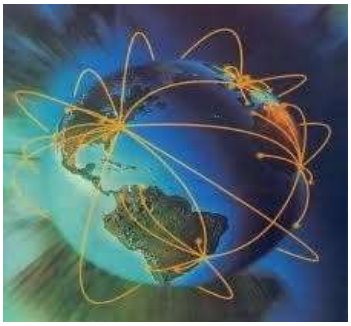
CHAPITRE 07

LE MODELE TCP/IP



But du chapitre

A la fin de ce chapitre l'étudiant connaitra les différentes fonctionnalités de la couche réseau, entre autre :

- L'adressage IP.
  - C'est quoi une adresse IP.
  - Les différentes classes des adresses IP.
    - La classe A, B, C, D et E.
  - Les différents types des adresses IP.
    - Les adresses IP réservées, privées et publiques.
  - Le découpage en de sous réseaux.
    - Le masque de sous réseau.
    - La gestion des sous réseaux.
  - Le principe de fonctionnement du service NAT.
- Le routage.
  - C'est quoi une table de routage.
  - Le routage à vecteur de distance.
  - Le routage à état de liens.

1 Introduction

La couche liaison assure le transfert de données au sein d'un même réseau LAN, tandis que la couche réseau assure le transfert de données entre différent réseaux LAN. En effet, dans un réseau LAN où les équipements sont, généralement, en liaison directe, la couche liaison assure la transmission de données de l'émetteur au récepteur, et pour le transfert de données entre des équipements de réseaux différents, il faut trouver un chemin pour que l'émetteur puisse atteindre le récepteur, ce qui est assuré par la couche réseau.

Dans ce chapitre, nous nous focalisons sur les fonctionnalités de la troisième couche du modèle OSI. Pour ce faire, nous allons étudier directement les fonctionnalités de la couche Internet de la pile protocolaire TCP/IP. Nous commençons par un petit rappel sur la pile de protocoles TCP/IP, ensuite nous présentons les différentes fonctionnalités du protocole IP (qui est le protocole de la couche Internet), à savoir l'adressage, le routage, etc.

2 Histoire de l'internet

L'internet est né en 1969 comme projet *DARPA* pour *Defense Advanced Research Projects Agency* aux USA. Son objectif était :

- La mise en œuvre d'une commutation de paquets.
- L'interconnexion des universités participant aux projets *ARPA*.

Le tout premier réseau constituait de quatre ordinateurs. Après en 1972, c'était la naissance du projet *ARPNET* avec une centaine d'ordinateurs. La technologie d'internet est basée sur les deux protocoles IP et TCP dont la spécification n'a eu lieu qu'en 1974 avec la spécification du protocole NCP (Network Control Program), qui est l'ancêtre de TCP.

Pour une histoire bien détaillée sur l'évolution de l'internet et ses protocoles, l'étudiant est invité à consulter [].

3 Architecture d'Internet

Dans le réseau Internet, qui est un réseau WAN, le transfert de données d'un terminal source à un terminal de destination passe par le nuage du réseau constitué des équipements intermédiaires, à savoir les routeurs, qui assurent l'acheminement des données (l'identification de la destination et le choix du chemin). Donc, ce sont les routeurs qui gèrent l'acheminement et le routage entre les réseaux.

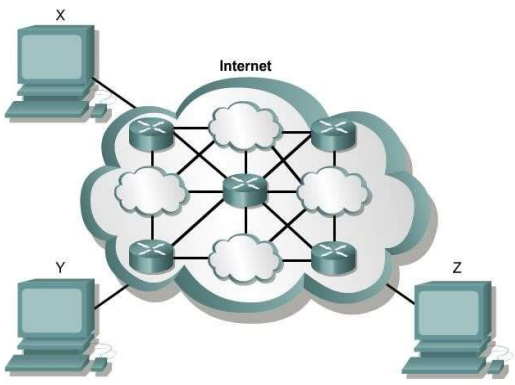


Figure 71. L'architecture internet.

4 Terminologie

Le mot « INETRNET » signifie *INETRconnexion NETworks* qui veut dire l'interconnexion des réseaux. Donc l'Internet est le réseau des réseaux. Dans ce qui suit quelques termes techniques qu'on utilise généralement quand on parle d'Internet :

- *Internet.* L'internet avec un "I" majuscule signifie le réseau mondial qui fonctionne selon IP.
- *Un internet.* C'est un ensemble de réseau (généralement des LAN) interconnectés à l'aide du protocole IP.
- *Un intranet.* C'est un réseau qui utilise les protocoles TCP/IP, et fournit les services internet mais seulement à l'intérieur d'un réseau local (il n'est pas accessible par l'extérieur).
- *Hôte (Host), système terminal, end-system.* C'est la machine (généralement un ordinateur) connectée à un réseau et via laquelle l'utilisateur peut utiliser les services du réseau.
- *Routeur, système intermédiaire.* C'est un équipement qui possède plusieurs interfaces réseau lui permettant de jouer le rôle d'inter-connecteur. Il est capable d'acheminer des paquets IP et il travaille à la couche « réseau » de la hiérarchie TCP/IP.

5 Le modèle TCP/IP

A la différence du modèle OSI qui est un modèle théorique, le modèle TCP/IP est une pile protocolaire. Il est imposé comme la norme d'Internet, et il repose sur l'utilisation obligatoire du protocole IP. En effet, chaque couche de la pile TCP/IP comporte différents protocoles assurant les différentes fonctionnalités de la couche, sauf la couche Internet dont toutes les fonctionnalités s'articulent autour du protocole IP (voir *Figure 72*).

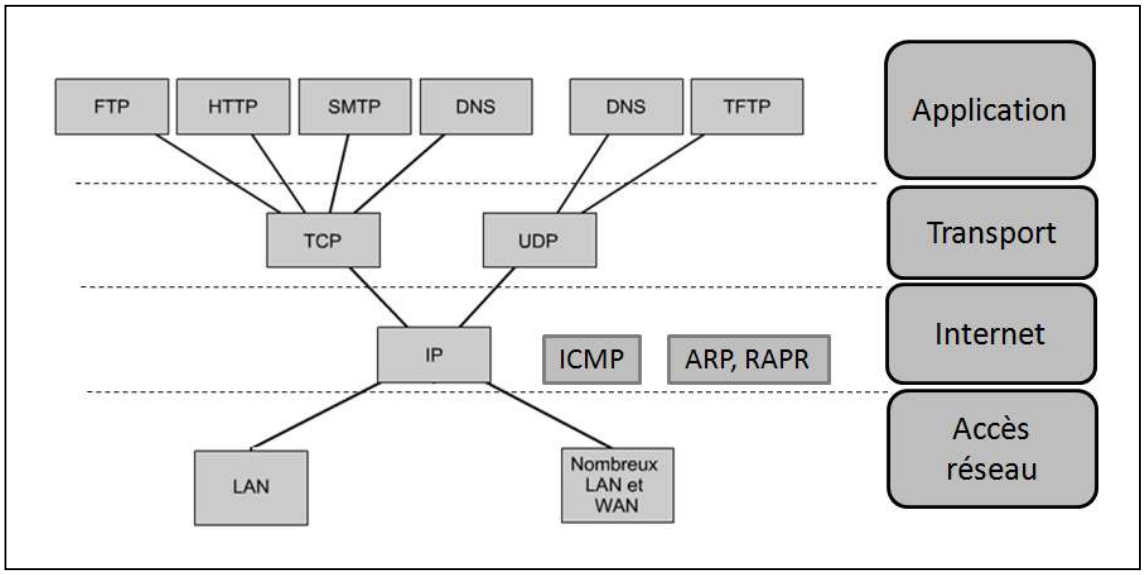


Figure 72. Différent protocoles de la pile TCP/IP.

