# Couche réseau

## Définition

La couche réseau construit une voie de communication de bout à bout à partir de voies de communication avec ses voisins directs. Ses apports fonctionnels principaux sont donc …

* le **routage**  
  Détermination d'un chemin permettant de relier les 2 hôtes distants ;
* le **relayage**  
  Retransmission d'un PDU (*Protocol Data Unit* ou Unité de données de protocole) dont la destination n'est pas locale pour le rapprocher de sa destination finale.

Cette couche est donc la seule à être directement concernée par la topologie du réseau.   
C'est aussi la dernière couche supportée par tous les hôtes du réseau pour le transport des données utilisateur : les couches supérieures sont réalisées uniquement dans les machines d'extrémité.

Le PDU de cette couche est souvent appelé paquet. La fonction de relayage (terme OSI) est parfois appelée acheminement.

**Remarques** …  
Cette couche est la plus caractéristique d'une architecture réseau.   
C'est pourquoi l'architecture prend souvent le nom du protocole principal de niveau réseau.

Déterminer un chemin est une tâche complexe normalement réalisée dans les grands réseaux par des protocoles dédiés dont le rôle est de découvrir la topologie du réseau et d'en tirer la meilleure route. Les protocoles de routage se différencient par les critères de choix des routes et la précision de la topologie découverte. En dehors du cas des petits réseaux, le routage est hiérarchique : la précision de la connaissance de l'environnement d'un routeur décroît avec la distance.

Si les routeurs n'ont pas de couche supérieure à la couche réseau du point de vue des hôtes utilisateurs du réseau, ils peuvent supporter des protocoles de niveau transport et au-dessus pour la gestion du réseau (supervision et exécution des protocoles de routage par exemple).   
Bien que les données calculées par les protocoles de routage soient utilisées par la couche réseau, ce ne sont pas des protocoles de niveau réseau car ils ne servent pas à transporter les données des hôtes utilisateurs du réseau. D'ailleurs, dans le monde IP, les protocoles de routage non local (i.e. hors RIP) sont transportés par TCP.

Voici les principaux protocoles de la couche Réseau …

* **Protocoles IP** (v4 et v6) ;
* **Protocole ARP** ;
* **Protocole ICMP** ;
* **Protocole IGMP**.

### Mode de transmission du protocole Internet

* **Diffusion dirigée (*Unicast*)**   
  Adresse MAC -- 0A:00:81:2F:42:51  
  Adresse désignant une seule interface ;
* **Multi diffusion (Multicast)**   
  Adresse MAC -- 01:XX:XX:XX:XX:XX (premier octet impair)  
  Adresse désignant plusieurs stations (groupe de diffusion) ;
* **Adresse de diffusion globale (Broadcast address)**  
  Adresse MAC -- FF:FF:FF:FF:FF:FF  
  Adresse de diffusion qui désigne l’ensemble des stations du domaine de collision.concerné

|  |  |  |
| --- | --- | --- |
| Une image contenant flou  Description générée automatiquement | Une image contenant jouet, poupée, graphiques vectoriels  Description générée automatiquement | Une image contenant graphiques vectoriels  Description générée automatiquement |
| Monodiffusion (**unicast**) | Multidiffusion (*multicast*) | Diffusion générale (*broadcast*) |

## Le protocole IP (v4 et v6)

Les protocoles TCP/IP se situent dans un modèle souvent nommé famille de protocoles TCP/IP.  
Les protocoles TCP et IP ne sont que deux des membres de la suite de protocoles IP.

Le protovole IP (*Internet Protocol*) est un protocole qui se charge de l'acheminement des paquets pour tous les autres protocoles de la famille TCP/IP. Il fournit un système de remise de données optimisé sans connexion. Le terme optimisé souligne le fait qu'il ne garantit pas que les paquets transportés parviennent à leur destination, ni qu'ils soient reçus dans leur ordre d'envoi. La fonctionnalité de somme de contrôle du protocole ne confirme que l'intégrité de l'entête IP. Ainsi, seuls les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP (et de leur ordre de réception).

Le protocole IP travaille en mode non connecté, c'est-à-dire que les paquets émis par le niveau 3 sont acheminés de manière autonome (datagrammes), sans garantie de livraison.

