TD Adressage IP

1. Adresses IP

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP (*Internet Protocol*), qui utilise des adresses numériques, appelées adresses IP, composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Par exemple, *193.49.146.124* est l'adresse IP du serveur Web du département informatique de l'université d'Angers (www.info.univ-angers.fr). Chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau.

Pour communiquer avec un ordinateur situé sur un réseau sur lequel on est connecté, il suffit alors de connaître son adresse IP pour le situer grâce à une table de correspondance, construite par le protocole ARP, permettant de connaître une adresse physique (adresse de la carte réseau) à partir de l'adresse logique (adresse IP). Néanmoins, dans les très grands réseaux (et Internet en est un énorme), cette résolution d'adresse peut s'avérer problématique puisque cela impose de disposer de gigantesques tables de correspondance permettant de situer l'ensemble des machines connectées, ce qui induit des temps de réponse très grands.

Ainsi, plutôt qu'un énorme réseau unique, Internet représente l'interconnexion d'une multitude de petits réseaux, et c'est au sein de ces petits réseaux que l'on donne des adresses aux machines pour leur envoyer l'information. Cela permet de séparer le problème de localisation d'une machine en deux sous-problèmes : dans un premier temps situer le réseau sur lequel la machine à joindre se trouve, et dans un second identifier la machine sur ce réseau. Ce découpage permet de simplifier très largement le problème de résolution d'adresses.

Néanmoins, cela implique de connaître deux adresses distinctes : celle du réseau sur lequel la machine se trouve et celle de la machine sur ce réseau. L'adresse IP d'une machine comporte en fait ces deux d'informations :

- Une partie des bits de l'adresse IP désigne le réseau (*netID*),
- Une autre désigne les ordinateurs de ce réseau (*host-ID*).

C'est là où le masque de sous-réseau entre en jeu, c'est lui qui joue le rôle de séparateur entre ces deux adresses. C'est lui qui définit quelle partie de l'adresse correspond au réseau et quelle autre correspond à la machine sur celui-ci. Le masque est donc indissociable de l'adresse IP. Une adresse seule ne voudra rien dire puisqu'on ne saura pas quelle est la partie réseau et quelle est la partie machine. De la même façon, un masque seul n'aura pas de valeur puisqu'on n'aura pas d'adresse sur laquelle l'appliquer. L'adresse IP et le masque sont donc liés l'un à l'autre.

2. Rappels sur le codage binaire

Avant d'entrer plus dans le détail en ce qui concerne les adresses IP et les masques de sous-réseau, faisons un rapide rappel des notions de codage binaire qui nous seront utiles pour la suite...

Dans un ordinateur, les données sont représentées sous forme binaire, pour des raisons de commodité de stockage et de transfert. Sous cette forme, seules deux valeurs sont autorisées : 0 et 1. Les autres entiers peuvent toutefois être représentés : 0 (0), 1 (1), 10 (2), 11 (3), 100 (4), 101 (5), ... etc.

L'unité est le bit (0 ou 1). Les bits sont regroupés en octets (8 bits). 1 Ko (*kilo octet*) =2^{10} octets=1024 octets, 1 Mo (*méga octet*) = 2^{10} Ko, 1 Go (*giga octet*) = 2^{10} Mo.

Tout nombre entier *N* peut être exprimé de la manière suivante dans la base *b* :
$N_b = C_{n-1}b^{n-1} + C_{n-2}b^{n-2} + C_{n-3}b^{n-3} + \ldots + C_1b^1 + C_0b^0$
*o*ù *b* désigne la base, C_i des coefficients tels que $0 \leq C_i \leq b - 1$ et *n* le nombre de chiffres pour écrire *N* dans la base *b*. Ainsi, dans la base *b*, N_b s'écrit comme suit : $N_b = C_{n-1}\,C_{n-2}\ldots C_0$.
Exemple en base 10, $573 = 5.10^2+7.10^1+3.10^0$ (*b=10, C_0=3, C_1=7, C_2=5)*

2.1. Conversion de base 10 en base 2

La méthode la plus simple consiste à faire successivement des divisions entières par 2. Par exemple, pour convertir 167 (base 10) en base 2.

