Autres équipements

Pour contrecarrer le développement un peu anarchique des architectures de réseau et la prolifération de solutions constructeur, le modèle de référence a eu pour objectif la standardisation des architectures réseau. L'objectif visé était d'éviter de passer d'une architecture à une autre par le biais de passerelles, toujours coûteuses et complexes à mettre en oeuvre.

L'arrivée en force des interfaces IP est de nature à résoudre en grande partie le problème de l'hétérogénéité. Cependant, les solutions pour transporter un paquet IP restent très diverses, que ce soit à l'intérieur d'une entreprise ou dans un réseau d'opérateur.

Cela explique pourquoi l'interconnexion de technologies différentes rend nécessaire le recours à des passerelles permettant de relier différentes catégories de réseaux. Avec la multiplication des réseaux, Internet, mobiles, sans fil, etc., à laquelle on assiste depuis quelques années, ces passerelles sont devenues indispensables, tant pour les constructeurs que pour les utilisateurs.

De plus, les équipements intermédiaires que l'on rencontre le long d'un chemin pour résoudre des problèmes spécifiques sont également en plein développement, comme les pare-feu et les appliances en tout genre permettant d'assurer le contrôle du trafic ou la répartition de charge. Ce chapitre étudie ces différents équipements en commençant par les passerelles.

Les passerelles

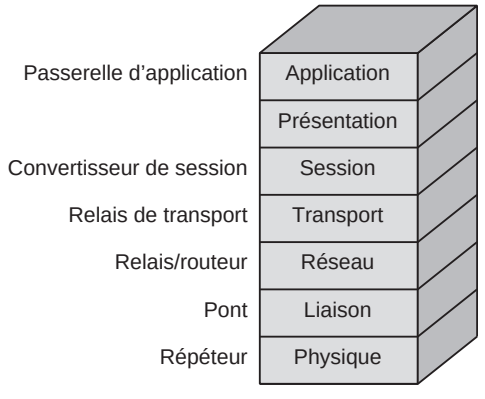
On ne peut plus concevoir un réseau sans un passage vers l'extérieur. Il faut interconnecter les réseaux pour qu'ils puissent s'échanger des informations. Le nœud qui joue le rôle d'intermédiaire s'appelle une passerelle, ou gateway (terme générique). Ce nœud intermédiaire peut être plus ou moins complexe, suivant la ressemblance ou la dissemblance des deux réseaux à interconnecter. Si les deux réseaux sont identiques, la passerelle est extrêmement simple. À l'inverse, si les deux architectures à interconnecter sont dissemblables, les moyens à mettre en œuvre deviennent vite lourds et complexes.

Si l'on s'en tient strictement à la définition d'une passerelle, on peut réaliser une interconnexion de réseaux à n'importe quel niveau de l'architecture du modèle de référence. Cependant, la règle générale est la suivante : l'utilisation d'une passerelle de niveau N est nécessaire lorsque les couches inférieures à N sont différentes mais que toutes les couches, à partir de la couche N + 1, sont identiques.

Les trois catégories de passerelles les plus répandues sont les ponts, les routeurs et les relais. On distingue également les ponts-routeurs (bridge-routers), qui, bien que non normalisés, sont largement utilisés.

Une hiérarchie de noms a été définie pour prendre en compte le niveau de l'interconnexion en se référant au modèle de référence. Ces différents niveaux sont illustrés à la figure 27.1. Un répéteur est une passerelle de niveau 1, ou physique ; un pont est une passerelle de niveau 2, ou trame ; un relais est une passerelle de niveau 3, ou paquet ; un relais de transport est une passerelle de niveau 4, ou message, etc.

Figure 27.1
Hiérarchie des passerelles



Les termes « commutateur » et « routeur » ne sont pas liés à un niveau. Un commutateur est un organe de type pont lorsque la commutation est effectuée au niveau 2 et de type relais lorsqu'elle est effectuée au niveau 3. Par exemple, un commutateur Ethernet est de type pont tandis qu'un commutateur X.25 est un relais. De même, un routeur est de type pont lorsque le routage est effectué au niveau 2 et de type relais lorsque le routage est effectué au niveau 3. Le terme « routeur » a été tellement associé au routage IP de niveau 3 qu'il semble naturel d'utiliser ce terme pour indiquer un relais de niveau paquet. Cela n'est toutefois exact que pour le monde IP, qui représente tout de même quasiment 99 p. 100 des relais de niveau 3. C'est la raison pour laquelle nous avons indiqué à la figure 27.1 le mot routeur à côté du mot relais pour exprimer que la quasi-totalité des relais sont des routeurs IP.

Les répéteurs

Un répéteur est une passerelle de niveau physique entre deux réseaux comportant un niveau trame commun. Par exemple, un répéteur Ethernet est un équipement qui répète automatiquement les trames d'un brin Ethernet vers un autre brin Ethernet.

Le rôle du répéteur est d'envoyer une trame plus loin que ne le permet un simple câble, dont la longueur est limitée par l'atténuation du signal. Si nous prenons l'exemple d'Ethernet à 10 Mbit/s, un câble coaxial blindé ne peut permettre de dépasser une longueur de 500 m sous peine de voir le taux d'erreur devenir inacceptable.

Regardons plus précisément le cas du réseau Ethernet. Nous savons que la longueur maximale d'un réseau Ethernet est limitée à 2,5 km *(voir le chapitre 16)*, puisque le temps de propagation d'une extrémité à l'autre du support physique ne peut dépasser 51,2 µs. La question est de savoir comment atteindre ces 2,5 km si la longueur maximale d'un brin ne peut excéder 500 m. La réponse est simple : il suffit de connecter des brins les uns aux autres en utilisant des répéteurs.