**Principes guidant IP**

Dès l’origine deux principes de base ont guidés les concepteurs d’Internet pour la création du protocole de transport (en occurrence IP). Ces deux principes sont les suivants …

* La **communication de bout en bout**  
  Une communication se fait entre deux partenaires et ce sont ces derniers qui en gèrent les modalités. On sait que la commutation des paquets implique la présence de plusieurs intervenants intermédiaires (souvent désignés comme aiguilleurs dans le langage Internet) et que ces intermédiaires sont transparents et ne participent pas dans la communication (en fait ils ne sont que des relais).  
  Les nœuds d’extrémités sont considérés comme intelligents, permettant ainsi le déploiement d’applications client/serveur à l'aide du réseau.
* La **livraison au meilleur effort**Ce principe implique que tous les éléments intermédiaires (aiguilleurs) de la connexion n’offre aucune garantie quant au transport des paquets entre les nœuds d’extrémités. Ils « font de leur mieux » pour rendre les paquets à destination. IP n’est donc pas selon ce principe un protocole fiable. Toutefois, on le considère comme étant robuste. Agissant ainsi le protocole n’utilise pas de ressources supplémentaires aux intermédiaires pour fournir une qualité de service à priori.   
  Seulement les nœuds d’extrémités vont utiliser un protocole de la couche Transport du modèle OSI pour garantir cette livraison (ce qui n’est pas le cas des nœuds intermédiaires).  
  C’est pourquoi le protocole TCP est implicitement lié au protocole IP.

**Configuration IP**Toute configuration IP doit comporter les données suivantes …

* l’**adresse IP**   
  (unique à l’hôte) ;
* le **masque de sous-réseau** ;
* l’**adresse** **de la passerelle par défaut**   
  (un aiguilleur est traditionnellement appelé ainsi pour le réseau Internet).  
  La passerelle est la porte d’entrée sur le réseau Internet ;
* l’**adresse** **d’un serveur DNS**  
  Le serveur DNS est l’intermédiaire qui résout un nom convivial comme www.profsavard.info en une adresse valide de destination comme 206.167.36.22.

Toute configuration IP valide doit obligatoirement comporter les deux premiers éléments.   
Sans ces informations il sera impossible pour un hôte de communiquer avec un hôte distant (qu’il soit dans son propre réseau ou sur le réseau Internet).   
Quant au troisième il est essentiel si un hôte veut communiquer avec un hôte distant hors de son propre réseau local.   
Enfin, sans le quatrième élément, l’utilisateur devra toujours connaître l’adresse exacte pour rejoindre un hôte en dehors de son réseau local.

**Adresses IPv4**

Pour pouvoir établir une communication avec un autre hôte branché au réseau Internet une machine (ou nœud) doit obligatoirement posséder une adresse IP unique.

Cette adresse peut être caractérisée comme étant statique ou dynamique.

* Une **adresse statique est généralement attribuée manuellement** par un administrateur réseau.   
  Certains nœuds du réseau Internet nécessitent une adresse qui ne sera pas modifiée (ce qui est le cas de la plupart des serveurs).
* Une **adresse dynamique est une adresse qui sera attribuée de manière automatique** lors de l’ouverture d’un hôte.   
  Cette adresse est généralement attribuée par un serveur DHCP[[1]](#footnote-2).

Plusieurs avantages liés à la présence d’un serveur DHCP …

* **Attribution automatique de la configuration IP** à un hôte;
* **Résolution du problème d’un réseau** qui possède plus d’hôtes que d’adresses disponibles.

**Anatomie d’une adresse IPv4**Une adresse IP se divise en deux parties …

* La **première représente la partie réseau**.   
  Il est important de préciser ici qu’un réseau est un regroupement logique de plusieurs hôtes.   
  Cette partie réseau est attribuée par un responsable fournisseur et est unique pour le réseau Internet
* La **seconde partie d’une adresse IPv4 est l’identifiant unique** pour un hôte de ce réseau.   
  Cette partie est gérée localement par les responsables du réseau interne. C’est cette partie qui est attribuée dynamiquement ou statiquement[[2]](#footnote-3).  
  Cette partie identifiant doit être obligatoirement unique au réseau interne.

