CHAPITRE 5

Couche Réseau

5.1 Introduction

La fonction de base assurée par la couche réseau est le routage des données (qui s'appellent à ce niveau paquets ou datagrammes) entre équipements distants.

Afin de garantir un routage efficace des paquets, cette couche veille à l'établissement des meilleurs chemins entre les équipements communicants. Et ce en se basant sur des standards déterminant les mécanismes d'acheminement, de contrôle de congestion, de structuration d'adresse et de structuration des paquets, etc.

IP, ou Internet Protocole, est le principal protocole utilisé à ce niveau et il est la base d'autres protocoles de la couche supérieure notamment, TCP et UDP. C'est un protocole sans connexion ce qui veut dire qu'aucune connexion n'est établie entre les équipements communicants avant l'échange des données. Ces dernières sont divisées en datagrammes, gérées indépendamment et routées d'une manière indépendante à leur destination.

5.2 Interconnexion des réseaux et routage

L'interconnexion des réseaux est une technique essentielle permettant à deux ou plusieurs réseaux informatiques de communiquer entre eux. Cela permet aux utilisateurs d'un réseau d'accéder aux ressources d'un autre réseau distant, comme des fichiers, des applications ...

Il existe plusieurs façons permettant d'interconnecter des réseaux :

1. **Répéteur et concentrateur** : Est un équipements d'interconnexion de niveau 1 qui reçoit un signal et le retransmet. Il est souvent utilisé dans les systèmes de télécommunication pour étendre la portée d'un signal.

2. **Pont (en anglais, Bridge)** : Est un dispositif matériel de niveau 2 permettant de relier deux réseaux informatiques. Il fonctionne en analysant les adresses MAC des paquets de données et en les transmettant au réseau approprié.

3. **Commutateur (Switch)** Est un équipements d'interconnexion de niveau 2 permettant de relier plusieurs réseaux informatiques. Il fonctionne de la même façon que le pont et utilisent tous les deux (pont et commutateur) des tables de commutation.

4. **Routeur** Est un équipement d'interconnexion de niveau 3 permettant de relier des ordinateurs situés sur des réseaux différents. Il fonctionne en analysant les adresses IP des paquets de données pour déterminer le chemin à emprunter pour acheminer le paquet.

5.2.1 Réseau physique et logique

Un réseau informatique peut être divisé en deux catégories principales : Réseau physique et Réseau logique :

5.2.1.1 Réseau physique

Constitue la partie visible et tangible d'un réseau. Il comprend l'ensemble des équipements permettent aux appareils de se connecter physiquement, à savoir, les câbles, les commutateurs, les routeurs, etc.

5.2.1.2 Réseau logique

Le réseau logique est la partie invisible et abstraite d'un réseau. Il est défini par les règles et les protocoles qui permettent aux appareils de communiquer entre eux.

Dans un réseau physique, et afin d'acheminer les trames de données entre les machines connectées, les équipements d'interconnexion se basent sur l'adresse Mac de destination. Cependant, cette opération est inappropriée, pour un réseau vaste (tel que Internet) car :

- Les adresses Mac sont affectées par le constructeur et ne dépendent pas de la structure de réseaux.
- Elles ne permettent pas de regrouper des machines dans un réseau identifiable, ni y localiser un équipement.

Une solution alternative a été mise en œuvre pour faire face à ce problème. Elle consiste à utiliser des adresses de niveau supérieur (des adresses logiques IP) permettant de créer un réseau logique (réseau IP) au-dessus d'un ou d'un ensemble de réseaux physiques. Ainsi, et pour des raisons d'optimisation à titre d'exemple, nous pouvons découper un vaste réseau en un ensemble de sous-réseaux indépendants, chacun avec son propre ensemble de règles et de protocoles.

5.3 Adressage IP

L'adressage IP est le type d'adressage utilisé dans Internet. Il est conçu pour être Hiérarchiques, et il permet d'identifier les machines et ainsi que le réseau auquel elles appartiennent.

Une adresse IP est décomposée en deux parties : **l'identificateur du réseau**, où se trouve l'équipement, et **l'identificateur de la machine** elle-même.

Chaque équipement dans un réseau (machine ou routeur) doit avoir une adresse IP unique et propre à lui. Nous distinguons deux formes d'adressage IP : L'adressage IPV4 et IPV6.

5.3.1 Adressage IPV4

Une adresse IPV4 tient sur 32 bits soit 4 octets. Elle est souvent écrite en notation décimale pointée : les octets sont séparés par des points, et chaque octet est représenté par un nombre décimal compris entre 0 et 255. 124.22.40.1 est un exemple d'une adresse IPV4.

