

Protocoles et services de base internet

Copyright © GUINKO Tonguim Ferdinand - IBAM - Université
de Ouagadougou
La reproduction non autorisée d'une œuvre protégée constitue un
délit

21 octobre 2009

Table des matières

| | | |
|----------|---------------------------------------|----------|
| 1 | Adressage ip, ports, socket | 3 |
| 1.1 | Ports | 3 |
| 1.1.1 | Port matériel | 3 |
| 1.1.2 | Port logiciel | 3 |
| 1.1.2.1 | Définition | 3 |
| 1.1.2.2 | Utilité | 4 |
| 1.1.2.3 | Attribution des ports | 4 |
| 1.2 | Socket | 5 |
| 1.3 | Adressage IP | 5 |
| 1.4 | Définition d'une adresse IP | 5 |
| 1.4.1 | Les classes d'adresses | 6 |
| 1.4.1.1 | Généralités | 6 |
| 1.4.1.2 | Étendue de chaque classe | 7 |
| 1.4.1.3 | Les réseaux privés | 8 |
| 1.4.2 | Le masque de sous réseau | 9 |
| 1.5 | Liens utiles | 10 |

Chapitre 1

Adressage ip, ports, socket

1.1 Ports

1.1.1 Port matériel

Un port matériel est conçu pour accueillir un certain type de périphériques. Il est soumis à des normes aussi bien sur ses caractéristiques physiques (forme, considérations électriques ou optiques) que logiques (quel fils/patte/connecteur sert à quoi, que signifie tel ou tel signal en entrée, en sortie).

Les ports matériels se répartissent en :

- ports internes destinés soit à relier à une carte mère des périphériques internes au boîtier de l'ordinateur (disques, barrettes de mémoire ou même processeur en considérant un socket comme un port matériel) soit à insérer une carte d'extension enfichable sur un bus interne (on parle alors de connecteur d'extension).
- ports externes permettant de communiquer avec différents périphériques, souvent via un câble, quoique on trouve aussi notamment dans le cas des portables des connecteurs d'extension reliés à un bus (par exemple PCCard).

1.1.2 Port logiciel

1.1.2.1 Définition

Correspondant à la couche de transport du modèle OSI, la notion de port logiciel permet, sur un ordinateur donné, de distinguer différents interlocuteurs. Ces interlocuteurs sont des programmes informatiques qui, selon les cas, écoutent ou émettent des informations sur ces ports. Un port est distingué par son numéro. Pour fonctionner sur un ordinateur, un programme doit avoir accès au système d'exploitation, et doit donc ouvrir des portes pour pouvoir entrer dans le système d'exploitation. Lorsqu'on quitte le programme, la porte n'a plus besoin d'être ouverte. Les problèmes de sécurité surviennent lorsque certains programmes oublient de refermer ces dites portes (les "Ports"), ou même tout simplement lorsque la configuration mal maîtri-

sée de l'ordinateur ouvre des ports sans aucune utilité. Cela donne lieu à des failles de sécurité informatiques, car si une porte n'est pas refermée, n'importe qui peut l'emprunter.

1.1.2.2 Utilité

Grâce à cette abstraction, on peut exécuter plusieurs logiciels serveurs sur une même machine, et même simultanément des logiciels clients et des serveurs, ce qui est fréquent sur les systèmes d'exploitation multitâches et multiutilisateurs.

1.1.2.3 Attribution des ports

Pour chaque port, un numéro lui est attribué, qui est codé sur 16 bits, ce qui implique qu'il existe un maximum de 65 536 ports (2¹⁶) par ordinateur ¹. L'attribution des ports est faite par le système d'exploitation, sur demande d'une application. Cette dernière peut demander à ce que le système d'exploitation lui attribue n'importe quel port, à condition qu'il ne soit pas déjà attribué. L'application peut ensuite l'utiliser comme bon lui semble. Lorsqu'un logiciel client veut dialoguer avec un logiciel serveur, aussi appelé service, il a besoin de connaître le port écouté par ce dernier. Les ports utilisés par les services devant être connus par les clients, les principaux types de services utilisent des ports qui sont dits réservés. Par convention, ce sont tous ceux compris entre 0 et 1 023 inclus et leur utilisation par un logiciel serveur nécessite souvent que celui-ci s'exécute avec des droits d'accès particulier. Les services utilisant ces ports sont appelés les WellKnown Services (les services les plus connus).