Une adresse IP peut être publique ou privée …

* Une **adresse publique est une adresse que doit posséder tout hôte qui veut établir une communication sur le réseau Internet**.   
  Ceci permet d’établir une session sans intermédiaire interne (comme un serveur proxy).
* Une **adresse privée est une adresse qui permet aux hôtes d’un même réseau de communiquer entre eux sans toutefois pouvoir ouvrir une session avec un hôte sur le réseau Internet**.   
  Par défaut, les aiguilleurs (la porte de sortie sur le réseau Internet) sont configurés pour ne pas laisser passer les paquets provenant d’un hôte possédant une adresse privée.  
  Le protocole NAT[[3]](#footnote-4) permet de faire le lien entre un hôte possédant une adresse privée et un serveur proxy possédant une adresse publique. Ce serveur proxy devient à la fois traducteur entre adresses privées et adresses publiques et aiguilleur.

**Méthode d’attribution des identificateurs IPv4**

* **Prévoir l’avenir**Tenir compte de la croissance future du réseau   
  (surtout dans la planification des sous-réseaux)
* **Assurer l’unicité**Bien identifier les sous-réseaux
* **Éviter les adresses à accès limité**  
  Adresses de réseau, diffusion, bouclage, …

Une adresse IPv4 est composée de 32 bits dont une partie sert à identifier le réseau et une partie pour identifier les hôtes composant ce réseau.

|  |  |
| --- | --- |
| Identifiant réseau | Identifiant hôte |
| ç 32 bits è | |

La partie de ces 32 bits attribuée à chacune des parties varie selon la classe.

**Adressage IPv4**

|  |
| --- |
| **Classe A 0RRR RRRR HHHH HHHH HHHH HHHH HHHH HHHH\*** |
| * 7 bits pour l'identification réseau ou 27 è128 réseaux |
| * **Réseaux possibles**: **1**.0.0.0 à **126**.0.0.0 donc 126 réseaux **Exclusions**:  les réseaux 0.0.0.0 (utilisé dans les tables d’aiguillage) et 127.0.0.0 (réservé pour l’adresse de bouclage) **Adresses privées**:  le réseau 10.0.0.0 |
| * 24 bits disponibles pour l'hôte ou 224 è16 777 216 - 2 (numéro de réseau et adresse de diffusion générale) |

|  |
| --- |
| **Classe B** **10RR RRRR RRRR RRRR HHHH HHHH HHHH HHHH\*** |
| * 14 bits pour identifier les réseaux ou 214 è16 384 réseaux |
| * **Réseaux possibles**: 128.0.0.0 à 191.255.0.0 **Adresses privées**:  le réseau 172.16.0.0 |
| * 16 bits disponibles pour l'hôte ou 216 è 65 536 - 2 (numéro de réseau et adresse de diffusion générale) |

|  |
| --- |
| **Classe C** **110R RRRR RRRR RRRR RRRR RRRR HHHH HHHH\*** |
| * 21 bits pour identifier les réseaux ou 221 è 2 097 152 réseaux possibles |
| * **Réseaux possibles**: 192.0.0.0 à 223.255.255.0 **Adresses privées**:  les réseaux 192.168.0.0 à 192.168.255.0 |
| * 8 bits disponibles pour l'hôte ou 28 è 256 - 2 (numéro de réseau et adresse de diffusion générale) |
| **Classe D 1110 RRRR RRRR RRRR RRRR RRRR HHHH HHHH\*** |
| * **Adresses possibles:** 224.0.0.0 à 239.255.255.255 |

|  |
| --- |
| **Classe E**  **1111 0RRR RRRR RRRR RRRR RRRR HHHH HHHH\*** |
| * Adresses possibles: 240.0.0.0 et plus |

**\*** **R** = bits pour l’identification du réseau et **H** = bits pour l’identification de l’hôte.

## Masque de sous-réseau (IPv4)

Le masque de sous réseau est un élément essentiel à toute configuration IP. Il complète et caractérise l’adresse IP.

### Fonctions

Les deux fonctions du masque de sous-réseau sont les suivantes ...

**Première fonction**  
Déterminer si un hôte distant est un hôtes attaché à son réseau local ou encore est un hôte extérieur, connecté sur Internet.  
C’est donc un élément essentiel.  
Pour déterminer si l’hôte à rejoindre est interne ou externe à son réseau, il y a comparaison binaire (AND) entre son adresse et son masque de sous-réseau et l’adresse distante et son propre masque de sous-réseau.

* Le résultat de cette comparaison peut-être de deux ordres:  
  **Identique**  
  Cela signifie que l’hôte à rejoindre est sur son propre réseau, et peut alors directement communiquer avec ce dernier.  
  **Différent**  
  Il doit alors acheminer le ou les paquets à sa passerelle par défaut, qui alors, à l’aide de sa table d’aiguillage, fera suivre les données jusqu’au destinataire final.

