.
- *Utilisation de l'algorithme RFP (Reverse Forwarding Path).* Lorsqu'un message arrive sur un routeur, ce dernier détermine si le message a suivi le chemin que lui-même utilise pour joindre l'émetteur. Si c'est le cas, il est vraisemblable que ce message a emprunté le plus court chemin depuis l'émetteur et qu'il s'agit du paquet d'origine. Le routeur envoie alors une copie du message sur toutes ses interfaces (sauf sur celle d'où provient le message). Dans le cas contraire, il considère le message comme un doublon et le rejette.

Pour les communications de groupe, il faut adapter les méthodes précédentes et faire vivre le groupe : un utilisateur nouveau peut se joindre à un groupe ou il peut en partir. Cela suppose l'utilisation d'un système de gestion de groupes qui crée ou supprime des groupes, autorise un utilisateur à rejoindre ou quitter un groupe, etc. Ces tâches de gestion des groupes sont transparentes pour l'algorithme de routage. Elles sont prises en compte par un protocole comme IGMP (*Internet Group Management Protocol*, RFC 2236). En revanche, les routeurs doivent savoir à quels groupes appartiennent les utilisateurs. Ils sont soit directement informés par les hôtes, soit les processus IGMP sont interrogés périodiquement. Les informations de routage sont alors communiquées aux voisins du routeur et se propagent ainsi à travers le réseau.

3.2 Utilisateurs mobiles

Les utilisateurs d'ordinateurs portables souhaitent lire leur courrier ou accéder au système de fichiers traditionnel, même quand ils sont en déplacement. Avant de router un message vers eux, il faut d'abord les localiser. Par définition, les équipements *fixes* ne se déplacent jamais. Ils sont connectés au réseau par des liaisons filaires (câbles en cuivre ou fibres optiques) ; les équipements *migrateurs* changent de site de temps à autre et n'utilisent le réseau que lorsqu'ils y sont physiquement raccordés. Enfin, les équipements *itinérants* se déplacent et

accèdent en permanence ou de façon intermittente au réseau. On peut même envisager des réseaux où tous les équipements sont mobiles ! On considère généralement les équipements migrateurs et les équipements itinérants comme des équipements *mobiles*.

Tous les équipements mobiles disposent d'un *site de domiciliation permanente* qui ne change jamais. Ils possèdent une adresse permanente qui ne suffit plus pour les localiser. L'envoi de messages pour des utilisateurs mobiles suppose un routage qui fonctionne d'après leurs adresses permanentes, quel que soit le lieu où ils se trouvent. On découpe généralement l'espace de déplacement en petites unités appelées *zones* (une *cellule radio*, par exemple). Chaque zone possède un ou plusieurs *agents extérieurs* (*foreign agents*) qui assurent le suivi des équipements mobiles se trouvant momentanément dans la zone. Une zone dispose en outre d'un *agent de domiciliation* (*home agent*) qui gère les équipements domiciliés dans la zone mais actuellement présents dans une autre zone.

Pour chaque mobile, un dialogue s'instaure entre son agent de domiciliation et les agents extérieurs des différentes zones qu'il visite. Ce dialogue dépend du parcours du mobile et de sa vitesse de déplacement. Les routeurs obtiennent, grâce à ce dialogue, les informations qui localisent le mobile dans la zone où il se trouve. Ils peuvent ainsi calculer la route pour l'atteindre.

3.3 RÉSEAUX *PEER-TO-PEER*

Un grand nombre de personnes possédant des connexions Internet permanentes souhaitent communiquer pour partager directement leurs ressources au moyen de réseaux peer-to-peer. Cette technologie est utilisée dans de nombreuses applications intéressantes et légales. Elle est souvent associée à l'idée de copies illégales de fichiers audio ou vidéo.

Il existe deux types principaux de réseaux *peer-to-peer* : les architectures totalement distribuées et les architectures hybrides. Dans la première, tous les équipements sont symétriques (on ne parle plus de client ni de serveur, puisque tout équipement est à la fois client et serveur). Il n'y a pas de contrôle central, ni de rapports hiérarchiques entre équipements. Il faut donc localiser un équipement en absence d'annuaire centralisé, car personne ne souhaite héberger et maintenir la base de données des ressources et de tous les équipements concernés. Cela suppose l'utilisation d'algorithmes particuliers, puisqu'il faut d'abord connaître l'équipement qui offre la ressource recherchée puis trouver le chemin pour l'atteindre. Dans la seconde, une station gère la base de données qui permet la localisation des ressources et des équipements et facilite donc le routage au sein du réseau.

Résumé

L'acheminement des messages à travers un ou plusieurs réseau(x) nécessite des connaissances sur le réseau et l'état de ses liaisons. Les routeurs organisent cet acheminement. Ils utilisent pour cela des algorithmes classiques de recherche du meilleur chemin dans un graphe. Il y a deux grandes familles d'algorithmes de routage : ceux à vecteurs de distance calculent le plus court chemin au sens du nombre de routeurs traversés ; ceux à état des liens estiment le coût des différents tronçons du réseau. Leur mise en œuvre dans un grand réseau n'est pas simple. Les routeurs échangent entre eux des informations de contrôle dont le but est la construction d'une table de routage pour chacun. Cette table donne, pour chaque destination, la route à emprunter ainsi que son coût. Pour faciliter les opérations de routage, les réseaux sont découpés en systèmes autonomes et le problème est d'abord résolu à l'intérieur d'un système puis entre deux systèmes, éventuellement avec des protocoles différents pour transporter les informations de routage.