Guy Pujolle

Cours réseaux et télécoms

Avec exercices corrigés

Avec la contribution de Olivier Salvatori

3e édition

ISBN : 978-2-212-12414-9

EYROLLES

13

Les réseaux IP

C'est le réseau Internet qui a introduit le protocole IP. Ce protocole a été ensuite repris pour réaliser des réseaux privés, tels les réseaux intranets et extranets ou les réseaux mis en place pour la domotique. Ces réseaux IP présentent de nombreuses propriétés communes. Ce cours examine ces propriétés en décrivant le fonctionnement des réseaux IP puis en détaillant les principaux protocoles à mettre en œuvre pour obtenir un réseau performant.

- Les environnements IP
- Les protocoles ARP et RARP
- DNS *(Domain Name Service)*
- ICMP *(Internet Control Message Protocol)*
- RSVP *(Resource reSerVation Protocol)*
- RTP *(Real-time Transport Protocol)*
- NAT *(Network Address Translation)*
- IP Mobile
- Fonctions supplémentaires

Les environnements IP

DARPA *(Defense Advanced Research Projects Agency).*– Agence du ministère de la Défense américain chargée des projets de recherche militaire.

Arpanet.– Premier réseau à commutation de paquets développé aux États-Unis par la DARPA.

Le principal intérêt du protocole IP est son adoption quasi universelle. C'est au milieu des années 70 que l'agence américaine *DARPA (Defense Advanced Research Projects Agency)* développe un concept de réseaux interconnectés, Internet. L'architecture et les protocoles de ce réseau acquièrent leur forme actuelle vers 1977-1979. À cette époque, la DARPA est connue comme le premier centre de recherche sur les réseaux à transfert de paquets, et c'est elle qui crée le réseau *Arpanet*, à la fin des années 60.

Le réseau Internet démarre véritablement en 1980, au moment où la DARPA commence à convertir les protocoles du réseau de la recherche à TCP/IP. La migration vers Internet est complète en 1983, quand le bureau du secrétariat de la Défense américain rend obligatoires ces protocoles pour tous les hôtes connectés aux réseaux étendus.

NSF *(National Science Foundation).*– Fondation de l'État américain qui subventionne les projets de recherche importants.

En 1985, la *NSF* (*National Science Foundation)* commence à développer un programme destiné à mettre en place un réseau autour de ses six centres de supercalculateurs. En 1986, elle crée un réseau fédérateur, le NSFNET, pour relier tous ses centres de calcul et se connecter à Arpanet. C'est l'ensemble de ces réseaux interconnectés qui forme Internet, auquel viennent s'ajouter petit à petit de nombreux réseaux nouveaux.

L'adoption des protocoles s'élargit alors aux entreprises privées, qui, à la fin des années 80, sont pour la plupart reliées à Internet. De plus, elles utilisent les protocoles TCP/IP pour leurs réseaux d'entreprise, même s'ils ne sont pas connectés à Internet. Ces réseaux privés s'appellent des intranets. Le prolongement permettant aux utilisateurs externes de s'interconnecter sur un intranet s'appelle un extranet.

C'est alors que se développent des opérateurs offrant des accès au réseau Internet, les FAI (fournisseurs d'accès à Internet), encore appelés ISP *(Internet Service Provider)*. Aujourd'hui, les ISP développent leurs propres réseaux, ou intranets, qui ne sont autres que des réseaux Internet contrôlés par un seul opérateur. À terme, on peut anticiper la disparition du réseau Internet d'origine au profit d'une dizaine de réseaux intranets mondiaux.

Cette croissance rapide induit des problèmes de dimensionnement et encourage les chercheurs à proposer des solutions pour le nommage et l'adressage de la nouvelle population.

De nos jours, des centaines de sociétés importantes commercialisent des produits TCP/IP. Ce sont elles qui décident de la mise sur le marché de nouvelles technologies, et non plus les chercheurs, comme à l'origine. Pour prendre en compte cette nouvelle réalité politique et commerciale, l'IAB *(Internet Activities Board)* s'est réorganisé en 1989. Depuis, la structure de l'IAB comprend

deux organismes : l'IRTF *(Internet Research Task Force)* et l'IETF *(Internet Engineering Task Force)*.

L'IETF se concentre sur les problèmes de développement à court et moyen terme. Cet organisme existait déjà dans l'ancienne organisation. Son succès a été l'un des motifs de sa restructuration. L'IETF s'est élargi pour prendre en compte des centaines de membres actifs travaillant sur plusieurs sujets en même temps. Il se réunit au complet pour écouter les rapports des groupes de travail et pour débattre des modifications et des ajouts portant sur TCP/IP. L'IRTF coordonne les activités de recherche sur les protocoles TCP/IP et l'architecture Internet en général. Sa taille est moins importante que celle de l'IETF.

Les documents de travail sur Internet, les propositions pour l'ajout ou la modification de protocoles et les normes TCP/IP sont publiés sous la forme d'une série de rapports techniques, appelés RFC *(Request For Comments)*. Les RFC sont disparates ; elles peuvent couvrir des sujets précis ou vastes et faire figure de normes ou seulement de propositions.

Récemment, l'IAB a commencé à prendre une part active dans la définition des normes. Tous les trois mois, il publie une RFC, appelée *IAB Official Protocol Standards*, qui rend compte du processus de normalisation et des nouvelles normes.

L'IAB attribue à chaque protocole de TCP/IP un état et un statut. L'état du protocole spécifie l'avancement des travaux de normalisation de la façon suivante :

- Initial *(initial) :* le protocole est soumis pour être examiné.
- Norme proposée *(proposed standard) :* le protocole est proposé comme norme et subit la procédure initiale.
- Norme de travail *(draft standard) :* le protocole a passé l'examen initial et peut être considéré comme étant dans sa forme semi-finale. Au moins deux implémentations indépendantes sont produites, et le document les décrivant est étudié par le groupe de travail *ad hoc*. Des modifications avant la norme finale sont souvent introduites après ces premières expérimentations.
- Norme *(standard) :* le protocole a été examiné et est accepté comme une norme complète. Il fait officiellement partie de TCP/IP.
- Expérimental *(experimental) :* le protocole n'est pas soumis à normalisation mais reste utilisé dans des expérimentations.
- Historique *(historic) :* le protocole est périmé et n'est plus utilisé.

Normalement, les protocoles soumis doivent être passés en revue par le groupe de travail correspondant de l'IETF. L'IAB vote ensuite pour son avancement dans le processus de normalisation.

Le statut du protocole indique sous quelles conditions il doit être utilisé. Ces différents statuts sont les suivants :

- Exigé *(required) :* toutes les machines et passerelles doivent implémenter le protocole.
- Recommandé *(recommended) :* toutes les machines et passerelles sont encouragées à implémenter le protocole.
- Facultatif *(elective) :* on peut choisir d'implémenter ou non le protocole.
- Utilisation limitée *(limited use) :* le protocole n'est pas spécifié pour une utilisation générale (par exemple, un protocole expérimental).
- Non recommandé *(non recommended) :* l'utilisation du protocole n'est pas recommandée (par exemple, un protocole périmé).

Comme expliqué précédemment, l'architecture IP implique l'utilisation du protocole IP, qui possède comme fonctions de base l'adressage et le routage des paquets IP. Le niveau IP correspond au niveau paquet de l'architecture OSI, mais avec une forte différence entre IPv4 et IPv6. IPv4 correspond à un protocole très simple, qui ne résout que les problèmes d'interconnexion, tandis qu'IPv6 a pour vocation de représenter complètement le niveau paquet.

Au-dessus d'IP, deux protocoles ont été choisis : TCP et UDP, qui sont abordés au cours 11, « Les protocoles de niveau supérieur ». Ces protocoles correspondent au niveau message (couche 4) de l'architecture OSI. Ils intègrent une session élémentaire, grâce à laquelle TCP et UDP prennent en charge les fonctionnalités des couches 4 et 5. La différence réside dans leur mode : avec connexion pour TCP et sans connexion pour UDP. Le protocole TCP est très complet, ce qui garantit une bonne qualité de service, en particulier sur le taux d'erreur des paquets transportés. Étant un protocole en mode sans connexion, UDP supporte des applications moins contraignantes en qualité de service.

Le niveau application, qui se trouve au-dessus de TCP-UDP dans le modèle Internet, regroupe les fonctionnalités des couches 6 et 7 de l'OSI. Le cours 12, « Exemples d'applications », détaille quelques applications des réseaux IP.

Questions-réponses

Question 1.– *Pourquoi les ISP préfèrent-ils développer leur propre réseau plutôt qu'employer le réseau Internet ?*

Réponse.– Le réseau Internet étant une interconnexion de réseaux, il ne permet pas d'offrir une qualité de service. En développant leur propre réseau intranet, les ISP contrôlent beaucoup mieux la qualité de service de leur réseau.

Question 2.– *Quels avantages les sociétés peuvent-elles tirer de l'utilisation du protocole IP ?*

Réponse.– Le Web étant devenu un grand standard, les entreprises ont développé des systèmes d'information compatibles et se sont placées dans l'environnement IP.

Question 3.– *Le réseau Internet propose un service de type best effort. Il est impossible d'y garantir un temps de réponse précis, d'où la difficulté de faire passer dans ce réseau de la parole téléphonique, qui demande un temps maximal de traversée de 300 ms. Dans le cadre de l'application de parole téléphonique, montrer que ce temps maximal de traversée du réseau peut être remplacé par un temps de traversée de 300 ms pour au moins 95 p. 100 des paquets.*

Réponse.– Si suffisamment de paquets arrivent à temps au récepteur, la parole téléphonique peut encore se dérouler. En effet, un paquet IP de téléphonie transporte entre 20 et 50 ms de parole. Aujourd'hui, les récepteurs savent prendre en compte ces trous de quelques dizaines de millisecondes, à condition qu'il n'y en ait pas trop. Une perte de 5 p. 100 de paquets est en général acceptable (le pourcentage acceptable dépend du degré de compression).

Question 4.– *En supposant des débits suffisamment importants des accès au réseau Internet (2 Mbit/s, par exemple), peut-on réaliser simplement de la télévision diffusée ?*

Réponse.– Oui, car la télévision diffusée accepte un retard important. Si le débit du réseau est suffisant, il est possible de resynchroniser le canal de télévision.

Les protocoles ARP et RARP

Internet propose l'interconnexion de réseaux physiques par des routeurs. C'est un exemple d'interconnexion de systèmes ouverts. Pour obtenir l'interfonctionnement des différents réseaux, la présence du protocole IP est nécessaire dans les nœuds qui effectuent le routage entre les réseaux. Globalement, Internet est un réseau à transfert de paquets. Les paquets traversent plusieurs sous-réseaux pour atteindre leur destination, sauf bien sûr si l'émetteur se trouve dans le même sous-réseau que le récepteur. Les paquets sont routés dans les passerelles situées dans les nœuds d'interconnexion. Ces passerelles sont des routeurs. De façon plus précise, ces routeurs transfèrent des paquets d'une entrée vers une sortie, en déterminant pour chaque paquet la meilleure route à suivre.

Le réseau Internet a été développé pour mettre en relation des machines du monde entier, auxquelles on a pris soin d'attribuer des adresses IP. Ces adresses IP n'ont aucune relation directe avec les adresses des cartes coupleurs qui permettent aux PC de se connecter au réseau. Ces dernières sont des adresses physiques.

Pour envoyer un datagramme sur Internet, le logiciel réseau convertit l'adresse IP en une adresse physique, utilisée pour transmettre la trame. La traduction de l'adresse IP en une adresse physique est effectuée par le réseau sans que l'utilisateur s'en aperçoive.

Le protocole ARP *(Address Resolution Protocol)* effectue cette traduction en s'appuyant sur le réseau physique. ARP permet aux machines de *résoudre* les adresses sans utiliser de *table statique*. Une machine utilise ARP pour déterminer l'adresse physique du destinataire. Elle diffuse pour cela sur le sous-réseau une requête ARP qui contient l'adresse IP à traduire. La machine pos-

résolution d'adresse.–Détermination de l'adresse d'un équipement à partir de l'adresse de ce même équipement à un autre niveau protocolaire. On résout, par exemple, une adresse IP en une adresse physique ou en une adresse ATM.

table statique.– Table de correspondance qui n'est pas modifiée automatiquement par le réseau lorsque interviennent des changements dans la configuration.

sédant l'adresse IP concernée répond en renvoyant son adresse physique. Pour rendre ARP plus performant, chaque machine tient à jour, en mémoire, une table des adresses résolues et réduit ainsi le nombre d'émissions en mode diffusion. Ce processus est illustré à la figure 13-1.

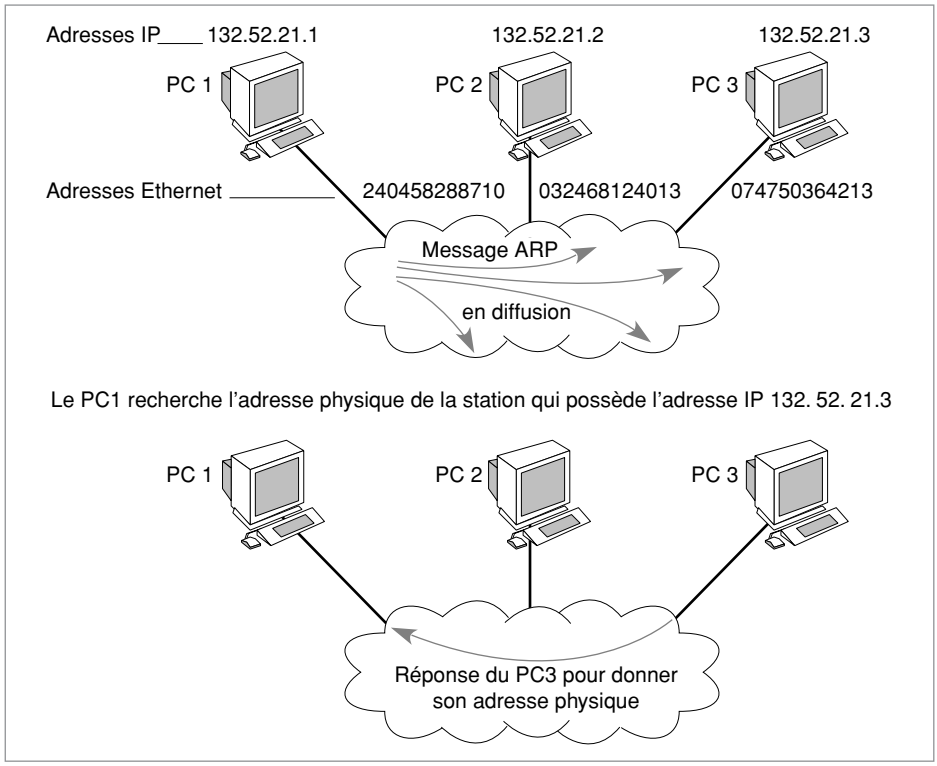

Figure 13-1. *Fonctionnement du protocole ARP.*

adresse logique.– Adresse qui n'est pas physique, c'est-à-dire qui n'est pas attachée à une connexion déterminée par son emplacement géographique. Les adresses logiques Internet sont les adresses IP.