Dans la suite, un petit rappel sur les fonctionnalités de chacune des couches du modèle TCP/IP est présenté.

5.1 La couche Application

Cette couche regroupe les différents protocoles offrant des services réseaux, comme par exemple :

- *Le transfert de fichiers* ou données volumineuses assuré par :
  - Le protocole *FTP – File Transfer Protocol*.
    Il est Orienté connexion (il utilise le protocole TCP au lieu d'UDP). Ainsi il assure un service fiable.
  - Le protocole *TFTP – Trivial File Transfer Protocol.*
    Il assure un service non orienté connexion (il utilise le protocole UDP).
- *Le courrier électronique :* assuré par le protocole *SMTP–Simple Mail Transfer Protocol*
- *La connexion à distance :* assuré par le protocole *Telnet – Terminal Network.* Il permet un accès à distance à un ordinateur via un autre (l'ouverture d'une session à distance).
- *Administration réseau :* assuré par le protocole *SNMP– Simple Network Management Protocol.* Il permet d'administrer les différents équipements du réseau, qui comporte entre autres :
  - La surveillance et le contrôler des équipements du réseau.
  - La gestion des configurations, des statistiques, des performances et de la sécurité.
- *Gestion de noms :* assuré par le protocole *DNS –Domain Name System.* Il est utilisé pour convertir les noms de domaine en adresses IP et inversement.

5.2 *La couche Transport*

La fonctionnalité principale de cette couche est l'établissement d'une liaison logique entre l'hôte source et l'hôte de destination (de bout en bout). Les protocoles de cette couche sont : *TCP (orienté connexion) et UDP (orienté sans connexion).*

Les fonctionnalités communes entre les deux protocoles sont :

- La segmentation et le réassemblage des données (l'unité de données est le segment).
- L'envoi des segments de données d'un équipement à un autre.

En plus de ces fonctionnalités, le protocole TCP assure :

- L'établissement des connexions de bout en bout (service orienté connexion).
- Le contrôle de flux à l'aide des fenêtres glissantes.
- La fiabilité et le contrôle d'erreurs.

5.3 *La couche Internet*

La principale fonctionnalité de cette couche est le routage (acheminement) des données de la source à la destination. Le routage dépend des deux points suivants :

- L'identification de la machine dans le réseau, ce qui est assuré par l'adressage IP.
- L'acheminement des données en choisissant le meilleur chemin entre la source et la destination.

Les protocoles qui s'exécutent au niveau de cette couche sont :

- *Le protocole IP*.
  C'est le protocole principal de cette couche.
- *Le protocole ICMP (Internet Control Message Protocol).*

Il assure la fonction de messagerie et de contrôle dans le réseau. Par exemple, la signalisation de problèmes entre routeurs à l'aide des messages d'erreurs échangés entre eux est assurée par ICMP.

- *Le protocole ARP (Address Resolution Protocol)*

  Il permet de déterminer l'adresse MAC (physique) d'une machine dont on connait l'adresse IP (@IP → @MAC).

- Le protocole RARP (*Reverse Address Resolution Protocol*)

  L'inverse du protocole ARP. Il détermine l'@IP correspondante à une @ MAC.

- *Les algorithmes de routage*

  Ils déterminent les meilleurs chemins selon différentes métriques (le nombre de sauts, la bande passante, la charge, etc.) pour router les données.

6 Le protocole IP et ses fonctionnalités

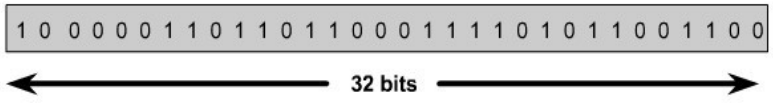
Les deux fonctionnalités principales du protocole IP sont :

- *L'adressage IP :* qui permet d'identifier d'une façon unique chaque machine dans le réseau. Par la suite et dans le cadre de l'étude de cette fonctionnalité, nous abordons principalement les points suivants :
  - Qu'est-ce qu'une adresse IP ?
  - Comment les @IP sont structurées en classes ? Et quelles sont ces classes ?
  - Quels sont les différents types des @IP (réservées, privées, publiques) ?
  - Le découpage et la gestion des sous réseaux.
  - Le service NAT (Network Adress Translation).
- *Le routage :* qui consiste à acheminer les données de la source vers la destination. Nous allons voir lors de l'étude de cette fonctionnalité :
  - C'est quoi une Tables de routage ?
  - Les différentes classes de protocoles de routage.

6.1 *L'adresse IP*

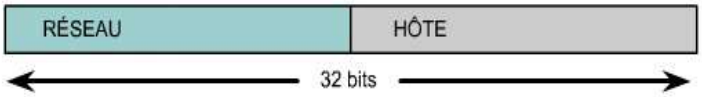
Tout équipement sur à un réseau TCP/IP doit disposer d'une *adresse IP unique*. Cette adresse est l'identificateur de cet équipement, et permet de le localiser dans le réseau. L'adresse IP a les caractéristiques suivantes :

- Elle est une séquence de 32 bits composée de 1 et de 0. *Exemple :*



- Cette suite de bits est exprimée sous forme de quatre nombres décimaux séparés par des points. *Exemple :* l'@IP précédente : 10000011.01101100.01111010.11001100 → 131.108.122.8.204.
- Chaque élément d'une @ IP est un octet → il représente une valeur entre 0 et 255.
- Chaque adresse IP comporte deux parties :

- *« Partie Réseau »* : elle identifie le réseau auquel la machine est connectée.
- *« Partie Hôte »* : ou la « Partie machine » elle identifie la machine dans le réseau auquel elle est connectée.



Selon le nombre de bits réservés à la partie réseau et ceux laissés à la partie machine, différentes classes d'@IP existent.

6.2 *Classes des adresses IP*

Les adresses IP sont réparties en différentes classes pour permettre une adaptation à des réseaux de différentes tailles. En effet, le nombre de machines par réseau dépend du nombre de bits réservés à la partie machine, donc plus il y a de bits dans la partie machine plus la taille du réseau est grande et inversement. Cette répartition des adresses IP en des classes a permis un choix large pour des réseaux de différentes tailles.

Pour déterminer la classe d'une @IP :

- *En représentation binaire :* la séquence de bits située au début de l'adresse détermine la classe de l'adresse.
- *En représentation décimale* : la valeur du premier nombre de l'@IP permet de connaître la classe de l'adresse. Pour chaque classe d'adresses, le premier octet de l'adresse peut prendre une valeur dans un intervalle bien défini.

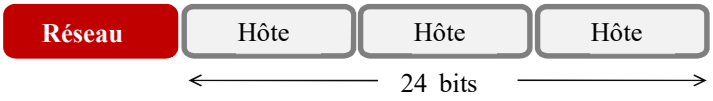
Il existe cinq classes d'adresses IP :

- La classe A → pour les réseaux de très grande taille.
- La classe B → pour les réseaux de taille moyenne.
- La classe C → pour les réseaux de petite taille.
- La classe D → réservée à la diffusion multicast.
- La classe E → réservée à l'expérimentation.

6.2.1 Classe A

Une adresse IP de classe A est caractérisée somme suit :

- La *partie réseau* : contient le premier octet.
- La *partie hôte* : contient les trois octets suivants.



- Le premier bit du premier octet est toujours à **0**. Donc, on peut reconnaître une adresse IP de classe A si sa représentation binaire commence par le bit 0.

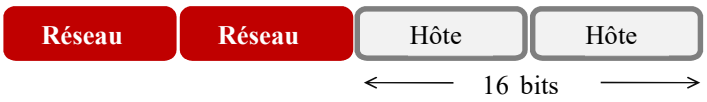
- Le premier octet de l'adresse est compris entre : **0**0000000 → 0 (en décimal) et **0**1111111 → 127 (en décimal).
- Etant donné que les valeurs 0 et 127 sont réservées (ne peuvent pas être utilisées), donc une adresse de classe A commence par une valeur entre 1 et 126.