Les répéteurs n'empêchent pas les collisions mais rendent difficile leur répétition sur le brin suivant. En effet, un répéteur n'est pas autre chose qu'un registre à décalage, c'est-à-dire un ensemble de registres dans lesquels les informations sous forme de 0 et de 1 viennent se mémoriser et se décalent pour laisser entrer un nouvel élément binaire. Le registre d'entrée s'attend à recevoir un 0 ou un 1 et non un signal provenant d'une superposition. Il est donc très difficile de répéter des signaux qui ne sont ni des 0 ni des 1. C'est la raison pour laquelle les répéteurs remplacent les éléments en collision par une série de bits spécifiques permettant aux autres stations de détecter la collision.

Les répéteurs peuvent éventuellement changer de support physique tout en respectant la structure de la trame en cours d'acheminement. Par exemple, on peut passer d'un support métallique à une fibre optique ou à un support hertzien d'un réseau sans-fil. C'est la raison pour laquelle il est possible de réaliser des réseaux Ethernet ayant des parties métalliques, optiques et hertziennes.

En résumé, un répéteur est un organe inintelligent qui permet d'allonger la longueur du support physique, au contraire d'un pont, qui filtre les messages sur leur adresse de destination.

Les ponts

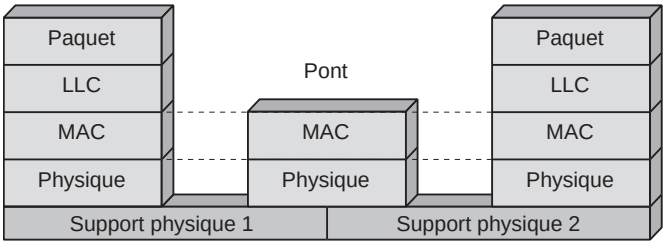
Le pont, ou bridge, est une passerelle de niveau 2. Cet équipement de réseau assez simple à mettre en œuvre a beaucoup évolué depuis l'apparition des premiers réseaux Ethernet.

Un pont unit des réseaux proches ou distants en remontant jusqu'au niveau trame. Il reçoit une trame et calcule la ligne de sortie grâce à un algorithme de routage ou à la table de commutation. Il filtre les trames reçues en examinant l'adresse de niveau 2 et en ne laissant passer que les trames destinées à l'extérieur.

L'architecture d'un pont est illustrée à la figure 27.2. Le pont crée un réseau virtuel à partir d'un ensemble de sous-réseaux, en ignorant les protocoles des couches supérieures. Les couches MAC peuvent être compatibles ou non. Dans le premier cas, le pont est

conçu pour relier des réseaux de même type (Ethernet, Token-Ring, etc.). Dans le second cas, il faut remonter au niveau supérieur, c'est-à-dire à la couche LLC commune puis réencapsuler la trame LLC dans la couche MAC. Le niveau physique pouvant être différent d'un sous-réseau à un autre, on peut qualifier le pont d'interconnexion de deux ou plusieurs supports physiques.

Figure 27.2
Architecture d'un pont



Le pont enregistre dans des tables internes les adresses de toutes les stations connectées au réseau. Si une station est ajoutée ou enlevée, le système doit être reconfiguré. C'est la raison pour laquelle les ponts ne peuvent *a priori* être utilisés que dans des environnements bien localisés. Dès que le nombre de stations est important, la gestion des adresses devient très complexe.

L'interconnexion de sous-réseaux par des ponts permet des débits élevés, puisque le nombre de niveaux à traverser est petit et qu'on ne remonte que d'un niveau pour arriver au niveau trame. Les passerelles de niveau paquet, ou relais, sont moins puissantes puisque, à chaque passage d'un relais, il faut traverser les niveaux 1 puis 2 pour arriver au niveau 3.

Deux grands protocoles de routage de niveau pont, le Source-Routing et le Spanning-Tree, ont été développés respectivement pour les réseaux Token-Ring et Ethernet. Ces protocoles sont toujours utilisés mais parfois pour d'autres catégories de réseaux.

Le protocole Source-Routing

Normalisé par le comité IEEE 802.5, le protocole Source-Routing a été utilisé au départ pour l'interconnexion de réseaux Token-Ring. Ce protocole est toujours fortement utilisé dans d'autres contextes, aussi bien issus des réseaux IP que des réseaux locaux.

Lorsqu'une station X veut envoyer des informations à une station Y, elle envoie en diffusion une trame de découverte du chemin. Un pont qui voit arriver une trame de ce type y ajoute sa propre adresse et retransmet cette trame vers tous les réseaux, à l'exception de celui par lequel la trame est arrivée. La station destination Y voit donc arriver une ou plusieurs trames et retourne à X toutes les trames reçues en utilisant les informations d'acheminement trouvées dans chacune. Ensuite, X peut utiliser les routes que le protocole lui a permis de découvrir. Son choix est guidé par divers paramètres, tels que délais d'acheminement, nombre de ponts traversés, longueur de trame permise, etc.

Les trames constituées par chaque station présentent la structure suivante : elles commencent par l'adresse de destination, suivie de l'adresse source, des informations de routage, de l'adresse DSAP (Destination Service Access Point), de l'adresse SSAP (Source Service Access Point), des données de contrôle et enfin des données à transporter,

pour se terminer par une zone FCS (Frame Check Sequence). Cette suite s'exprime par la séquence :

@Dest.~@Source~Info-routage~DSAP~SSAP~Contrôle~Données~FCS.