5.3.1.1 Les classes d'adresses

Les classes d'adresses IP sont un système de classification des adresses IP qui a été initialement développé pour optimiser le routage des paquets sur Internet. Ce système est basé sur la répartition des adresses IP en cinq classes. Une brève comparaison entre les différentes classes d'adresses est présentée dans le tableau suivant :

Classe	Nombre d'hôtes pouvant être connectés	Exemple d'utilisation
Classe A	- le premier octet de l'adresse IP est réservé à l'identification du réseau (Le premier bit du poids fort est toujours à 0, les 7 bits suivants servent à l'identification du n° de réseau) - les trois octets suivants étant réservés à l'identification des hôtes.	Cette classe est destinée aux grands réseaux, tels que les réseaux d'entreprise ou gouvernementaux.
Classe B	- les deux premiers octets de l'adresse IP sont réservés à l'identification du réseau (les deux premiers bits du poids fort prennent toujours les valeurs 10, les 14 bits suivants servent à l'identification du n° de réseau) - les deux octets suivants étant réservés à l'identification des hôtes.	destinée aux réseaux de taille moyenne, tels que les réseaux d'universités ou d'entreprises.
Classe C	- les trois premiers octets sont réservés à l'identification du réseau (les trois premier bits de poids fort prennent les valeurs 110, les 21 bits suivants servent à l'identification du n° de réseau) - le dernier octet étant réservé à l'identification des hôtes.	destinée aux réseaux de petite taille, tels que les réseaux domestiques ou de bureau.
Classe D	les quatre derniers octets de l'adresse IP sont réservés aux adresses de diffusion multicast.	Ces adresses sont utilisées pour envoyer des messages à un ensemble de destinataires.
Classe E		cette classe est réservée à des utilisations futures.

Remarque: Le système d'adressage par classes d'adresses IP est obsolète depuis l'apparition de l'adressage IPv6.

Le nombre d'hôtes pouvant être connectés à un réseau est calculé en se basant sur la formule suivante : $nombred'htes = 2^{Nombredebitsidentifiantslapartiehotedelaclasse} - 2$.

Les deux adresses à enlever représentent l'adresse de broadcast et l'adresse du réseau (voir sous-réseau).

Par conséquent, pour chaque classe d'adresse nous pouvons trouver :

- Classe A : le nombre d'hôtes pouvant être connectés à un réseau de classe A est de $2^{24} - 2$, soit 16777214.
- Classe B : le nombre d'hôtes pouvant être connectés à un réseau de classe B est de $2^{16} - 2$, soit 65534.
- Classe C : le nombre d'hôtes pouvant être connectés à un réseau de classe C est de $2^{8} - 2$, soit 254.

Quelques exemples d'adresses IP pour les différentes classes :

Classe A : 10.0.0.1 Classe B : 172.16.0.1 Classe C : 192.168.0.1 Classe D : 224.0.0.1 Classe E : 255.255.255.255

5.3.1.2 Adresses particulaires

Un ensemble d'adresses particulières sont énumérées dans la suite :

- **Adresse réseau :** Chaque réseau possède une adresse obtenue en remplaçant le champ (bits) Identifiant de machine par "0". Selon la classe d'adresse :

  - La machine 62.166.13.21 appartient au réseau 62.0.0.0 (classe A). Les trois octets (24 bits) représentant la partie hôte sont mis à 0.

  - La machine 144.16.130.27 appartient au réseau 144.16.0.0 (classe B). Les deux octets (16 bits) représentant la partie hôte sont mis à 0.

  - La machine 195.11.13.7 appartient au réseau 195.11.13.0 (classe C). Le dernier octet (8 bits) représentant la partie hôte est mis à 0.

- **Adresse de diffusion (broadcast address) :** Cette adresse est obtenue en remplaçant le champ (bits) Identifiant de machine par "1". Le paquet, dont le champ Identifiant machine d'une adresse d'un réseau distant est en plein 1, sera reçu par toutes machines appartenant à ce réseau. Par exemple :

  - L'adresse de diffusion du réseau 195.11.13.0 est 195.11.13.255 (classe C).

- **Adresse de boucle locale (loopback address) :** L'adresse de loopback (127.0.0.1) est une adresse réservée pour les tests locaux. Autrement dit, tout message envoyé à cette adresse ne circule jamais dans le réseau, cependant, il revient directement à son expéditeur.