De façon inverse, une station qui se connecte au réseau peut connaître sa propre adresse physique sans avoir d'adresse IP. Au moment de son initialisation *(bootstrap)*, cette machine doit contacter son serveur afin de déterminer son adresse IP et ainsi de pouvoir utiliser les services TCP/IP. Dans ce cas, le protocole RARP *(Reverse ARP)* permet à la machine d'utiliser son adresse physique pour déterminer son *adresse logique* sur Internet. Par le biais du mécanisme RARP, une station peut se faire identifier comme cible en diffusant sur le réseau une requête RARP. Les serveurs recevant le message examinent leur table et répondent au client. Une fois l'adresse IP obtenue, la machine la stocke en mémoire vive et n'utilise plus RARP jusqu'à ce qu'elle soit réinitialisée.

Dans la version IPv6, les protocoles ARP et RARP ne sont plus utilisés et sont remplacés par un protocole de découverte des voisins, appelé ND *(Neighbor Discovery)*, qui est un sous-ensemble du protocole de contrôle ICMP, que nous examinerons ultérieurement.

Questions-réponses

Question 5.– *Montrer que le mécanisme ARP marche bien si le réseau physique sous-jacent permet une diffusion simple. Les réseaux Ethernet et ATM peuvent-ils répondre à cette contrainte ?*

Réponse.– Le réseau physique doit effectuer une diffusion pour autoriser la correspondance d'adresse. Le réseau Ethernet est particulièrement adapté pour répondre à cette contrainte. En revanche, le réseau ATM n'est pas un réseau permettant d'effectuer de la diffusion simplement. Il faut donc utiliser d'autres mécanismes, comme la simulation d'une diffusion, en s'adressant à un serveur qui connaisse les correspondances d'adresses.

Question 6.– *Montrer que l'utilisation du protocole RARP par un ISP peut lui permettre de gérer efficacement un ensemble d'adresses IP.*

Réponse.– Les ISP ayant un grand nombre d'abonnés, ils n'ont pas la possibilité d'avoir suffisamment d'adresses IP pour les prendre tous en charge simultanément. Dans ce cas, au fur et à mesure des demandes de connexion, les ISP décernent des adresses *via* le protocole RARP.

Question 7.– *Les réseaux Infonet correspondent aux réseaux IP pour la domotique. Pourquoi le protocole IP semble-t-il intéressant pour ce type de réseau ?*

Réponse.– Plusieurs raisons peuvent être évoquées. La première concerne l'adressage. Il existe suffisamment d'adresses dans IPv6 pour en affecter une à tous les appareils domestiques : ampoules, branchements, capteurs, etc. Le protocole IP devenant un standard de connexion, il est tentant de connecter les réseaux de domotique à Internet. Enfin, les protocoles du monde IP correspondent assez bien aux types d'applications des réseaux de domotique.

Infonet.– Nom des réseaux IP interconnectant les équipements domotiques (capteurs, équipements domestiques, etc.).

domotique.– Désigne le processus d'informatisation de la maison, depuis les commandes automatiques et à distance jusqu'aux réseaux domestiques.

DNS *(Domain Name Service)*

Comme expliqué précédemment, les structures d'adresses sont complexes à manipuler, dans la mesure où elles se présentent sous forme de groupes de chiffres décimaux séparés par un point ou deux-points, de type abc:def:ghi:jkl, avec une valeur maximale de 255 pour chacun des quatre groupes. Les adresses IPv6 tiennent sur 8 groupes de 4 chiffres décimaux. Du fait que la saisie de telles adresses dans le corps d'un message deviendrait vite insupportable, l'adressage utilise une structure hiérarchique différente, beaucoup plus simple à manipuler et à mémoriser.

Le DNS permet la mise en correspondance des adresses physiques et des adresses logiques.

La structure logique prend une forme hiérarchique et utilise au plus haut niveau des domaines caractérisant principalement les pays, qui sont indiqués par deux lettres, comme *fr* pour la France, et des domaines fonctionnels comme :

- *com* (organisations commerciales) ;
- *edu* (institutions académiques) ;

- *org* (organisations, institutionnelles ou non) ;
- *gov* (gouvernement américain) ;
- *mil* (organisations militaires américaines) ;
- *net* (opérateurs de réseaux) ;
- *int* (entités internationales).

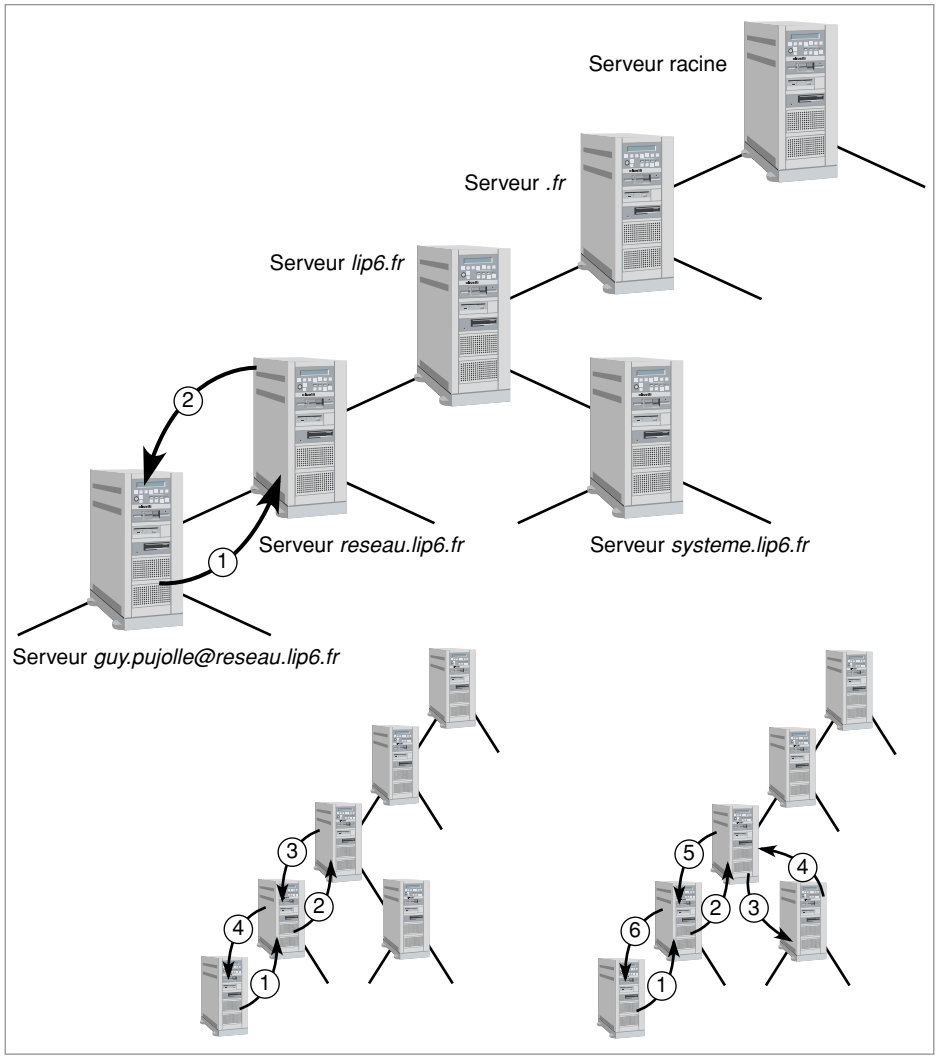

Figure 13-2. *Fonctionnement du DNS.*

À l'intérieur de ces grands domaines, on trouve des sous-domaines, qui correspondent à de grandes entreprises ou à d'importantes institutions. Par exemple, *lip6* représente le nom du laboratoire LIP 6, ce qui donne l'adresse *lip6.fr* pour le personnel de ce laboratoire. Ce domaine peut lui-même être décom-

posé en deux domaines correspondant à des départements différents, par exemple *reseau.lip6.fr* et *systeme.lip6.fr*. À ces différents domaines correspondent des serveurs, qui sont capables d'effectuer la correspondance d'adresse.

Les *serveurs de noms* du DNS sont hiérarchiques. Lorsqu'il faut retrouver l'adresse physique IP d'un utilisateur, les serveurs qui gèrent le DNS s'envoient des requêtes de façon à remonter suffisamment dans la hiérarchie pour trouver l'adresse physique du correspondant. Ces requêtes sont effectuées par l'intermédiaire de petits messages, qui portent la question et la réponse en retour.

serveur de noms.– Serveur pouvant répondre à des requêtes de résolution de nom, c'est-à-dire capable d'effectuer la traduction d'un nom en une adresse. Les serveurs de noms d'Internet sont les serveurs DNS.

La figure 13-2 illustre le fonctionnement du DNS. Dans cette figure le client *guy.pujolle@reseau.lip6.fr* veut envoyer un message à *xyz.xyz@systeme.lip6.fr*. Pour déterminer l'adresse IP de *xyz.xyz@systeme.lip6.fr*, une requête est émise par le PC de Guy Pujolle, qui interroge le serveur de noms du domaine *réseau.lip6.fr*. Si celui-ci a en mémoire la correspondance, il répond au PC. Dans le cas contraire, la requête remonte dans la hiérarchie et atteint le serveur de noms de *lip6.fr*, qui, de nouveau, peut répondre positivement s'il connaît la correspondance. Dans le cas contraire, la requête est acheminée vers le serveur de noms de *systeme.lip6.fr*, qui connaît la correspondance. C'est donc lui qui répond au PC de départ dans ce cas.

Le format d'une requête DNS est illustré à la figure 13-3.

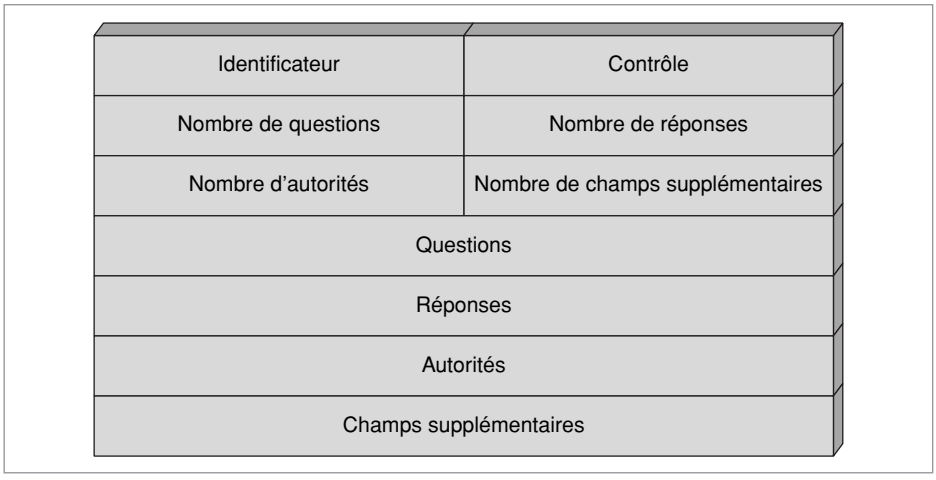

Figure 13-3. *Format d'une requête DNS.*

Les deux premiers octets contiennent une référence. Le client choisit une valeur à placer dans ce champ, et le serveur répond en utilisant la même valeur de sorte que le client reconnaisse sa demande. Les deux octets suivants contiennent les bits de contrôle. Ces derniers indiquent si le message est une requête du client ou une réponse du serveur, si une demande à un autre site doit être effectuée, si le message a été tronqué par manque de place, si le message de réponse provient du ser-

veur de noms responsable ou non de l'adresse demandée, etc. Pour le récepteur qui répond, un code de réponse est également inclus dans ce champ.

Les six possibilités suivantes ont été définies :

- 0 : pas d'erreur.
- 1 : la question est formatée de façon illégale.
- 2 : le serveur ne sait pas répondre.
- 3 : le nom demandé n'existe pas.
- 4 : le serveur n'accepte pas la demande.
- 5 : le serveur refuse de répondre.

La plupart des requêtes n'effectuent qu'une demande à la fois. La forme de ce type de requête est illustrée à la figure 13-4. Dans la zone Question, le contenu doit être interprété de la façon suivante : 6 indique que 6 caractères suivent ; après les 6 caractères de réseau, 4 désigne les 4 caractères de *lip6*, 2 les deux caractères de *fr* et enfin 0 la fin du champ.

Le champ Autorité permet aux serveurs qui ont autorité sur le nom demandé de se faire connaître. Enfin, la zone Champs supplémentaires permet de transporter des informations sur le temps pendant lequel la réponse à la question est valide.

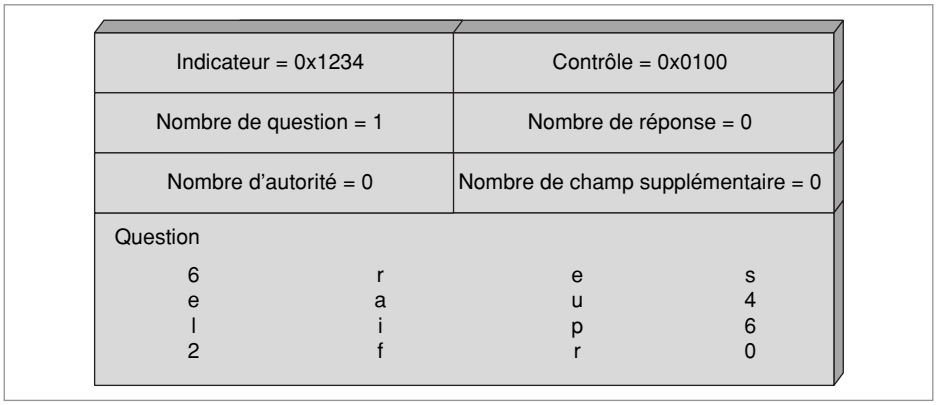

Figure 13-4. *Requête DNS avec une seule demande.*

Questions-réponses

Question 8.– *L'application DNS peut utiliser les protocoles aussi bien TCP qu'UDP. Lequel des deux protocoles est-il utilisé dans les deux cas suivants : pour la requête d'un utilisateur vers le serveur et pour la requête d'un serveur vers un autre serveur afin de mettre à jour sa table de routage ?*

Réponse.– Dans le premier cas UDP, pour aller vite. Dans le second cas TCP, de façon à garantir que les informations sont transportées de façon fiable.