La longueur des adresses destination et source est de 2 ou 6 octets, et celle de chaque élément de l'information de routage de 2 octets.

Le protocole Spanning-Tree

Normalisé par le comité IEEE 802.1, le protocole Spanning-Tree est prévu pour l'interconnexion de tout type de réseau. Il consiste en la constitution, à partir de n'importe quelle topologie, d'un arbre qui recouvre parfaitement le réseau et dans lequel, à partir de n'importe quelle feuille de l'arbre, tout point du réseau est accessible.

Pour le bon fonctionnement du protocole, le réseau doit satisfaire aux conditions suivantes :

- Une identification unique (ID) doit être associée à chaque pont du réseau.
- Le pont ayant le plus petit ID doit être choisi comme racine de l'arbre.

Les ponts échangent des messages appelés Hello, dans lesquels ils indiquent leur ID ainsi que l'ID du pont qu'ils considèrent comme la racine de l'arbre par lequel doivent transiter leurs trames. Lorsqu'ils reçoivent une ID inférieure à celle désignée comme leur pont racine, ils rectifient l'ID du pont qui leur sert de racine pour prendre la nouvelle valeur. En d'autres termes, ils déterminent un nouveau pont racine. Avec le temps, chaque pont finit par déterminer la racine de l'arbre, c'est-à-dire le pont racine. Ensuite, chaque pont calcule la distance qui le sépare de la racine. Cette distance est calculée de proche en proche : à chaque pont traversé les distances sont incrémentées de 1.

Sur chaque réseau physique, un pont est choisi comme étant le plus proche de la racine. Si deux ponts d'un même réseau sont à la même distance de la racine, la plus petite ID est choisie. Tout le trafic issu de ce réseau et à destination d'un autre réseau physique passe par ce pont, appelé pont élu. Grâce à ce protocole, tout réseau physique est assimilable à un arbre virtuel, et il n'existe pas de boucle dans le réseau.

On peut reprocher à ce protocole des performances éventuellement dépendantes de la topologie du réseau. De plus, si les ID des ponts ne sont pas définies par le gestionnaire du réseau mais par le constructeur, le pont élu comme racine est indépendant de la volonté du gestionnaire et peut constituer un goulet d'étranglement.

Les relais-routeurs

Comme nous l'avons indiqué au début de ce chapitre, « relais » est le terme normalisé pour indiquer une passerelle de niveau 3, ou paquet. Comme le monde IP a maintenant quasiment l'exclusivité du niveau 3, la tendance est d'utiliser le terme « routeur » pour exprimer un relais de niveau paquet IP. Malheureusement, ce terme peut prêter à confusion lorsqu'on parle d'un routeur de niveau trame. Le concept de routeur n'est pas lié à un niveau mais à une technologie. Parler de routeur, c'est donc le plus souvent parler de routeur IP, et c'est ce que nous allons faire dans ce chapitre. Cependant, il faut se rappeler qu'un routeur de niveau 2 est imaginable, même si ce n'est pas un cas classique, si les trames contiennent l'adresse complète du destinataire. Pour l'étude des routeurs nous renvoyons le lecteur au chapitre 26.

Les routeurs multiprotocoles

Les routeurs multiprotocoles se distinguent par l'éventail de protocoles réseau gérés ainsi que par le nombre et le type des interfaces réseau supportées. Ces produits sont relativement complexes, ce qui explique qu'un faible nombre de sociétés se soit spécialisé dans ces routeurs.

Un routeur multiprotocole possède plusieurs interfaces de niveau trame et plusieurs protocoles de niveau paquet. Lorsque la trame se présente dans le routeur, elle est décapsulée de façon que le paquet soit récupéré. Après examen de la zone d'adresse du paquet, celui-ci peut être transcodé dans le format paquet d'un autre protocole avant d'être encapsulé dans une nouvelle structure de trame.

Les routeurs multiprotocoles peuvent supporter un pont-routeur, ou bridge-router *(voir plus loin)*. Le nœud peut dans ce cas reconnaître la référence ou l'adresse de niveau trame et router ou commuter la trame sans remonter au niveau paquet. Si la référence ou l'adresse de niveau trame n'est pas reconnue, on passe au niveau paquet pour router le paquet sur l'adresse de niveau 3.

À la différence d'un pont, un routeur peut isoler certains segments du réseau et créer des domaines. Il permet d'offrir une bonne isolation entre chaque réseau connecté, évitant ainsi la propagation des signaux émis en broadcast. Actuellement, les vitesses atteintes par les routeurs d'entreprise sont de 10 000 à 15 000 paquets/s et avoisinent souvent les 100 000 paquets/s. Du fait de l'augmentation constante des débits des applications, il a fallu, à la fin des années 90, se pencher sur la conception de routeurs beaucoup plus puissants, en particulier pour les opérateurs, capables de router de un à mille millions de paquets par seconde. Nous les détaillons à la section suivante.

Les gigarouteurs

La nouvelle génération de routeurs haut débit, appelés gigarouteurs ou térarouteurs, repose sur une distribution de la table de routage et du traitement du paquet dans l'interface d'accès puis sur l'utilisation d'un commutateur pour transporter le paquet d'un port d'entrée vers un port de sortie.

La figure 27.3 donne une idée de l'architecture d'un gigarouteur. Les gigarouteurs permettent aux ports d'accès d'atteindre des vitesses de 2,5 Gbit/s. On parle de térarouteur pour des vitesses de 10 à 40 Gbit/s. La transmission de paquets IP à ces vitesses est exploitée aujourd'hui par les techniques IP sur SONET et IP sur WDM ou MPLS.

