Chapitre 4- RIL : Adressage IP

Le rôle fondamental de la couche réseau (niveau 3 du modèle OSI) est de déterminer la route que doivent emprunter les paquets. Cette fonction de recherche de chemin nécessite une identification de tous les hôtes connectés au réseau. De la même façon que l'on repère l'adresse postale d'un bâtiment à partir de la ville, la rue et un numéro dans cette rue, on identifie un hôte réseau par une adresse qui englobe les mêmes informations.

Le modèle TCP/IP utilise un système particulier d'adressage qui porte le nom de la couche réseau de ce modèle : l'adressage IPv4. En fait, le protocole IPv4 sert à véhiculer trois types de trafic distincts.

unicast
Le trafic unicast désigne une communication entre un hôte source unique et un hôte destination unique lui aussi.

multicast
Le trafic multicast désigne une communication entre un hôte source unique et un groupe d'hôtes qui ont choisi de recevoir le flux émis par la source. L'émission d'une chaîne de télévision est l'analogie usuelle pour ce type de trafic. L'émission est permanente et seuls les téléviseurs réglés pour recevoir cette chaîne affichent la vidéo de cette chaîne.

Broadcast
Le trafic broadcast désigne un flux émis par un hôte à destination de tous les autres hôtes appartenant au même domaine de diffusion. Ce type de trafic ne peut exister que sur les réseaux dits de diffusion comme **Ethernet**. Par exemple, le protocole ARP utilise une trame de diffusion (broadcast) pour interroger tous les autres hôtes du réseau pour savoir à quelle adresse MAC correspond l'adresse IPv4 connue.

4.1 - PRÉSENTATION DU PROTOCOLE IPv4

4.1.1 - Qu'est-ce qu'IPv4
IPv4 est la première version du protocole IP et celle qui est utilisée actuellement. Ce protocole est défini dans la RFC 791.

- ***RFC (Request for Comments)***

✓ Série de documents techniques et organisationnels au sujet d'Internet,

✓ Les RFC font office de standards,
⇨ http://www.rfc-editor.org (liste complète en anglais),
⇨ http://abcdrfc.free.fr/ (traduction partielle en français).

Le rôle du protocole IP

Le protocole IP fait partie de la couche Internet de la suite de protocoles TCP/IP. C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des

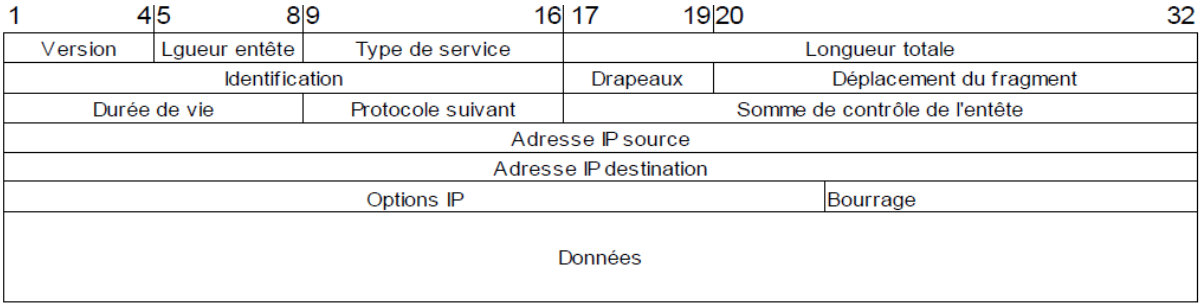
datagrammes IP (les paquets de données), sans toutefois en assurer la « livraison ». Il s'affranchit des réseaux physiques traversés. En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.

