

LES COUCHES RESEAUX IP ET X25

Deux réseaux de transport de données cohabitent en France. X25 qui est un réseau qui fonctionne à partir de circuits virtuels et IP qui es un réseau à base de datgramme qui supporte directement INTERNET.

1 - RESEAU IP

Le protocole IP constitue la couche réseau qui offre le service pour TCP, UDP, ... IP procure un service non connecté non fiable par datagramme. Le RFC 791 paru en 1981 est sa spécification officielle. Un excellent ouvrage : Le routage dans INTERNET par Huitema ed. Eyrolles.

Adressage

Chaque adresse INTERNET est codée sur 32 bits. Elle ne désigne pas un hôte mais une interface réseau. Un hôte qui a plusieurs interfaces aura plusieurs adresses. Quelques adresses sont particulières :

0.0.0.0	Un hôte inconnu
255.255.255.255	Tous les hôtes
x.y.z.0	Un hôte inconnu sur le réseau x.y.z
x.y.z.255	Tous les hôtes sur le réseau x.y.z
0.0.0.z	L'hôte z sur ce réseau
127.0.0.1	L'hôte local

Format d'un paquet IP

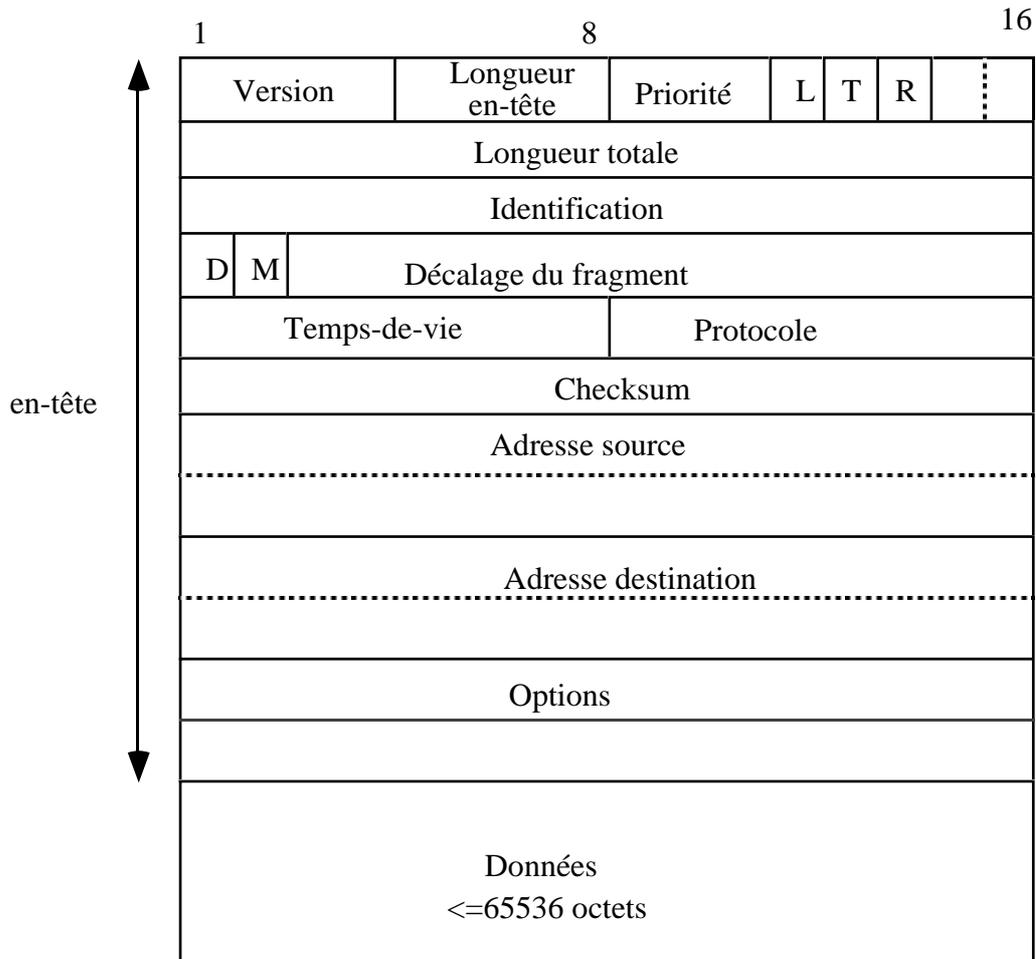


Figure 1. Format d'un paquet IP.

Le format d'un paquet IP est donné figure 1. Les 4 octets des mots de 32 bits sont transmis en grand indien. La longueur de l'en-tête est de 5 à 15. En réalité afin d'accélérer les routages, les 5 premiers mots sont toujours traités sur des registres et on ne mentionne pas d'option. La version est 4 ce qui signifie un adressage à 4 numéros. La version 6 qui est en cours d'expérimentation sera 6.

Les champs priorité et type de service permettent d'accélérer les transaction en choisissant éventuellement le meilleur support. Le champs priorité influe sur les files d'attente 111 désigne le contrôle du réseau c'est la séquence la plus prioritaire. Pour le type de service il y a 4 indicateurs : délai, débit, fiabilité, coût. Par exemple 1111 signifie la sortie qui achemine le plus vite avec le plus gros débit la plus fiable et ... la moins chère.

Seuls les bits 3-6 du type de service sont exploités. Le bit 3 minimise le délai, le bit 4 maximalise le débit, le bit 5 maximalise la fiabilité, le bit 6 minimise le coût monétaire.

Chaque paquet IP reçoit une identification construite par le service qui l'utilise.