- **Adresses privées :** Les adresses privées sont des adresses IP qui ne sont pas routables sur Internet. Elles sont utilisées pour les réseaux locaux, tels que les réseaux domestiques ou de bureau. Les adresses privées sont définies, conformément aux différentes classes, dans les plages suivantes :

  Classe A : 10.0.0.0/8 Jusqu'à 10.255.255.255/8
  Classe B : 172.16.0.0/12 Jusqu'à 172.31.255.255/12
  Classe C : 192.168.0.0/16 Jusqu'à 192.168.255.255/16

  Pour rendre les adresses privées accessibles par Internet, nous devons évoquer le service de conversion d'adresse assuré par les routeurs. Ce mécanisme est le NAT (Network Address Translation), permet de correspondre une adresse privée avec une adresse IP public, unique et routable sur Internet.

5.3.1.3 Notions de masque

Une adresse IP est généralement divisée en deux parties : La partie réseau et la partie hôte. Afin d'identifier l'une de l'autre nous utilisons ce qu'on appelle Masque réseau (ou sous-réseau). La figure 5.1 illustre la structure d'un Masque de réseau.

Comme illustré dans la figure, les bits en plein "1" du masque représentent la partie réseau, tandis que, les bits à "0" correspondent à la partie station (ou hôte). C'est à travers le masque du réseau (sous-réseau) qu'une machine peut savoir et vérifier son appartenance dans la hiérarchie d'adresses.

Dans le plan d'adressage par classes d'adresses (A, B et C), présenté au-dessus, on parle du **"masque par défaut"**.

Parfois l'identifiant réseau est étendu pour occuper d'autres bits de la partie ID-machine. Ces bits supplémentaires doivent être indiqués dans le nouveau Masque, et on ne parle plus dans ce cas de masque par défaut.

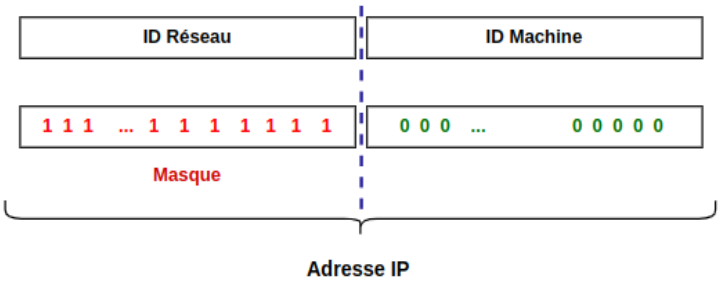


Fig. 5.1 Structure du masque sous-réseau

5.3.1.4 Notions de sous-réseaux (subnet)

Pour des raisons de structuration, amélioration des performances du réseau et de préservation d'adresses IP, nous pouvons diviser un réseau identifié par son adresse IP (adresse principale ou racine) en un ensemble de sous réseaux possédant chacun sa propre adresse IP dérivée de celle dite adresse racine.

Les adresses des sous-réseaux créées sont obtenues en exploitant le champ Identifiant de machine de l'adresse IP. Ce dernier se décompose désormais en **un identifiant de sous-réseau** et un **identifiant de machine** comme illustré dans la figure 5.2.

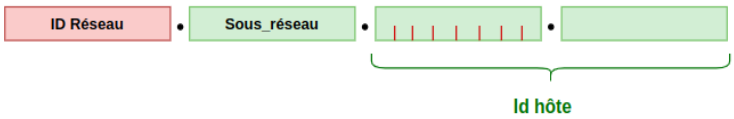


Fig. 5.2 Extension de l'ID réseau

C'est l'administrateur local qui effectue cette opération. En effet, il réserve un ensemble de bits à consacrer à l'identifiant de sous-réseau et qui va les regrouper avec le masque de sous-réseau (subnet mask).

Remarque : Pour qu'une adresse IP soit valide, le nombre de bits correspondant à la partie ID-machine doit être toujours supérieur ou égale à 2.