Nombre	Résultat de la division par 2	Reste
167	83	1
83	41	1
41	20	1
20	10	0
10	5	0
5	2	1
2	1	0
1	0 *(Condition d'arrêt)*	1

Le bit le plus significatif est le reste de la dernière division et le bit le moins significatif est le reste de la première division. Donc le résultat est : $167_{10}=10100111_2$

2.2. Conversion de base 2 en base 10

La conversion d'un nombre binaire naturel en base décimale se fait en utilisant la formule ci-dessus. Exemple : 00101101 => $0*2^7+0*2^6+1*2^5+0*2^4+1*2^3+1*2^2+0*2^1+1*2^0= 45$

2.3. Conversion d'une adresse IP de base 10 en base 2

Pour convertir une adresse IP en base 10 de la forme A.B.C.D en binaire, il suffit de convertir sur huit bits chacun des 4 nombres A, B, C et D séparément.

2.4. Conversion d'une adresse IP de base 2 en base 10

Pour convertir une adresse IP en base 2 en base 10, il s'agit de calculer le décimal correspondant à chaque octet de l'adresse (chaque groupe de huit bits).

3. Les masques de sous-réseau

Comme l'adresse IP, le masque est une suite de 4 octets, soit 32 bits. Chacun des bits d'un masque détermine si le bit correspondant dans l'adresse IP code pour l'adresse réseau ou l'adresse machine. Ainsi, l'association entre une adresse IP et un masque permet de séparer ces deux informations.

La partie réseau s'obtient en réalisant un ET logique entre les deux séries d'octets :

```
      192.168.0.140      = 11000000.10101000.00000000.10001100
ET    255.255.255.128    = 11111111.11111111.11111111.10000000
-------------------------------------------------------------------------------
      192.168.0.128      = 11000000.10101000.00000000.10000000
```

La partie machine s'obtient en réalisant un ET logique entre l'adresse IP et le complément à 1 du masque :

```
                192.168.0.140                 = 11000000.10101000.00000000.10001100
ET  Complément_a_1(255.255.255.128)   = 00000000.00000000.00000000.01111111
-------------------------------------------------------------------------------------------------------------
                0.0.0.12                      = 00000000.00000000.00000000.00001100
```

Ainsi, les bits à 1 du masque déterminent la partie réseau de l'adresse et les bits à 0 ceux de la partie machine.

3.1. Adresses spécifiques (réseau, broadcast)

Il existe des adresses spécifiques au sein d'un réseau. La première adresse d'une plage ainsi que la dernière ont un rôle particulier. La première adresse d'une plage représente l'adresse du réseau. Celle-ci est très importante car c'est grâce à elle qu'on peut identifier les réseaux et router les informations d'un réseau à un autre. La dernière adresse d'une plage représente ce que l'on appelle l'adresse de broadcast. Cette adresse est celle qui permet de faire de la diffusion à toutes les machines du réseau. Ainsi, quand on veut envoyer une information à toutes les machines, on utilise cette adresse.

3.2. Choisir un masque selon un nombre de machines

La plupart du temps, le choix de l'adressage se fait en fonction des besoins exprimés, et des limites de ce que l'on a le droit de faire. Une certaine plage vous est allouée par votre fournisseur d'accès. Il est alors possible de découper cette plage en différents réseaux. Ce découpage se fait en fonction du masque que l'on choisit.