Les commutateurs forment le cœur des routeurs très haut débit pour permettre de réaliser des accès à plusieurs centaines de mégabits voire de gigabits par seconde.

Les bridge-routers

Les bridge-routers, aussi appelés b-routeurs ou ponts-routeurs, ont pour rôle d'allier le meilleur des deux technologies. Ils intègrent, selon les produits, les trois couches basses, physique, liaison et paquet, et essaient d'agir sur le niveau liaison lorsqu'ils en ont la possibilité, faute de quoi ils remontent au paquet pour traiter l'adresse de niveau paquet.

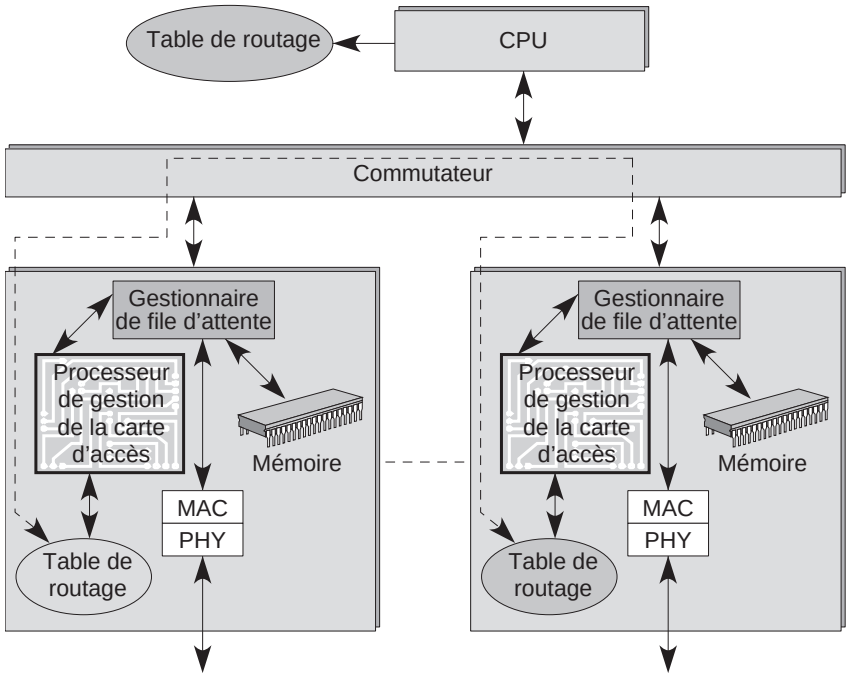


Figure 27.3
Architecture d'un gigarouteur

En d'autres termes, les bridge-routers reçoivent une trame qui est traitée comme si l'organe était un pont. Si le pont de niveau trame ne permet pas de déterminer la direction dans laquelle il faut envoyer la trame, celle-ci est décapsulée pour récupérer le paquet qu'elle transporte dans sa zone de données. La passerelle a maintenant un paquet à examiner, et elle joue le rôle de passerelle de niveau 3 qui est généralement un routeur IP.

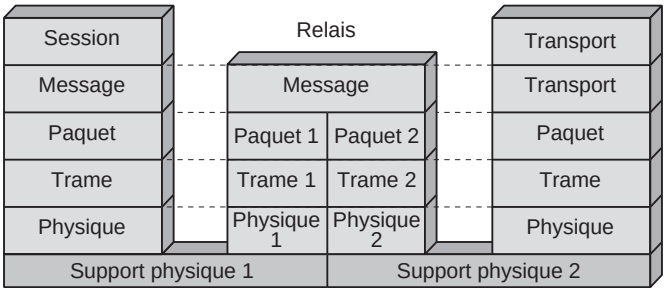
Le bridge-router est un organe assez complexe puisqu'il demande une gestion des tables de niveau trame et de niveau paquet. En revanche, c'est un équipement très performant du point de vue des possibilités de traitement des références et des adresses.

Les relais de transport

Les relais de transport se situent au niveau 4 de l'architecture du modèle de référence. Leur utilisation est recommandée lorsqu'on veut interconnecter des réseaux de niveau message différents. Par exemple, si l'on veut interconnecter une communication sous TCP et une autre sous UDP, il faut passer par des relais de transport. Ces relais peuvent être aussi appelés des routeurs de niveau message, ou routeurs de niveau 4. Il faut en effet remonter jusqu'au niveau transport pour reconstituer le message et examiner l'adresse du niveau correspondant, c'est-à-dire l'adresse qui se trouve dans le message. En pratique, la gamme de leur utilisation est moins variée, et il existe peu de produits de ce type sur le marché.

L'architecture d'un relais est illustrée à la figure 27.4.

Figure 27.4
Architecture d'un relais



Les techniques de tunneling

Les techniques d'interconnexion que nous avons rencontrées jusqu'à présent ne concernent que la translation : on translate l'information à transporter d'une trame vers une autre trame ou d'un paquet vers un autre paquet. Une autre méthode, totalement différente, appelée encapsulation, consiste à placer une trame à l'intérieur d'une autre trame ou un paquet à l'intérieur d'un autre paquet.