**Seconde fonction**  
Permettre à l’administrateur local de séparer un réseau en sous-entités. Cette option permet de gérer plus facilement des grands réseaux.  
Il permet également aux distributeurs d’adresses Internet de récupérer (à l’aide de CIDR) des réseaux entiers déjà attribué afin de les attribuer de nouveau à d’autre réseaux.

**Avantages**  
Les avantages d’utiliser des sous-réseaux sont les suivants ...

* Utilisation optimisée de l’espace d’adressage.
* Administration simplifiée:  
  Permet d’administrer les sous-réseaux de manière indépendante et efficace.   
  Permet de gérer plus efficacement des parties du réseau qui ont des exigences contradictoires.
* Possibilité de structurer un réseau interne sans affecter les réseaux externes.  
  Seul l’aiguilleur du réseau destination doit connaître la présence des sous-réseaux.
* Sécurité améliorée.  
  La structure du sous-réseau est invisible à l’externe donc la sécurité est améliorée indirectement.

### Internet Protocol version 6 (IPv6)

Au début des années 90, l’évolution du réseau Internet semblait compromise à court terme car le protocole IP (Internet Protocol) limitait le nombre d’équipements qui pouvaient s’y connecter.

À sa création, ce réseau ne devait servir qu’à relier une centaine de machines mais de nombreuses catégories d’utilisateur sont très vite venues s’y joindre. On y trouvait les scientifiques, les universitaires, puis en 1992, le réseau fut ouvert aux activités commerciales ainsi qu’aux particuliers. Depuis, le nombre d’équipements connectés ne cesse d’augmenter et on approche de la saturation du réseau.

Les chercheurs ont repoussé cette saturation afin de développer une nouvelle version du protocole IP qui sera nommé IPv6. IPv6 prend en compte les avancées issues des recherches sur les réseaux menées depuis 25 ans.

Elle porte notamment sur …

* l’**auto configuration** ;
* la **mobilité** ;
* la **diffusion multipoints**  
  et
* la **sécurité**.

IPv6 est le protocole de la prochaine génération d'Internet et c'est pour cela qu'on l'appelle aussi IPng, initiales de ***Internet Protocol Next Generation***.  
On s'attend à ce que IPv6 remplace graduellement IPv4, avec une période de transition de plusieurs années de coexistence.

**Avantages d’IPv6**

* **Échelonnement**  
  IPv6 possède des adresses de 128 bits face aux adresses de 32 bits de Ipv4. Par conséquent, le nombre d'adresses IP disponibles est multiplié par   
  7,9 \* 1028
* **Sécurité**  
  IPv6 assure la sécurité dans ses spécifications en utilisant le cryptage de l'information et l'authentification de l'expéditeur de ladite information.
* **Applications en temps réel**Afin d'offrir un meilleur support pour le trafic en temps réel (par exemple, vidéoconférence), IPv6 comprend l'étiquetage de flux dans ses spécifications. Avec ce système, les aiguilleurs peuvent reconnaître à quel flux d'un extrême à l'autre appartiennent les paquets qui se transmettent.
* **Plug and Play**  
  IPv6 comprend dans sa forme standard un mécanisme plug and play, ce qui facilite aux utilisateurs la connexion de leurs équipements au réseau.   
  La configuration se réalisera automatiquement.
* **Spécifications plus claires et optimisées**IPv6 suivra les bonnes pratiques de IPv4 et éliminera les caractéristiques non utilisées ou obsolètes de IPv4, ce qui permettra d'optimiser le protocole d'Internet.   
  L'idée est de conserver l'aspect positif et d'éliminer les inconvénients du protocole actuel.

Les travaux de recherche sont à ce jour terminés et de nombreuses implantations sont disponibles aussi bien pour les équipements d’interconnections que les ordinateurs.

**Nombre d'adresses IPv6 disponibles**

Le nombre d'adresses IP disponibles en IPv6 est égal au plus grand numéro qui puisse être représenté avec 128 bits, c'est-à-dire …  
2128 = 3.4 \* 1038

**Adressage IPv6**

La taille d'une adresse IPv6 est de 16 octets (128 bits). Cette taille, suffisamment importante, permet d'établir un plan d'adressage hiérarchisé en trois niveaux.