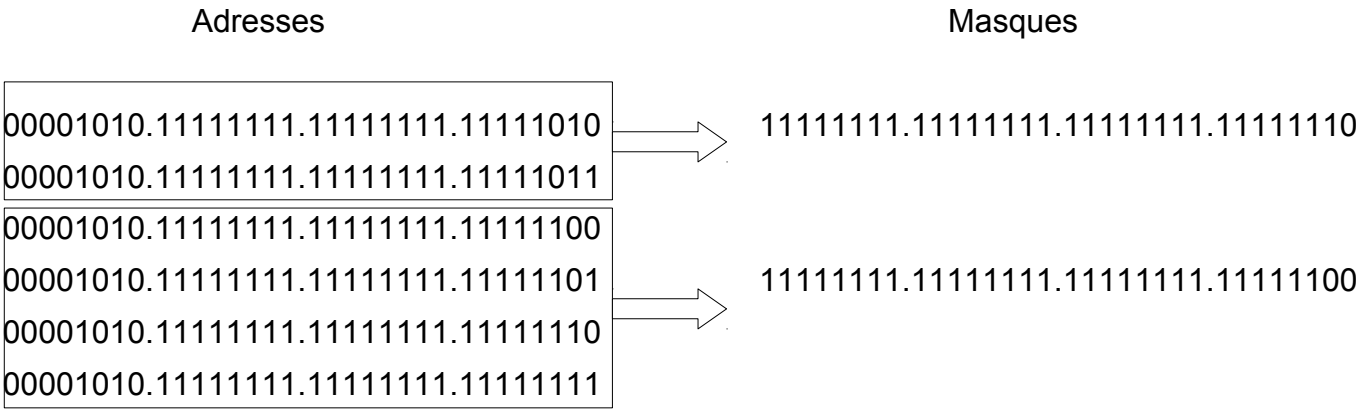
Le masque détermine le nombre de machines qu'il pourra y avoir sur un réseau. C'est donc souvent selon les nombres de machines que l'on veut connecter à chaque réseau que l'on choisit son masque. Étant donné que l'on travail en binaire, le nombre de machines possible au sein d'un réseau sera une puissance de 2. Pour un nombre de machines donné, il faudra donc choisir la puissance de 2 immédiatement supérieure pour pouvoir adresser les machines. Ainsi, disons que l'on possède le réseau 193.225.34.0/255.255.255.0 et que l'on veut faire un sous-réseau de 60 machines au sein de celui-ci. On veut 60 machines, il faut ajouter deux adresses pour le réseau et le broadcast, ce qui fait 62 adresses au total. La puissance de 2 supérieure à 62 est 64, soit 2^6. Donc dans notre masque, 6 bits seront à 0 pour identifier la partie machine, et les 26 bits restants seront à 1. Ce qui donne: 11111111.11111111.11111111.11000000 soit 255.255.255.192 en décimal. 4 plages de sous-réseau sont alors disponibles :

- De 193.225.34.0 à 193.225.34.63
- De 193.225.34.64 à 193.225.34.127
- De 193.225.34.128 à 193.225.34.191
- De 193.225.34.192 à 193.225.34.255

3.3. Choisir un masque pour couvrir une plage d'adresses donnée

Déterminer un masque pour un plage d'adresses donnée n'est pas toujours chose aisée : il n'est pas forcément évident qu'il soit possible de couvrir un ensemble des adresses en ne définissant qu'un seul réseau. Par exemple, si l'on dispose des adresses de 10.255.255.250 à 10.255.255.255, il n'est pas possible de déterminer un masque définissant un réseau englobant l'ensemble des adresses sans en inclure d'autres : un masque de 255.255.255.248 associé à

l'ensemble de ces adresses inclut les adresses 10.255.255.248 et 10.255.255.249 dans le réseau, alors que des masques supérieurs divisent la plage en plusieurs réseaux. L'objectif est alors de découper la plage en un minimum de sous-réseaux. Pour notre exemple cela donne :



Une méthode simple pour découper au mieux (en un minimum de sous-réseaux) une plage d'adresses donnée est la suivante :

1. Soit x la première adresse non encore associée à un masque
2. Soit y le masque 255.255.255.255
3. Tant que y ne permet pas l'inclusion d'adresses hors de la plage, passer son dernier bit dont la valeur est 1 à 0
4. Passer le premier bit du masque y dont la valeur est 0 à 1
5. Associer le masque y à toutes les adresses pouvant être sur le même réseau que x selon y. Si il reste des adresses sans masque reprendre en 1.

3.4. Classes d'adresses

Comme nous l'avons vu, le masque de sous-réseau permet de segmenter l'ensemble des adresses de l'Internet en différents réseaux. Mais cette segmentation ne s'est pas faite n'importe comment : on a découpé la plage d'adresses disponible en cinq parties distinctes. Les classes A, B, C, D et E, que l'on appelle aussi adresses globales.