Question 9.– *Quelle est la difficulté posée par les configurations dynamiques sur le DNS ? (La station IP qui se connecte réclame une adresse IP, qui lui est fournie par le routeur de rattachement.) Montrer que la sécurité devient un service prépondérant dans ce cas de gestion dynamique.*

Réponse.– Le DNS doit pouvoir être mis à jour de façon dynamique. Dès qu'une station reçoit une nouvelle adresse, elle doit en avertir le DNS local. La sécurité devient un service important puisqu'un utilisateur pourrait assez facilement se faire passer pour un autre.

Question 10.– *Proposer plusieurs solutions de gestion du DNS pour gérer un client mobile.*

Réponse.– Une première solution consisterait à mettre à jour les DNS de façon continuelle, mais cela se révèle particulièrement complexe dès que le nombre d'utilisateurs mobiles augmente et que les clients changent de domaine. Une seconde possibilité est de leur affecter des adresses provisoires au fur et à mesure des changements et de tenir à jour la correspondance entre ces adresses provisoires et l'adresse de base.

ICMP *(Internet Control Message Protocol)*

La gestion et le contrôle sont des processus fortement imbriqués dans les nouvelles générations de réseaux IP. La différence entre les deux processus s'estompe de fait par l'accroissement de la vitesse de réaction des composants, de telle sorte qu'un contrôle, qui demande une réaction en temps réel, n'est plus très loin d'un processus de gestion.

Dans le système en mode sans connexion, chaque passerelle et chaque machine fonctionnent de façon autonome. De même, le routage et l'envoi des datagrammes se font sans coordination avec le récepteur. Ce système marche bien tant que les machines ne rencontrent pas de problème et que le routage est correct, mais cela n'est pas toujours le cas.

Outre les pannes matérielles et logicielles du réseau et des machines qui y sont connectées, des problèmes surviennent lorsqu'une station est déconnectée du réseau, que ce soit temporairement ou de façon permanente, ou lorsque la durée de vie du datagramme expire, ou enfin lorsque la congestion d'une passerelle devient trop importante.

Pour permettre aux machines de rendre compte de ces anomalies de fonctionnement, on a ajouté à Internet un protocole d'envoi de messages de contrôle, appelé ICMP *(Internet Control Message Protocol)*.

Le destinataire d'un message ICMP n'est pas un processus application mais le logiciel Internet de la machine. Ce logiciel IP traite le problème porté par le message ICMP à chaque message reçu.

Les messages ICMP ne proviennent pas uniquement des passerelles. N'importe quelle machine du réseau peut envoyer des messages à n'importe quelle autre machine. Les messages permettent de rendre compte de l'erreur

avalanche.– Grande quantité de messages ou de paquets qui sont émis quasiment simultanément.

en remontant jusqu'à l'émetteur d'origine. Les messages ICMP prennent place dans la partie données des datagrammes IP. Comme n'importe quels autres datagrammes, ces derniers peuvent être perdus. En cas d'erreur d'un datagramme contenant un message de contrôle, aucun message de rapport de l'erreur n'est transmis, afin d'éviter les *avalanches*.

Comme pour le protocole IP, deux versions du protocole ICMP sont disponibles, la version associée à IPv4 et celle associée à IPv6. La version ICMPv6 est particulièrement importante, car elle regroupe tous les messages de contrôle et d'information de différents protocoles de la première génération.

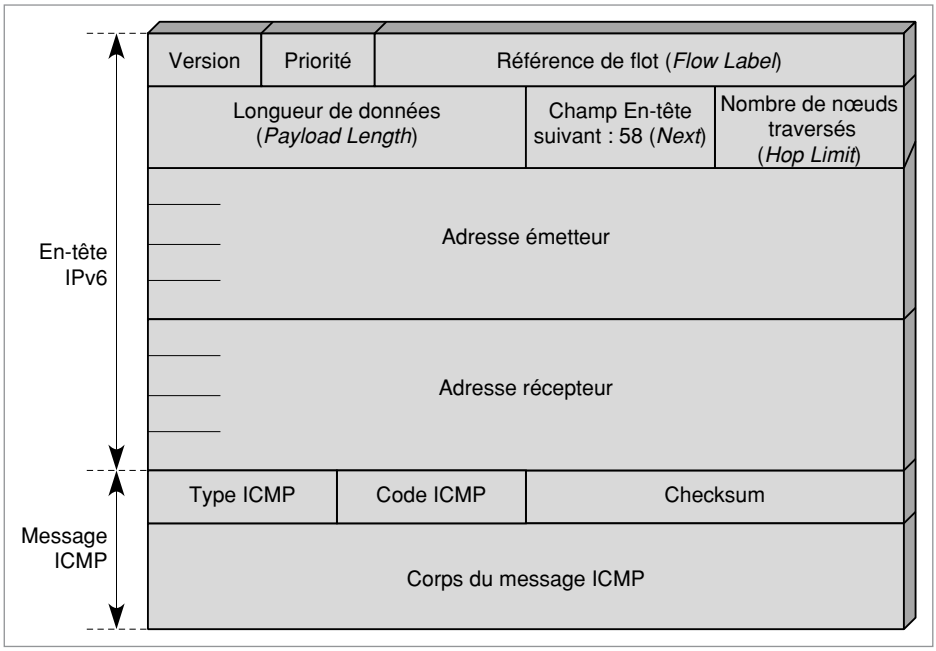

Figure 13-5. *Format des messages ICMP.*

La figure 13-5 illustre le format des messages ICMP. L'en-tête de la partie ICMP comprend un octet « type » de message, suivi d'un octet « code », suivi de deux octets de checksum. Le type et le code différencient les différents messages ICMP. Il en existe 14 types différents. Ces messages sont les suivants :

- 1 : message d'erreur, impossible d'atteindre la destination ;
- 2 : message d'erreur, paquet trop volumineux ;
- 3 : message d'erreur, temps dépassé ;
- 4 : message d'erreur, problème de paramètre ;
- 128 : message de requête d'écho ;
- 129 : message de réponse d'écho ;
- 130 : requête d'entrée dans un groupe ;

- 131 : rapport sur l'entrée dans un groupe ;
- 132 : fin d'appartenance à un groupe ;
- 133 : sollicitation d'un routeur ;
- 134 : émission d'un routeur ;
- 135 : sollicitation d'un voisin (Neighbor Solicitation) ;
- 136 : émission d'un voisin (Neighbor Advertisement) ;
- 137 : message de redirection.

Le checksum ne s'applique ni au paquet IP, ni à la partie ICMP, mais à un ensemble de champs qui contiennent la partie ICMP, tels que les adresses émetteur et récepteur, la zone de longueur du paquet IP et le champ indiquant ce qui est encapsulé, c'est-à-dire la valeur 58, dans le cas présent.

ICMP prend encore beaucoup plus d'importance dans la version IPv6. Le protocole ARP *(Address Resolution Protocol)* disparaît et est remplacé par une fonction d'ICMP : ND *(Neighbor Discovery)*. Cette fonction permet à une station de découvrir le routeur dont elle dépend ainsi que les hôtes qu'elle peut atteindre localement. La station se construit une base de connaissances en examinant les paquets transitant par son intermédiaire. Elle est ainsi à même de prendre ultérieurement des décisions de routage et de contrôle.

La correspondance entre l'adresse IP d'une station et les adresses locales représente la fonction de résolution d'adresses. C'est le travail de ND. La station qui utilise ND émet une requête *Neighbor Solicitation* sur sa ligne. L'adresse du destinataire est *FF02::1:pruv:wxyz*, qui représente une adresse *multicast* complétée par la valeur *pruv:wxyz* des 32 derniers bits de l'adresse de la station.

multicast.– Mode de diffusion correspondant à une application multipoint. Une adresse multicast indique une adresse de groupe et non pas d'une seule entité.

La valeur du champ *Next Header*, ou En-tête suivant *(voir le cours 10, « Les protocoles de niveau paquet »)*, dans le format IPv6 est 58. Cela indique un message ICMP, dont le code est 135, indiquant une requête *Neighbor Solicitation*. Si la station n'obtient pas de réponse, elle effectue ultérieurement une nouvelle demande. Les stations qui se reconnaissent au moment de la diffusion émettent vers la station d'émission un *Neighbor Advertisement*. Pour discuter avec un utilisateur sur un autre réseau, la station a besoin de s'adresser à un routeur. La requête *Router Solicitation* est utilisée à cet effet. La fonction ND permet au routeur gérant la station de se faire connaître. Le message de réponse contient de nombreuses options, comme le temps de vie du routeur : si le routeur ne donne pas de nouvelles dans un temps donné, il est considéré comme indisponible.

Les messages *Router Solicitation* et *Router Advertisement* ne garantissent pas que le routeur qui s'est fait connaître soit le meilleur. Un routeur peut s'en apercevoir et envoyer les paquets de la station vers un autre routeur grâce à une redirection *(Redirection)* et en avertissant le poste de travail émetteur.

Une dernière fonction importante de ND provient de la perte de communication avec un voisin. Cette fonction est effectuée grâce à une requête *Neighbor Unreachability Detection* (message spécifique portant le type 136).

La figure 13-6 illustre les messages de la fonction ND.

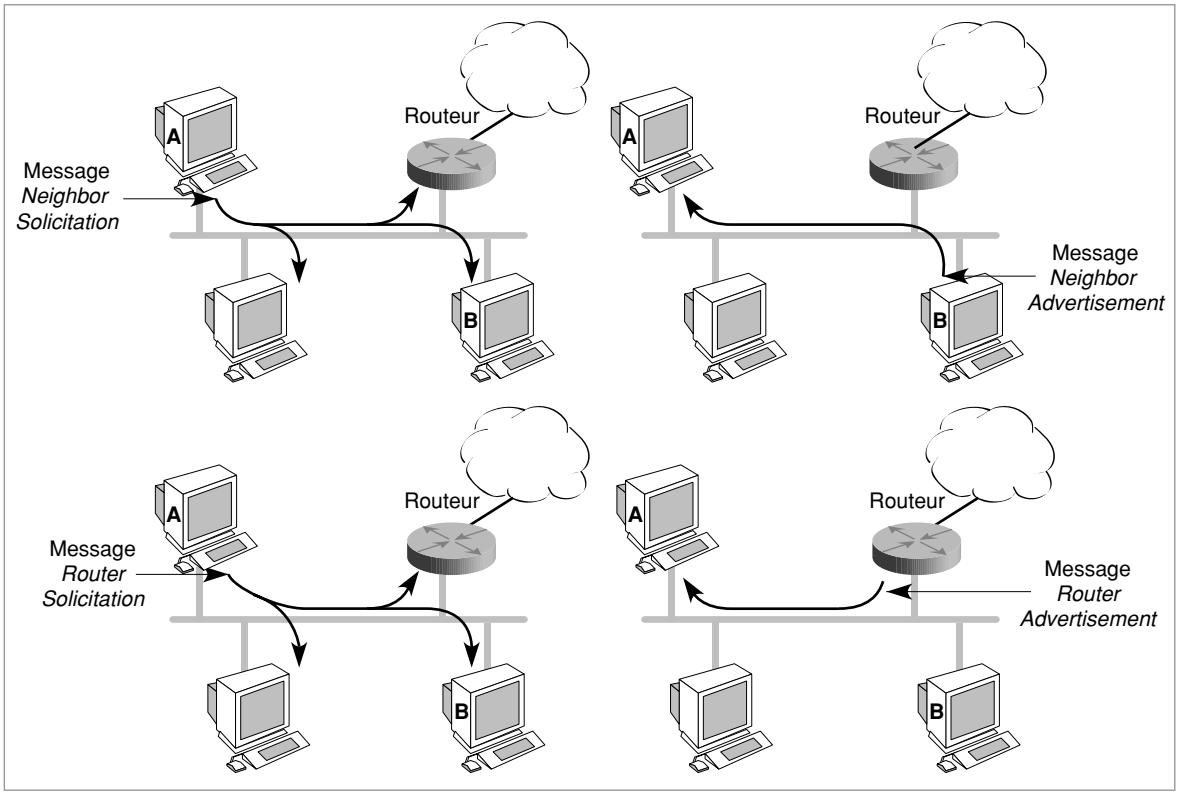

Figure 13-6. *Messages de la fonction ND (Neighbor Discovery).*

Questions-réponses

Question 11.– *Montrer que les valeurs des messages ICMP comprises entre 1 et 127 correspondent à des messages de rapport d'erreur et que, à partir de 128, ce sont des messages d'information.*

Réponse.– 4 valeurs seulement sur 127 sont utilisées dans les paquets ICMP, et ce sont bien des messages qui présentent un rapport d'erreur. À partir de la valeur 128, les paquets ICMP transportent des messages contenant des informations.

Question 12.– *Pourquoi le checksum s'applique-t-il à des zones particulières et non pas seulement à la partie ICMP ?*

Réponse.– Parce qu'il faut protéger les messages de contrôle efficacement. En particulier, il faut protéger les adresses d'émission et de réception de façon à être sûr de l'identité de l'émetteur et du récepteur. Il faut aussi protéger la longueur du paquet et s'assurer que le paquet interne est bien un paquet ICMP. La valeur 58 doit donc aussi faire partie de cette zone protégée que l'on appelle le *pseudo-header.*

pseudo-header.– En-tête modifié par le retrait ou l'ajout de certains champs, pris en compte par la zone de détection d'erreur dans son calcul. En-tête partiel d'un paquet ICMP ne reprenant que les zones les plus importantes.

Question 13.– *À quoi peuvent servir les messages ICMP de types 130, 131 et 132 ?*

Réponse.– Le protocole ICMPv6 reprend les fonctionnalités du protocole IGMP *(Internet Group Multicast Protocol)* de première génération. Ces fonctionnalités consistent à gérer les adresses multicast, c'est-à-dire à accepter de nouveaux entrants dans un groupe d'utilisateurs, ainsi quà gérer ceux qui sortent du groupe et à indiquer la fin de vie du groupe.

RSVP *(Resource reSerVation Protocol)*

RSVP semble le plus intéressant des protocoles de nouvelle génération. Il s'agit d'un protocole de signalisation, qui a pour fonction d'avertir les nœuds intermédiaires de l'arrivée d'un flot correspondant à des qualités de service déterminées.

Cette signalisation s'effectue sur un flot *(flow)* envoyé vers un ou plusieurs récepteurs. Ce flot est identifié par une adresse IP ou un port de destination, ou encore par une référence de flot (flow-label dans IPv6).