Les adresses de cette classe sont réservées aux réseaux de très grande taille (plus de 16 millions d'adresses hôtes).

6.2.2 Classe B

Une adresse de la classe B est caractérisée comme suit :

- La *partie réseau* : contient les deux premiers octets.
- La *partie hôte* : contient les deux autres octets.



- Les deux premiers bits du premier octet sont toujours à **10.** Donc, on peut reconnaître une adresse IP de classe B si sa représentation binaire commence par la suite 10.
- Le premier octet de l'adresse est compris entre : **10**000000 → 128 (en décimal) et **10**111111 → 191 (en décimal).
- Une adresse de classe B (en représentation décimale) commence par une valeur entre 128 et 191.

Les adresses de cette classe sont réservées aux réseaux de taille moyenne ou grande.

6.2.3 La classe C

Une adresse IP de classe C est caractérisée comme suit:

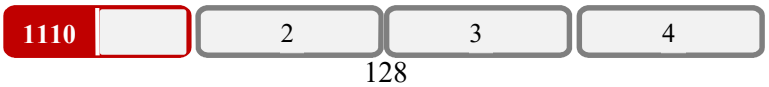
- La *partie réseau* : contient les trois premiers octets.
- La *partie hôte* : contient le dernier octet.

- Les trois premiers bits sont à **110**. Donc, on peut reconnaître une adresse IP de classe C si sa représentation binaire commence par la suite 11à.
- Le premier octet de l'adresse est compris entre : **110**00000 → 192 (en décimal) et **110**11111 → 223 (en décimal).
- Une adresse de classe C commence par une valeur entre 192 et 223.

Les adresses de cette classe sont les plus utilisées, et elles sont réservées aux réseaux de petite taille (254 hôtes maximum).

6.2.4 La classe D

Les adresses Ip de la classe D sont réservées à la diffusion multicast. Elles sont caractérisées comme suit :



- Les quatre premiers bits doivent correspondre à **1110**.
- Le premier octet est de l'adresse est compris entre : **1110**0000 → 224 (en décimal) et **1110**1111 → 239 (en décimal).
- Une adresse de multicast (classe D) commence par une valeur entre 224 et 239.

Une adresse de multicast est une adresse réseau unique qui achemine les paquets associés à une adresse de destination vers des groupes prédéfinis d'adresses IP.

6.2.5 La classe E

Les adresses de la classes E sont réservées à des fins expérimentales par IETF.

- Les quatre premiers bits sont toujours à **1**.
- Le premier octet est compris entre : **1111**0000 → 240 (en décimal) et **1111**1111 → 255 (en décimal).

On note qu'aucune adresse de classe E n'est disponible sur Internet.

Classe d'@ IP	Plage d'adresses	Bits de valeur sup	# bits Partie réseau	# réseaux	# hôtes/ réseau
Classe A	1-126 00000001-01111110	0	8	126	16777214
Classe B	128-191 10000000-10111111	10	16	16384	65534
Classe C	192-223 11000000-11011111	110	24	2097152	254
Classe D	224-239 11100000-11101111	1110	28	SO	SO
Classe E	240-255 11110000-11111111	1111		SO	SO

Remarques.

1) Pour déterminer la partie réseau et hôte d'une adresse IP, on doit d'abord identifier la classe de l'adresse.
2) La plage d'adresses ***127.x.x.x*** est réservée et utilisée pour les tests et diagnostiques.

6.3 *Types des adresses IP*

Une adresse IP peut être réservée, privée ou publique :

6.3.1 Adresses IP réservées

Certaines adresses IP sont réservées et ne peuvent pas être affectées à des machines. Ces adresses sont :

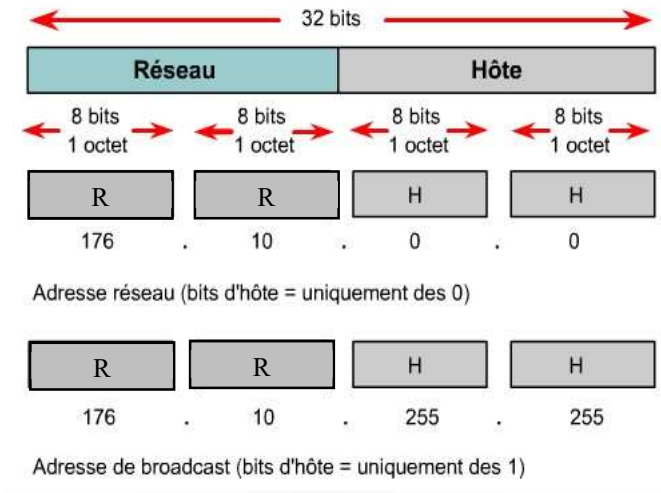
- *L'adresse réseau :*
  - L'adresse dont tous les bits hôte sont à 0.

- Elle est utilisée pour identifier le réseau lui-même (voir l'exemple ci-dessous).

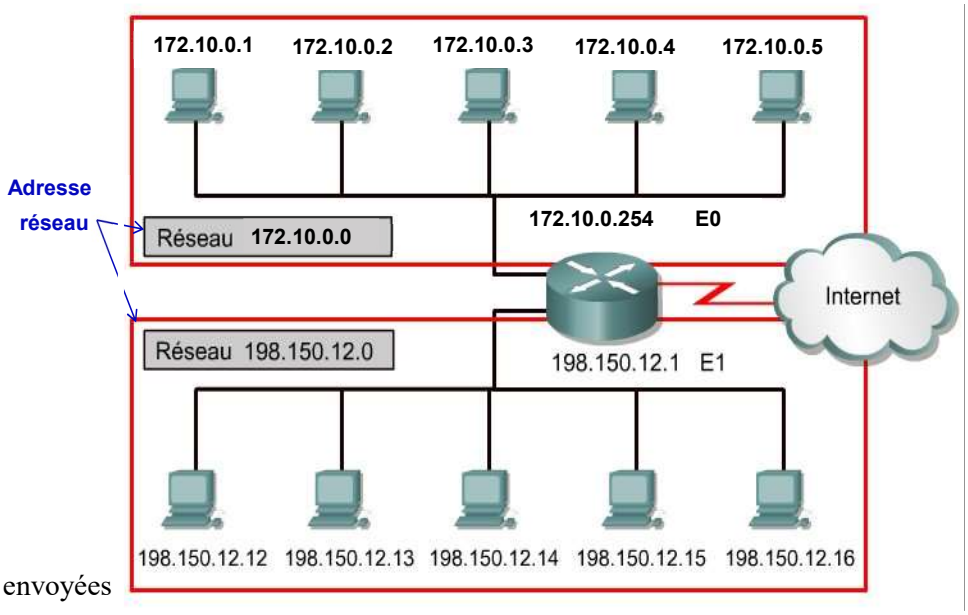
- *L'adresse de broadcast :*
  - L'adresse IP dont tous les bits hôte sont à 1.
  - Elle est utilisée pour diffuser des paquets vers tous les équipements d'un réseau.

Exemple. Soit l'adresse IP : 176.10.34. 102 → C'est une adresse de classe B car le premier octet est entre 128 et 191. Dans un réseau de classe B, les 16 derniers bits forment la partie hôte, ainsi les deux adresses réservées sont :

- L'adresse réseau est : 176.10.**0.0**.
- L'adresse de broadcast est : 176.10.**255.255** (notez que 255 Correspond à la valeur décimale d'un octet dont tous les bits sont à 1, c.-à-d. 11111111).