La longueur maximum est sur 16 bits mais en réalité les machines ne peuvent échanger que des paquets d'au plus 576 octets. Les paquets sont donc en général fragmentés et le décalage des fragments est donc contenu dans un paquet IP.

Le temps de vie est décrémenté de 1 à chaque passage dans un routeur. Quand la destination finale est atteinte, le protocole est utilisé pour savoir à quelle application le paquet doit être transmis. La liste des numéros international de protocole est publiée régulièrement sous forme de RFC. Le checksum est un calcul effectuée sur l'ensemble du paquet pour garantir son intégrité. Il est calculé en effectuant le complément à un du total en complément à 1 de tous les mots de 16 bits de l'en-tête.

Le champs protocole identifie le protocole qui a fourni le paquet à IP (UDP, TCP, ...).

La somme de contrôle (checksum) est calculé à partir de l'en-tête du paquet par complément à 2 de la somme des mots de 16 bits de l'en-tête.

Le paquet contient les numéros des hôtes source et destination.

Les options comportent des possibilités qui ne sont pas supportées par tous les routeurs. Il s'agit de :

- sécurité,
- enregistrement de la route suivie,
- estampillage horaire,
- routage peu strict de la source,
- routage strict de la source.

Les routeurs utilisent leurs tables pour l'envoi du paquet. Ils effectuent le traitement suivant :

1 - recherche d'une entrée associée à l'adresse IP destinataire et si cette adresse est trouvée envoi sur le circuit concerné,

2 - recherche d'une entrée concernant le réseau IP dont dépend le destinataire et si cette adresse est trouvée envoi sur le circuit concerné,

3 - recherche d'une entrée standard nommée « default » vers laquelle le paquet IP est envoyé.

L'étape 2 est liée à l'utilisation de masques de sous-réseau.

Exemple : 147.210 est le numéro de réseau correspondant à reamur. Le masque de sous-réseau 255.255.0.0 permet d'isoler dans un numéro IP, les deux premiers numéros. Si dans un routeur l'adresse IP 147.210.34.5 est demandée et si une entrée de type 147.210.0.0 existe alors le paquet sera directement routé vers le réseau reamur.