* **Topologie publique utilisant 48 bits** ;
* **Topologie de site sur 16 bits** ;
* **Topologie d'interface sur 64 bits**.

Une adresse IPv6 est donc longue de 128 bits, soit 16 octets, contre 32 bits pour IPv4.   
La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une **écriture hexadécimale**, où les **8 groupes de 2 octets (16 bits par groupe)** sont séparés par un signe deux-points …  
**2001:0db8:0000:85a3:0000:0000:ac1f:8001  
2A01:E35:2421:4BE0:CDBC:C04E:A7AB:ECF3**

Il est permis d'**omettre de 1 à 3 chiffres zéros non significatifs dans chaque groupe** de 4 chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à:  
2001:db8:0:85a3:0:0:ac1f:8001

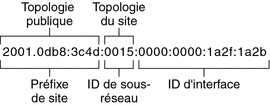
De plus, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux-points (::)19. Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en:  
2001:db8:0:85a3::ac1f:8001

|  |  |
| --- | --- |
| Préfixe | Description |
| ::/8 | Adresses réservées |
| 2000::/3 | Adresses unicast routables sur Internet |
| fc00::/7 | Adresses locales uniques |
| fe80::/10 | Adresses locales lien (auto-configuration) |
| ff00::/8 | Adresses multicast |
| ::1/128 | **A**dresse de bouclage (semblable à 127.0.0.1 en IPv4) |
| 0:0:0:0:0:0:0:0 ou encore notée :: | Adresse utilisée pendant l'initialisation de l'adresse IPv6 d'une machine. Cela est une phase transitoire |

**Attribution des adresses IP**

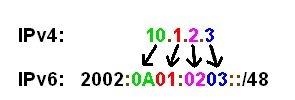
L'utilisation de préfixes séparés pour les adresses affectées à un fournisseur et les adresses affectées à une zone géographique constitue un compromis entre deux différentes visions du futur réseau Internet. Chacun de ces fournisseurs dispose d'une fraction réservée de l'espace d'adressage (adresses unicast = 1/8 de cet espace). Les 5 premiers bits qui suivent le préfixe 0010 (2000::/3) sont utilisés pour indiquer dans quel " registre " se trouve le fournisseur d'accès. Actuellement, trois registres sont opérationnels, pour l'Amérique du nord, l'Europe et l'Asie. Jusqu'à 29 nouveaux registres pourront être ajoutés ultérieurement.

Chaque registre est libre de diviser les 15 octets restants comme il l'entend. Une autre possibilité est d'utiliser un octet pour indiquer la nationalité du fournisseur et de laisser toute liberté aux octets suivant pour définir une structure d'adresses spécifique.



Insertion d’une Adresse IPv4 dans une adresse IPv6

Il est possible d’encapsuler une adresse IPv4 dans un réseau IPv6.  
Elle prend la forme suivante …



## Protocole ICMP

ICMP (*Internet Control Messaging Protocol*) est le protocole de gestion de la suite TCP/IP, qui est requis dans chaque mise en œuvre TCP/IP et autorise deux nœuds d'un réseau IP à partager des informations d'erreur ainsi que l'état IP.   
ICMP est utilisé par l'utilitaire *ping* pour déterminer l'accessibilité d'un système distant

Avec ICMP, les hôtes et les aiguilleurs (*routers*) qui utilisent la communication IP peuvent faire état des erreurs et échanger des informations sur le contrôle limité et sur l'état.

Les messages ICMP sont généralement envoyés automatiquement dans l'un des cas suivants ...

* Un p**aquet (datagramme) IP ne peut pas atteindre sa destination** ;
* Un **aiguilleur IP (passerelle) ne peut pas transmettre les paquet**s et donne des informations sur l'état de la transmission ;
* Un **aiguilleur IP redirige l'hôte d'envoi pour utiliser un meilleur itinéraire** vers la destination.