Supposons que le réseau dont l'adresse 176.10.0.0 est connecté par un routeur à un autre réseau local (LAN) de classe C dont l'adresse réseau est 198.150.12.**0** (voir Figure ci-dessous).



Les données envoyées 1 (émettrice), à une machine du réseau 198.150.12.0, par exemple la machine 198.150.12.14 (réceptrice), seront visibles en

dehors du réseau local de la machine émettrice sous la forme 172.10.0.0 (les numéros de machines ne sont pris en compte que localement). C'est pour cela on ne peut pas attribuer une adresse réseau à une machine.

6.3.2 Les adresses IP privées

Les adresses privées sont des adresses à utilisation privée et interne. Comme par exemple l'utilisation interne dans un intranet non public, qui est le cas d'un réseau domestique par exemple. Il existe trois intervalles d'adresses privées correspondants aux trois premières classes des adresses IP :

- *Classe A* : de 10.0.0.0 à 10.255.255.255
- *Classe B* : de 172.16.0.0 à 172.31.255.255
- *Classe C* : de 192.168.0.0 à 192.168.255.255

L'idée de l'utilisation des adresses privée est proposée comme solution au problème de pénurie des adresses IP publiques. En effet avec la pénurie des adresses IP, on a spécifié une plage d'adresses pour chaque classe comme privée, et peut être utilisée par différents réseau mais localement. Donc deux réseaux différents peuvent avoir la même adresse IP privée. Ainsi il suffit que le réseau entier (et pas chaque machine du réseau) soit identifié d'une manière unique dans le réseau public, ce qui résulte en une économie d'adresses IP.

Les adresses contenues dans ces plages ne sont pas acheminées sur les routeurs d'Internet (les routeurs Internet les rejettent immédiatement), et on dit qu'elles ne sont pas routables. Donc seule l'adresse attribuée à tout le réseau est publique est ainsi routable, et les données envoyées par chaque machine du réseau seront identifiées par l'adresse publique du réseau au lieu de l'adresse de la machine qui les a envoyées. Le mécanisme qui s'occupe de faire la correspondance entre l'adresse routable du réseau et les adresses privées des différentes machines du réseau est le NAT (voir ci-après).

6.3.3 Les adresses IP publiques

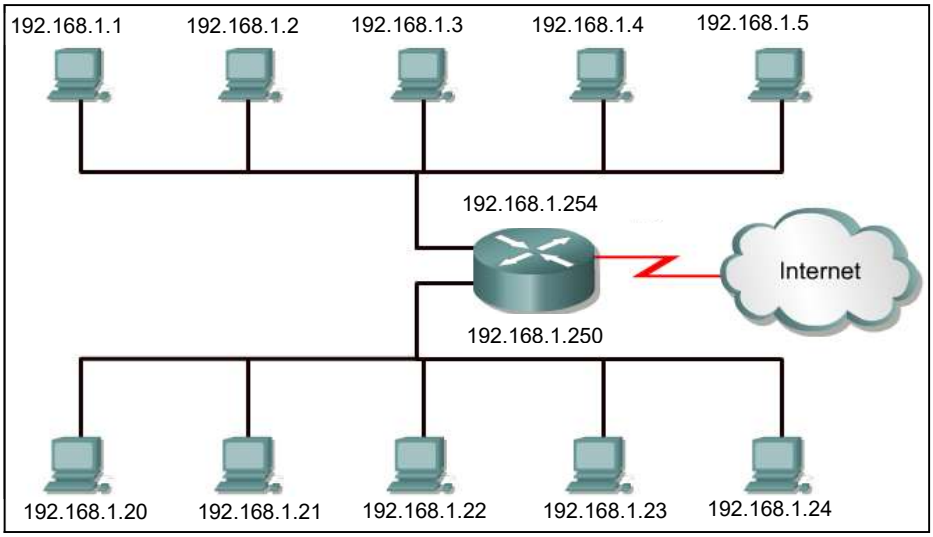
Les machines d'un réseau public doivent disposer d'une adresse IP unique. Ces adresses sont obtenues auprès d'un fournisseur d'accès Internet (FAI). Pour éviter d'avoir une même adresse IP publique utilisée deux fois, un organisme à savoir l'IANA −*Internet Assigned Numbers Authority* gère scrupuleusement les adresses IP disponibles.

L'attribution des adresses IP peut se faire de deux façons :

- *Statique* : l'équipement possède toujours la même adresse, et on parle ici d'une adresse IP statique.
- *Dynamique* : l'équipement a une adresse différente à chaque connexion réseau, et on parle ici d'une adresse IP dynamique.

N.B. Les réseaux privés qui ne sont pas connectés à Internet peuvent utiliser n'importe quelle adresse, pourvu qu'elle soit unique.

Exemple : Dans la configuration ci-dessous, le modèle d'adressage réseau est incorrect, car les deux réseaux ont la même adresse publique qui est 192.168.1.0. Notez que dans cette configuration on a deux réseaux, car il y a un routeur qui connecte deux groupes de machines (chacun des deux groupes constitue un réseau).



6.4 *NAT- Network Adress Translation*

Le NAT est le service de traduction d'adresses réseau, et qui consiste à faire correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables (voir *Figure 70*).

Le service NAT permet de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, ce qui permet de diminuer significativement le nombre d'adresses IP uniques utilisées, et ainsi pallier l'*épuisement des adresses IPv4*.

Notez que le NAT permet de rendre les adresses privées d'un réseau invisibles depuis Internet, ce qui comporte un sens de sécurité. Ainsi, on peut attribuer à nos machines des adresses IP privées si la sécurité est une priorité.

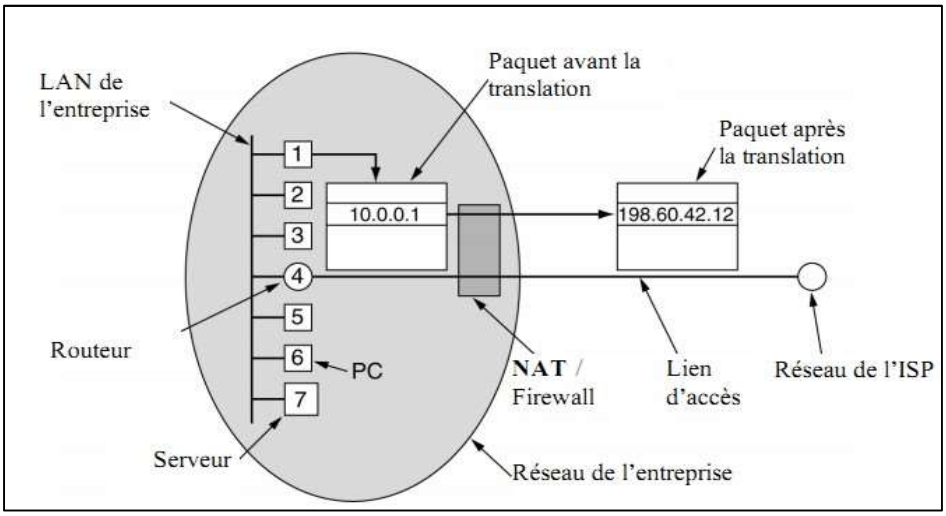


Figure 73. Fonctionnement du service NAT.

6.5 *Utilisation des adresses IP*

Le routage de paquets dans un réseau TCP/IP est similaire au fonctionnement du système postal :

- La lettre comporte un code postal qui désigne la ville de destination.

- Le code postal est utilisé pour remettre le courrier au bureau de poste de la ville de destination.
- Une fois le courrier est arrivé au bureau de la ville, le facteur utilise ensuite l'adresse de domicile du destinataire pour localiser la destination finale dans la ville, et ainsi remettre le courrier au concerné.