Le protocole IP détermine le destinataire du message grâce à 3 champs :

- *Le champ **adresse IP** : adresse de la machine*
- *Le champ **masque de sous-réseau** : un masque de sous-réseau permet au protocole IP de déterminer la partie de l'adresse IP qui concerne le réseau*
- *Le champ **passerelle par défaut** : Permet au protocole Internet de savoir à quelle machine remettre le datagramme si jamais la machine de destination n'est pas sur le réseau local*

4.1.2 - La trame IPv4

L'entête de la trame IPv4 est constitué de 14 champs répartis comme suit :



• **Version** (4 bits) : indique quelle est la version du protocole (ici 4)
• **Longueur de l'entête** : indique la longueur de l'entête du datagramme
• **Type de services** (8 bits) : indique aux routeurs comment doit être géré le datagramme
• **Longueur totale** (16 bits) : indique quelle est en octets la longueur totale du datagramme (entête et données)
• **Identification** (16 bits) : identifiant permettant de réassembler le datagramme
• **Drapeaux** : divers drapeaux de contrôle
• **Déplacement du fragment** : indique quelle est la position du paquet si celui-ci est un fragment de datagramme
• **Durée de vie** (8 bits) : indique le nombre de routeurs que peut traverser le datagramme
• **Protocole** (8 bits) : identifie le protocole de niveau supérieur (TCP, ICMP...) utilisé pour transmettre le message
• **Total de contrôle entête** (16 bits) : permet de détecter les erreurs de transmission dans l'entête.
• **Adresse IP source** (32 bits) : renseigne l'adresse IP de l'expéditeur
• **Adresse IP destination** (32 bits) : renseigne l'adresse IP du destinataire
• **Options IP éventuelles** (taille inférieure ou égale à 32 bits) : options concernant des fonctionnalités de mise au point
• **Bourrage** : le champ option n'a pas de taille fixe. Le bourrage permet de faire atteindre à ce champ une taille multiple de 32 bits (4 octets)

4.1.3 - Le système d'adressage

Les adresses IPv4 sont codées sur 32 bits ce qui permet d'attribuer 4 294 967 296 adresses. Elles sont notées sous la forme de 4 chiffres compris entre 0 et 255 sous la forme :

192.168.0.23

A cette adresse est également ajouté un masque indiquant à quel réseau appartient l'équipement auquel cette adresse a été attribuée. Ce masque indique quelle partie de l'adresse renseigne sur l'adresse du réseau et est noté de la manière suivante :
192.168.0.23/24 (notation moderne) ou **192.168.0.23/255.255.255.0** (notation ancienne)

Dans cet exemple, le **"/24"** (également, appelée notation "C.I.D.R.") indique que les 24 premiers bits composant l'adresse forme l'adresse du réseau, ici, le réseau a donc pour numéro : 102.168.0.0.

- CIDR : Classless Inter Domain Routing
- ✓ RFC 1518 et RFC 1519
- ✓ Convention qui spécifie le nombre de bits utilisé pour la partie réseau.

- ✓ Exemples :
- 142.12.42.145/24 <=> 142.12.42.145 255.255.255.0
- 153.121.219.14/20 <=> 153.121.219.14 255.255.240.0

- Facilite l'écriture des tables de routage.

4.1.3.1 - Classes d'adresses

Le protocole IPv4 défini 5 classes d'adresses nommées simplement adresse de classe A, B, C, D ou E. Ces classes définissent combien d'ordinateurs et de réseaux il est possible de constituer sur un site en vue de leur raccordement à Internet avec des adresses publiques qui sont attribuées par le fournisseur d'accès. Pour une utilisation dans un réseau local non connecté à Internet, il n'est pas obligatoire de suivre cette norme si ce n'est pas question d'habitude.

Bit :	1	2	3	4	8	16	24	32
Classe A	0	Adresse réseau			Identifiant de sous-réseau / identifiant d'équipement			
Classe B	1	0	Adresse réseau			Identifiant sous-réseau / équipement		
Classe C	1	1	0	Adresse réseau			Id sous-réseau / équip.	
Classe D	1	1	1	0	Adresse multi-destinataire			
Classe E	1	1	1	1	0	Adresses réservées		

- Les adresses de classe A sont reconnaissables sous leur forme binaire car leur premier bit est à zéro. Ces adresses sont comprises entre 1.0.0.0 et 126.0.0.0 et ont par défaut un masque de 255.0.0.0. Ces adresses sont utilisées pour les réseaux comportant plus de 65 536 ordinateurs. Elles attribuent 7 bits pour l'identification du réseau et 24 pour l'identification de chaque machine.