2 - QUELQUES PROTOCOLES TOURNANT SUR IP

Protocole ICMP

C'est le protocole de transport des diagnostics d'erreur. Bien que s'appuyant sur IP, il fait partie de la couche réseau et tourne sur tous les routeurs. Ces messages sont

émis sans provoquer de réponses. Tous les paquets ICMP commencent par 32 bits d'en-tête comprenant un champs type

- 0 réponse d'écho,
- 3 destination inaccessible
- 4 demande de ralentissement (Source Quench)
- 5 Redirection
- 8 Echo
- 9 Annonce de routeur
- 10 Sollicitation de routeur
- 11 TTL expiré
- 12 Problème de paramètre
- 13 Horodatage
- 14 Demande d'information
- 15 Réponse d'information

donnant le type du paquet et un champs code précisant le cas d'erreur

- réseau inaccessible
- hôte inaccessible
- protocole inaccessible
- port inaccessible
- fragmentation requise et DF=11
- echec de routage source.

La commande ping est l'implémentation de la fonction echo simple de ICMP. La commande traceroute s'appuie également sur ce protocole.

protocole ARP

Lorsqu'un hôte émet un paquet, il doit trouver l'adresse du prochain relai. Si l'adresse de destination est sur le même sous réseau que lui alors l'adresse du prochain relais est l'adresse de destination sinon c'est un routeur intermédiaire. L'hôte choisit ce routeur intermédiaire après avoir reçu (éventuellement après sollicitation) un paquet ICMP d'annonce de routeur. Une fois déterminé l'adresse intermédiaire, il faut lui associer une adresse media (par exemple le numéro de la carte Ethernet). Cette traduction est faite par le protocole ARP. Bien sur les hôtes maintiennent des caches avec des demandes ARP déjà satisfaites. Pour pouvoir commencer à travailler un hôte doit pouvoir connaitre son adresse afin d'émettre des paquets IP. Tant que c'est adresse n'est pas configurée il utilise l'adresse 0.0.0.0, la configuration s'effectue par le protocole RARP.

Protocole RIP

L'algorithme rentre dans la classe des vecteurs de distance. La métrique utilisée est le nombre de sauts (entre 1 et 15) et non les secondes.C'est un protocole pour les

routeurs internes à un réseau. Un tel réseau est identifié par un numéro de système autonome unique. Les paquets RIP sont émis au dessus de UDP sur le port 520. Les paquets d'annonce sont émis toutes les 30s. Si une route n'est pas annoncée pendant 3mn elle est supprimée de la table de routage. Le format d'un paquet est décrit à la figure 2. Le champs commande n'a que deux valeurs request ou response. Le champs version vaut 2. Le champs identifiant la famille d'adresse sert notamment à l'authentification. Ce champs a été rajouté dans la version 2 afin d'éviter les piratages et l'immobilisation du réseau par des pirates. L'identifiant de route permet un routage vers des passerelles extérieures (i.e. vers des réseaux qui n'ont pas le même numéro AS que le réseau local). Les masques de sous-réseau permettent de préciser pour quel sous-réseau l'information est valide. Le champs prochain relai permet de préciser une adresse qui n'est pas l'adresse standard de routage mais qui est plus efficace pour atteindre certaines parties de sous-réseau.