Ceci est appelé l'*adressage hiérarchique.*

Dans un réseau TCP/IP :

- Un paquet comporte un identificateur (l'adresse IP) pour les réseaux source et de destination.
- Un routeur utilise l'adresse IP du réseau (partie réseau) de destination afin de remettre le paquet au réseau approprié.
- Lorsque le paquet atteint un routeur connecté au réseau de destination, ce routeur localise l'ordinateur sur le réseau à l'aide de l'adresse IP (partie hôte).

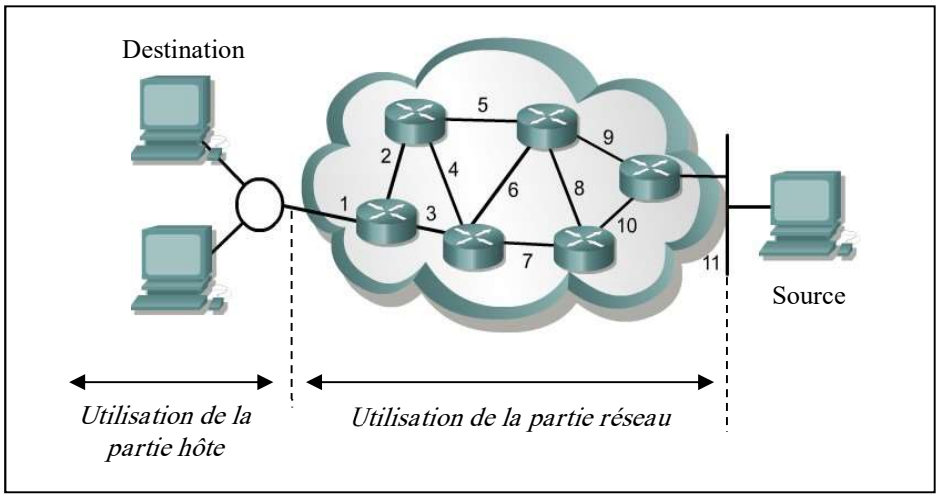


Figure 74. Utilisation des @ IP dans l'acheminement de données.

Pour extraire la partie réseau et la partie machine d'une adresse IP, les routeurs utilise ce qu'on appelle le *masque de réseau*.

6.6 *Masque de réseau*

Le masque de réseau est une adresse IP dont les bits de la partie réseau sont à 1 et ceux de la partie hôte à 0. Il est utilisé par les équipements pour extraire la partie réseau et la partie hôte d'une adresse IP en appliquant l'opération suivante :

$$Adresse\ réseau = Adresse\ IP\ [\boldsymbol{AND\ logique}]\ Masque\ de\ réseau$$

Exemple : Le masque de réseau d'une adresse de classes B est :

255.255.0.0 → 11111111.11111111.00000000.00000000

Donc pour la machine dont l'adresse IP est : 176.11.25.83, l'adresse du réseau auquel elle appartient est :

(176.11.25.83) AND (255.255.0.0) ⇨ 10110000. 00001011.00011001.0101011

AND 11111111.11111111.00000000.00000000

10110000. 00001011.00000000.0000000 ⇨176.11.0.0.

N.B. Le masque présente sa principale utilité dans le cas d'un découpage en sous réseaux.

6.7 *Le découpage en sous réseaux*

Le découpage en des sous-réseaux est la fragmentation d'un réseau en segments ou parties de plus petite taille et plus faciles à gérer. Le découpage en de sous réseaux assure une administration plus efficace du réseau ; il permet de confiner le broadcast, et ainsi garantir une certaine sécurité sur le réseau LAN.

Dans la conception d'un réseau à découper en de sous réseaux, on doit définir :

- Le nombre de sous-réseaux requis.
- Le nombre d'hôtes requis par sous réseau.

6.7.1 Comment faire le découpage ?

Pour découper un réseau en de sous réseaux on procède ainsi :

1) On définit le nombre de sous-réseaux requis, ainsi que le nombre d'hôtes nécessaires au sous-réseau de plus grande taille.
2) On emprunter des bits au champ d'hôte et on les désigne comme champ de sous-réseau. Le nombre de bits à emprunter dépend du nombre de sous réseau et/ou du nombre maximal d'hôtes requis par sous-réseau. La règle à respecter est la suivante :
    - Pour l'emprunt de *N* bits, on a :
        - Le nombre de sous-réseaux utilisables = $(2^{\text{nombre de bits empruntés}}) - 2$.
        - Le nombre d'hôtes utilisables = $(2^{\text{nombre de bits hôtes restants}}) - 2$.

On soustrait 2 correspondant aux adresses du réseau et de broadcast (car elles ne peuvent pas être attribuées à une machine).

Exemple : Concevoir un réseau qui requiert six sous-réseaux de 25 hôtes chacun.

On essaye jusqu'à arriver au bon choix.

- L'emprunt d'1 bit donne $2^2 - 2 = 0$ sous réseaux utilisables → Non.
- L'emprunt de 2 bits donne $2^2 - 2 = 2$ sous réseaux utilisables → Non.
- L'emprunt de trois bits donne :

    ⇨ $(2^3) - 2 = 6$, six sous-réseaux utilisables.

    ⇨ $(2^5) - 2 = 30$, trente (>25) hôtes utilisables pour chaque sous réseau.

Donc, l'emprunt de trois bits répond à nos besoins.

6.7.2 Conditions à respecter

Les conditions à respecter dans l'emprunt de bits sont :

- Le nombre minimal de bits pouvant être empruntés est deux, car l'emprunt d'un seul bit donne 0 sous réseaux (il donne l'adresse du réseau (0) et l'adresse de broadcast (255)).

- Le nombre maximal de bits pouvant être empruntés est égale au nombre de bits hôte – 2, car l'emprunt d'un nombre de bit plus grand donne des sous-réseaux comportant 0 hôtes.

N.B. Il est possible d'itérer le découpage plusieurs fois → Adressage hiérarchique de plusieurs niveaux.

6.7.3 Le masque de sous réseau

Le masque de sous réseau est une adresse IP dont les bits de la partie réseau ainsi que ceux empruntés pour créer les sous réseaux sont à 1, et ceux qui reste de la partie hôte à 0. Il permet de déterminer le réseau et le sous-réseau auxquels un hôte donné appartient.

Exemple : Le masque de réseau d'une adresse de classe C est :

11111111.11111111.11111111.00000000 → 255.255.255.0

Si trois bits sont empruntés pour créer des sous réseaux, le masque de sous réseau est :

11111111.11111111.11111111.**111**00000 → 255.255.255.224

En utilisant le format dit « format de barre oblique », le masque est : 255.255.255.224/27, où 27 indique le nombre total de bits utilisés pour la partie réseau et sous-réseau.

6.7.4 La gestion des sous réseaux

On utilise le masque de sous réseau pour déterminer le réseau et le sous-réseau auxquels une machine donnée appartient, comme suit :

$$Adresse\ de\ sous\ réseau\ =\ Adresse\ IP\ \ [\boldsymbol{AND\ logique}]\ \boldsymbol{M}asque\ de\ sous\ réseau.$$

Exemple : Soit l'adresse IP d'une machine est 201.10.11.65 dans un réseau dont le masque est 255.255.255.224. Quelle est l'adresse de sous réseau auquel la machine appartient ?

11001001.00001010.00001011.01000001
AND 11111111.11111111.11111111.11100000
11001001.00001010.00001011.01000001 ⇨ 201.10.11.64

Donc, l'@ du sous réseau est : 201.10.11.64

6.7.5 Exemples d'application

Application 01.

On a un réseau de classe B avec un masque de sous-réseau 255.255.240.0. Quel est le nombre maximum d'ordinateurs que l'on peut raccorder à chacun des sous réseaux ?