Dans la vision des opérateurs de télécommunications, le protocole est lié à une réservation qui doit être effectuée dans les nœuds du réseau, sur une route particulière ou sur les routes déterminées par un multipoint. Les difficultés rencontrées pour mettre en œuvre ce mécanisme sont de deux ordres : comment déterminer la quantité de ressources à réserver à tout instant et comment réserver des ressources sur une route unique, étant donné que le routage des paquets IP fait varier le chemin à suivre ?

Dans la vision des opérateurs informatiques, le protocole RSVP ne donne pas d'obligation quant à la réservation de ressources ; c'est essentiellement une signalisation de passage d'un flot.

Le protocole RSVP effectue la signalisation (avec ou sans réservation) à partir du récepteur, ou des récepteurs dans le cas d'un multipoint. Cela peut paraître surprenant à première vue, mais cette solution s'adapte à beaucoup de cas de figure, en particulier au multipoint. Lorsqu'un nouveau point s'ajoute au multipoint, celui-ci peut réaliser l'adjonction de réservations d'une façon plus simple que ne pourrait le faire l'émetteur.

Les paquets RSVP sont transportés dans la zone de données des paquets IP. La partie supérieure des figures 13-7 à 13-9 illustre les en-têtes dIPv6. La valeur 46 dans le champ En-tête suivant d'IPv6 indique qu'un paquet RSVP est transporté dans la zone de données.

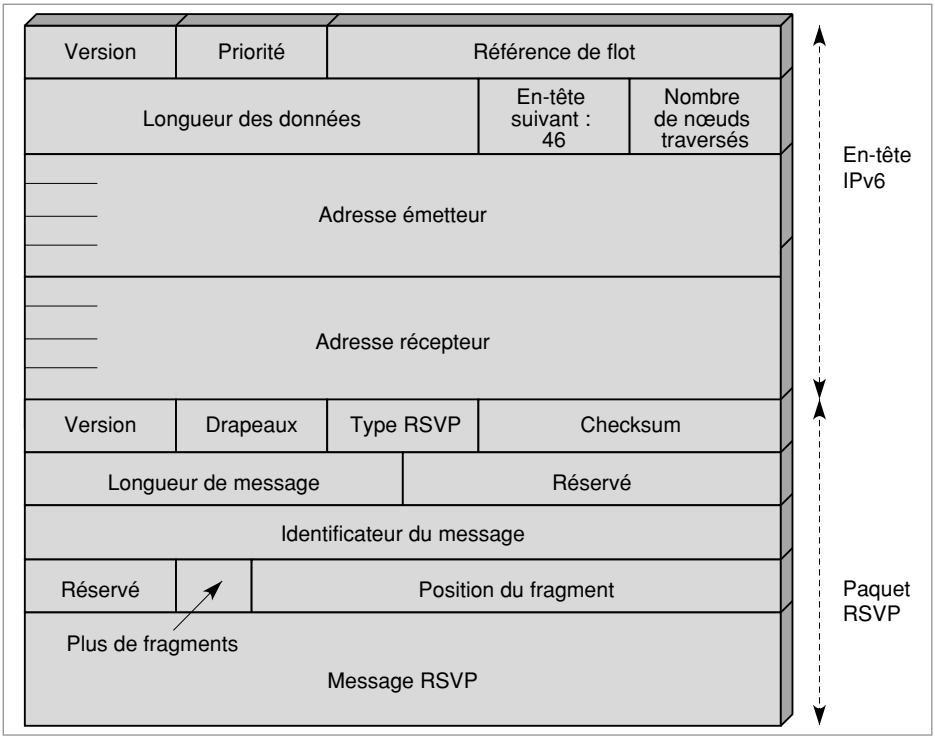

Figure 13-7. *Format du message RSVP.*

Les champs du protocole RSVP

Outre deux champs réservés, le paquet RSVP contient les dix champs suivants :

- Le premier champ indique le numéro de la version en cours de RSVP.
- Les quatre bits Flags (drapeaux) sont réservés pour une utilisation ultérieure.
- Le type caractérise le message RSVP. Actuellement, deux types sont les plus utilisés : le message de chemin et le message de réservation.

  Les valeurs qui ont été retenues pour ce champ sont les suivantes :

  1 : *path message ;*
  2 : *reservation message ;*
  3 : *error indication in response to path message ;*
  4 : *error indication in response to reservation message ;*
  5 : *path teardown message ;*
  6 : *reservation teardown message.*
- Le champ Checksum permet de détecter des erreurs sur le paquet RSVP.
- La longueur du message est ensuite indiquée sur 2 octets.
- Un premier champ est réservé aux extensions ultérieures.
- La zone Identificateur du message contient une valeur commune à l'ensemble des fragments d'un même message.
- Un champ est réservé pour des extensions ultérieures.
- Le bit Plus de fragments indique que le fragment n'est pas le dernier. Un zéro est mis dans ce champ pour le dernier fragment.

- Le champ Position du fragment indique l'emplacement du fragment dans le message.

La partie Message RSVP regroupe une série d'objets. Chaque objet se présente de la même façon, avec un champ Longueur de l'objet, sur 2 octets, puis le numéro de l'objet, sur 1 octet, qui détermine l'objet, et enfin 1 octet pour indiquer le type de l'objet.

Les spécifications de RSVP contiennent les descriptions précises des chemins suivis par les messages, y compris les objets nécessaires et l'ordre dans lequel ces objets apparaissent dans le message.

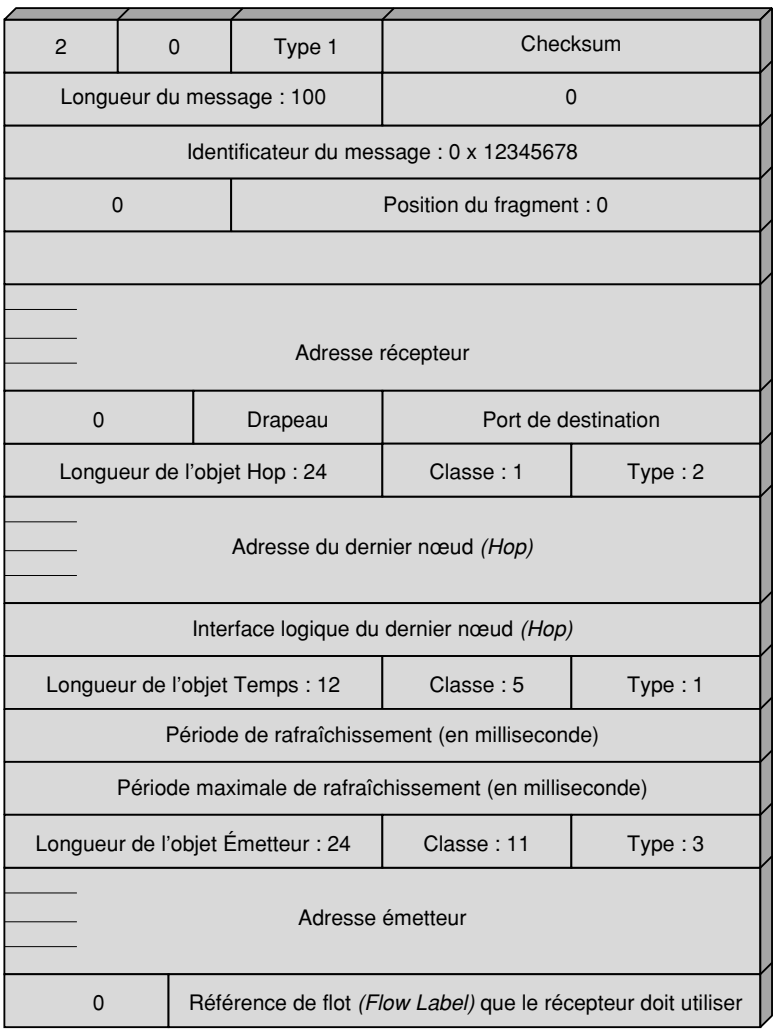

Figure 13-8. *Partie message permettant de déterminer le chemin RSVP.*

Les figures 13-8 et 13-9 donnent deux exemples de messages RSVP. La figure 13-10 décrit en complément le format d'indication des erreurs dans RSVP.

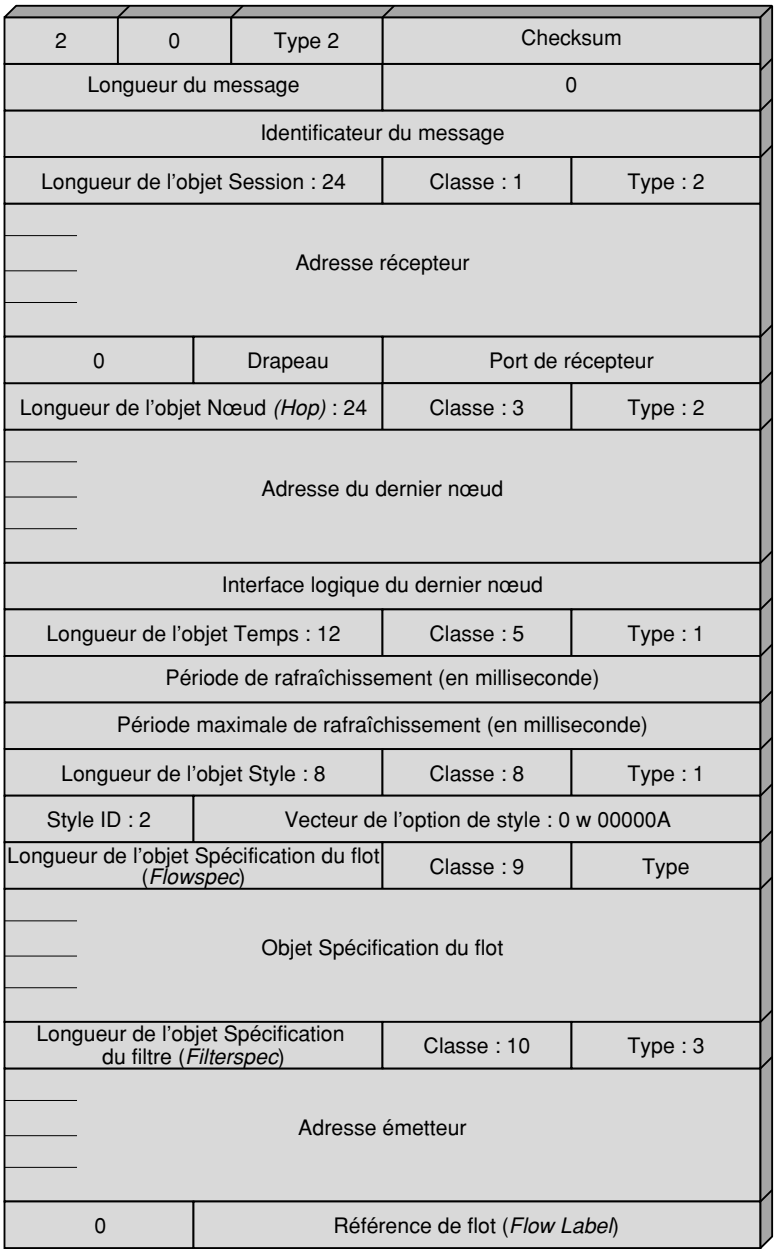

Figure 13-9. *Paquet de réservation de RSVP.*

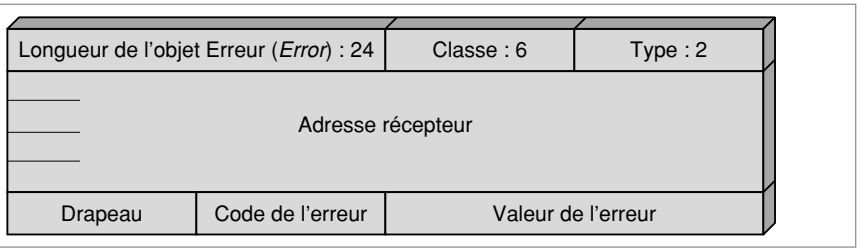

Figure 13-10. *Format d'indication des erreurs dans RSVP.*

Questions-réponses

Question 14.– *La réservation RSVP s'effectue du récepteur vers l'émetteur. Montrer que cette solution est bien adaptée lorsque les récepteurs ont des caractéristiques différentes.*

Réponse.– Lorsque l'émetteur effectue la réservation, la demande est uniforme jusqu'au récepteur puisque l'émetteur ne connaît pas les terminaux récepteurs. Il peut toutefois se produire un gâchis de bande passante. Lorsque la réservation remonte depuis le récepteur, celui-ci fait sa demande pour son cas particulier. S'il ne peut recevoir que 64 Kbit/s, ce n'est pas la peine d'ouvrir un canal à 2 Mbit/s, comme pourrait le proposer l'émetteur. Aux points de jonction des demandes de réservation RSVP (routeur de concentration de trafic), un calcul doit être effectué pour que tous les récepteurs concernés soient satisfaits.

Question 15.– *Montrer que RSVP prend assez bien en compte la dynamique du transport, c'est-à-dire la possibilité de changer de route.*

Réponse.– Le protocole RSVP utilise des soft-state (états mous). Cela signifie qu'à défaut de rafraîchissements réguliers, les références de la route s'effacent automatiquement. Le protocole RSVP peut donc ouvrir une nouvelle route n'importe quand sans trop se soucier de l'ancienne route. Cela offre une bonne dynamique à l'ensemble du processus.

Question 16.– *Comment associer les paquets qui arrivent dans un routeur avec les réservations qui ont pu être effectuées par un protocole RSVP ?*

Réponse.– L'association entre les ressources réservées et les paquets d'un flot s'effectue grâce au numéro de *flow-label* (référence du flot) du protocole IPv6, lorsque ce protocole est utilisé. Dans le cas d'IPv4, la solution préconisée est d'utiliser le protocole UDP pour encapsuler le paquet RSVP de façon à récupérer les numéros de ports qui permettent de reconnaître le flot.

flow-label (référence de flot).– Référence associée à un flot IP. Tous les paquets du flot porte la même référence.

RTP *(Real-time Transport Protocol)*

L'existence d'applications temps réel, comme la parole numérique ou la visioconférence, est un problème pour Internet. Ces applications demandent une qualité de service (QoS) que les protocoles classiques d'Internet ne peuvent offrir. RTP *(Real-time Transport Protocol)* a été conçu pour résoudre ce pro-

blème, qui plus est directement dans un environnement multipoint. RTP a à sa charge aussi bien la gestion du temps réel que l'administration de la session multipoint.