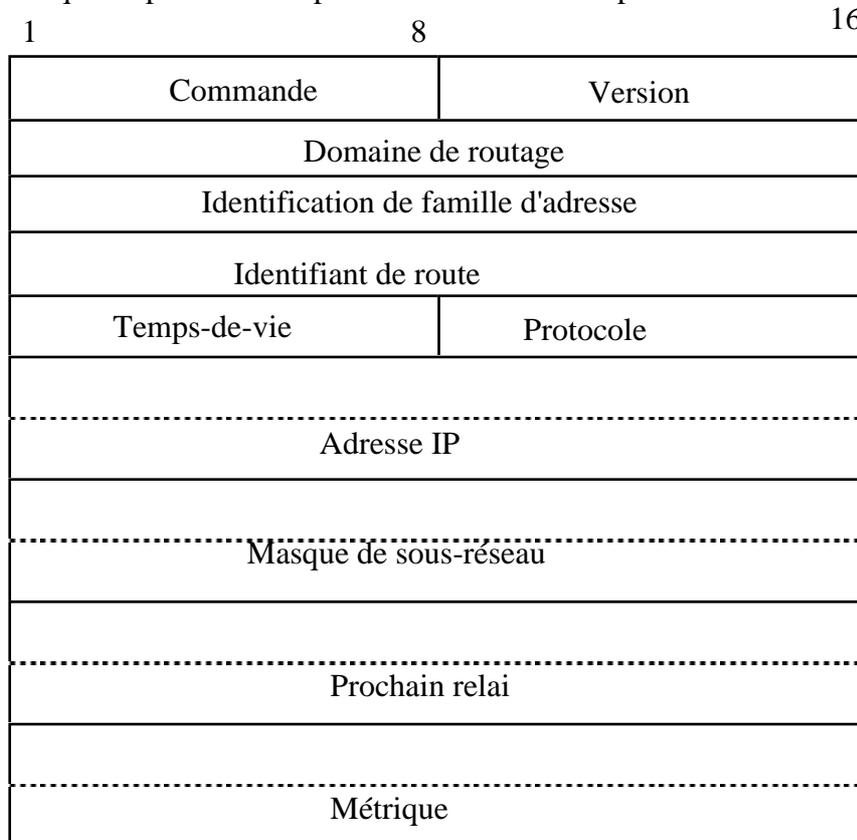


Figure 2. Format d'un paquet RIP

Protocole OSPF

Il s'agit d'un protocole basé sur les vecteurs de distance basée sur le temps mais utilisant des procédés de diffusion. Ce protocole permet de prendre en compte des identifiants de réseaux. La différence essentielle tient au fait qu'ospf calcule à partir d'une base de donnée le meilleur chemin à un instant donné. L'algorithme ne garde pas seulement le meilleur accès à un routeur mais tous les accès qui lui sont communiqués. L'évaluation de ces algorithmes conduit à ne communiquer les bases de données que toutes les 30mn ce qui est très inférieur à RIP. Ce protocole est en cours d'évolution notamment pour les liaisons multipoints, les AS différents.

Protocole BGP

Ce protocole est une évolution logique du protocole EGP qui permet de gérer les passerelles extérieures (i.e. la liaison entre plusieurs AS). Le protocole EGP ne permet qu'une gestion de réseau ayant une topologie en étoile ce qui est insuffisant compte tenu de la croissance d'INTERNET. L'innovation essentielle est la substitution aux vecteurs de distance de vecteurs de chemin qui permettent la prévention des boucles dans une topologie complexe. Les chemins sont les diverses listes des réseaux à traverser pour transiter du réseau local aux autres réseaux. Ce protocole est implémenté au-dessus de TCP. Les boucles sont détectées lors de la réception des routes. Si le réseau local détecte son propre numéro AS dans la liste il ignore le message. Pour gérer les chemins entre AS on utilise une liste d'attributs constituée de

- la liste des AS traversés,
- la liste des réseaux accessibles,
- des métriques,
- des choix "politiques".

L'échange initial de BGP consiste à établir une liaison bilatère. Cette étape est authentifiée. Après connexion, les EGP distants échangent des messages de mise à jour. Chaque message ne décrit qu'un seul chemin. On a donc un bloc constitué de

- un marqueur
- longueur du message
- type du message (MAJ, sondage, erreur)
- longueur des attributs
- liste des réseaux.

BGP même dans sa dernière version (4) ne permet pas un routage dépendant de la source. On est obligé d'encapsuler les paquets IP dans des paquets IP.