Bits	ID-Machine	Description
2 bits	11 = broadcast 00 = le réseau lui-même 01 = station 1 10 = station 2	c'est le nombre minimum de bits permettant d'adresser un sous-réseau et deux stations

Table 5.1 Nombre minimum de bits pour la création de sous-réseau

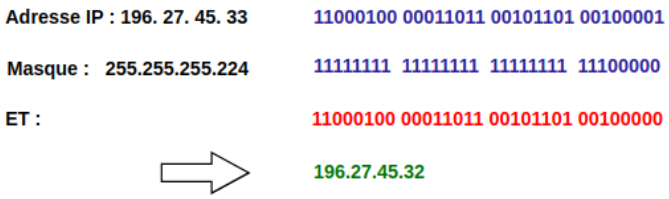
* Lorsqu'un équipement d'un sous-réseau veut communiquer un message à un autre, il compare sa propre adresse bit à bit avec celle du destinataire, en se basant sur le masque de sous-réseau. S'il y a égalité sur toute la partie identifiée par les 1 du masque, les deux équipements se trouvent dans le même sous-réseau et le message peut donc être transmis directement. Dans le cas contraire, les messages doivent être envoyés au routeur. C'est le seul équipement qui assure l'acheminement des messages vers l'extérieur du sous-réseau.

* Avec le masque de sous-réseau nous pouvons distinguer la partie qui identifie le sous-réseau et celle correspondant à la partie machine d'une adresse IP. Ainsi, une opération d'un ET logique entre le masque

Table 5.2 Allocation d'adresses avec la notation CIDR

Besoin de l'organisation	**Classe d'adresses**	**Masque utilisé**
< 64 @	Une subdivision de classe C	/26
< 128 @	Une subdivision de classe C	/25
< 256 @	1 réseau de classe C	/24
< 1024 @	4 réseaux de classe C contigus	/22
< 4096 @	16 réseaux de classe C contigus	/20

de sous-réseau et une adresse machine, permet à cette dernière de savoir dans quel sous-réseau elle se trouve. Plus de détails sont illustrés ci-après :



Le résultat 193.27.45.32 est l'adresse du sous-réseau auquel appartient la machine 193.27.45.33.

5.3.1.5 Les adresses sans classe CIDR

Le CIDR (Classless Inter Domain Routing) est un mécanisme développait en 1994 avec l'idée d'organiser les adresses IP indépendamment de leurs classes d'adresses. Désormais, le masque d'un sous-réseau indiquant le nombre de bits correspondant à l'identification de la partie réseau est configuré d'une manière libre par l'administrateur réseau.

Exemple: Un fournisseur d'accès à internet a attribué l'adresse IP 19.21.46.0 /22 à une organisation. Cela signifie que les 22 bits (/22) servent à identifier la partie réseau de l'adresse (C'est la suite de bits qui est strictement intouchable par l'admin). En ce qui concerne le reste des bits, l'administrateur peut les affecter librement selon les besoins de l'organisation. Il peut même utiliser des masques /23, /25 mais jamais un masque de taille inférieure à 22 bits.

Le tableau 5.2 montre des exemples d'allocation d'adresses en fonction des besoins exactes de l'organisation.

Le principal inconvénient de la technique CIDR est qu'elle impose la création de sous-réseaux de taille homogène. Cela signifie qu'une mauvaise anticipation des besoins en matière de dimensionnement des sous-réseau peut entraîner un gaspillage d'adresses IP ou une pénurie future.

5.3.1.6 Technique VLSM (Variable Length Subnet Mask)

Le VLSM est une technique de découpage d'un réseau IP en sous-réseaux de tailles différentes. Contrairement à la méthode classique qui utilise un masque de sous-réseau fixe pour tous les sous-réseaux, le VLSM permet d'adapter la taille du masque en fonction des besoins spécifiques de chaque segment du réseau. l'exemple suivant détaille la technique du VLSM.

Exemple : Face à un parc de 2100 machines, l'administrateur réseau a choisi de scinder le réseau en 3 sous-réseaux de tailles différentes, comme représenté dans la figure. 5.3.

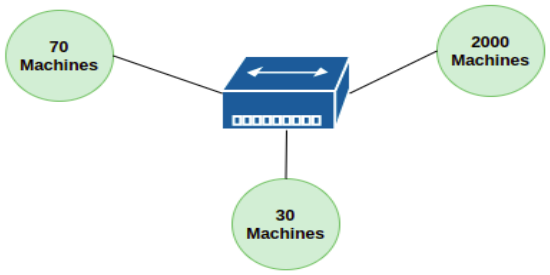


Fig. 5.3 Un réseau d'une entreprise regroupant 2100 machines

Afin de segmenter le réseau en fonction des besoins spécifiques en utilisant la technique VLSM, il est nécessaire de suivre les étapes suivantes :

1. Prioriser les sous-réseaux en fonction de leur taille, du plus grand au plus petit. On commence par traiter le sous-réseau de 2000 machines, puis celui de 70 machines, et enfin le sous-réseau regroupant les 30 machines.