### Messages ICMP

Différents types de messages ICMP sont identifiés dans l'en-tête ICMP.   
Les messages ICMP étant traités dans des paquets IP, ils ne sont pas fiables.

|  |  |  |
| --- | --- | --- |
| **Message ICMP** | **Description** | |
| **Requête d'écho** (*Echo request*) | | Détermine si un nœud IP (un hôte ou un aiguilleur) est disponible sur le réseau. |
| **Réponse d'éch**o (*Echo reply*) | | Répond à une requête d'écho ICMP. |
| **Destination inaccessible** (*Destination unreachable*) | | Informe l'hôte qu'un paquet ne peut pas être livré. |
| **Extension de source** (*Source quench*) | | Informe l'hôte pour réduire la vitesse à laquelle il envoie les paquets à cause de la congestion. |
| Redirection (*Redirect*) | | Informe l'hôte d'un itinéraire préféré. |
| **Dépassement de la temporisation** (*Time* *exceeded*) | | Indique que la durée de vie TTL (Time-to-Live) d'un paquet IP a été dépassée. |

## Multidiffusion

En informatique, le terme multi-diffusion (*multicast*) définit une connexion réseau multipoint.

### Définition

On entend par multi-diffusion le fait de communiquer simultanément avec un groupe d'ordinateurs identifiés par une adresse spécifique (adresse de groupe).

### Avantages

L'avantage de ce système par rapport à la classique monodiffusion (*unicast*) devient évident quand on veut diffuser de la vidéo. En streaming on envoie une image autant de fois que l'on a de connexions simultanées. Comme résultat ... moins de perte de temps, de ressources du serveur et surtout de bande passante.

En multidiffusion le paquet n'est émis qu'une seule fois et sera aiguillé (routé) vers tous les hôtes du groupe de diffusion.

### Protocoles

En multidiffusion, le protocole IP utilise les adresses de la classe d'adresses D (224.0.0.1 à 239.255.255.254).   
Les adresses IP de multidiffusion 224.0.0.1 à 224.0.0.255 ont un rôle spécifique à utilisation locale.

Les paquets de données sont aiguillés sur le réseau selon l'adresse des destinataires encapsulée dans la trame transmise. Normalement, seuls les destinataires interceptent et décodent les paquets qui leurs sont adressés.

Exemple d'une adresse IP locale pouvant servir à une communication de multidiffusion …  
224.0.0.1 ;   
Exemple d'une adresse IP Internet pouvant servir à une communication de multidiffusion …  
239.254.254.254.

Un groupe de multidiffusion se compose d'un ensemble d’hôtes. Il est entièrement dynamique (un hôte peut rejoindre ou quitter le groupe à tout moment) et ouvert (une station peut émettre un paquet dans un groupe sans en faire partie).

Un groupe de multidiffusion est désigné par une adresse IP (de 224.0.0.1 à 239.255.255.255).   
Lorsqu'un hôte veut envoyer un paquet à un groupe multidiffusion, il envoie ce paquet à l'adresse IP identifiant ce groupe (par ex : 224.1.2.3). La réception est réalisée par un aiguilleur abonné au groupe et le paquet est alors dupliqué et renvoyé grâce à une trame de niveau 2 Multicast.

Le protocole IGMP est utilisé par le protocole IP pour l'adhésion aux groupes de multidiffusion.

### Utilisation

L'usage de la multidiffusion sur Internet est encore limité aux universités ou utilisé en interne par les fournisseurs d'accès Internet (diffusion des chaînes de télévision pour certains).  
Certaines radio web expérimentent un flux de multidiffusion pour la diffusion de leurs programmes.

## Protocole IGMP

IGMP (*Internet Group Management Protocol*) est historiquement défini dans l'Annexe I de la RFC 1112.   
Sa raison d'être est que les datagrammes ayant une adresse de multidiffusion sont à destination d'un groupe d'utilisateurs dont l'émetteur ne connait ni le nombre ni l'emplacement. L'usage de la multidiffusion étant par définition dédié aux applications comme la radio ou la vidéo sur le réseau Internet, donc consommatrices de bande passante, il est primordial que les aiguilleurs (*routers*) poss<edent un moyen de savoir s'il y a des utilisateurs de tel ou tel groupe sur les réseaux locaux directement accessibles pour ne pas encombrer la bande passante associée avec des flux d'octets que personne n'utilise plus.

|  |  |
| --- | --- |
| **Document distribué sous licence** |  |

1. DHCP (*Dynamic Hosts Configuration Protocol*) est un protocole de la couche Applications. [↑](#footnote-ref-2)
2. Deux fournisseurs pour l’attribution des adresses réseau IPv4 ..  
    ICANN ou *Internet Corporation for Assigned Names and Numbers* et  
    RIR ou *Regional Internet Registries*. [↑](#footnote-ref-3)
3. NAT ou *Network Address Translation* [↑](#footnote-ref-4)