Sur une machine de type UNIX, le fichier */etc/services* rappelle la liste de ces services célèbres, dont les plus connus et les plus utiles sont notamment les ports :

- 21, pour l'échange de fichiers via FTP
- 22, pour l'accès à un shell sécurisé Secure SHell
- 23, pour le port telnet
- 25, pour l'envoi d'un courrier électronique via un serveur dédié SMTP
- 80, pour la consultation d'un serveur HTTP par le biais d'un navigateur web
- 110, pour la récupération de son courrier électronique via POP
- 143, pour la récupération de son courrier électronique via IMAP (IMAP ² est doté de fonctionnalités plus avancées que POP ³, voir les articles respectifs pour plus de détails)
- 443, pour les serveurs Web sécurisés HTTPS

Il faut toutefois noter que les conventions cidessus peuvent ne pas être respectées pourvu que le client et le serveur soient cohérents entre eux et que le nouveau numéro

¹Liste des ports :

<http://www.iana.org/assignments/portnumbers>

<http://nallignet.free.fr/articles.php?lng=frpg=48>

http://fr.wikipedia.org/wiki/Liste_des_ports_logiciels

²<http://fr.wikipedia.org/wiki/Imap>

³<http://fr.wikipedia.org/wiki/Pop3>

choisi ne soit pas déjà utilisé par ailleurs. La plupart des logiciels de communication permettent d'accéder à ce réglage ce qui est utile dans certains cas.

1.2 Socket

Dans le contexte des logiciels, on peut le traduire par « connecteur réseau ». Apparu dans les systèmes UNIX, un socket est un élément logiciel qui est aujourd'hui répandu dans la plupart des systèmes d'exploitation. Il s'agit d'une interface logicielle avec les services du système d'exploitation, grâce à laquelle un développeur exploitera facilement et de manière uniforme les services d'un protocole réseau.

Il lui sera ainsi par exemple aisé d'établir une session TCP, puis de recevoir et d'expédier des données grâce à elle. Cela simplifie sa tâche car cette couche logicielle, de laquelle il requiert des services en appelant des fonctions, masque le nécessaire travail de gestion du réseau, pris en charge par le système. Le terme socket désigne en pratique chaque variable employée dans un programme afin de gérer l'une des sessions. La combinaison « adresse IP :numéro de port » constitue ce que l'on appelle une « socket » (qui veut dire à peu près « connecteur » en anglais). Un socket identifie pleinement le service qui est concerné sur une machine donnée.

1.3 Adressage IP

Il est bon de savoir qu'il existe une adresse « MAC » (Media Access Control), écrite normalement en « dur » dans la ROM de l'interface réseau et donc théoriquement ineffaçable et infalsifiable (mais ce n'est que la théorie, tous les pirates vous le diront). Cette adresse est réputée unique et décidée par le constructeur de la carte. Elle est la seule adresse exploitée au niveau 2 pour l'identification des hôtes qui dialoguent. Cette méthode ne permettant pas l'interconnexion de réseaux, il est nécessaire d'ajouter dans la couche supérieure (niveau 3), une adresse logique qui sera attribuée par l'administrateur du réseau, en coordination avec les organismes chargés de gérer l'attribution de ces adresses. Dans le cas qui nous intéresse ici, il s'agit de l'adresse IP.

1.4 Définition d'une adresse IP

Internet Protocol

Dans sa version 4 (IPv4), IP définit une adresse sur 4 octets, soit 32 bits. Chaque adresse IP de 32 bits identifie un emplacement d'un système hôte sur le réseau de la même façon qu'une adresse de rue identifie une maison dans une ville.

De la même façon qu'une adresse de rue a un format standard en deux parties "un nom de rue et un numéro de maison", chaque adresse IP est séparée en deux parties : un ID de réseau et un ID d'hôte.