Les fonctions de RTP sont les suivantes :

- Le séquencement des paquets par une numérotation. Cette numérotation permet de détecter les paquets perdus, ce qui est important pour la recomposition de la parole. La perte d'un paquet n'est pas un problème en soi, à condition qu'il n'y ait pas trop de paquets perdus. En revanche, il est impératif de repérer qu'un paquet a été perdu de façon à en tenir compte et à le remplacer éventuellement par une synthèse déterminée en fonction des paquets précédent et suivant.
- L'identification de ce qui est transporté dans le message pour permettre, par exemple, une compensation en cas de perte.
- La synchronisation entre médias, grâce à des *estampilles.*
- L'indication de *tramage :* les applications audio et vidéo sont transportées dans des trames *(frames)*, dont la dimension dépend des codecs effectuant la numérisation. Ces trames sont incluses dans les paquets afin d'être transportées. Elles doivent être récupérées facilement au moment de la dépaquétisation pour que l'application soit décodée simplement.
- L'identification de la source. Dans les applications en multicast, l'identité de la source doit être déterminée.

estampille.– Marque indiquant des valeurs de paramètres temporelles.

tramage.– Façon de construire des structures (les trames) dans lesquelles sont entreposées les informations à transporter.

RTP utilise le protocole RTCP *(Real-time Transport Control Protocol)*, qui transporte les informations supplémentaires suivantes pour la gestion de la session :

- Retour de la qualité de service lors de la demande de session. Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS. Ces rapports comprennent le nombre de paquets perdus, la *gigue* et le délai aller-retour. Ces informations permettent à la source de s'adapter, c'est-à-dire, par exemple, de modifier le degré de compression pour maintenir la QoS.
- Synchronisation supplémentaire entre médias. Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix et l'image, ou même une application numérisée sur plusieurs niveaux hiérarchiques, peuvent voir les flots générés suivre des chemins distincts.
- Identification. Les paquets RTCP contiennent des informations d'adresse, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Contrôle de la session. RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement une indication de leur comportement.

gigue.– Paramètre indiquant la variance d'une distribution. La gigue d'un réseau, ou plutôt du temps de réponse d'un réseau, permet de savoir si les paquets arrivent à peu près régulièrement ou au contraire très irrégulièrement.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations ci-dessus. La périodicité est calculée en fonction du nombre de participants à l'application.

Deux équipements intermédiaires, les translateurs *(translator)* et les mixeurs *(mixer)*, permettent de résoudre des problèmes d'homogénéisation lorsqu'il y a plusieurs récepteurs. Un translateur a pour fonction de traduire une application codée dans un certain format en un autre format, mieux adapté au passage par un sous-réseau. Par exemple, une application de visioconférence codée en MPEG-2 peut être décodée et recodée en MPEG-4 si l'on souhaite réduire la quantité d'informations transmises. Un mixeur a pour rôle de regrouper plusieurs applications correspondant à plusieurs flots distincts en un seul flot conservant le même format. Cette approche est particulièrement intéressante pour les flux de paroles numériques.

Comme nous venons de le voir, pour réaliser le transport en temps réel des informations de supervision, le protocole RTCP *(Real Time Control Protocol)* a été ajouté à RTP, les paquets RTP ne transportant que les données des utilisateurs. Le protocole RTCP autorise les cinq types de paquets de supervision suivants :

- 200 : rapport de l'émetteur ;
- 201 : rapport du récepteur ;
- 202 : description de la source ;
- 203 : au revoir ;
- 204 : application spécifique.

Ces différents paquets de supervision indiquent aux nœuds du réseau les instructions nécessaires à un meilleur contrôle des applications temps réel.

Le format des messages RTP

Le format des messages RTP est illustré à la figure 13-11.

Les deux premiers octets contiennent six champ distincts. Les deux premiers bits indiquent le numéro de version (2 dans la version actuelle). Le troisième bit indique si des informations de bourrage (padding) ont été ajoutées. Si la valeur de ce bit est égale à 1, le dernier octet du paquet indique le nombre d'octets de bourrage. Le bit suivant précise s'il existe une extension au champ d'en-tête de RTP, mais, en pratique, aucune extension n'a été définie jusqu'à présent par l'IETF. Le champ suivant, Contributor Count, indique le nombre d'identificateurs de contributeurs à la session RTP qui doivent être spécifiés dans la suite du message (jusqu'à 15 contributeurs peuvent être recensés). Le bit Marker met à la disposition de l'utilisateur une marque indiquant la fin d'un ensemble de données. Les sept éléments binaires suivants complètent les deux premiers octets et indiquent ce qui est transporté dans le paquet RTP.

Suite p. 280

Suite de la page 279

Les valeurs possibles de ces éléments sont les suivantes :

0 : PCMU audio	10 : L16 audio (stéréo)	26 : JPEG video
1 : 1016 audio	11 : L16 audio (mono)	27 : CUSM video
2 : G721 audio	12 : LPS0 audio	28 : nv video
3 : GSM audio	13 : VSC audio	29 : PicW video
4 : audio	14 : MPA audio	30 : CPV video
5 : DV14 audio (8 kHz)	15 : G728 audio	31 : H261 video
6 : DV14 audio (16 kHz)	16-22 : audio	32 : MPV video
7 : LPC audio	23 : RGB8 video	33 : MP2T video
8 : PCMA audio	24 : HDCC video	
9 : G722 audio	25 : CelB video	

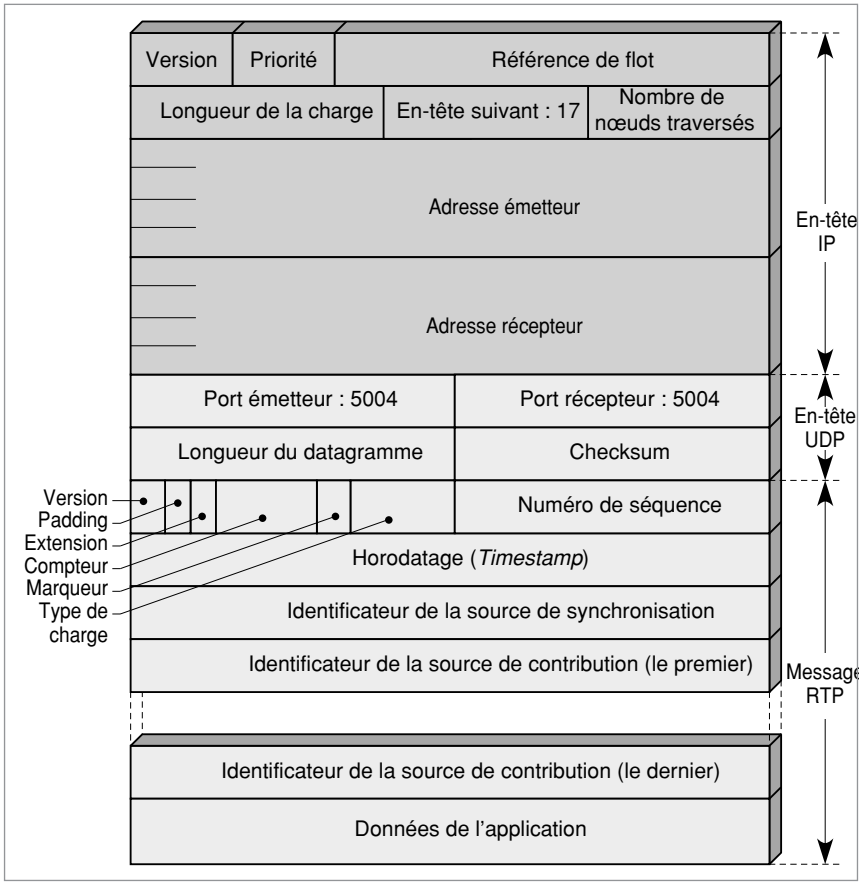

Figure 13-11. *Format des messages RTP.*

Viennent ensuite un champ de numéro de séquence, qui permet de déterminer si un paquet est perdu, puis un champ d'horodatage (Timestamp), suivi des identificateurs de sources de synchronisation (SSRC) et de sources contributrices (CSRC).

Questions-réponses

Question 17.– *Quel protocole de niveau transport est-il préférable d'employer pour transporter des messages RTP ?*

Réponse.– Le protocole préconisé est UDP, qui permet d'atteindre plus facilement un temps réel.

Question 18.– *RTP peut-il effectuer des réservations de ressources dans les routeurs traversés ? De ce fait, peut-il vraiment apporter une qualité de service sur un flot à débit constant ?*

Réponse.– Non, RTP ne travaille qu'au niveau applicatif. De ce fait, RTP ne peut garantir aucune qualité de service sur un flot à débit constant. RTP travaille justement à optimiser le flot par rapport à la capacité du réseau.

Question 19.– *Les routeurs d'extrémité peuvent recevoir des translateurs et des mixeurs capables de modifier le flot RTP. Quelle application peut-on en faire ?*

Réponse.– Ces translateurs et ces mixeurs peuvent modifier un flot pour l'adapter au récepteur. Si l'on suppose que deux récepteurs distincts acceptent de faire partie d'une même conférence audio, avec chacun un codage différent, il faut au moins un translateur pour transformer le flot destiné à l'un des récepteurs en une syntaxe acceptable. Un mixeur peut, quant à lui, rassembler deux images émanant de deux stations terminales et les assembler sous un même document.

NAT *(Network Address Translation)*

Le protocole IP version 4, que nous utilisons massivement actuellement, offre un champ d'adressage limité et insuffisant pour permettre à tout terminal informatique de disposer d'une adresse IP. Une adresse IP est en effet codée sur un champ de 32 bits, ce qui offre un maximum de 2^{32} adresses possibles, soit en théorie 4 294 967 296 terminaux raccordables au même réseau.

Pour faire face à cette pénurie d'adresses, et en attendant la version 6 du protocole IP, qui offrira un nombre d'adresses beaucoup plus important sur 128 bits, il faut recourir à un partage de connexion en utilisant la translation d'adresse, ou NAT (*Network Address Translation*).

adresse IP publique.– Adresse IP qui est comprise par l'ensemble des routeurs d'Internet et qui peut donc être routée sur Internet.

Ce mécanisme se rencontre fréquemment à la fois en entreprise et chez les particuliers. Il distingue deux catégories d'adresses : les *adresses IP publiques*, c'est-à-dire visibles et accessibles de n'importe où (on dit aussi routables sur Internet), et les *adresses IP privées*, c'est-à-dire non routables sur Internet et adressables uniquement dans un réseau local, à l'exclusion du réseau Internet.

adresse IP privée.– Adresse IP qui n'est pas comprise par les routeurs d'Internet. C'est une adresse qui n'est comprise que dans un environnement privé.

Le NAT consiste à établir des relations entre l'adressage privé dans un réseau et l'adressage public pour se connecter à Internet.

Adresses privées et adresses publiques

Dans le cas d'un réseau purement privé, et jamais amené à se connecter au réseau Internet, n'importe quelle adresse IP peut être utilisée. Dès qu'un réseau privé peut être amené à se connecter sur le réseau Internet, il faut distinguer les adresses privées des adresses publiques. Pour cela, chaque classe d'adresses IP dispose d'une plage d'adresses réservées, définies comme des adresses IP privées, et donc non routables sur Internet. La RFC 1918 récapitule ces plages d'adresses IP, comme l'indique le tableau 13.1.

Classe d'adresses	Plages d'adresses privées	Masque réseau	Espace adressable
A	10.0.0.0 à 10.255.255.255	255.0.0.0	Sur 24 bits, soit 16 777 216 terminaux
B	172.16.0.0 à 172.31.255.255	255.240.0.0	Sur 20 bits, soit 1 048 576 terminaux
C	192.168.0.0. à 192.168.255.255	255.255.0.0	Sur 16 bits, soit 65 536 terminaux

Tableau 13-1. *Plages d'adresses privées*

Dans ce cadre, et avant d'introduire la notion de NAT, les utilisateurs qui possèdent une adresse IP privée ne peuvent communiquer que sur leur réseau local, et non sur Internet, tandis qu'avec une adresse IP publique, ils peuvent communiquer avec n'importe quel réseau IP.

L'adressage privé peut être utilisé librement par n'importe quel administrateur ou utilisateur au sein de son réseau local. Au contraire, l'adressage public est soumis à des restrictions de déclaration et d'enregistrement de l'adresse IP auprès d'un organisme spécialisé, l'IANA (*Internet Assigned Numbers Authority*), ce que les *FAI* effectuent globalement en acquérant une plage d'adresses IP pour leurs abonnés.

FAI (fournisseur d'accès Internet).– En anglais ISP (*Internet Service Provider*) : opérateur qui commercialise des accès à Internet.

La figure 13-12 illustre un exemple d'adressage mixte, dans lequel on distingue les différentes communications possibles, selon un adressage de type privé ou public.

Partager une adresse IP privée

Moyennant la souscription d'un accès Internet auprès d'un FAI, ce dernier fournit à ses utilisateurs une adresse IP privée. Dans un même foyer ou une même entreprise, deux utilisateurs ne peuvent communiquer en même temps sur Internet avec cette seule adresse IP fournie. Les adresses IP privées conviennent généralement pour couvrir un réseau privé, de particulier ou d'entreprise, mais pas pour communiquer directement avec les réseaux publics.

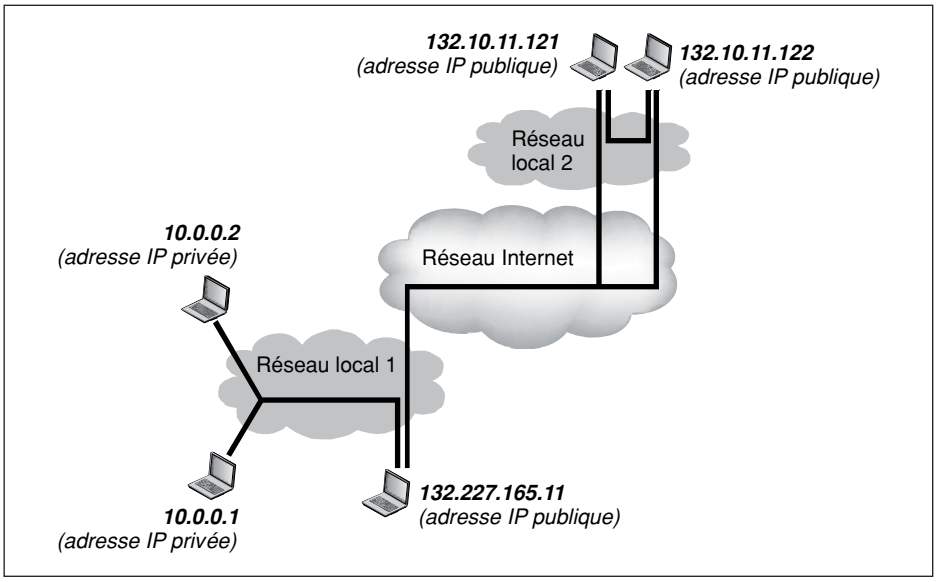

Figure 13-12 *Adressage mixte privé-public*

Pour résoudre ce problème et permettre à un terminal disposant d'une adresse IP privée de communiquer avec le réseau public, le processus de NAT fait intervenir une entité tierce entre un terminal, ayant une adresse IP privée, et tout autre terminal ayant une adresse IP publique. Ce mécanisme consiste à insérer un boîtier entre le réseau Internet et le réseau local afin d'effectuer la translation de l'adresse IP privée en une adresse IP publique. Aujourd'hui, la plupart des boîtiers, ou *InternetBox*, des FAI proposent à leurs abonnés cette fonctionnalité. Toutes les machines qui s'y connectent reçoivent par le biais du service DHCP (*Dynamic Host Configuration Protocol*) une adresse IP privée, que le boîtier se charge de translater en une adresse IP publique.