Solution :

255.255.240.0 → 11111111.11111111.11110000.00000000

La partie réseau a une longueur de 20 bits, la partie hôte a une longueur de 12 bits. Il peut donc y avoir 2^{12} - 2 = 4094 machines par sous réseau.

Application 02.

Soit une machine dont l'adresse IP est 172.30.0.141/25 :

a) Quelle est l'adresse de sous-réseau auquel la machine appartient ?
b) Quel est l'identificateur (le numéro) de la machine dans le sous réseau ?
c) Quelle est l'adresse de diffusion (broadcast) de ce sous réseau ?
d) Quelle est la plage des adresses valides au sein du même sous-réseau ?

Solution

a) Pour trouver l'adresse de sous réseau, on applique l'opération logique ET entre l'adresse IP de la machine et le masque de sous-réseau.
   On a l'adresse est 172.30.0.141/25 donc le masque est : 11111111.11111111.11111111.10000000
   10101100.00011110.00000000.10001101
   AND 11111111.11111111.11111111.10000000
   10101100.00011110.00000000.10000000 → 172.30.0.128.
   L'adresse de sous réseau est : 172.30.0.128.
b) Cette machine est la machine n° 13 dans le sous réseau. On a l'adresse de la machine est : 10101100.00011110.00000000.1**0001101** → 13.
c) L'adresse de diffusion est obtenue en mettant les bits de la partie machine à 1. Donc pour l'adresse de sous réseau 172.30.0.128 → 10101100.00011110.00000000.10000000, l'adresse de diffusion est 10101100.00011110.00000000.1**1111111** → 172.30.0.255.
d) Pour connaitre la plage des adresses possibles dans le même sous réseau, il suffit de prendre l'ensemble des adresses sans l'adresse de diffusion (172.30.0.255) ni de réseau (172.30.0.128), et donc pour notre sous réseau, on a la plage suivante : 172.30.0.129 à 172.30.0.254 (126 machines).

Application 03

a) Quel masque de sous-réseau faut-il utiliser pour une adresse classe B si on veut avoir de sous-réseaux d'au maximum 1000 ordinateurs ?
b) On dispose de l'adresse réseau 168.27.0.0. Proposez un masque de sous réseaux qui nous permet de définir au moins 14 sous-réseaux disposant chacun d'au moins 2000 adresses hôte.

Solution

a) Le réseau est de classe B, donc le masque par défaut : 11111111.11111111.00000000.00000000 → 255.255.0.0. Pour avoir 1000 ordinateurs par sous réseau, il faut laisser dans la partie machine au maximum 10 bits car 2^{10} - 2 = 1022 ≥ 1000. Ainsi, il reste pour la partie sous réseau 16 – 10 = 6 bits, et le masque de sous-réseaux est donc :
   11111111.11111111.11111100.00000000 → 255.255.252.0.
b) L'adresse 168.27.0.0 est de classe B, donc le masque par défaut est :
   11111111.11111111.00000000.00000000 → 255.255.0.0.

1er solution : Pour définir 14 sous réseau, il faut emprunter 4 bits de la partie machine car $2^4 - 2 = 14 \geq 1000$. Ainsi, il reste pour la partie machine 16 – 4 = 12 bits, ce qui donne $2^{12} – 2 = 4094 \geq 2000$ machines par sous réseau. Donc, le masque de sous-réseaux est donc :
11111111.11111111.11110000.00000000 → 255.255.240.0.
2eme solution : Pour avoir 2000 ordinateurs par sous réseau, il faut laisser dans la partie machine au maximum 11 bits car $2^{11} - 2 = 2046 \geq 2000$. Ainsi, il reste pour la partie sous réseau 16 – 11 = 5 bits, et le masque de sous-réseaux est donc :
11111111.11111111.11111000.00000000 → 255.255.248.0.

6.8 *IP version 4 et 6*

Avec la croissance rapide d'Internet et du nombre de machines qui y sont connectées, on a rencontré un problème de pénurie d'adresses IP publiques avec la version actuelle du protocole IP, qui est IPv4. Pour remédier à ce problème, un nouveau système d'adressage est développé, à savoir la norme IPv6 qui :

- Fournit un espace d'adressage beaucoup plus important que celui d'IPv4.
- Encode les adresses sur 128 bits au lieu de 32. Exemple : A524 :72D3 :2C80 :DD02 :0029 : EC7A :002B : EA73 c'est une adresse IP version 6.

7 Routage

Le routage est l'acheminement des données de la source vers la destination tout en empruntant le chemin le plus efficace. L'efficacité ici est déterminée selon différentes métriques, à savoir : le nombre de routeurs par lesquels le chemin passe, le délai des liaisons qui froment le chemin, leurs bandes passantes, leurs coûts, charge, fiabilité, etc. donc le chemin le plus efficace peut être le chemin le plus court, ou le moins chargé, ou le plus fiables, etc.

L'équipement qui assure la fonctionnalité du routage est le routeur, et les programmes qui l'implémentent sont appelés *algorithmes de routage*. Les algorithmes de routage utilisent diverses combinaisons des métriques pour établir les meilleures routes possibles pour les données. Ces routes une fois définies sont stockées dans des Tables de routage.

7.1 *Table de routage (TR)*

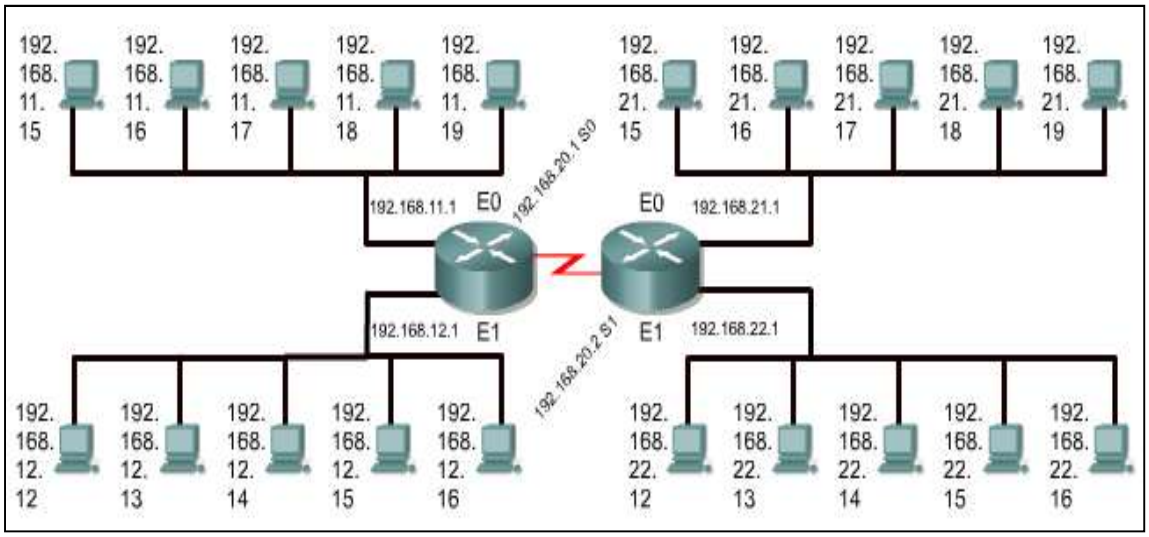
La table de routage contient les informations d'acheminement nécessaires à la transmission des données sur le réseau. C'est l'équivalent d'une base de données contenant les informations sur les routes construites par les algorithmes de routage, et utilisée dans le processus de sélection du chemin.

Les informations d'acheminement, les plus importantes, contenues dans les tables de routage sont :

- *Type de protocole :* le type de protocole de routage utilisé.
- *Le saut suivant :* la destination est soit directement connectée, sinon si elle est atteinte par le biais d'un autre routeur, on le désigne comme « saut suivant ».