2. Déterminer le nombre de bits nécessaires pour que le nombre maximal d'adresses IP disponibles par sous-réseau ($2^n - 2$) soit supérieur ou égal au nombre d'hôtes à adresser sur ce sous-réseau.

   Étant donné que le premier sous-réseau de la figure 5.3 comporte 2000 machines, il est nécessaire d'allouer au minimum 11 bits pour adresser chacune d'entre elles de manière unique. Puisque, $2^n - 2 = 2048 - 2 = 2046 > 2000$.

3. Identifier le préfixe d'adresse IP, en soustrayant le nombre de bits alloués au sous-réseau du nombre total de bits dans une adresse IP (32 bits). On obtient alors : $32 - 11 = 21$, Ceci implique que l'identification du premier sous-réseau, capable d'accueillir jusqu'à 2000 machines, nécessitera un masque de sous-réseau de $/21$. On est passé donc d'un masque de /16 à /21 et les 5 bits nouvellement masqués servent à l'identification des sous-réseaux.

   - Pour identifier le masque de sous-réseau correspondant au premier sous-réseau, on remplace les 21 bits de la partie réseau par des 1. Cela nous donne : $11111111.11111111.11111000.00000000/21$. Ce masque est équivalent à l'adresse décimale 255.255.248.0.
   - Pour identifier l'adresse du sous-réseau, on remplace les bits correspondant à la partie hôte par des zéros. Ce qui donne : 172.16.00010000.00000000 /21. Cette adresse est équivalente à 172.16.16.0 /21.

     Remarque: Les 5 bits nouvellement masqués ont été remplacés par la suite 00010 car le troisième octet de l'adresse de départ contient la valeur 16. Toute modification de cette séquence entraîne la création d'un nouveau sous-réseau avec le même masque /21.
   - Afin de déterminer la première adresse machine de ce sous-réseau, il faut remplacer les bits de la partie hôte par des zéros, à l'exception du bit correspondant au point faible. Cette opération résulte en l'adresse 172.16.00010000.00000001 /21, qui est équivalente à l'adresse 172.16.16.1 /21.
   - Pour trouver la dernière adresse IP utilisable dans ce sous-réseau, il faut remplacer tous les bits de la partie hôte par des 1, excepté le bit correspondant au point faible à zéro. Cette opération résulte en l'adresse 172.16.00010111.11111110 /21, qui est équivalente à l'adresse 172.16.23.254 /21.

- Enfin pour déterminer l'adresse de broadcast dans ce sous-réseau, il faut remplacer tous les bits de la partie hôte par des 1. Cette opération aboutit à l'adresse de 172.16.23.255 /21.

Pour le second sous-réseau, une nouvelle plage d'adresses est requise. En remplaçant le bit du poids faible de la séquence nouvellement masquée par 1 (00010 -> 00011), l'adresse obtenue est 172.16.24.0/21. C'est au sein de cette plage que nous allons attribuer des adresses à notre deuxième sous-réseau. $2^7 - 2 = 128 - 2 = 126 > 70$.

De la même manière, répétez les étapes 2 et 3 pour identifier les sous-réseaux restants.

5.3.2 Adressage IPV6

Le nombre d'objets connectés dans le monde ne cesse pas de croître actuellement, et il devrait atteindre selon les estimations les 43,2 milliards en 2023. Étant donné que le système d'adressage IPV4 actuel est limité à 32 bits, il ne permettra plus de contenter et de couvrir cette demande croissante d'adresses.

L'adressage IPv6 est le nouveau système d'adressage utilisé par la version 6 du protocole Internet (IPv6). Il est développé principalement pour répondre aux limitations de l'IPv4.

L'IPV6 utilise des adresses de 128 bits, ce qui permet d'adresser environ 3,4 × 1038 (soit plus de 340 sextillions) équipements à travers le monde. La figure 5.4 montre la structure d'une adresse IPv6.

Les adresses IPv6 sont notées en **hexadécimal**, elles sont divisées en huit groupes de 16 bits (appelé **hextet**) séparés par deux-points. Par exemple, l'adresse IPv6 illustrée dans la figure 5.4 est valide.

Il existe plusieurs mécanismes permettant de raccourcir une adresse IPV6, notamment :

- Le premier zéro (à gauche) d'un hextet est facultatif. Dans l'adresse illustrée à la figure 5.4, l'hextet 0cd7 peut être remplacé par cd7.
- Un hextet qui contient quatre zéros peut-être écrit qu'avec un seul zéro.
- Il est possible de regrouper une série de zéros par deux petits points. Alors que, ce procédé ne peut être fait qu'une seule fois dans l'adresse.