- Les adresses de classe B ont leurs deux premiers bits commençant par 10. Elles permettent d'allouer des adresses comprises entre 128.1.0.0 et 191.255.0.0 avec le masque par défaut qui est de 255.255.0.0. Elles sont utilisées sur les réseaux intermédiaires comportant entre 256 (28) et 65 535 ordinateurs. 14 bits sont alloués pour l'identification du réseau et 16 pour identifier chaque ordinateur.

- Les adresses de classe C ont leurs 3 premiers bits commençant par 110. Les adresses qu'elles permettent d'allouer sont comprises entre 192.0.1.0 et 233.255.255.0 et le masque par défaut est 255.255255.0. Elles sont utilisées pour les petits réseaux comportant moins de 256 machines. 21 bits sont attribués à l'identification du réseau et 8 à l'identification de chaque ordinateur.

- Les adresses de classe D sont identifiables grâce à leurs 4 premiers bits qui sont 1110 et sont comprises entre 224.0.0.0 et 239.255.255.255. Ce sont des adresses multidestinataires.

- Enfin, les adresses de classe E, reconnaissables à leurs 5 premiers bits égaux à 11110 sont réservées pour une utilisation ultérieure. Elles sont comprises entre 240.0.0.0 et 255.255.255.255

Chacune de ces classes réserve des adresses privées pour les réseaux privés devant être raccordés à un réseau public. Pour la classe A, ce sont des adresses commençant par 10.x.x.x, en classe B : 172.16.x.x à 172.31.x.x et en classe C : 192.168.x.x. A priori, aucun équipement n'a le droit de communiquer sur un réseau public avec une adresse privée. Ces plages sont définies dans la RFC 1918.

Plages d'adresses réservées pour les réseaux locaux :

- ✓ 10.0.0.1 à 10.255.255.254,
- ✓ 172.16.0.1 à 172.31.255.254,
- ✓ 192.168.0.1 à 192.168.255.254,

Adresse réservée pour les tests : 127.0.0.1

4.1.3.2 - Masques de sous-réseaux

Un masque de sous-réseau par défaut est employé sur des réseaux TCP/IP non divisés en sous-réseaux. Tous les hôtes nécessitent un masque de sous-réseau, même sur des réseaux à segment unique. Le masque de sous-réseau par défaut utilisé est fonction de la classe d'adresse.
Dans le masque de sous-réseau, tous les bits correspondant à l'ID de réseau sont à 1. La valeur décimale dans chaque octet est 255. Tous les bits correspondant à l'ID d'hôte sont à 0.

- ***Sous-réseaux***
  - ***Pourquoi ?***

- ✓ Utilisation hétérogène de moyens de couche physique,
- ✓ Réduction de l'encombrement,

- ✓ Economise les temps de calculs,
- ✓ Isolation d'un réseau
- ✓ Renforcement de la sécurité,
- ✓ Optimisation de l'espace réservé à une adresse IP.

- ***Le masque permet de segmenter un réseau en plusieurs sous-réseaux.***

Exemple de masque :
255.255.255.224 => 11111111.11111111.11111111.**111**00000

Détermination du sous-réseau d'une machine :
200.100.40.33 => 11001000.01100100.00101000.00100001

On effectue et **ET** logique avec le masque de sous-réseau :

200.100.40.32 => 11001000.01100100.00101000.00100000

- ***Nombre de sous réseaux : 2 RFC s'appliquent:***
- ✓ RFC 1860 : 2^n – 2 , n étant le nombre de bits à 1
- ✓ RFC 1878 : 2^n
  - ⇨ Adresse des sous réseaux
- Nombre de machines du sous réseau :
- ✓ 2^m – 2, m étant le nombre de bits de la partie hôte

4.1.3.3 - Adresses particulières

Un certain nombre d'adresses particulières sont définies par IPv4. Ces adresses sont réservées à des usages particuliers.