L'ID de réseau, également appelé adresse de réseau (NetID ou SubnetID), identifie un segment de réseau unique dans un réseau d'interconnexion TCP/IP plus grand. Tous les systèmes associés au même réseau et partageant l'accès à ce réseau ont un ID de réseau commun dans leur adresse IP complète. Cet ID est également utilisé pour identifier de manière unique chaque réseau dans le réseau d'interconnexion le plus grand. L'ID d'hôte, également appelé adresse d'hôte (HostID), identifie un nœud TCP/IP (une station de travail, un serveur, un routeur ou un autre périphérique TCP/IP) dans chaque réseau. L'ID d'hôte de chaque périphérique identifie un seul système dans son propre réseau. Voici un exemple d'adresse IP de 32 bits : 10000100 01101011 00010000 11001001. Pour faciliter l'adressage IP, les adresses sont exprimées en notation décimale pointée. L'adresse IP de 32 bits est segmentée en quatre octets de 8 bits. Les octets sont convertis en décimales (système de numérotation base 10) et sont séparés par des points. C'est la raison pour laquelle, dans l'exemple précédent, l'adresse IP est 132.107.16.201 une fois convertie en notation décimale pointée.

L'illustration suivante présente un exemple de vue d'une adresse IP (132.107.16.201) telle qu'elle est divisée dans les sections de réseau et d'ID d'hôte. La partie d'ID de réseau (132.107) est signalée par les deux premiers nombres de l'adresse IP. La partie d'ID d'hôte (16.201) est signalée par les deux derniers nombres de l'adresse IP.

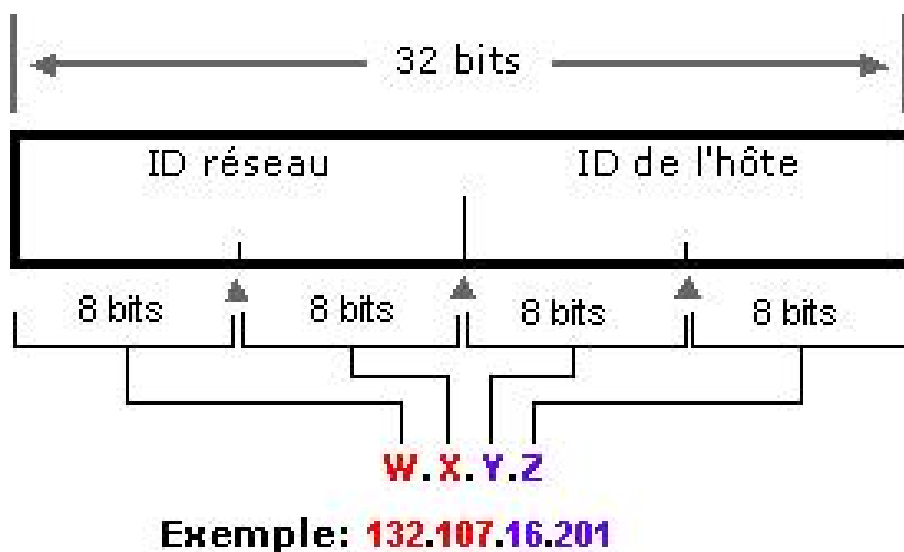


FIG. 1.1 – Représentation du format d'une adresse IPv4

1.4.1 Les classes d'adresses

1.4.1.1 Généralités

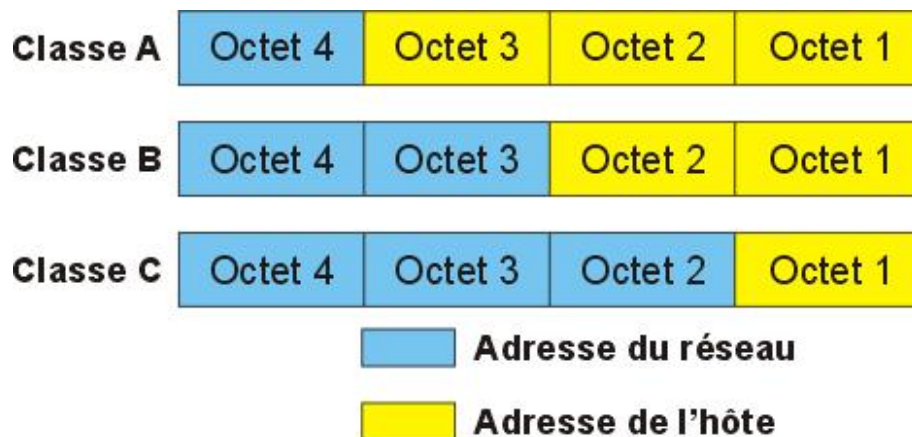
La communauté de Internet a défini cinq classes d'adresses. Les adresses des Classes A, B et C sont utilisées pour une affectation aux nœuds TCP/IP. La classe d'adresse définit quels bits sont utilisés pour le réseau ainsi que les parties d'ID d'hôte de

chaque adresse. La classe d'adresse définit également le nombre de réseaux et d'hôtes qui peuvent être pris en charge par réseau. Le tableau suivant utilise w.x.y.z pour indiquer les quatre valeurs d'octet d'une adresse IP donnée.