Nous avons vu que la longueur d'une adresse IPV6 est de 128 bits et se compose de huit champs de 16 bits chacun qui sont délimités par deux petits points.

Dans l'exemple présenté dans la figure 5.4, les trois premiers champs représentent le préfixe du réseau donné par le fournisseur à une entreprise. Le champ suivant (16 bits) est l'ID du sous-réseau qui est défini par l'administrateur du réseau selon la topologie interne de l'entreprise. Les quatre champs les plus à droite représentent l'ID d'interface qui est soit configuré automatiquement à partir de l'adresse MAC de l'interface ou soit configurer manuellement au format EUI-64.

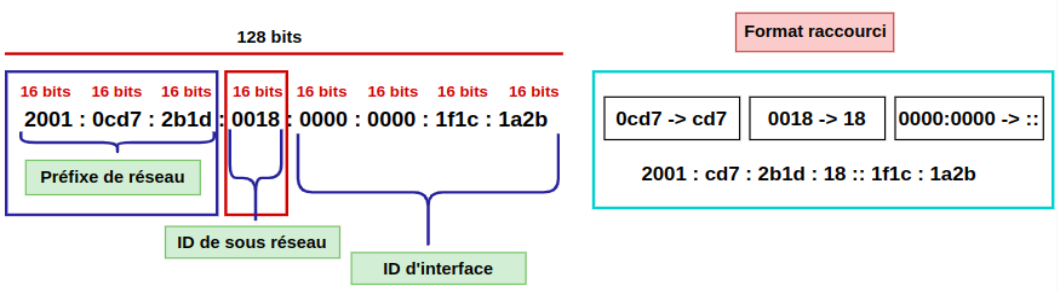


Fig. 5.4 Adresse IPV6.

Comme en IPV4, la notion du CIDR est utilisée en IPV6. C'est-à-dire avec un slash à la fin de l'adresse suivi de la longueur du préfixe en bits. Le préfixe de notre adresse illustré à la figure 5.4 fait

48 bits. Il s'agit des trois premiers champs situés plus à gauche. L'adresse IPV6 (dans les deux formats, normal et raccourci) avec la notation CIDR est illustrée dans la figure 5.5.

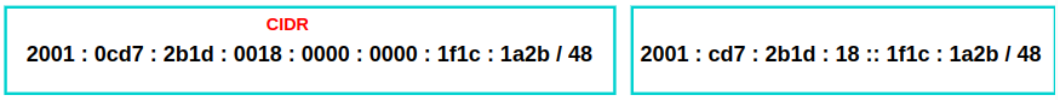


Fig. 5.5 Adresse IPV6 avec la notation CIDR.

L'adresse du réseau est obtenue en remplaçant tous les bits correspondant à l'ID hôte par des zéros (voir la figure 5.6).

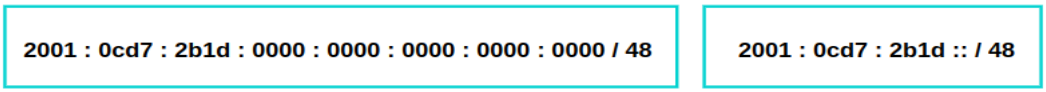


Fig. 5.6 Adresse réseau.

Et en fin si on veut inclure en plus le sous-réseau interne qui fait 16 bits, le préfixe de sous-réseau ferait alors 64 bits (48bits du préfixe réseau plus les 16 bits de i'ID de sous-réseau), voir figure 5.7.

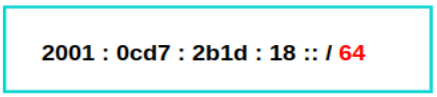


Fig. 5.7 Adresse du sous réseau.

IPV6 prend en charge plusieurs types d'adresse en fonction de son utilisation, notamment :

- **Adresses unicast :** Ces adresses sont utilisées pour les connexions point à point. Elles permettent d'identifier une interface réseau unique.
- **Adresses multicast :** Ces adresses sont utilisées pour identifier un groupe d'interfaces réseau. Le trafic d'une adresse multicast est destiné à plusieurs destinations en même temps.
- **Adresses anycast :** Ce sont des adresses virtuelles utilisées pour identifier une ou un groupe d'interfaces physiques. Cependant, le trafic sera envoyé seulement à une seule interface.
- **Adresse de broadcast :** Contrairement à l'IPV4, ces adresses n'existent plus en IPV6.
- **Adresses fe80::/10 :** Ces adresses sont appelées adresses link-local et sont utilisées pour communiquer sur un même segment de réseau.