a- La boucle locale

La boucle locale correspond à une interface réseau virtuelle présente sur la quasi-totalité des équipements. Elle est utilisée pour les communications entre les processus. Ces processus peuvent aussi bien être des jeux ou les systèmes d'impression sur Unix (Cups).
Dans la pratique, l'adresse de cette interface est toujours **127.0.0.1/8**. Normalement, un paquet émis sur cette interface ne devrait jamais apparaître sur un réseau.
b - Les adresses de broadcast

Les adresses de broadcast (adresses de diffusion) correspondent à l'adresse la plus haute que l'on puisse trouver sur un réseau. Par exemple, pour le réseau **192.168.0.0/24**, l'adresse de broadcast sera **192.168.0.255**.

- ***Adresse de diffusion :***
- ✓ Mettre tous les bits de la partie hôte à 1

L'adresse de broadcast 255.255.255.255 est principalement utilisée par les équipements ne disposant pas d'adresse IP sur le réseau (par exemple, lors d'une auto-configuration via

DHCP). Les équipements utilisant cette adresse de broadcast annoncent généralement l'adresse IP **0.0.0.0** (pas d'adresse IP).

4.1.3.4 Distribution des adresses IP

- Organisme **IANA** (Internet Assigned Numbers/ Naming Authority):
- ✓ Distribue les adresses IP aux FAI (Fournisseurs d'accès à Internet).

- Organisme **InterNIC** (Internet Network Information Center):
- ✓ Attribution des parties d'identifiant réseau pour les dispositifs directement reliés à internet.

4.2 - PROTOCOLES ASSOCIÉS

4.2.1 - La résolution d'adresse physique

La résolution d'adresse physique permet de faire le lien entre l'adresse IPv4 logique d'une machine et son adresse physique. Afin de comprendre pourquoi la résolution d'adresse physique est difficile avec certaines technologies de réseaux, nous allons considérer le cas de la technologie ethernet qui est la plus utilisée dans les réseaux locaux.
Sur les réseaux ethernet, les adresses physiques sont codées sur 48 bits ce qui rend impossible de créer un lien direct entre ce type d'adresses et une adresse IPv4 codée sur 32 bits. Aussi, il a été créé un protocole spécifique permettant de réaliser un lien indirect entre ces deux adresses. Il s'agit du protocole ARP (Address Resolution Protocol) qui fournit un système efficace et simple de faire cette résolution.

Quand un ordinateur A veut connaître l'adresse physique d'un ordinateur B, il diffuse une trame spéciale sur le réseau demandant à l'ordinateur B de répondre en indiquant son adresse physique. Tous les ordinateurs du réseau reçoivent cette trame mais seul l'ordinateur B reconnaît son adresse IP. Il renvoie alors la réponse. A enregistre alors cette adresse dans une table de correspondances et peut alors directement transmettre à B le datagramme IP en se servant de l'adresse physique.
Cette technologie fait donc appel à un second protocole de couche 3 en plus du protocole IP. Ce protocole multiplie également le nombre de trames de diffusion circulant sur le réseau et est donc susceptible de provoquer des saturations.

4.2.2 - Le protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est défini dans la RFC 792. Il a pour rôle l'échange de messages d'information de base entre des équipements communiquant. Les messages diffusés par ICMP servent à la gestion des erreurs aussi bien qu'à la transmission d'informations. Ces paquets peuvent être émise dans plusieurs cas tel que :

• L'utilisation de la commande ping permettant de vérifier si un poste est bien configuré sur le réseau
• Dans le cas d'un paquet dont la durée de vie a expirée
• ....

Le format des paquets ICMP est simple : Un champ "type" indique de quel type est le message ICMP, un champ code permet d'avoir des informations plus détaillées, un checksum, une suite de champ dont le contenu varie suivant le type de message et enfin, une partie du paquet IP ayant provoqué l'émission du paquet ICMP.

4.2.3 - Le protocole IGMP

Le protocole IGMP (Internet Group Message Protocol) est défini dans la RFC 1112. Son rôle est de gérer les groupes multicast dans IPv4.