- *Métrique de routage :* la métrique utilisée pour déterminer le meilleur chemin. Par exemple : le nombre de sauts dans le cas du protocole RIP.
- *Interfaces de sortie :* l'interface à partir de laquelle les données doivent être envoyées pour atteindre le saut suivant.

Exemple de table de routage. Considérons le réseau dans la figure suivante :



Les tables de routage deux routeurs sont :

Table de routage (routeur gauche)

@ réseau	Saut	Interface
192.168.11.0	0	E0
192.168.12.0	0	E1
192.168.20.0	0	S0
192.168.21.0	1	S0
192.168.22.0	1	S0

Table de routage (routeur droit)

@ réseau	Saut	Interface
192.168.21.0	0	E0
192.168.22.0	0	E1
192.168.20.0	0	S1
192.168.11.0	1	S1
192.168.12.0	1	S1

7.1.1 Utilisation des TR pour déterminer le chemin

Le routage d'un paquet d'une source à une destination peut être comparé à une personne conduisant sa voiture d'un endroit de la ville à un autre[1] :

Personne conduisant une voiture	**Routeur acheminant un paquet**

→ Le conducteur consulte une carte qui lui indique les rues à prendre pour arriver à sa destination	→ Le routeur consulte sa table de routage pour connaître les routes à suivre pour acheminer le paquet à sa destination.
→ Le conducteur passe par la voiture d'un carrefour à un autre.	→ Le paquet circule d'un routeur à un autre lors de chaque saut.
→ À chaque carrefour, le conducteur peut choisir de prendre à gauche, à droite ou de continuer tout droit.	→ Le routeur, aussi, choisit l'interface de sortie à partir de laquelle le paquet sera envoyé au prochain routeur.
→ Le conducteur prend ses décisions en fonction de certains facteurs (l'état du trafic, le nombre de voies, si une route est fréquemment fermée ou pas).	→ Le routeur prend sa décision en fonction de la charge, de la bande passante, du délai, du coût et de la fiabilité d'une liaison de réseau.

Donc, pour acheminer les données de la source vers la destination, les routeurs procèdent ainsi :

- A la réception d'un paquet, le routeur vérifie l'adresse de destination.
- Il cherche dans sa table de routage une correspondance de l'adresse de destination pour déterminer le chemin à suivre.
- Déterminer le chemin revient à définir l'interface à partir de laquelle le routeur va envoyer le paquet pour qu'il arrive à destination.
- Le premier routeur rencontré sur ce chemin est appelé saut suivant.
- Chaque saut correspond à un routeur rencontré sur le chemin du paquet, et le nombre de sauts constitue la distance parcourue.

7.1.2 Construction des tables de routage

Les routes d'une table de routage peuvent être des :

- Routes statiques : configurés manuellement par l'administrateur réseau.
- Routes dynamiques : acquises d'autres routeurs à l'aide d'un protocole de routage.

Donc, on peut remplir les tables de routages manuellement, ou bien on configure le routeur pour qu'il exécutent un protocole de routage, celui-ci s'occupe de remplissage de ces tables en échangeant des informations entre les autres routeurs.

7.1.3 Mise à jour des tables de routage

Afin de mettre à jour leurs tables de routage, les routeurs s'envoient des messages de mise à jour où ils échangent leurs tables de routages. Noter que le statut d'une route peut changer à tout moment (route devient défaillante, trop chargée, etc.), pour cela une mise à jour est nécessaire.

La mise à jour peut-être :

- Périodique, où à chaque intervalle de temps bien défini les routeurs procèdent à la mise à jour (échangent de leurs tabes).
- Lorsque des changements sont intervenus dans la topologie du réseau.

Cette mise à jour peut-être aussi par :

- Transmission de l'intégralité de la table.
- Transmission seulement des modifications.

7.2 *Protocole de routage*

Le rôle d'un protocole de routage est de :

- Créer les tables de routage, ainsi de les gérer et les mettre à jour.
- Déterminer le meilleur chemin possible pour acheminer les données de la source vers leur destination.

Etant donné que le réseau Internet est divisé en des partitions, appelées « système autonome ». Chaque système autonome comporte un ensemble de réseaux. Considérant cette partition, deux familles de protocoles de routage existent :

- *Les protocoles IGP (Interior Gateway Protocol.* C'est la classe des protocoles de routage qui acheminent les données au sein d'un système autonome.
- *Les protocoles EGP (Exterior Gateway Protocol)* (remplacé par BGP). C'est la famille des protocoles de routage qui acheminent les données entre les systèmes autonomes.

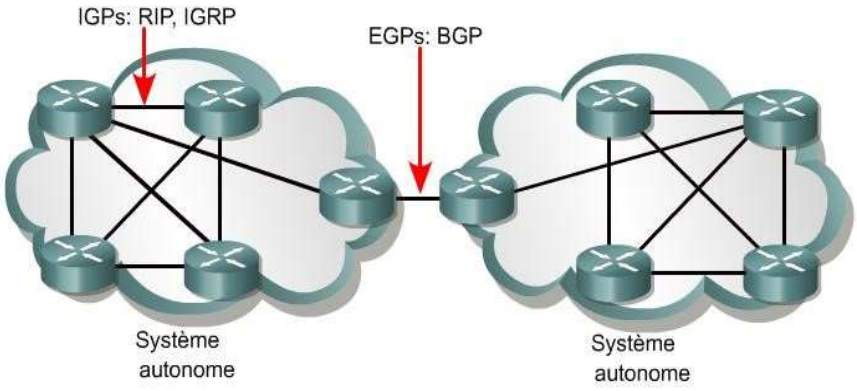


Figure 75. Routage à l'intérieur et à l'extérieur des systèmes autonomes du réseau Internet.

Dans ce qui suit, nous nous intéressons seulement aux protocoles IGP.

7.2.1 Protocoles IGP

L'objectif du protocole de routage est d'obtenir une table de routage avec les meilleures routes (les routes optimales de la source vers la destination). Le sens de meilleur et optimal dépend de la métrique utilisée dans le choix du chemin. Selon la métrique utilisée, deux types de protocoles IGP existent :

- *Protocoles à vecteur de distance.*
- *Les protocoles à état de liens.*

7.2.1.1 Les protocoles à vecteur de distance

Un protocole à vecteur de distance :

- Utilise la métrique « nombre de sauts » pour sélectionner le meilleur chemin, et donc la distance du chemin est représentée par le nombre de sauts vers la destination.
- Détermine la direction et la distance vers n'importe quelle destination, et sauvegardent ces informations dans une table de routage.
- Envoie périodiquement, soit l'intégralité ou une partie des entrées, des tables de routage aux routeurs adjacents. Donc, que ce soit il y a des modifications dans la topologie du réseau ou non, l'échange de table de routage aura lieu périodiquement.
- Lorsqu'un routeur reçoit une mise à jour de routage, il vérifie tous les chemins connus et modifie, le cas échéant, sa propre table de routage.

Un routeur exécutant un protocole à vecteur de distance procède ainsi :

- Il découvre son voisinage et les ajoute comme destination à sa table de routage avec une distance d'1 saut.
- Il échange sa table de routage avec ses voisins et met à jour sa propre table.
- Pour chaque nouvelle entrée reçue qui n'existe pas dans sa table de routage, il l'ajoute à sa table avec une distance augmentée d'un saut par rapport à celle reçue pour cette même entrée.

Les protocoles RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced IGRP) sont des exemples de protocoles à vecteur de Distance.

Exemple.