La figure 13-13 illustre un exemple dans lequel une passerelle NAT réalise une translation d'adresses pour quatre terminaux. Cette passerelle possède deux interfaces réseau. La première est caractérisée par une adresse IP publique (132.227.165.221). Connectée au réseau Internet, elle est reconnue et adressable normalement dans le réseau. La seconde interface est caractérisée par une adresse IP non publique (10.0.0.254). Connectée au réseau local, elle ne peut communiquer qu'avec les terminaux qui possèdent une adresse IP non publique de la même classe.

Lorsqu'un terminal ayant une adresse IP privée tente de se connecter au réseau Internet, il envoie ses paquets vers la passerelle NAT. Celle-ci remplace l'adresse IP privée d'origine par sa propre adresse IP publique (132.227.165.221). On appelle cette opération une translation d'adresse. De

cette manière, les terminaux avec une adresse IP privée sont reconnus et adressables dans le réseau Internet par une adresse IP publique.

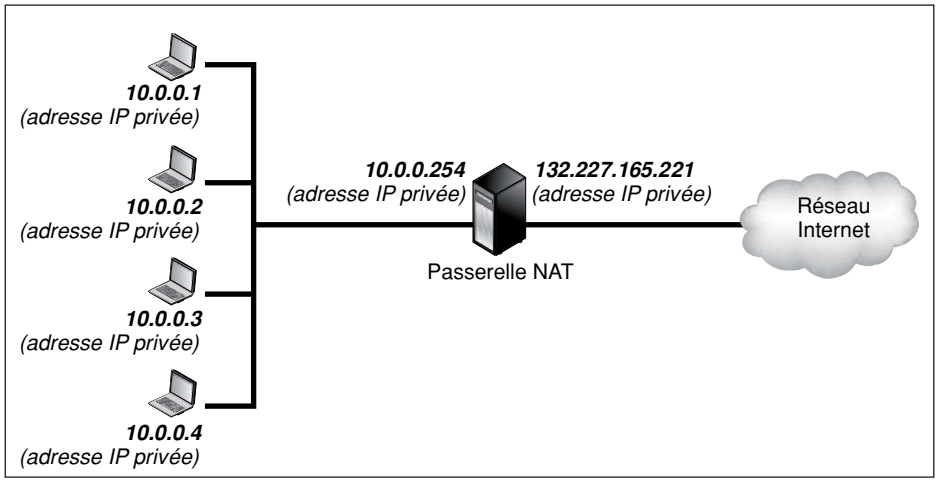

Figure 13-13 *Translation d'adresses*

La translation d'adresse est bien sûr réalisée dans les deux sens d'une communication, afin de permettre l'émission de requêtes aussi bien que la réception des réponses correspondantes. Pour cela, le boîtier NAT maintient une table de correspondance des paquets de manière à savoir à qui distribuer les paquets reçus.

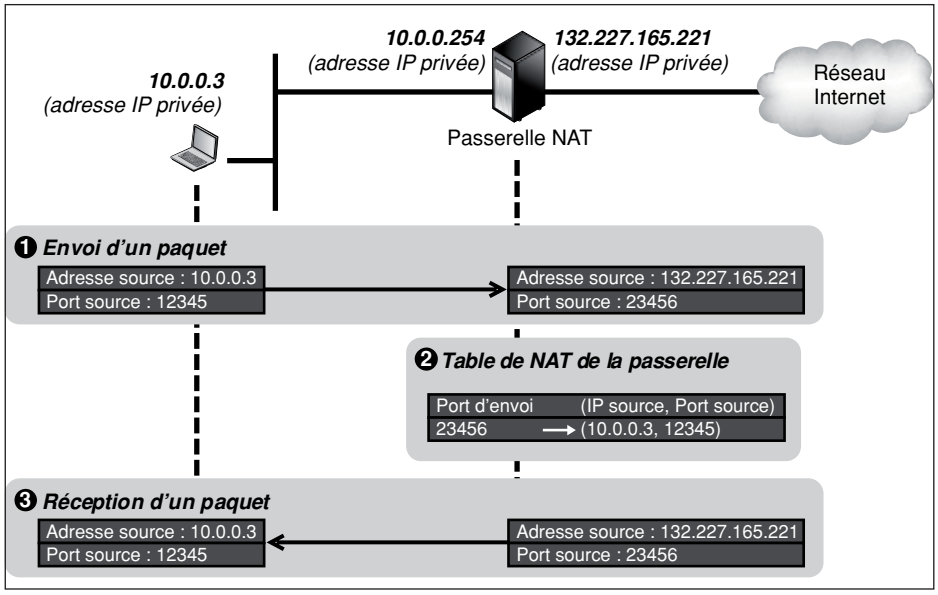

Figure 13-14 *Modification de paquets lors du NAT*

Par exemple, si un émetteur dont l'adresse IP est 10.0.0.3 envoie vers la passerelle NAT un paquet à partir de son port 12345, la passerelle NAT modifie le paquet en remplaçant l'adresse IP source par la sienne et le port source par un port quelconque qu'elle n'utilise pas, disons le port 23456. Elle note cette correspondance dans sa table de NAT. De cette manière, lorsqu'elle recevra un paquet à destination du port 23456, elle cherchera cette affectation de port dans sa table et retrouvera la source initiale.

Ce cas est illustré à la figure 13-14.

Avantages du NAT

Le premier atout du NAT est de simplifier la gestion du réseau en laissant l'administrateur libre d'adopter le plan d'adressage interne qu'il souhaite. Étant privé, le plan d'adressage interne ne dépend pas de contraintes externes, que les administrateurs ne maîtrisent pas toujours. Par exemple, si une entreprise utilise un plan d'adressage public et qu'elle change de FAI, elle doit modifier l'adresse de tous les terminaux qui composent son réseau. Au contraire, avec le NAT et un plan d'adressage privé, le choix d'un nouveau fournisseur d'accès Internet n'a pas d'impact sur les terminaux. Dans ce cas, l'administrateur n'a pas besoin de reconfigurer les adresses IP de tous les terminaux de son réseau. Il lui suffit de modifier, au niveau de la passerelle NAT, le pool d'adresses IP publiques, qui est affecté dynamiquement aux adresses IP privées des terminaux du réseau local.

Le deuxième atout du NAT est d'économiser le nombre d'adresses IP publiques. Le protocole réseau IP, qui est utilisé dans l'Internet actuel dans sa version 4, présente une limitation importante, car le nombre d'adresses IP disponible est faible comparé au nombre de terminaux susceptibles d'être raccordés au réseau Internet. Comme cette ressource est rare, sa mise à disposition à un coût pour les administrateurs qui souhaitent en bénéficier.

Le NAT comble cette pénurie d'adresses propre à la version 4 d'IP en offrant la possibilité d'économiser les adresses IP à deux niveaux distincts. Tous les terminaux d'un réseau local n'ont pas forcément besoin d'être joignables de l'extérieur, mais peuvent se limiter à une connexion interne au réseau. Par exemple, des serveurs d'intranet, des annuaires d'entreprise, des serveurs dédiés aux ressources humaines avec des informations confidentielles de suivi du personnel ou bien encore des serveurs de tests n'ont pas à être joignables à partir du réseau Internet, mais seulement en interne au sein de l'entreprise. En conséquence, ces serveurs peuvent se suffire d'une adresse IP privée, qui ne sera jamais « nattée » par le boîtier NAT puisque ces serveurs reçoivent des requêtes mais n'en émettent jamais.

Un deuxième niveau d'économie d'adresses IP publique est opéré avec le mécanisme que nous avons mentionné à la section précédente, qui permet de masquer plusieurs terminaux disposant chacun d'une adresse IP privée avec une seule adresse IP publique, en jouant sur les ports utilisés. Cette méthode est très couramment employée, car elle n'impose aucune condition quant au nombre de terminaux susceptibles d'accéder à Internet dans le réseau local.

Un autre avantage important du NAT concerne la sécurité. Les terminaux disposent en effet d'une protection supplémentaire, puisqu'ils ne sont pas directement adressables de l'extérieur. En outre, le boîtier NAT offre la garantie que tous les flux transitant entre le réseau interne et l'extérieur passent toujours par lui. Si un terminal est mal protégé et ne dispose pas d'un pare-feu efficace, le réseau dans lequel il se connecte peut ajouter des mécanismes de protection supplémentaires au sein de la passerelle NAT, puisqu'elle représente un passage obligé pour tous les flux. Globalement, l'administrateur concentre les mécanismes de sécurisation à un point de contrôle unique et centralisé. Cela explique que, bien souvent, les boîtiers NAT sont couplés avec des pare-feu filtrant les flux.

Les trois catégories de NAT

Le mécanisme de NAT que nous avons pris comme exemple précédemment, consistant à jouer sur les ports pour masquer plusieurs terminaux avec une adresse IP unique, est un cas particulier. Il repose sur une translation de port appelée NPT (*Network Port Translation*). Lorsqu'elle se combine avec le NAT, on parle de NAPT (*Network Address and Port Translation*).

Bien que les concepts soient différents, le processus de NAT inclut fréquemment par abus de langage le processus de NPT. En réalité, il faut distinguer trois formes de NAT, le NAT statique, le NAT dynamique et NATP. Ces formes peuvent se combiner selon les besoins de chaque utilisateur et les politiques d'administration établies dans un réseau. D'autres formes de classification du NAT sont possibles. La RFC 3489 en recense quatre types, par exemple. Nous nous contenterons de détailler dans les sections suivantes les formes les plus courantes.

Le NAT statique

Dans le NAT statique, à toute adresse IP privée qui communique avec l'extérieur, une adresse IP publique fixe lui est affectée. Avec ce type de NAT, les utilisateurs du réseau local sont joignables de l'extérieur, car la passerelle réalise la correspondance d'une adresse IP locale en une adresse IP publique dans les deux sens. C'est un avantage indéniable, en particulier pour la téléphonie, car un utilisateur à l'extérieur du réseau privé peut appeler un abonné à l'intérieur du réseau privé puisqu'il connaît son adresse IP fixe.

Ce cas de figure est illustré à la figure 13-15. Le terminal ayant l'adresse IP privée 10.0.0.4 n'a pas de correspondance d'adresse IP publique, car c'est un serveur interne. Les administrateurs font l'économie d'une adresse IP pour ce serveur et s'assurent en outre que ce dernier n'est pas joignable directement de l'extérieur. Un changement de FAI ne remet pas en cause le plan d'adressage en local.

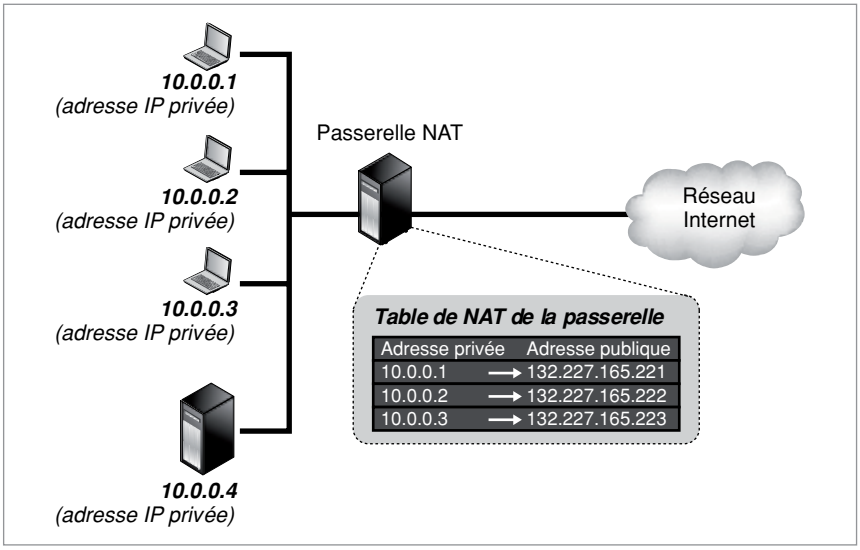

Figure 13.15 *Le NAT statique*

Le NAT dynamique

Avec le NAT dynamique, une plage d'adresses IP publiques est disponible et partagée par tous les utilisateurs du réseau local. Chaque fois qu'une demande d'un utilisateur local (avec une adresse privée) parvient à la passerelle NAT, celle-ci lui concède dynamiquement une adresse IP publique. Elle maintient cette correspondance pour une période fixe, mais renouvelable selon l'activité de l'utilisateur, qui assure le suivi des communications.

Avec ce type de NAT, les utilisateurs locaux ne sont joignables de l'extérieur que s'ils ont une entrée dans la table de la passerelle NAT, autrement dit que s'ils entretiennent une activité avec le réseau Internet. En effet, les correspondants externes ne peuvent s'adresser qu'à la passerelle NAT pour envoyer leur flux. Or tant que le correspondant interne n'a pas d'activité réseau, aucune entrée ne lui est attribuée dans la table de NAT. De plus, l'adresse IP qui leur est affectée est temporaire et peut être différente à la prochaine connexion, ce qui restreint les possibilités d'être joignable de l'extérieur.

Il existe même une forme de NAT particulière, appelée NAT symétrique ou « *full cone* » dans la RFC 3489, qui consiste à établir une correspondance entre l'adresse IP privée et publique selon la destination d'une communication. Autrement dit, un utilisateur du réseau local aura une certaine adresse IP publique lorsqu'il communique avec un correspondant extérieur et une autre adresse IP publique lorsqu'il communique avec une autre destination.

Le modèle dynamique offre une plus grande souplesse d'utilisation que le modèle statique puisque les associations d'adresses IP privées et publiques n'ont pas besoin d'être mentionnées statiquement par l'administrateur, mais sont attribuées automatiquement. En outre, il présente l'avantage d'optimiser au maximum les ressources. Si un utilisateur n'exploite pas sa connexion Internet et se contente de sa connexion locale, la passerelle NAT n'a pas besoin de lui attribuer une adresse IP. Le NAT dynamique est cependant plus complexe puisqu'il impose à la passerelle NAT de maintenir les

Suite p. 288

Suite de la page 287

états des connexions pour déterminer si les utilisateurs exploitent leur adresse IP publique ou s'il est possible, passé un certain délai, de les réutiliser.