Les tableaux suivant sont utilisés pour présenter les éléments suivants :

- 1. Comment la valeur du premier octet (w) d'une adresse IP donnée, indique de manière efficace la classe de l'adresse.
- 2. Comment les octets d'une adresse sont divisés en ID de réseau et en ID d'hôte.
- 3. Le nombre de réseaux et d'hôtes possibles par réseau disponible pour chaque classe.

| classe | valeur de W | ID réseau | ID hôte | Nb réseaux | Nb hôtes réseau |
|--------|-------------|--|---------|--------------------|-------------------------|
| A | 1 - 126 | w | x.y.z | $2^7 - 2 / 126$ | $2^{24} - 2 / 16777214$ |
| B | 128 - 191 | w.x | y.z | $2^{14} / 16384$ | $2^{16} - 2 / 65534$ |
| C | 192 - 223 | w.x.y | z | $2^{21} / 2097152$ | $2^8 - 2 / 254$ |
| D | 224 - 239 | Réservé pour un adressage multi destinataire | | | |
| E | 240 - 254 | | | | |



NB : Comme vous le voyez, la classe A permet de créer peu de réseaux, mais avec beaucoup d'hôtes dans chaque réseau, La classe C faisant l'inverse. La classe D multicast, est destinée à faire de la diffusion d'information pour plusieurs hôtes simultanément.

1.4.1.2 Étendue de chaque classe

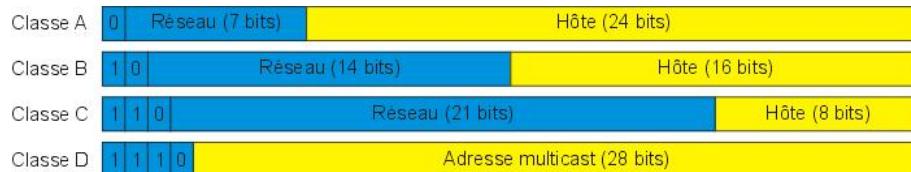
Comment fait on pour savoir à quelle classe appartient une adresse? Il y a deux méthodes pour le savoir :

La triviale, qui consiste à apprendre par cœur le tableau La subtile, qui consiste à retenir la règle, qui est logique

Voici donc la règle :

La classe est définie par les bits les plus lourds (les plus à gauche) Le bit le moins significatif pour la classe est toujours un 0 Les autres sont tous à 1 La classe A est signalée par un seul bit, donc obligatoirement un 0

La classe B par deux bits, donc 1 0 La classe C par trois bits, donc 1 1 0 La classe D (multicast) par 4 bits donc 1 1 1 0



Il existe même une classe E, dont les bits les plus lourds sont 11110, qui est « réservée à un usage ultérieur ». Si l'on arrive à retenir la définition ou son image, il devient facile de retrouver l'étendue de chaque classe :

| Première adresse | Dernière adresse | |
|------------------|------------------|-------------------------|
| 2cA | 0.0.0.1 | 127.255.255.254 (*)% |
| 2cB | 128.0.0.1 | 191.255.255.254% |
| 2cC | 192.0.0.1 | 223.255.255.254 |
| 2cD | 224.0.0.1 | 239.255.255.254 |

(*) L'adresse qui correspond à « localhost ». Cette adresse locale est nécessaire au fonctionnement

A ce stade, nous pourrions penser qu'il peut y avoir, par exemple, 128 réseaux de classe A, avec la possibilité d'avoir 16 777 216 hôtes dans chaque réseau. Cela est bien entendu, un peu plus compliqué. Il y a déjà quelques adresses que l'on ne peut pas attribuer à un hôte :

L'adresse d'hôte =0 (exemple : 192.168.1.0 dans une classe C)

Par convention, l'adresse IP dont la partie hôte est nulle est réservée à l'identification du réseau. L'adresse d'hôte avec tous ses bits à 1 (exemple : 192.168.1.255) Par convention, cette adresse signifie que tous les hôtes du réseau 192.168.1.0 sont concernés (Adresse de broadcast).