Par exemple, l'interconnexion d'un réseau IPv6 avec un réseau IPv4 peut se faire de la façon suivante. Supposons qu'un client IPv6 souhaite transmettre un paquet IPv6 à un client qui travaille sur une machine terminale IPv6. Supposons également que le seul réseau qui interconnecte ces deux machines soit l'Internet de type IPv4. Une première solution serait de faire une translation, c'est-à-dire de transférer l'intérieur du paquer IPv6 dans le paquet IPv4 et, à l'arrivée, de transférer à nouveau le contenu du paquet IPv4 dans un paquet IPv6. Cette solution est possible mais complexe, car il faut redéfinir complètement les zones de supervision des paquets translatés. C'est la raison pour laquelle on préfère utiliser une autre méthode : dans la machine terminale de l'émetteur, on encapsule le paquet IPv6 à l'intérieur d'un paquet IPv4. Le paquet IPv4 est transporté sur Internet, et, à l'arrivée, on décapsule le paquet IPv4 pour retrouver le paquet IPv6. On a en fait utilisé le réseau IPv4 comme un tunnel.

Pour interconnecter deux réseaux sans recourir à une passerelle, l'utilisation d'un tunnel est classique. C'est ce qu'on appelle faire du tunneling.

Translation et encapsulation

Les deux principaux niveaux d'interconnexion sont, comme nous l'avons vu :

- le niveau liaison, avec des ponts ;
- le niveau réseau, avec des routeurs.

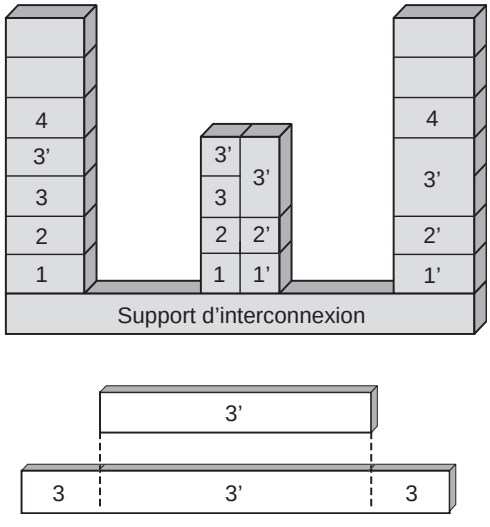
Si l'on reste au niveau pont, deux solutions sont envisageables : la translation et l'encapsulation.

Dans la translation, les adresses source et destination des stations terminales sont véhiculées dans les en-têtes. Dans l'encapsulation, une trame complète venant du réseau local est incluse dans la trame du réseau qui va servir de tunnel. Cette méthode ne demande pas de traitement de la trame, mais, comme elle n'est pas normalisée, elle

présente l'inconvénient de se restreindre à un monde homogène, c'est-à-dire d'aller d'une station terminale avec un protocole X à une station terminale utilisant le même protocole X.

La figure 27.5 illustre l'architecture d'une technique d'encapsulation de niveau paquet. On suppose qu'une machine terminale d'une entreprise utilise le protocole IPv6 et qu'elle veuille se connecter à réseau local IPv6. Le client est représenté par la pile de gauche et l'entreprise par la pile de droite. Le protocole indiqué avec la valeur 3' est donc IPv6. Pour interconnecter cette station et le réseau local, seul le réseau Internet IPv4 est disponible. IPv4 est représenté par le protocole indiqué par la valeur 3. La station terminale encapsule son paquet IPv6 (protocole 3') dans un paquet IPv4 (protocole 3). Ce paquet IPv4 est transporté sur Internet jusqu'au routeur d'accès de l'entreprise, qui est symbolisé par la pile de protocoles du milieu. Dans ce routeur, le paquet IPv4 (protocole 3) est décapsulé pour retrouver le paquet IPv6 (protocole 3'). Ce paquet IPv6 est ensuite transporté en IPv6 dans le réseau local, représenté par la partie droite du schéma.

Figure 27.5
Encapsulation de niveau paquet



La même solution s'offre au concepteur de réseau pour interconnecter des machines IPv4 par l'intermédiaire d'un réseau IPv6. Il suffit d'encapsuler le paquet IPv4 dans le paquet IPv6 puis, à l'arrivée, de décapsuler le paquet IPv6 pour retrouver le paquet IPv4.

Les deux solutions d'encapsulation sont comparables. Celle qui sera la plus pratiquée dépendra de la façon de passer d'IPv4 à IPv6. Une première solution consiste à supposer qu'un opérateur se décide à proposer un réseau IPv6 pour effectuer le transfert des paquets pour la simple raison qu'avec IPv6 il pourra offrir plus de services à ces clients qu'avec IPv4. Les clients resteront sûrement encore quelque temps en IPv4 avant de passer en IPv6. Il suffira alors d'encapsuler les paquets IPv4 dans les paquets IPv6 de l'opérateur. Maintenant, si ce sont les clients qui décident de passer en IPv6 — parce qu'ils peuvent indiquer plus d'informations dans leurs zones de supervision — mais que les opérateurs restent en IPv4, on aura des encapsulations de paquets IPv6 dans des paquets IPv4.

Les pare-feu

Les fonctionnalités des pare-feu sont analysées en détail au chapitre 34. Nous introduisons dans ce chapitre ces équipements réseau car ils deviennent de plus en plus nécessaires dans les réseaux d'aujourd'hui, même pour un particulier dès lors qu'il se rattache à Internet.

Un pare-feu, ou coupe-feu ou encore firewall, est, comme son nom l'indique, un équipement dont l'objectif est de séparer le monde extérieur du monde intérieur à protéger. Son rôle est de ne laisser entrer que les paquets dont l'entreprise est sûre qu'ils ne posent pas de problème.