5.4 Protocoles utilisés dans la couche réseau

5.4.1 Protocole IPV4

IPv4 est un protocole principal au fonctionnement d'Internet. Il est utilisé par des milliards d'appareils (i.e, machines hôtes et routeurs) chaque jour pour communiquer entre eux. C'est un protocole sans connexion, ce qui signifie que chaque paquet de données est envoyé indépendamment des autres paquets.

IPv4 est divisé en deux parties principales : l'en-tête IP et la charge utile. plus de détails sur le format d'un paquet IPV4 sont présentés dans la section suivante.

5.4.1.1 Format du datagramme IP

La structure d'un datagramme IPV4 est illustrée dans la figure 5.8.

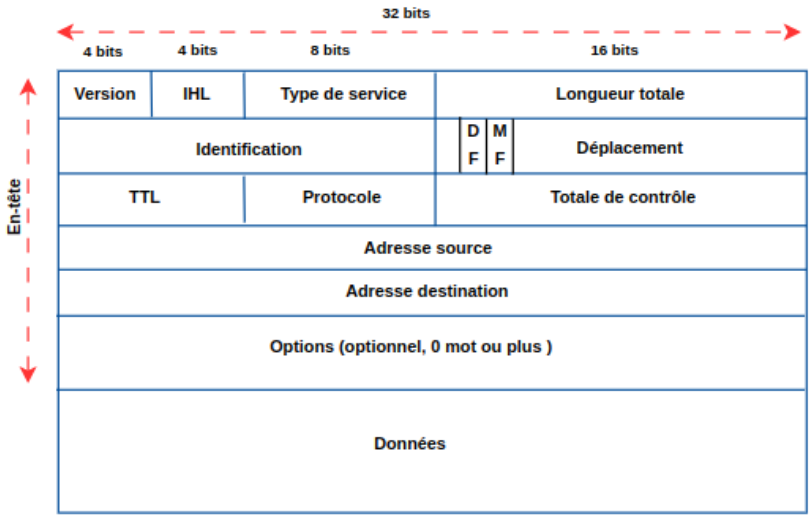


Fig. 5.8 Format d'un datagramme IP.

L'en-tête IP contient des informations sur le paquet de données, telles que l'adresse IP source, l'adresse IP de destination, le type de protocole et la longueur du paquet. Ces informations sont décrites par des mots de 32 bits.

- **Version :** Ce champ de 4 bits identifie la version du protocole IP. la version est utilisée pour vérifier la validité du datagramme.
- **Longueur de l'en-tête :** Ce champ codé sur 4 bits permet d'identifier le nombre de mots de 32 bits de l'en-tête. Un en-tête IP contient au maximum 15 mots de 32 bits, soit 60 bytes.
- **Type de services (ToS) :** Ce champ de 8 bits permet de spécifier la façon dont le datagramme doit être traité. Cette technique, appelée services différenciés ou gestion de qualité de service, est abandonnée et les 8 bits de ce champ sont toujours mis à 0.
- **Longueur totale :** Ce champ exprime en octets la taille totale du datagramme (en-tête + données). Il est codé sur 16 bits ce qui permet de créer des paquets dont la taille maximale peut atteindre 64 Ko. Cependant, la majorité des réseaux imposent des tailles inférieures et ceci nécessite de passer par le mécanisme de la fragmentation. Ce dernier est indiqué dans le deuxième mot de 32 bits suivant :
- **Identification :** Codé sur 16 bits, permet de spécifier le numéro du datagramme. Ce numéro est utilisé pour réassembler les fragments, portant le même identifiant, du datagramme initial chez le destinateur.
- **DF / MF :** Ces deux bits sont situés après un premier bit non utilisé, et sont utilisés comme drapeaux :

  - DF (Don't Fragment) : Ce bit autorise la fragmentation du datagramme s'il est mis à 0 et l'interdit quand il est à 1.

- MF (More Fragment) : Il permet d'indiquer s'il s'agit du dernier fragment (dans ce cas MF=0) ou il existe encore d'autres à suivre (MF= 1).

- **Déplacement :** Ce champ est codé sur 13 bits, il permet de spécifier la position du début du fragment par rapport au datagramme initial. Par convention, chaque fragment doit avoir une taille qui est un multiple de 8 octets.

  Le troisième mot de 32 bits contient trois champs :

- **Durée de vie (TTL, Time To Live) :** Codé sur 8 bits, il permet d'indiquer le nombre maximal de sauts que le datagramme peut effectuer. Ce numéro est décrémenté chaque fois que le datagramme traverse un routeur, et détruit lorsqu'il atteint la valeur nulle.