Un routeur RIP a La table de routage suivante :

table de routage du routeur

Destination	Routeur de prochain pas
200.1.1.0	Connexion directe
201.12.5.27	200.1.1.11
202.10.10.33	200.1.1.12
202.10.13.43	200.1.1.15
201.12.5.0	200.1.1.10
202.10.10.0	200.1.1.11
203.4.0.0	200.1.1.12

Pour chacune des destinations suivantes, spécifiez s'il est possible de router vers la destination, si oui, indiquez le prochain pas :

1) 202.10.10.12
2) 201.12.5.28
3) 203.4.3.11
4) 202.10.10.33
5) 202.10.13.100

Solution:

1) 202.10.10.12 : oui, le prochain pas est 200.1.1.11.
2) 201.12.5.28 : oui, le prochain pas est 201.1.1.10.
3) 203.4.3.11 : non cette adresse n'est pas routable.
4) 202.10.10.33 : oui, le prochain pas est 200.1.1.12.
5) 202.10.13.100 : non cette adresse n'est pas routable.

7.2.1.2 Les protocoles à état de liens

Les protocoles à état de liens sont conçus pour pallier les limitations des protocoles de routage à vecteur de distance. Pour un protocole de routage a état de liens :

- La métrique utilisée est l'« état de la liaison », à savoir la charge de la liaison, sa fiabilité, sa bande passante, etc.
- La mise à jour des tables de routage se faite seulement lorsque des changements sont intervenus dans la topologie du réseau, c'est-à-dire dès qu'un routeur a détecté la modification d'une liaison (route), il crée une MAJ de routage à état de liens concernant cette liaison.
- Des informations sur la topologie sont échangées entre les routeurs, ce qui permet à chaque routeur de construire une vision globale sur la topologie du réseau, contrairement aux protocoles à vecteur de distances où les routeurs ne sauvegardent que les meilleures distances vers les différentes destinations.
- Utilisant cette vision topologique, le protocole peut converger rapidement vers une table de routage optimale.
- La quantité d'informations transmises est importante et nécessitent beaucoup de ressources par rapport aux protocoles à vecteur de distance.
- A la différence d'un protocole à vecteur de distance, pour un protocole à état de liens chaque routeur possède :
    - Une table de ses voisins, appelé Neighbors Table.
    - Une base de données de la topologie du réseau, appelé Topology Database.
    - Une table de routage, appelé Routing table.

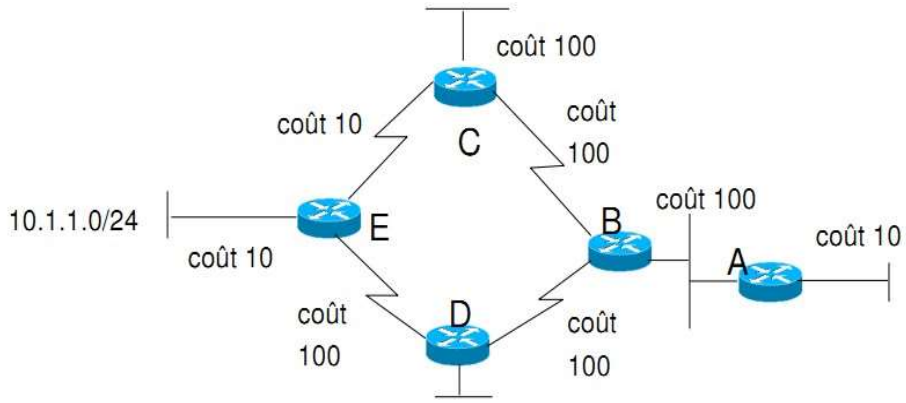
Un routeur exécutant un protocole à état de lien procède ainsi :

- Il découvre son voisinage et conserve une liste de tous ses voisins.
- Il échange les informations sur son voisinage avec ses voisins. Ainsi tous les routeurs échangent des informations topologiques entre eux.
- Chaque routeur stocke les informations topologiques reçues dans une base de données.
- Il exécute l'algorithme SPF pour calculer les meilleures routes.
- Il place ensuite la meilleure route vers chaque sous-réseau dans sa table de routage.

Les protocoles OSPF (*Open Shortest Path First*) et IS-IS (*Intermediate System-to Intermediate System*) sont des exemples de protocoles à état de liens.

Exemple.

Considérons le réseau dans la figure suivante :



Donc, selon un vecteur à distances, B dit à A : « le sous-réseau 10.1.1.0, métrique = 3 ». Cependant, selon un protocole états de liens, B donne à A toutes les informations topologiques en sa possession, et ainsi A va apprendre et calculer :

- A vers 10.1.1.0/24 : par C, coût 220
- A vers 10.1.1.0/24 : par D, coût 310

Ainsi, A va mettre dans sa table de routage la route vers 10.1.1.0/24 par C.

7.3 *Protocole routé*

Les protocoles de routage permettent aux routeurs de déterminer le meilleur chemin possible pour acheminer les données de la source vers leur destination. Une fois le chemin est défini, le protocole IP transporte les données sur le réseau. On dit que IP est un *protocole routé.*

Les caractéristiques du protocole IP se résument comme suit :

- IP est le système d'adressage hiérarchique des réseaux le plus largement utilisé.
- Il définit le format et l'usage des champs dans un paquet.
- C'est un protocole non orienté connexion (aucune connexion à un circuit dédié n'est établie avant la transmission).
- Peu fiable (Il ne s'assure pas de la bonne livraison des données envoyées sur le réseau)
- Axé sur l'acheminement au mieux (best-effort Delivery).
- Il détermine le meilleur chemin pour les données en fonction du protocole de routage.

7.3.1 Le paquet IP

Le paquet IP a la structure suivante :

0 4	8		16 19	24 31
VERS	HLEN	Type de service	Longueur totale	
Identification			Indicateurs	Décalage de fragment
Durée de vie		Protocole	Somme de contrôle d'en-tête	
Adresse IP source				
Adresse IP de destination				
Options IP (s'il y a lieu)				Remplissage
Données				
. . .				

- ***Version*** **:** indique le format de l'en-tête du paquet IP selon la version d'IP (IPv4 ou IPv6).
- ***Longueur d'en-tête IP (HLEN) :*** indique la longueur de l'en-tête du datagramme.
- ***Type de service (ToS) :*** codé sur 8 bits, contient des informations destinées au protocole de couche supérieure.
- ***Longueur totale (16 bits) :*** spécifie la taille totale du paquet en octets, données et en-tête inclus.
- ***Identification (16 bits) :*** identifie le datagramme actuel (le numéro de séquence).
- ***Drapeaux (3 bits) :*** les deux bits de poids faible contrôlent la fragmentation. Un bit indique si le paquet peut être fragmenté ou non, et l'autre si le paquet est le dernier fragment.
- ***Durée de vie (TTL) :*** indique le nombre de sauts par lesquels un paquet peut passer. Lorsque le compteur atteint zéro, le paquet est éliminé.
- ***Protocole (8 bits) :*** indique le protocole de couche supérieure (TCP ou UDP) qui va recevoir les paquets.
- ***Somme de contrôle de l'en-tête (16 bits) :*** aide à garantir l'intégrité de l'en-tête IP.
- ***Adresse source (32 bits) :*** contient l'adresse IP du nœud émetteur du paquet.
- ***Adresse de destination (32 bits) :*** contient l'adresse IP du nœud destinataire.
- ***Options :*** prend en charge diverses options (la sécurité, etc.).
- ***Remplissage :*** assure que l'entête IP est un multiple de 32 bits (des zéros sont ajoutés à ce champ).
- ***Données :*** contient les données des couches supérieures.

8 Conclusion

La couche réseau trouve toute son utilité dans les réseaux WAN où il faut trouver toute une route pour acheminer les données d'un équipement à un autre. Ce chapitre a présenté l'essentiel de la couche réseau qui assure cette tâche tout en détaillant les différentes procédures qui contribuent à cette fin, à savoir l'adressage, le routage, etc. Pour ce faire, les différentes procédures sont présentées tout en étudiant le protocole IP vu que c'est lui qui les assure.