Les pare-feu offrent de nombreuses fonctions, dont la principale est de trier ce qui entre ou ce qui sort et de décider d'une action lorsque la reconnaissance a été effectuée. Les actions peuvent aller du rejet du paquet, à sa compression-décompression, en passant par son examen par un antivirus, son ralentissement, son accélération, etc.

Divers moyens sont mis en œuvre pour reconnaître un paquet et plus généralement le flot, comme la reconnaissance de l'application qui transite par le coupe-feu, l'adresse de destination ou l'adresse source, la machine et l'application sur laquelle le distant veut se connecter, etc.

Les pare-feu se distinguent par le niveau auquel ils travaillent. En règle générale, ils sont de niveau 4, ou message : on essaie de trouver dans le message de niveau TCP un moyen de reconnaître l'application. Les utilisateurs se différencient par leurs adresses source et destination mais surtout, dans la première génération, par le numéro de port, qui indique l'application en cours. Par exemple, le port 80 indique une application HTTP. Cependant, les numéros de port sont de moins en moins fiables car les attaquants se servent des ports ouverts et souvent du port 80 en utilisant le protocole HTTP comme d'une capsule dans laquelle ils intègrent leur message. Le concept de numéro de port est introduit aux chapitres 8 et 9 pour IP et TCP.

L'utilisation de numéro de port est assez restrictive, dans la mesure où de plus en plus d'applications possèdent des ports dynamiques, comme FTP, la plupart des applications P2P (Peer-to-Peer) ou les signalisations téléphoniques. De plus, deux clients peuvent déterminer entre eux un numéro de port sur lequel ils souhaitent communiquer.

L'évolution des pare-feu a consisté à monter dans les couches de protocoles de façon à atteindre la couche application afin de pouvoir déterminer l'application en cours. On appelle pare-feu applicatif, ou pare-feu de niveau 7, les pare-feu qui sont capables de distinguer clairement les applications. Si le reproche longtemps adressé aux pare-feu était de prendre beaucoup de temps et de ne pas être capables de déterminer les applications au fil de l'eau, cela n'est plus vrai aujourd'hui. Les produits de pare-feu applicatifs introduits sur le marché depuis quelque temps ne prennent pas plus de temps que la plupart des équipements réseau rencontrés dans le monde IP. Nous pouvons citer le cas du boîtier QoSMOS, qui est capable de filtrer et de déterminer les applications dans un laps de temps très court, de telle sorte que la sortie des paquets n'est retardée que d'un temps maximal égal au temps de traversée d'un routeur courant.

Le pare-feu s'installe souvent dans un boîtier dédié pour simplifier sa mise en œuvre, mais il peut également se trouver en différents points du réseau, allant du routeur au commutateur, en passant par un serveur spécialisé ou le poste client.

Les proxy

Les proxy permettent de rompre avec le modèle classique client-serveur d'une communication en interdisant une connexion directe du client au serveur. Il existe deux types principaux de proxy, les proxy de type applicatif et les proxy de type circuit.

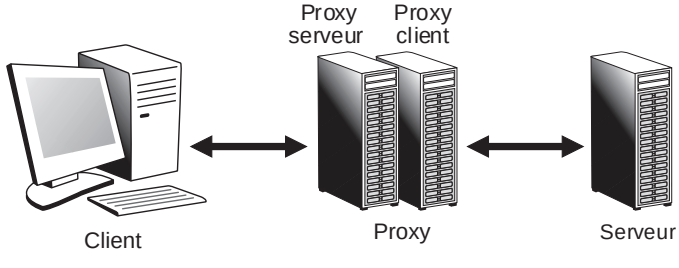
Les proxy applicatifs interviennent au niveau 7, ou application, avec pour objectif de casser le modèle client-serveur pour passer au modèle client-client. Les seconds ne permettent pas une connexion TCP de bout en bout et sont plutôt destinés à du trafic sortant d'utilisateurs authentifiés.

Les proxy applicatifs

Comme expliqué précédemment, les proxy applicatifs interviennent au niveau application du modèle de référence. Leur objectif est de rompre avec le modèle client-serveur classique en le remplaçant par un double modèle client-serveur, comme illustré à la figure 27.6. La relation directe est coupée pour être remplacée par deux relations avec le proxy faisant la transition entre les deux relations c'est-à-dire entre le proxy jouant le rôle de serveur et le proxy jouant le rôle de client. En d'autres termes, une connexion TCP de bout en bout est remplacée par deux connexions mises bout à bout grâce au proxy.

Cette solution apporte une bonne sécurité puisqu'il faut exécuter l'application dans le proxy, ce qui permet de vérifier que le flot de paquets ne forme pas une attaque. On peut réaliser des pare-feu de type proxy qui sont équivalents à des pare-feu de niveau 7. L'inconvénient majeur de cette solution est la lourdeur et la difficulté d'obtenir de bonnes performances.

Figure 27.6
Proxy applicatif



Les proxy circuit

Les proxy de type circuit ont pour objectif de vérifier que la suite de paquets sur un chemin, ou circuit virtuel, est conforme aux RFC correspondantes. En effet, beaucoup d'attaques s'effectuent en insérant dans le flux normal de paquets des paquets d'attaque. Avec un proxy circuit, les différents champs des paquets sont vérifiés afin de garantir qu'aucun paquet ne porte une attaque.

Cette solution offre également une bonne sécurité en demandant une authentification de l'utilisateur qui va utiliser le chemin, au début de sa connexion.