Un groupe multicast est un ensemble d'équipement écoutant sur un même adresse IP. Cette technologie peut être entre autre utilisée dans le cas de la diffusion de flux en continu tel que des flux de radio sur Internet ou pour la télévision sur ADSL.

4.3. Principaux protocoles Internet et RFC correspondantes

Titre/Protocole	Description	RFC
Internet Official Protocol Standards	Etat de la standardisation de l'Internet	**1720**
Assigned Numbers	Valeurs que l'on retrouve dans les PDU.	**1700**
Host Requirements - Communications	Pile protocolaire nécessaire aux équipements qui peuvent se connecter à l'Internet.	**1122**
Host Requirements - Applications	Application qui doit se trouver dans les équipements connecté à l'internet.	**1123**
Internet Protocol (IP)	Définition du protocole IP	**791**
Internet Control Message Protocol (ICMP)	Définition du protocole ICMP	**792**
User Datagram Protocol (UDP)	Définition du protocole UDP	**768**
Transmission Control Protocol (TCP)	Définition du protocole TCP	**793**
Telnet Protocol	Définition des messages échangés par les applications	**854,855**

	telnet (terminal virtuel)	
File Transfer Protocol (FTP)	Définition des messages échangés par les applications ftp (transfert de fichiers)	**959**
Simple Mail Transfer Protocol (SMTP)	Définition des messages échangés par les applications de courrier électronique.	**821**
Domain Name System (DNS)	Définition des messages échangés par les serveurs de nom (correspondance entre le nom d'un équipement et une adresse IP).	**13**
Routing Information Protocol (RIP)	Définition du protocole de routage	**1058**
Point-to-Point Protocol (PPP)	Définition de la mise en place de IP au-dessus d'une liaison série en utilisation le protocole PPP.	**1661**
PPP in HDLC Framing	Idem	**1662**
Address Resolution Protocol (ARP)	Définition d'un protocole de résolution d'adresse permettant de mettre en correspondance une adresse IP de niveau 3 et une adresse Ethernet de niveau 2	**826**
Reverse Address Resolution Protocol (RARP)	Définition d'un protocole de résolution d'adresse permettant de mettre en correspondance une adresse Ethernet une adresse IP.	**903**

4.4. ADRESSAGE IP AVEC IP VERSION 6.0

Les ID de réseaux disponibles dans IPv4 sont de plus en plus rares. Une nouvelle version a donc été mise au point **IPv6**.

IPv6 utilise **16 octets**. Il comporte 8 paires d'octets séparées par des virgules. Les octets sont représentés en notation hexadécimale. IPv6 est une nouvelle structure de paquets incompatible avec les systèmes IPv4, mais offrant plusieurs avantages tels qu'un espace d'adressage étendu, un format d'en-tête simplifié, la prise en charge d'un trafic dépendant du temps, ainsi que la possibilité d'ajouter de nouvelles fonctionnalités.

- ⇨ L'espace d'adressage étendu constitue l'une des principales caractéristiques d'IPv6. IPv6 utilise des adresses source et de destination à 128 bits (4 fois plus grandes qu'avec IPv4). Exemple d'adresse IP valide avec IPv6 : **4A3F :AE67 :F240 :56C4 :3409 :AE52 :440F :1403**

- ⇨ Les en-têtes IPv6 sont conçus pour minimiser le traitement de l'en-tête IP en déplaçant les champs non essentiels et les champs d'option dans des en-têtes d'extension placés après l'en-tête IP.

- ⇨ Un nouveau champ dans l'en-tête IPv6 permet la pré-allocation de ressources réseau sur le chemin afin que les services à dépendance temporelle tels que les services vocaux et vidéo bénéficient d'une bande passante garantie avec des retards fixes.

- ⇨ IPv6 peut facilement être étendu pour incorporer de nouvelles fonctionnalités par l'ajout d'en-têtes d'extension après l'en-tête IPv6 de base. La prise en charge de nouveaux matériels ou de nouvelles technologies d'application est ainsi incorporée.

- ⇨ IPv6 est défini dans le **RFC 1883**.