Ce modèle ressemble à celui déployé avec la téléphonie RTC. Le nombre de lignes sortantes d'un commutateur téléphonique d'entreprise et même d'immeubles de particuliers est généralement inférieur au nombre de lignes entrantes. Autrement dit, tous les abonnés disposent d'un téléphone, mais tous ne peuvent appeler en même temps. Dans la pratique, il est assez exceptionnel que tous les abonnés appellent en même temps, si bien que ces derniers ne perçoivent pas cette restriction, qui permet aux opérateurs de limiter le nombre de lignes. Avec le NAT dynamique, les notions sont différentes, mais le principe est le même : l'attribution des adresses IP se fait à la demande, avec les limitations du nombre d'adresses IP publiques disponibles que cela suppose.

Le NAPT

Variante du NAT dynamique, le NAPT (*Network Address Port Translation*) est en fait celui que nous avons présenté précédemment sans le nommer. Il consiste à attribuer une même adresse IP à plusieurs utilisateurs d'un même réseau local.

Comme nous l'avons expliqué, pour associer une même adresse IP publique à deux terminaux ayant une adresse privée distincte, la passerelle NAT joue sur les ports des applications : une requête envoyée à partir du port A d'une source est retransmise avec le port B de la passerelle, tandis qu'une requête émise à partir du port C d'une autre source est retransmise avec le port D de la passerelle. De cette manière, la passerelle peut contrôler et distinguer chacune des demandes qui lui parviennent.

L'inconvénient de cette méthode est que seuls les utilisateurs du réseau local peuvent amorcer une communication vers l'extérieur. Autrement dit, ils ne peuvent répondre à une communication qu'ils n'ont pas préalablement initiée. Les correspondants externes à la passerelle NAT ne possèdent en effet des entrées que pour une adresse IP et un port source privés. Or si le port source est mentionné, c'est qu'une application a déjà été ouverte par le terminal du réseau local. Le correspondant externe n'a aucun moyen d'établir une telle association en lieu et place du terminal dont il ignore la véritable adresse IP.

Le NAPT est sans conteste la méthode la plus économe puisqu'elle permet de masquer tout un réseau local avec une seule adresse IP. Elle est la plus couramment employée chez les particuliers et les petites et moyennes entreprises.

Questions-réponses

Question 20.– *Pourquoi IPv6 permet-il de se passer de la technique NAT ? Que cela change-t-il ?*

Réponse.– Parce que le nombre d'adresses en IPv6 est suffisant pour donner une adresse IP à chaque machine. Cela implique que chaque objet connecté à Internet pourra garder une adresse unique, ce qui supprime les tables de correspondance.

Question 21.– *Les* InternetBox *utilise-t-elles des NAT ?*

Réponse.– Oui. Les opérateurs n'ayant pas suffisamment d'adresses IP publiques, ils utilisent pour le grand public des NAT. En revanche, pour les *InternetBox* d'entreprise, des adresses publiques sont en général utilisées pour permettre aux entreprises d'avoir une adresse IP fixe.

Question 22.– *Le NAT est-il utilisé pour connecter les équipements du domicile derrière une* InternetBox *? En déduire qu'il est possible de mettre deux NAT l'un derrière l'autre.*

Réponse.– Oui. L'InternetBox gère en général un NAT pour interconnecter plusieurs équipements dans le domicile. Comme l'adresse de l'*InternetBox* peut être une adresse privée, il est possible de mettre deux NAT en série.

IP Mobile

Le protocole IP est de plus en plus souvent présenté comme une solution possible pour résoudre les problèmes posés par les utilisateurs mobiles. Le protocole IP Mobile peut être utilisé sous la version 4 d'IP, mais le manque potentiel d'adresses complique la gestion de la communication avec le mobile. La version 6 d'IP est utilisée pour son grand nombre d'adresses disponibles, ce qui permet de donner des adresses temporaires aux stations en cours de déplacement.

Une station possède une adresse de base et un *agent* qui lui est attaché. Cet agent a pour rôle de suivre la correspondance entre l'adresse de base et l'adresse temporaire.

agent.– Programme qui effectue la liaison entre deux entités.

Lors d'un appel vers la station mobile, la demande est acheminée vers la base de données détenant l'adresse de base. Grâce à l'agent, il est possible d'effectuer la correspondance entre l'adresse de base et l'adresse provisoire et d'acheminer la demande de connexion vers le mobile. Cette solution est illustrée à la figure 13-16.

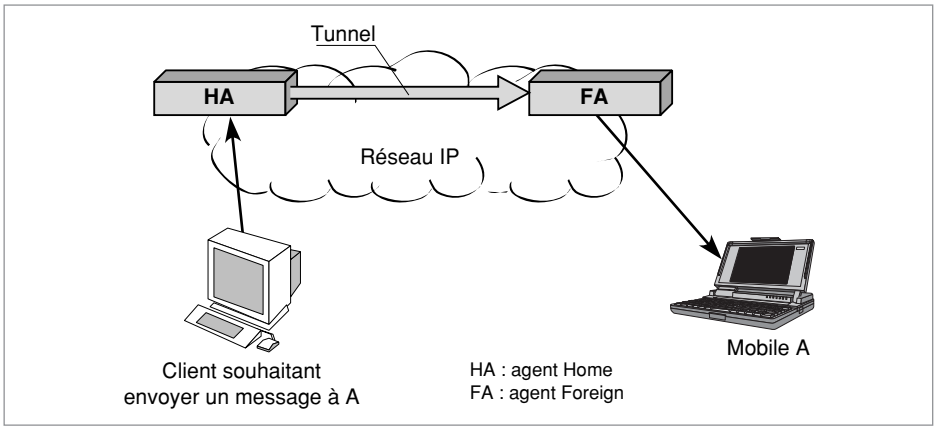

Figure 13-16. *Mise en place d'une communication dans IP Mobile.*

Ce dispositif est semblable à celui utilisé dans les réseaux de mobiles, qu'il s'agisse de la version européenne GSM ou américaine IS 95.

La terminologie en vigueur dans IP Mobile est la suivante :

- Nœud mobile *(Mobile Node) :* terminal ou routeur qui change son point d'attachement d'un sous-réseau à un autre sous-réseau.
- Agent mère, ou encore agent Home *(Home Agent) :* correspond à un routeur du sous-réseau sur lequel est enregistré le nœud mobile.
- Agent visité, ou encore agent Foreign *(Foreign Agent) :* correspond à un routeur du sous-réseau visité par le nœud mobile.

L'environnement IP Mobile est formé des trois fonctions relativement disjointes suivantes :

- Découverte de l'agent *(Agent Discovery) :* le mobile, lorsqu'il arrive dans un sous-réseau, recherche un agent susceptible de le prendre en charge.
- Enregistrement : lorsqu'un mobile est hors de son domaine de base, il enregistre sa nouvelle adresse (Care-of-Address) auprès de son agent Home. Suivant la technique utilisée, l'enregistrement peut s'effectuer soit directement auprès de l'agent Home, soit par l'intermédiaire de l'agent Foreign.
- *Tunnelling :* lorsqu'un mobile se trouve en dehors de son sous-réseau, il faut que les paquets lui soient délivrés par une technique de tunnelling, qui permet de relier l'agent Home à l'adresse Care-of-Address.

tunnelling.– Action de mettre un tunnel entre deux entités. Un tunnel correspond à un passage construit pour aller d'un point à un autre sans tenir compte de l'environnement. Dans un réseau, un tunnel correspond à un transport de paquets entre les deux extrémités. Ce transport doit être transparent, c'est-à-dire indépendant des équipements ou des couches de protocoles traversés.

Les figures 13-17 et 13-18 illustrent les schémas de communication mobiles en vigueur dans IPv4 et IPv6.

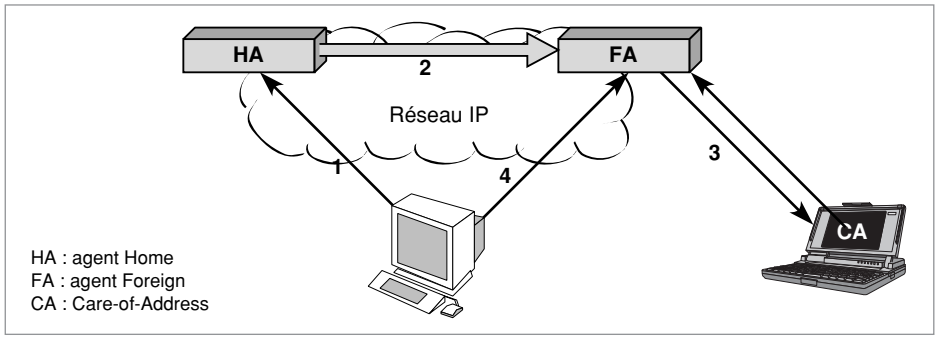

Figure 13-17. *La communication IP Mobile dans IPv4.*

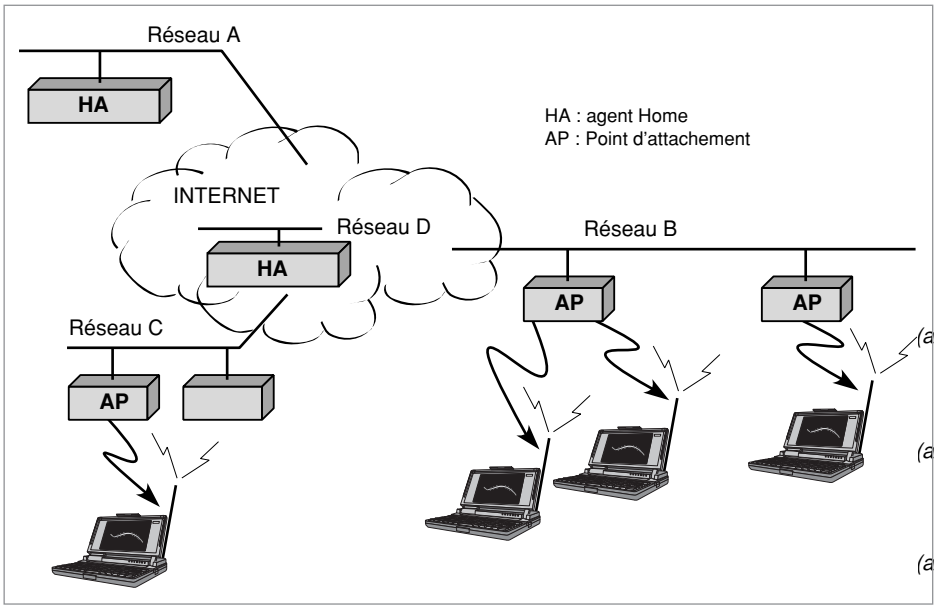

Figure 13-18. *La communication IP Mobile dans IPv6.*

Questions-réponses

Question 23.– *Le schéma de base proposé par IP Mobile consiste à passer par le réseau mère (Home) lors d'une émission d'une source vers le mobile et à émettre directement vers le récepteur lorsqu'il s'agit d'une communication du mobile vers un récepteur. Peut-on envisager de ne plus passer par le réseau mère dans le cas d'une réception par le mobile ?*

Réponse.– L'un des choix possibles proposés par l'IETF consiste, pour l'agent visité (Foreign), à envoyer à l'agent mère (Home) un *message BU (Binding Update)* lui demandant d'indiquer à un correspondant qui veut le joindre son adresse temporaire.

Question 24.– *Comment un mobile peut-il acquérir une adresse temporaire puisqu'il ne connaît rien* a priori *du réseau dans lequel il entre ?*

Réponse.– Les agents Home et Foreign indiquent leur présence sur la partie du réseau sur laquelle ils opèrent par l'émission régulière d'agents Advertisement, qui sont décrits à la section consacrée à ICMP. Les mobiles sont à l'écoute et en déduisent s'ils sont dans leur réseau mère ou dans un réseau visité. Si le mobile se situe sur un réseau visité, il acquiert une adresse temporaire (Care-of-Address). Une autre solution consiste pour le mobile à envoyer une demande de sollicitation, toujours en utilisant le protocole ICMP.

Question 25.– *La micromobilité indique un changement de cellule de la part du mobile sans que l'agent mère (Home) en soit averti. Comment considérer cette micromobilité ?*

Réponse.– La micromobilité peut sexercer lorsqu'un même agent visiteur gère plusieurs sous-réseaux, ou cellules. Dans ce cas, c'est l'agent visiteur qui gère de façon transparente les changements de sous-réseaux. Cette micromobilité devient particulièrement utile lorsque l'utilisateur change très souvent de sous-réseau, ou de cellule pour les portables GSM ou UMTS.

message BU *(Binding Update).*– Message de contrôle, de l'agent visité (Foreign) à l'agent mère (Home) pour lui demander d'avertir un émetteur de la nouvelle adresse de son correspondant (adresse Care-of-Address).

IPsec

La solution proposée par le protocole IPsec (IP sécurisé) introduit des mécanismes de sécurité au niveau du protocole IP, de telle sorte que le protocole de transport peut être absolument quelconque. Le rôle de ce protocole est de garantir l'intégrité, l'authentification, la confidentialité et la protection contre les techniques rejouant des séquences précédentes. L'utilisation des propriétés d'IPsec est optionnelle dans IPv4 et obligatoire dans IPv6.

L'authentification a pour fonction de garantir l'identité de l'émetteur. Pour cela, une signature électronique est ajoutée dans le paquet IP.

La confidentialité doit être garantie pour les données ainsi que, éventuellement, pour leur origine et leur destination. La façon de procéder consiste à chiffrer par des algorithmes *ad hoc* tout ou partie du paquet. Nous explicitons ce chiffrement un peu plus loin dans cette section.

Des associations de sécurité peuvent être mises en place, de façon à permettre à deux utilisateurs de partager une information secrète, appelée un secret. Cette association doit définir des paramètres de sécurité communs.

IPsec autorise deux types de passerelles de sécurité, l'une mettant en relation deux utilisateurs de bout en bout, l'autre servant d'intermédiaire entre une passerelle et une autre ou entre une passerelle et un hôte.

Le format des paquets IPsec est illustré à la figure 13-18. La partie la plus haute de la figure correspond au format d'un paquet IP dans lequel est encapsulé un paquet TCP. La partie du milieu illustre le paquet IPsec, et l'on voit qu'entre l'en-tête IP et l'en-tête TCP vient se mettre l'en-tête d'IPsec. Dans cette solution, le chiffrement commence avec l'en-tête IPsec, et l'en-tête du paquet IP n'est pas chiffré. Un attaquant peut au moins déterminer le couple de stations terminales en train de communiquer.