Les appliances

Les appliances sont des boîtiers qui possèdent une ou plusieurs fonctions bien déterminées et qui s'insèrent facilement dans le réseau. L'avantage de ces boîtiers est généralement de pouvoir démarrer une nouvelle fonctionnalité sans avoir à programmer ni à adapter les logiciels existants. Les appliances peuvent servir à la sécurité, et donc intégrer un pare-feu, mais aussi, par le biais de fonctionnalités spécifiques, à la gestion de la qualité de service.

Cette section est essentiellement consacrée aux appliances permettant d'effectuer de la surveillance de la qualité de service et de l'accélération de flux IP.

Les appliances sur la surveillance des flux permettent de déterminer les différents flux qui transitent sur Internet et, après reconnaissance, de les traiter. Les traitements peuvent être extrêmement divers suivant les boîtiers (perte, compression, mise en attente, accélération, etc.).

Pour la reconnaissance de flux, de nombreuses possibilités sont aujourd'hui disponibles, la plus classique consistant à utiliser les numéros de port. Cependant, comme les applications les plus modernes utilisent des ports dynamiques, cette solution s'avère parfois désastreuse du point de vue de la reconnaissance des flots et donc de la sécurité ou de la gestion des flots de paquets IP. Une solution, développée par la société QoSMOS, consiste à reconnaître les flots par leur grammaire, c'est-à-dire l'ensemble des règles à suivre pour réaliser l'écriture des messages applicatifs. Comme la grammaire est unique pour chaque application, il est possible de reconnaître un flot, même s'il est encapsulé dans d'autres flots, comme dans des tunnels L2TP. Une fois le flot reconnu, le boîtier peut effectuer une fonction décidée par le gestionnaire du réseau et programmée à l'avance.

On peut classer parmi les appliances les commutateurs ou les routeurs de niveau 4 ou 7, c'est-à-dire capables de commuter ou de router en fonction d'informations recueillies au niveau message ou applicatif. Par exemple, en fonction d'un numéro de port ou d'une reconnaissance de l'application, la décision de routage ou de contrôle peut différer.

Nous pouvons également ranger dans les appliances les accélérateurs de flots IP. Ces accélérateurs intègrent un moyen permettant de faire parvenir à l'émetteur une réponse plus rapidement ou d'effectuer un transfert de données, d'un point vers un autre, en moins de temps que sans accélérateur. Les accélérations peuvent s'effectuer aux différents niveaux de l'architecture. En règle générale, plus le niveau est bas, plus l'accélération globale est importante. À l'inverse, plus le niveau est haut, plus l'accélération est lente et destinée à des applications particulières. Par exemple, il est possible de compresser le flux de niveau 1, et de réduire ainsi le nombre de paquets à transmettre, ou de diminuer leur taille, ce qui entraîne une charge moindre à l'intérieur du réseau et donc un meilleur temps de transit. Au niveau 2, on peut concevoir des accélérateurs pour la correction d'erreur lorsque le taux d'erreur est important.

Au niveau 3, on peut jouer sur les adresses IP et sur le contenu des en-têtes des paquets IP. Enfin, aux niveaux supérieurs, on peut travailler sur des applications particulières plutôt que sur toutes les applications simultanément, comme aux niveaux 1, 2 et 3.

Les appliances concernent également l'accélération par la mémorisation d'informations dans des caches intermédiaires, c'est-à-dire dans des mémoires tampons qui se situent relativement près des entrées du réseau des opérateurs. On met dans le cache soit des pages entières d'information, si celles-ci sont fortement demandées, de telle sorte qu'il ne soit pas nécessaire d'aller rechercher la page sur le serveur d'origine, qui peut se situer à l'autre bout de la terre. On peut également mémoriser une partie de la page et ne chercher que des informations complémentaires. Par exemple, pour une page Web qui possède un fond assez gourmand en octets, seul le fond est gardé en un cache à proximité du client, et seules sont demandées au serveur les informations de type texte à mettre à jour. Les débits mesurés dans cette solution ne représentent que 5 à 20 p. 100 du débit total nécessaire au transport de la page complète.

Conclusion

La convergence au niveau paquet vers la technologie IP n'empêche pas une persistance des techniques d'interconnexion de réseaux. En effet, au niveau trame, une forte diversité existe encore entre les trames ATM, Ethernet, LAP-F, PPP et Ethernet. De même, au niveau paquet, la percée d'IPv6 va demander des interconnexions IPv4-IPv6 pendant un certain temps encore.

La tendance des grands opérateurs est de faire converger tous leurs réseaux cœur (réseau téléphonique, réseaux de données, réseaux cœur des réseaux de mobiles, etc.) vers un réseau unique de transport de paquets IP. Pour acheminer ces données, les paquets IP sont soit routés dans des routeurs, soit encapsulés dans des trames, pour être le plus souvent commutés. Pour permettre une sécurité du transport de ces paquets, de nombreuses solutions sont commercialisées avec plus ou moins de puissance et de succès.

Nous avons vu que les appliances offraient diverses fonctions tout en restant généralement simples à mettre en œuvre. Leur rôle principal est d'améliorer les performances du réseau par des moyens extrêmement divers.