Evolution des protocoles de routages

Le protocole IDPR en cours d'élaboration permettra sans doute un routage dépendant de la source. C'est un protocole basé sur l'état des liaisons comme OSPF. Le multipoint actuellement est vu comme une extension de IP en utilisant un numéro spécial de réseau. L'expérimentation en cours en Europe est MBONE. Le protocole PIM définit la stratégie entre groupe clairsemé et groupe dense.

2 - RESEAU X25

Une liaison X25 comporte plusieurs voies logiques avec un maximum de 4096 voies divisé en 16 groupes de 256 voies. La voie 0 du groupe 0 sert messages de supervision entre équipements. Les voies sont donc multiplexées sur le support. Certains circuits peuvent être permanents occupent les voies de plus faible numéro.

Adressage

La norme X121 régit cet adressage. L'adresse comporte 16 chiffres dont 14 identifient l'abonné : pays (2), réseau (1), région (7), numéro local (3), extension locale (2). TRANSPAC ne respecte pas cette numérotation : préfixe (1), département (2), commutateur (3), abonné (3), extension locale (≤ 6).

Exemple 133000870015 représente REAUMUR.

Routage

La fonction de routage doit sur chaque commutateur trouver pour un appel entrant d'initialisation d'un circuit virtuel :

- une ligne de sortie disponible,
- choisir un canal logique sur cette ligne.

Le choix s'effectue en ordonnant les sorties possibles et en équilibrant les charges entre plusieurs sorties équivalentes. Il y a possibilité de bouclage. Le réseau peut effectuer un reroutage à la demande du client.

Fonctionnement

Les primitives suivantes sont implémentées :

- call request ---> demande de CV
- incoming call ---> appel d'ouverture de CV
- call accepted ---> retour de CV
- call connected ---> ouverture du CV
- Données ---> transmission des données
- clear request ---> fermeture de CV
- Clear confirmation ---> confirmation de fermeture
- clear indication ---> indication de fermeture de CV

Format des paquets

Pour ouvrir un CV l'appelant envoie un paquet d'appel sur la première voie logique libre de plus haut numéro. Ce paquet contient

- l'adresse réseau de l'émetteur,
- l'adresse réseau du destinataire,

Ces adresses sont codées en décimal sur 4 bits. Les longueurs d'adresse sont codées sur 4 bits. Un champ service complémentaire permet : taxation de l'appelé, paramétrage de la taille des paquets et des buffers de communications. Un champ utilisateur permet de transporter lors d'un appel des paramètres exploités par l'application serveur : nom d'application, login, ...

Le paquet données ne contient plus les adresses mais uniquement un numéro de voie logique qui correspond au CV initialisé. Les messages sont numérotés modulo 8 ou 128 suivant l'option de l'initialisation du circuit virtuel. Des bits permettent de :

- différencier les types de paquet (utilisateur ou contrôle)
- signaler un paquet fragmenté,
- assurer un contrôle de bout en bout par acquittement.

Le paquet de libération contient le numéro de voie logique à libérer ainsi que la cause de fermeture. Il contient des données utilisateurs comme pour l'initialisation.

Il existe d'autres type de paquet : interruption et confirmation d'interruption, réinitialisation et confirmation de réinitialisation, reprise et confirmation de reprise.

Cas particuliers PAD et PAV

L'avis X128 normalise le dialogue entre l'utilisateur d'un terminal et un Point d'accès de données qui permet de se connecter sur transpac. Après établissement du CV, le terminal est en mode connecté, il peut revenir en état commande par CTRL-P et exécuter des commandes interprétables par le PAD; par exemple LIB libère la connexion, SET n:x met le paramètre n à la valeur x. Les points d'accès videotex sont des PAD particuliers : la vitesse d'accès est 1200b/s mais de réception est 75b/s, ils utilisent des noms abrégés pour l'accès aux serveurs.