La partie basse de la figure 13-19 montre le format d'un paquet dans un tunnel IP. On voit que la partie intérieure correspond à un paquet IP encapsulé dans un paquet IPsec de telle sorte que même les adresses des émetteurs et des récepteurs sont cachées. Le nouvel en-tête IP comporte les adresses des passerelles où sont chiffrés et déchiffrés les paquets.

Dans un tunnel IPsec, tous les paquets IP d'un flot sont transportés de façon totalement chiffrée, même les en-têtes des paquets IP. Il est de la sorte impossible de voir les adresses IP ou même les valeurs du champ de supervision du paquet IP encapsulé.

La figure 13-20 illustre un tunnel IPsec. Ici, les adresses IP portées par le nouvel en-tête sont les adresses des passerelles d'entrée et de sortie de l'entreprise.

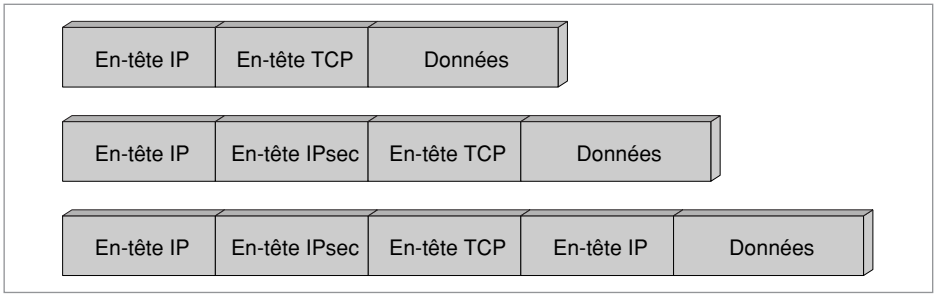

Figure 13-19. *Formats des paquets IPsec.*

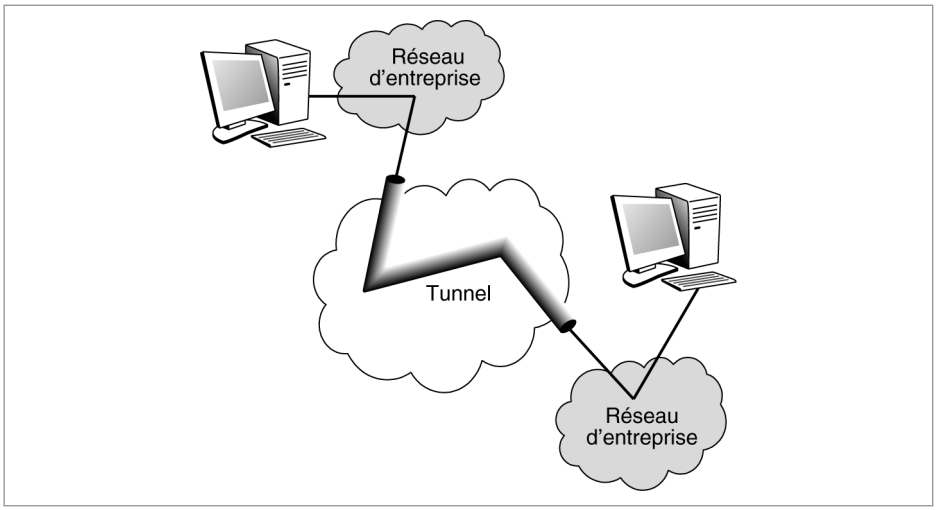

Figure 13-20. Un tunnel IPsec.

Questions-réponses

Question 26.– *Une possibilité d'attaque consisterait à capturer tous les paquets qui transitent dans un tunnel sans les comprendre, puisqu'ils sont chiffrés, puis à rejouer ce flot de paquets. Comment peut-on contrer une telle attaque ?*

Réponse.– Pour contrer cette attaque, il est possible de placer la valeur d'un compteur dans la partie chiffrée qui est vérifiée à la réception du paquet. Si l'on rejoue une séquence, le numéro du compteur n'est plus valable et le récepteur rejette les paquets.

Fonctions supplémentaires

L'installation et l'exploitation des logiciels TCP/IP requièrent une certaine expertise. Une première extension de ces logiciels consiste à automatiser l'ins-

tallation et la maintenance des logiciels, de façon à permettre à un utilisateur de relier sa machine au réseau sans avoir à valoriser les paramètres manuellement. De ce fait, un utilisateur peut connecter son ordinateur à Internet sans faire appel à un spécialiste pour installer les logiciels et mettre à jour les paramètres de configuration et de routage. En particulier, il est possible d'obtenir une configuration automatique d'un calculateur par de nouveaux protocoles permettant à une machine d'obtenir et d'enregistrer automatiquement toutes les informations sur les noms et adresses dont elle a besoin.

Des groupes de travail examinent les améliorations qui peuvent encore être apportées à ces techniques d'autoconfiguration. Le groupe consacré à l'apprentissage des routeurs travaille sur des protocoles qui permettent à une machine de découvrir les routeurs qu'elle peut utiliser. Actuellement, il est nécessaire de configurer l'adresse d'un routeur par défaut. Le protocole permettra de découvrir les adresses des passerelles locales et de tester en permanence ces adresses pour savoir lesquelles peuvent être utilisées à tout instant.

Le protocole DHCP *(Dynamic Host Configuration Protocol)* est utilisé pour initialiser et configurer dynamiquement une nouvelle machine connectée. Le protocole NDP *(Neighbor Discovery Protocol)* permet, grâce aux protocoles ARP et ICMP, l'autoconfiguration des adresses et la configuration de la MTU *(Maximum Transmission Unit)*. Nous allons détailler cette dernière.

overhead.– Partie des informations transportées qui ne provient pas de l'utilisateur mais de la gestion et du contrôle du réseau.

Le calcul de la MTU, ou taille maximale des données pouvant être contenues dans une trame physique, permet à une machine de rechercher la plus petite MTU sur un chemin particulier vers une destination donnée. La taille optimale d'un segment TCP dépend de la MTU, car les datagrammes plus grands que la MTU sont fragmentés, tandis que les datagrammes plus petits augmentent l'*overhead*. Si la MTU est connue, TCP peut optimiser le débit en construisant des segments assez larges, de façon à tenir dans un datagramme, ce dernier étant transporté dans une seule trame physique, la plus grande possible. De la même façon, UDP peut améliorer le débit en tenant compte de la MTU pour choisir la taille des datagrammes.

TCP/IP rend possible une interopérabilité universelle. Cependant, dans plusieurs environnements, les administrateurs ont besoin de limiter cette interopérabilité pour protéger les données privées. Ces restrictions correspondent au problème général de la sécurité. La fiabilité d'Internet est toutefois plus difficile à mettre en œuvre que celle d'un simple ordinateur, car Internet offre des services de communication beaucoup plus puissants. Le problème est de savoir comment un utilisateur s'appuyant sur TCP/IP peut s'assurer de la protection de ses machines et de ses données contre les accès non autorisés.

Un groupe de travail a exploré la question de la sécurisation de la messagerie en expérimentant un service de messagerie privée amélioré. L'idée est de permettre à l'émetteur de chiffrer son message et de l'envoyer sur un Internet ouvert sans permettre à une personne autre que le destinataire de le décrypter.

Des travaux sur le filtrage des paquets dans les passerelles ont produit une variété de mécanismes, qui permettent aux administrateurs de fournir des listes explicites de contrôle d'accès. Une liste d'accès spécifie un ensemble de machines et de réseaux au travers desquels la passerelle peut router les datagrammes. Si l'adresse n'est pas autorisée, le datagramme est détruit. Dans la plupart des implémentations, la passerelle enregistre la tentative de violation dans un journal. Ainsi est-il possible d'utiliser des filtres d'adresses pour surveiller les communications entre les machines.

Questions-réponses

Question 27.– *Comment un routeur indique-t-il au routeur précédent qu'il ne peut pendre en compte une fragmentation, parce que, par exemple, le bit de non-fragmentation a été positionné dans le paquet IPv4 ?*

Réponse.– Le routeur concerné envoie vers le routeur précédent un message ICMP avec le type 4 : « Message d'erreur, problème de paramètre ».

Question 28.– *Pourquoi le choix de la bonne valeur de la MTU est-il si important ?*

Réponse.– Le processus de *fragmentation-réassemblage* est lourd, ce qui pénalise énormément les performances. C'est la raison pour laquelle IPv6 utilise une procédure de détection de la bonne valeur de la MTU.

Question 29.– *Un pare-feu, ou firewall, est un organe qui protège l'accès d'un réseau privé et plus précisément des ports des protocoles TCP ou UDP. Comment peut procéder le pare-feu pour empêcher les accès à un certain nombre d'applications ?*

Réponse.– Il suffit que le pare-feu refuse tous les paquets qui possèdent un numéro de port correspondant à une application que l'on souhaite éviter. Par exemple, si l'on veut interdire les accès du protocole d'accès à distance *Telnet*, on rejette tous les paquets de port 23.

fragmentation-réassemblage.– Fonction de base du niveau transport consistant à fragmenter le message en paquets puis à réassembler ces paquets à la sortie pour retrouver le message de départ.

Telnet.– Application permettant à un équipement terminal de se connecter à un serveur distant. C'est ce que l'on nomme une émulation de terminal (le logiciel Telnet rend le terminal compatible avec le serveur).

Exercices

Les corrigés de ces exercices se trouvent pp. 478-480.

1

On considère la connexion d'un PC, appelé PC_A, à un autre PC, appelé PC_B, par l'intermédiaire d'un réseau ATM. Les deux PC travaillent sous un environnement IP.

a Expliquer comment s'effectue le transport d'un PC à l'autre.

b Si PC_A connaît PC_B par son adresse logique IP, comment peut s'effectuer la communication ? Peut-on utiliser le protocole ARP ?

c Si l'adresse de PC_A est 127.76.87.4 et celle de PC_B 127.76.14.228, ces deux stations étant sur un même réseau, à quelle classe d'adresse IP appartient ce réseau ?

d On suppose maintenant que les deux PC ne soient plus sur le même réseau mais sur deux réseaux ATM interconnectés par un routeur. Si, comme à la question 2, PC_A connaît PC_B par son adresse logique IP, comment peut s'effectuer la communication ?

e On suppose que le réseau sur lequel PC_A est connecté possède un serveur d'adresses, c'est-à-dire un serveur capable d'effectuer la correspondance entre les adresses IP du réseau et les adresses physiques des coupleurs ATM sur lesquels sont connectés les PC. Que se passe-t-il si PC_A lui envoie une requête de résolution de l'adresse IP de PC_B ?

f Montrer que si chaque sous-réseau qui participe au réseau Internet — sous-réseaux appelés LIS *(Logical IP Subnetwork)* — possède un tel serveur d'adresses, le problème global de la résolution d'adresse peut être résolu.

2

Avec les commandes demande d'écho (Echo Request) et réponse d'écho (Echo Reply) d'ICMP, il est possible de tester un réseau IP. La commande Ping est un petit programme qui intègre ces deux commandes pour réaliser des tests facilement. La commande Ping envoie un datagramme à une adresse IP et demande au destinataire de renvoyer le datagramme.

a Que mesure la commande Ping ?

b En retour de la commande Ping, on reçoit un message ICMP portant le numéro de type 3. Ce message indique que le paquet IP qui transporte le message ICMP de demande d'écho a vu la valeur de son champ Temps de vie, ou TTL *(Time To Live)*, dépasser la limite admissible. Que faut-il en déduire ?

c Si l'on est sûr de l'adresse IP du correspondant mais que le message de retour soit un message ICMP avec Destinataire inaccessible , que faut-il en déduire ?

d En règle générale, la commande Ping ne génère pas une seule commande d'écho mais plusieurs (souvent 4). Quelle en est la raison ?

3

Soit un réseau IP utilisant le protocole RSVP.

a Montrer que RSVP est un protocole de signalisation.

b RSVP effectue une réservation dans le sens retour, c'est-à-dire du récepteur vers l'émetteur. Pourquoi ?

c RSVP est un protocole multipoint, c'est-à-dire qu'il peut ouvrir des chemins allant de l'émetteur à plusieurs récepteurs. Montrer que la réservation s'effectuant des récepteurs vers l'émetteur est une bonne solution dans ce cas.

d Le protocole RSVP peut très bien ne faire aucune réservation explicite. Quel est dans ce cas l'intérêt de RSVP ?

4

Soit une application téléphonique sur Internet utilisant le protocole RTP/RTCP.

a L'émetteur et le récepteur doivent-ils posséder plusieurs ou un seul codec, un codec permettant de compresser plus ou moins la voix ?

b Le protocole RTCP a pour objectif d'indiquer au récepteur les performances du réseau. Est-ce un protocole indispensable à RTP ?

c Cette solution de gestion de la qualité de service au niveau de l'émetteur en adaptant les flux aux contraintes internes du réseau vous paraît-elle conforme à la philosophie d'Internet ?

d Si le réseau est capable d'offrir lui-même une qualité de service, le protocole RTP/RTCP est-il encore utile ?

5

Soit un réseau IP proposant de la qualité de service au travers d'une technique DiffServ.

a Les clients EF *(Expedited Forwarding)* ont la priorité la plus haute. Expliquer pourquoi les clients EF peuvent obtenir une qualité de service garantie.

b Montrer que, dans certains cas, cette garantie peut être remise en cause.

c Dans la classe AF *(Assured Forwarding),* il existe trois sous-classes. Montrer qu'aucune de ces sous-classes ne peut espérer obtenir une garantie sur le temps de transit du réseau.

d Montrer que les clients de la classe AF doivent être soumis à un contrôle de flux.

e Pourquoi les normalisateurs de l'IETF ont-ils proposé quatre classes, dites classes de *precedence,* ou priorité, dans chacune des trois classes de base ?

f Les clients best effort ont-ils le même service que dans l'Internet classique, n'offrant que la classe best effort ?

6 *Soit un réseau composé de terminaux mobiles IP qui peuvent se déplacer dans des cellules. Un client est enregistré dans la cellule où il a pris son abonnement.*

a Pourquoi son adresse IP n'est-elle pas suffisante pour que le réseau le retrouve lorsqu'il se déplace ?

b Si l'on donne à un utilisateur qui ne se trouve pas dans la cellule où il s'est enregistré une nouvelle adresse IP, comment peut-on faire le lien entre son adresse de base et sa nouvelle adresse ?

c Si l'utilisateur émet un paquet, doit-il utiliser son adresse de base ou l'adresse que le réseau lui a affectée ?

d Dans quel cas pourrait-il être intéressant de donner à un utilisateur qui souhaite joindre notre client son adresse provisoire, décernée par la cellule dans laquelle il se trouve ?