- **Protocole :** Spécifier le protocole auquel sont destinées les données transportées par le datagramme. Par exemple, 1 pour ICMP, 6 pour TCP, 17 pour UDP, etc. Il codé sur 8 bits.

- **Header checksum :** Ce champ de 16 bits permet de contrôler l'intégrité de l'en-tête du datagramme. Si une éventuelle erreur y détectée, le paquet sera directement écrasé.

- Les deux derniers champs de 32 bits indiquent, successivement, **l'adresse IP source** et **l'adresse IP destination**.

  Remarque : Ces cinq mots, présentés au-dessus, sont obligatoires et communs à tous les paquets IP.

- **Option :** Ce champ peut contenir des informations supplémentaires (options) sur le datagramme IP. Ces options doivent être structurées en mots de 32 bits. Ce qui nécessite l'indication de la longueur du datagramme IP (HL). Ce champ est optionnel, et il permet, par exemple, de surveiller le chemin traversé par les paquets dans un réseau, imposer un routage défini par la source, etc.

- **Données :** C'est la charge utile du datagramme IP. Elle contient les données réelles qui sont envoyées d'un appareil à l'autre.

5.4.1.2 Gestion de la fragmentation

Dans les situations ou la taille d'un datagramme IP dépasse la valeur du **Maximum Transmis Unit (MTU)** du réseau qu'il doit traverser, l'équipement (hôte ou routeur) en responsable doit le fragmenter.

Au niveau du routage, il est possible que chaque fragment traverse un chemin différent; Si l'un des fragments se perd, le paquet en question est considéré comme perdu.

Chaque technologie réseau possède sa propre MTU (voir tableau 5.3).

Technologies	MTU (en octets)
PPPoE	1492
Ethernet	1500
WiFi	2300
Token Ring	4464

Table 5.3 MTU vs. technologies réseaux

Maintenant, les champs du datagramme IPV4 qui vont être affectés par le mécanisme de la fragmentation sont ceux du second mot : Identification, Flag (DF, MF) et Déplacement. Le mécanisme de la fragmentation est détaillé par l'exemple suivant :

- prenons le réseau représenté dans la figure 5.9. La machine A du premier réseau (1) souhaite envoyer un datagramme à la machine B située dans le second réseau (2). La taille du paquet est de 4000 octets, tandis que le MTU du second réseau est limité à 1500 octets seulement. Sachant que le bit DF du champ flag du paquet est égal à 0 (fragmentation autorisée), le routeur va décider de fragmenter le paquet.

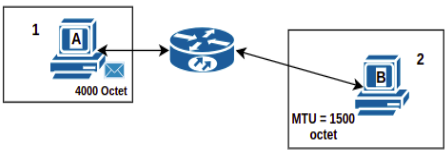


Fig. 5.9 Réseau de niveau 3

- Étant donné que l'entête du paquet est égal à 20 octets (datagramme sans option), il reste 3980 octets pour la partie donnée. De même pour le second réseau, la partie donnée réservée aux datagrammes qui y circulent ne doit pas dépasser $1500 - 20 = 1480$ octets.
- Nous divisons la partie donnée du paquet à fragmenter (3980) par la taille du fragment autorisée dans le second réseau (1480), $3980/1480 = 2,68$, nous obtenons la valeur 2.68. Cela signifie que notre paquet doit être divisé en deux fragments de 1480 octets et un troisième de $3980 - 2960(1480 * 2) = 1020$ octets.
- Chaque fragment créé doit comporter la même valeur d'identification indiquée dans le datagramme initial.
- Le champ MF doit être toujours déclaré à 1. Sauf le dernier fragment le remet à zéro pour indiquer qu'il s'agit du dernier.
- Enfin, le dernier champ Décalage fragment (Offset) est rempli ainsi :
  - le premier fragment prend la valeur 0 (puisque il s'agit du premier).
  - Le second fragment vient après 1480 octets reçus (après le 1^{er} fragment). Sauf que, les valeurs du champ offset doivent être exprimées en multiple de 8 ($2^{13} = 8192, 65536/8192 = 8$). Donc, il faut diviser $1480/8 = 185$. Par conséquent, la valeur de l'offset dans ce cas est égale à 185.
  - Pour le reste des fragments il suffit tout simplement de rajouter la valeur de l'offset à chaque fois jusqu'à l'arrivée au dernier fragment.