1.4.1.3 Les réseaux privés

Nous savons qu'une adresse Internet doit être unique dans un inter réseau. Cette considération, qui ne posait pas trop de problèmes pour des réseaux d'entreprise coupés du reste du monde, devient très restrictive à l'échelle de l'Internet où chaque adresse IP doit être unique à l'échelle planétaire. Ceci représente une contrainte énorme, et qui fait que la pénurie d'adresses IP est une catastrophe annoncée bien

plus certaine que celle du bug de l'an 2000. (Rassurezvous, le prochain protocole IP v6 prévoit de la marge, il faudra juste tout réapprendre).

Pour permettre aux entreprises de construire leur réseau privé, il a donc été réservé dans chaque classe A, B et C des adresses de réseaux qui ne sont jamais attribuées sur l'Internet (RFC 1918). Tout paquet de données contenant une adresse appartenant à ces réseaux doit être éliminé par le premier routeur établissant une connexion avec l'Internet.

Ces réseaux privés sont :

| Réseaux privés | Identification | |
|----------------|--------------------------------|---|
| 2cA | 10.0.0.0 127.0.0.0 | Pour les réseaux privés Pour l'interface de boucle locale (*)% |
| 2cB | 172.16.0.0 à 172.31.0.0 | Pour les réseaux privés% |
| 2cC | 192.168.0.0 à 192.168.255.0 | Pour les réseaux privés |

(*) L'adresse qui correspond à « localhost ». Cette adresse locale est nécessaire au fonctionnement

1.4.2 Le masque de sous réseau

Le masque de sousréseau a une importance que peu d'utilisateurs connaissent, elle est pourtant fondamentale. C'est un ensemble de 4 octets destiné à isoler :

- Soit l'adresse de réseau (NetID ou SubnetID) en effectuant un ET logique bit à bit entre l'adresse IP et le masque
- Soit l'adresse de l'hôte (HostID) en effectuant un ET logique bit à bit entre l'adresse IP et le complément du masque (!masque).

Les masques de sousréseau par défaut sont, suivant les classes d'adresses :

| Masque par défaut | Nombre d'octets pour l'hôte | |
|-------------------|-----------------------------|--------|
| 2cA | 255.0.0.0 | 3 (*)% |
| 2cB | 255.255.0.0 | 2% |
| 2cC | 255.255.255.0 | 1 |

(*) L'adresse qui correspond à « localhost ». Cette adresse locale est nécessaire au fonctionnement

Par défaut, un masque de sous réseau englobe donc la totalité de la classe.

Mais pourquoi « sous réseau » ?

Le principe en est simple : Imaginons que nous disposions d'une classe B. Nous disposons donc de deux octets pour les adresses d'hôtes, soit 65 534 hôtes possibles (les

adresses x.x.0.0 et x.x.255.255 sont réservées). Ca ferait tout de même beaucoup de machines sur le même réseau. En pareil cas, il est bien préférable d'organiser son réseau logique en plusieurs sous réseaux, connectés entre eux par des routeurs. Si par exemple, bien qu'étant en classe B, on choisit comme masque de sous réseau 255.255.255.0, nous obtiendrons 256 sous réseaux de 254 hôtes chacun dans le même réseau. Mais il est possible de définir des masques plus subtils. Deux hôtes, bien qu'appartenant au même réseau logique, s'ils sont placés dans des sous réseaux logiques différents, ne pourront communiquer entre eux que par l'intermédiaire d'un routeur. Cette solution est très commode pour des réseaux d'entreprise constitués de réseaux locaux distants et même pour des réseaux locaux comportant plusieurs centaines d'hôtes.

1.5 Liens utiles

Liste des ports logiciels

- <http://www.iana.org/assignments/portnumbers>
- <http://nallignet.free.fr/articles.php?lng=frpg=48>
- http://fr.wikipedia.org/wiki/Liste_des_ports_logiciels

Base de données de l'IANA (moteur de recherche)

- <http://shutdown76.free.fr/index.php?page=tools/port>

Liste des ports matériels

- http://fr.wikipedia.org/wiki/Liste_des_ports_materiels

Adressage IP

- <http://www.locoche.net/adresseIP.php>

Réseau (adressage, ports, socket ...)

- <http://christian.caleca.free.fr>