Classe A: Premier bit de l'adresse à 0, et masque de sous-réseau en 255.0.0.0. Ce qui donne la plage d'adresses 0.0.0.0 à 126.255.255.255 soit 16 777 214 adresses par réseau de classe A

Classe B: Deux premiers bits de l'adresse à 10 (1 et 0), et masque de sous-réseau en 255.255.0.0. Ce qui donne la plage d'adresses 128.0.0.0 à 191.255.255.255 soit 65 534 adresses par réseau de classe B

Classe C: Trois premiers bits de l'adresse à 110, et masque de sous-réseau en 255.255.255.0. Ce qui donne la plage d'adresses 192.0.0.0 à 223.255.255.255 soit 255 adresses par réseau de classe C

Classe D: Quatre premiers bits de l'adresse à 1110, et masque de sous-réseau en 255.255.255.240. Ce qui donne la plage d'adresses 224.0.0.0 à 239.255.255.255 soit 15 adresses par réseau de classe D

Classe E: Quatre premiers bits de l'adresse à 1111, et masque de sous-réseau en 255.255.255.240. Ce qui donne la plage d'adresses 240.0.0.0 à 255.255.255.255

Les classes A, B et C, sont réservées pour les utilisateurs d'Internet (entreprises, administrations,

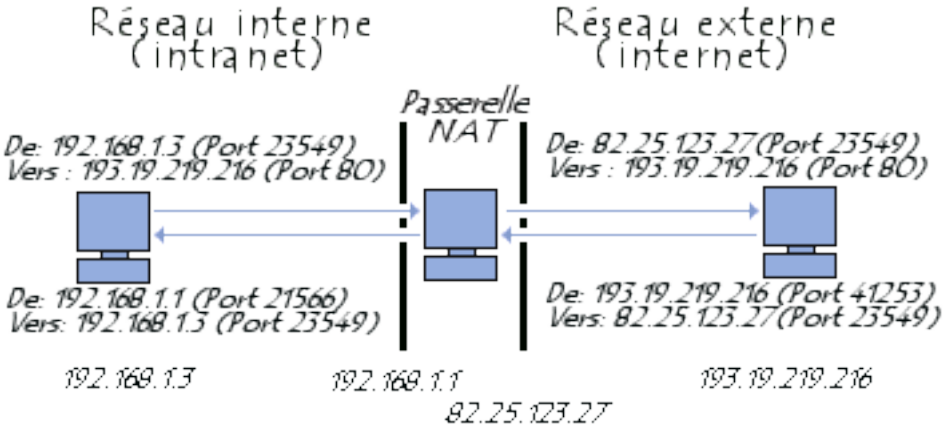
fournisseurs d'accès, etc) La classe D est réservée pour les flux multicast et la classe E est réservée à la recherche.

En respectant strictement ces classes, une entreprise demandant 80 000 adresses se verrait attribuer un réseau de classe A, et gâcherait par la même occasion (16 777 214 - 80 000=) 16 697 214 adresses !!! Il y a aujourd'hui pénurie d'adresses IP (les adresses que nous manipulons étant des adresses IPv4) mais une nouvelle version d'IP, Ipv6, a été créée et sera bientôt déployée massivement. Étant donné que l'adressage par classes s'est avéré incompatible avec l'évolution d'Internet, il a fallu imaginer un nouveau modèle qui simplifie à la fois le routage et permette un adressage plus fin. Pour cela, on a créé l'adressage CIDR (Classless Inter-Domain Routing). Cet adressage ne tient pas compte des classes globales et autorise l'utilisation de sous-réseaux au sein de toutes les classes d'adresses. Ainsi, une entreprise désirant 80 000 adresses ne se verra plus attribuer une classe A complète, mais un sous-réseau de cette classe A. Par exemple, on lui fournira non plus 16 millions d'adresses, mais 131 072 (la puissance de deux supérieure à 80 000) Ainsi les 16 millions d'adresses restantes pourront être utilisées pour d'autres entités. L'adressage CIDR ne tient donc plus du tout compte des masques associés aux classes d'adresses globales. On s'affranchit ainsi du découpage arbitraire et peu flexible en classes.

4. La translation d'adresses

Le mécanisme de translation d'adresses (en anglais *Network Address Translation* noté NAT) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4. En effet, le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à Internet de l'être.

Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation (littéralement une « traduction ») entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle.



Outre l'économie d'adresses, le mécanisme de translation d'adresses permet de sécuriser le réseau interne étant donné qu'il camoufle complètement l'adressage interne. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de la même adresse IP.

L'organisme gérant l'espace d'adressage public (adresses IP routables) a alors définit un espace d'adressage privé permettant à toute organisation d'attribuer des adresses IP aux machines de son réseau interne sans risque d'entrer en conflit avec une adresse IP publique allouée par l'IANA.

Ces adresses dites non-routables correspondent aux plages d'adresses suivantes (RFC 1918) :

- Classe A : plage de 10.0.0.0 à 10.255.255.255 ;
- Classe B : plage de 172.16.0.0 à 172.31.255.255 ;
- Classe C : plage de 192.168.0.0 à 192.168.255.55 ;

Toutes les machines d'un réseau interne, connectées à internet par l'intermédiaire d'un routeur et ne possédant pas d'adresse IP publique doivent utiliser une adresse contenue dans l'une de ces plages. Pour les petits réseaux domestiques, la plage d'adresses de 192.168.0.1 à 192.168.0.255 est généralement utilisée.

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP. C'est la raison pour laquelle le terme de « mascarade IP » (en anglais *IP masquerading*) est parfois utilisé pour désigner le mécanisme de translation d'adresse dynamique.

Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables le NAT dynamique utilise le mécanisme de translation de port (PAT - *Port Address Translation*), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

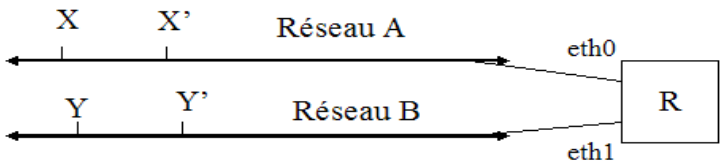
5. Le Routage IP

Pour interconnecter des réseaux IP, on utilise des routeurs IP. Les routeurs sont des boîtiers dédiés possédant un certain nombre d'interfaces (Ethernet, liaison série, …) permettant la communication entre les machines des différents réseaux. Pour que toutes les machines puissent envoyer un datagramme IP à n'importe quelle autre, il faut configurer chaque machine et chaque routeur. Pour cela, il faudra notamment configurer la table de routage de chaque routeur et chaque machine. On parle alors de routage IP.

Philosophie du routage IP :

- Aucune machine ni aucun routeur ne connaît le plan complet du réseau.
- Chaque machine et chaque routeur possède une table de routage : lorsqu'une machine veut envoyer un datagramme IP à une autre, elle regarde sa table de routage qui lui dit :
  - si le destinataire est directement accessible grâce à une interface
  - sinon l'adresse IP du routeur auquel il faut envoyer le datagramme. Ce routeur doit être directement accessible
- On indique à chaque étape le routeur suivant : on parle de "next hop routing".

Un premier exemple



8

Sur ce premier exemple d'interconnexion, 2 réseaux Ethernet A et B, comportant chacun deux machines (X et X' pour A et Y et Y' pour B), sont reliés par un routeur R. Lors de l'envoi d'un message, deux cas sont alors possibles :

- Lorsque X veut envoyer un datagramme à X', X va envoyer ce datagramme directement sur sa carte Ethernet sans passer par le routeur : on parle alors de remise directe.
- Lorsque X veut envoyer un datagramme IP à Y, X va envoyer ce datagramme à R qui le retransmettra à Y : on parle alors de remise indirecte.

Supposons maintenant les adresses IP suivantes pour les différentes entités du réseau :

- Sur le réseau A, on utilise les adresses IP du réseau 200.50.60.0 de masque 255.255.255.0.
- Sur le réseau B, on utilise les adresses IP du réseau 200.50.61.0 de masque 255.255.255.0.
- Machine X : une interface eth0 d'adresse IP 200.50.60.1
- Machine X' : une interface eth0 d'adresse IP 200.50.60.2
- Machine Y : une interface eth1 d'adresse IP 200.50.61.1
- Machine Y' : une interface eth1 d'adresse IP 200.50.61.2
- Le routeur R a 2 interfaces et il aura donc 2 adresses IP :
  - eth0 d'adresse IP 200.50.60.3
  - eth1 d'adresse IP 200.50.61.3

Une table de routage est constituée de lignes comportant des quadruplets : adresse, masque, passerelle, et interface permettant de savoir comment envoyer (quelle passerelle et interface utiliser) un message à une unité du réseau correspondant aux champs adresse et masque.