Références

Excellent livre sur la façon dont les protocoles ATM et IP peuvent coexister dans un même réseau. Ce n'est pas exactement de l'interconnexion, mais c'est une solution pour rendre homogène un monde hétérogène :

K. AHMAD – *Sourcebook of ATM and IP Internetworking*, Wiley-IEEE Press, 2004

L'interconnexion, en remontant au protocole TCP/IP, est une solution très utilisée, qui peut s'interpréter comme un cas particulier de l'interconnexion des sous-réseaux dans un environnement Internet. Le livre suivant décrit les passerelles utilisant TCP/IP :

G. BENNETT – *Designing TCP/IP Internetworks*, Wiley, 1997

Un livre plutôt commercial, qui introduit les différentes catégories de passerelles :

V. C. BRIDGES, V. C. MARNEY-PETIX – *Switches, Routers, Gateways*, Numidia Press, 2002

Un excellent livre sur les équipements réseau et les distinctions dans leur architecture :

A. B. CASLOW, V. PAVLICHENKO – *Cisco Certification: Bridges, Routers and Switches for CCIEs*, Prentice Hall, 2000

Livre dédié aux interconnexions *via* le protocole IP, c'est-à-dire la plupart des interconnexions du monde actuel :

D. CHOWDHURY – *Unified IP Internetworking*, Springer Verlag, 2001

Livre classique du domaine de l'interconnexion, assez général mais pédagogique :

D. COMER, D. L. STEVENS – *Internetworking with TCP/IP, Design, Implementation, and Internals*, Prentice Hall, 2001

Ce livre donne une bonne vision de l'interconnexion des réseaux locaux et des réseaux étendus :

G. HELD – *Internetworking LANs and WANs: Concepts, Techniques and Methods*, Wiley, 1998

Livre très général sur les réseaux et les interconnexions :

G. S. HURA, M. SINGHAL – *Data and Computer Communications: Networking and Internetworking*, CRC Press, 2001

Un livre avec un bon compromis entre la théorie et la pratique des pare-feu.

H. MANKELL, E. SEGERBERG – *Firewall*, Vintage Books, 2003

Livre très orienté vers les interconnexions *via* Internet :

E. M. NOAM – *Interconnecting the Network of Networks*, MIT Press, 2001

Le livre suivant introduit les éléments de base en matière d'interconnexion et en particulier pour les hauts débits :

C. PARTRIDGE – *Innovations in Internetworking*, Artech House, 1988

Excellente introduction à tous les équipements réseau, dont les passerelles :

R. PERLMAN – *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*, Addison Wesley, 1999

Excellent livre qui pose la problématique de la convergence des techniques de commutation et de routage. On s'aperçoit que la commutation est indispensable et que, à l'intérieur, les routeurs ne sont que de commutateurs :

R. PUZMANOVA – *Routing and Switching: Time of Convergence?*, Addison Wesley, 2001

Un excellent livre sur les appliances pour optimiser et sécuriser les réseaux :

> M. SYME, P. GOLDIE – *Optimizing Network Performance with Content Switching: Server, Firewall and Cache Load Balancing*, Pearson Education, 2003

Un très bon livre pour tout comprendre des pare-feu :

> J. R. VACCA – *Firewalls Clearly Explained*, Academic Press, 2004

Un livre très complet sur les architectures des routeurs et des serveurs dans le monde Internet :

> G. VARGHESE – *Internet Algorithmics: How To Build Fast Routers and Servers*, Pearson Education, 2004

Livre qui propose une analyse très détaillée des mécanismes d'interconnexion et qui est recommandé à ceux qui veulent aller plus loin :

> J. XU – *Topological Structure and Analysis of Interconnection Networks*, Kluwer Academic Publishers, 2002

Partie X

Le contrôle et la gestion

Les réseaux ne pourraient fonctionner s'il ne s'y trouvait un contrôle des flots qui y transitent et une gestion des équipements. La différence entre contrôle et gestion est parfois ténue. En règle générale, on considère qu'un contrôle correspond à une action temps réel, c'est-à-dire à une action qui doit être effectuée instantanément pour répondre à une demande ou à un problème de la part du réseau. La gestion correspond à une action qui n'a pas besoin d'être effectuée en temps réel. Par exemple, l'action d'arrêter un flot de paquets pour le rerouter, suite à la panne d'un nœud, est une action de contrôle. En revanche, l'envoi d'une facture à un utilisateur, c'est-à-dire le fait de récupérer les informations nécessaires à l'établissement de cette facture, est une action de gestion puisqu'il n'est pas nécessaire de le faire instantanément.

Cette partie contient quatre chapitres. Le chapitre 28 examine les fonctions de contrôle et s'intéresse aux moyens de contrôler les flux des utilisateurs pour que les clients obtiennent la qualité de service dont ils ont besoin. Cette qualité de service peut s'exprimer à l'aide de paramètres de performance, comme le temps de réponse ou le taux de perte des paquets.

Le chapitre 29 s'intéresse à la gestion d'un réseau et, de façon sous-jacente, aux grandes fonctionnalités de la gestion, telles la comptabilité, la planification, la sécurité, les pannes et la gestion des performances. Nous décrivons dans ce chapitre les différentes architectures de gestion qui peuvent être mises en place pour réaliser ces fonctions.

Les chapitres 30 et 31 présentent des technologies spécifiques, capables de mettre en place des contrôles ou de la gestion, voire, de plus en plus souvent, les deux à la fois, puisque les recherches actuelles tendent à intégrer les fonctions de contrôle et de gestion. Ces deux chapitres concernent, d'une part, les VPN et, d'autre part, les contrôles et la gestion par politique. Les VPN permettent, à partir d'un problème spécifié, de mettre en place une architecture apte à le résoudre. Par exemple, un VPN peut résoudre les problèmes de sécurité dans une entreprise. Les contrôles et la gestion par politique proposent une solution pour configurer le réseau de telle sorte qu'il puisse rendre exactement le service souhaité par les utilisateurs.