Dans notre exemple, la table de routage de la machine X est la suivante :

Adresse	Masque	Passerelle	Interface
200.50.60.0	255.255.255.0	200.50.60.1	200.50.60.1
200.50.61.0	255.255.255.0	200.50.60.3	200.50.60.1

- Dans la première ligne, la passerelle est égale à l'interface : cela signifie que pour envoyer un datagramme à une machine du réseau 200.50.60.0 de masque 255.255.255.0, X peut remettre directement ce datagramme au destinataire grâce à son interface 200.50.60.1.
- Dans la deuxième ligne, la passerelle est différente de l'interface : cela signifie que pour envoyer un datagramme à une machine du réseau 200.50.61.0 de masque 255.255.255.0, la remise est indirecte et X doit envoyer ce datagramme au routeur 200.50.60.3 grâce à son interface 200.50.60.1.

5.1. Route par défaut

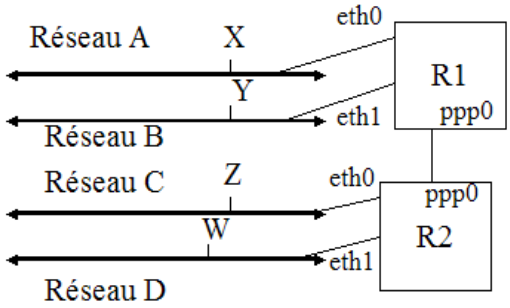
La table de X aurait pu alternativement s'écrire de cette façon :

Adresse	Masque	Passerelle	Interface
200.50.60.0	255.255.255.0	200.50.60.1	200.50.60.1
0.0.0.0	0.0.0.0	200.50.60.3	200.50.60.1

On a alors défini une route par défaut :

- Si X doit envoyer un datagramme IP à une machine du réseau 200.50.60.0, X doit envoyer directement ce datagramme sur son interface 200.50.60.1.
- Pour toutes les autres adresses IP (c'est la signification de 0.0.0.0 / 0.0.0.0), X envoie ce datagramme à l'adresse IP 200.50.60.3
- L'adresse IP 200.50.60.3 s'appelle la passerelle par défaut de X

Deuxième exemple



20

Sur ce deuxième exemple d'interconnexion, 4 réseaux Ethernet A, B, C et D sont reliés par deux routeurs R1 et R2, A et B sont reliés à R1 et C et D à R2. Supposons les adresses IP suivantes:

- Adresses IP des réseaux
  - Le réseau A utilise les adresses IP 200.50.60.0 de masque 255.255.255.0
  - Le réseau B utilise les adresses IP 200.50.61.0 de masque 255.255.255.0
  - Le réseau C utilise les adresses IP 200.50.62.0 de masque 255.255.255.0
  - Le réseau D utilise les adresses IP 200.50.63.0 de masque 255.255.255.0
- Adresses des machines
  - X possède une interface eth0 d'adresse IP 200.50.60.1
  - Y possède une interface eth0 d'adresse IP 200.50.61.1
  - Z possède une interface eth0 d'adresse IP 200.50.62.1
  - W possède une interface eth0 d'adresse IP 200.50.63.1
- Adresses IP des routeurs
  - R1 possède 3 interfaces : eth0 d'adresse IP 200.50.60.2, eth1 d'adresse IP 200.50.61.2 et ppp0 d'adresse IP 200.50.64.1.
  - R2 possède 3 interfaces : eth0 d'adresse IP 200.50.62.2, eth1 d'adresse IP 200.50.63.2 et ppp0 d'adresse IP 200.50.64.2.

Voir http://fr.wikibooks.org/wiki/Réseaux_TCP/IP_:_le_routage_IP_statique pour les tables de routage des deux exemples.