Le subnetting

1. Qu’est-ce que le subnetting ?

Le procédé appelé communément "subnetting" est l’action de diviser un réseau donné en une série de réseaux plus petits. Une plage d’adresses, de classe B par exemple, permet théoriquement d’adresser 65 534 hôtes différents et bien qu’il soit techniquement permis d’avoir un grand réseau de cette taille, cela risque de poser certains problèmes.

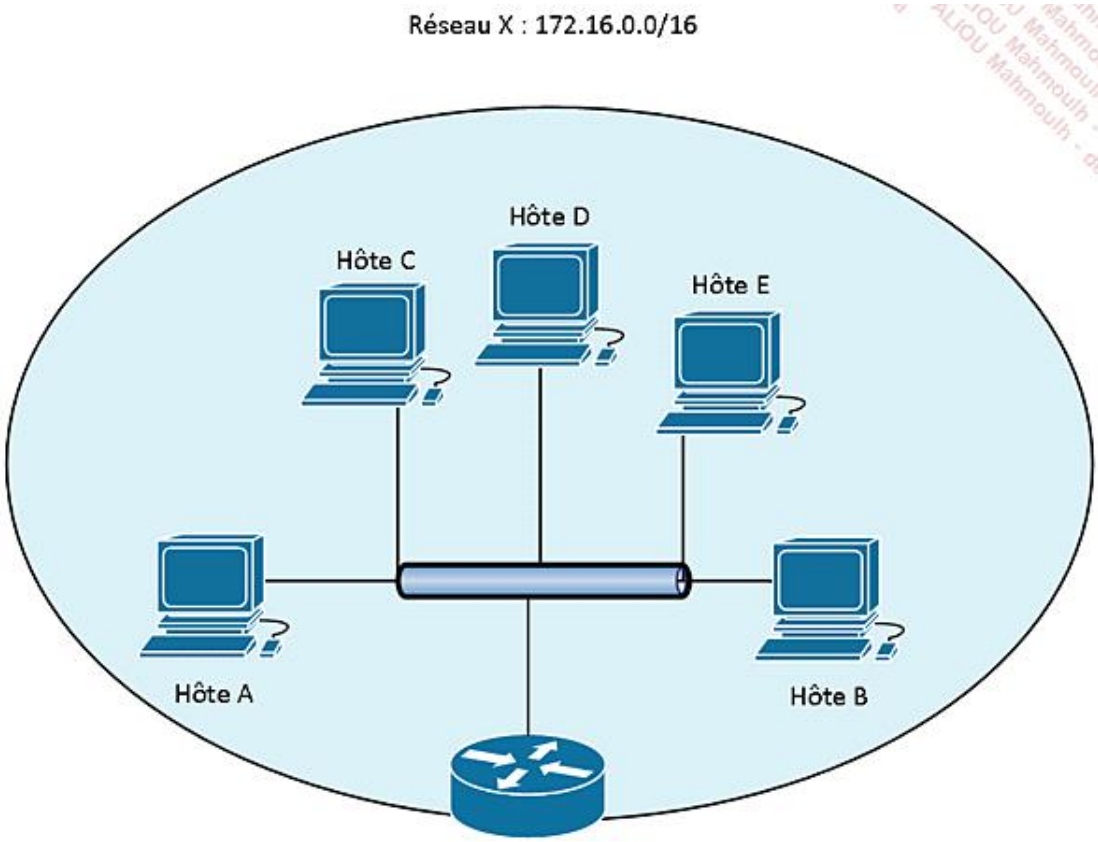
Un seul grand réseau signifie qu’un seul grand domaine de Broadcast existe. Pour rappel, les messages Broadcast sont nécessaires au fonctionnement d’IPv4. Un nombre très conséquent de messages Broadcast sur le réseau ne peut que dégrader les performances du réseau car un message Broadcast ne transporte pas, dans ce cas, des données utiles.

Pour les experts en sécurité, un tel réseau veut dire que toutes les machines sont capables de communiquer directement ensemble au niveau 2. Ce n’est pas une situation très appréciée car puisqu’il n’y a pas d’actions possibles sur l’organisation des adresses MAC étant donné qu’on ne peut pas facilement les modifier ou les attribuer, limiter les communications entre deux ou plusieurs machines devient compliqué en matière de maintenance.

Créer des réseaux plus petits avec le subnetting répond à ces deux problématiques (et à d’autres). Des réseaux différents, plus petits et qui contiennent moins d’hôtes, sont séparés par des équipements de niveau 3 qui ne transmettent pas les broadcasts.

Puisque l’adressage IP est logique, l’administration est libre d’organiser l’adressage de ses réseaux comme bon lui semble et donc de créer si nécessaire des silos de sécurité ce qui simplifie énormément la gestion des règles de filtrage.

Pour les besoins de cette section, un scénario simple va être créé. Il s’agit d’un réseau X dont l’adresse actuelle est 172.16.0.0/16. Ce réseau héberge un certain nombre d’hôtes (seuls cinq sont représentés sur le schéma).



Réseau IP initial

2. Planification de l'adressage

Avant d'examiner les calculs qui permettent de créer l'organisation de l'adressage, il faut auparavant réfléchir à la structure que l'on désire mettre en place.

Il faut donc examiner les besoins actuels afin de mettre en œuvre une structure qui fonctionne, qui réponde aux besoins actuels mais aussi éventuellement aux futurs besoins.

Deux critères sont importants à prendre en compte :

- Le nombre d'hôtes dans un réseau.
- Le nombre de sous-réseaux dans un réseau.

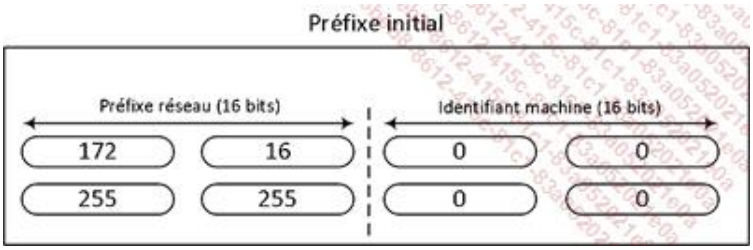
3. Le nombre d'hôtes dans un réseau

Si l'objectif est d'avoir des réseaux qui comportent au maximum 200 hôtes, il est possible de créer des réseaux plus petits, c'est-à-dire des réseaux ayant un nombre de bits moins importants qui seront disponibles pour adresser les machines.

Dans l'exemple, le réseau choisi est 172.16.0.0/16. Pour créer des réseaux plus petits, il faut déplacer le masque vers la droite afin de réduire le nombre de bits dédiés à l'adressage des hôtes.

Dans le tableau de la section La longueur de préfixe et la taille de réseau, il est indiqué qu'un réseau qui dispose de 8 bits pour les hôtes peut héberger 254 hôtes ce qui semble correspondre à l'objectif.

Utiliser 7 bits ne permet d'héberger que 126 hôtes et 9 bits autorise l'hébergement de 510 hôtes ce qui est trop. Le préfixe initial contient donc 16 bits (/16 !) pour la partie réseau et 16 bits pour la partie hôte.



Préfixe initial

Le nouveau découpage contient 24 bits pour la partie réseau et 8 bits pour la partie hôte.

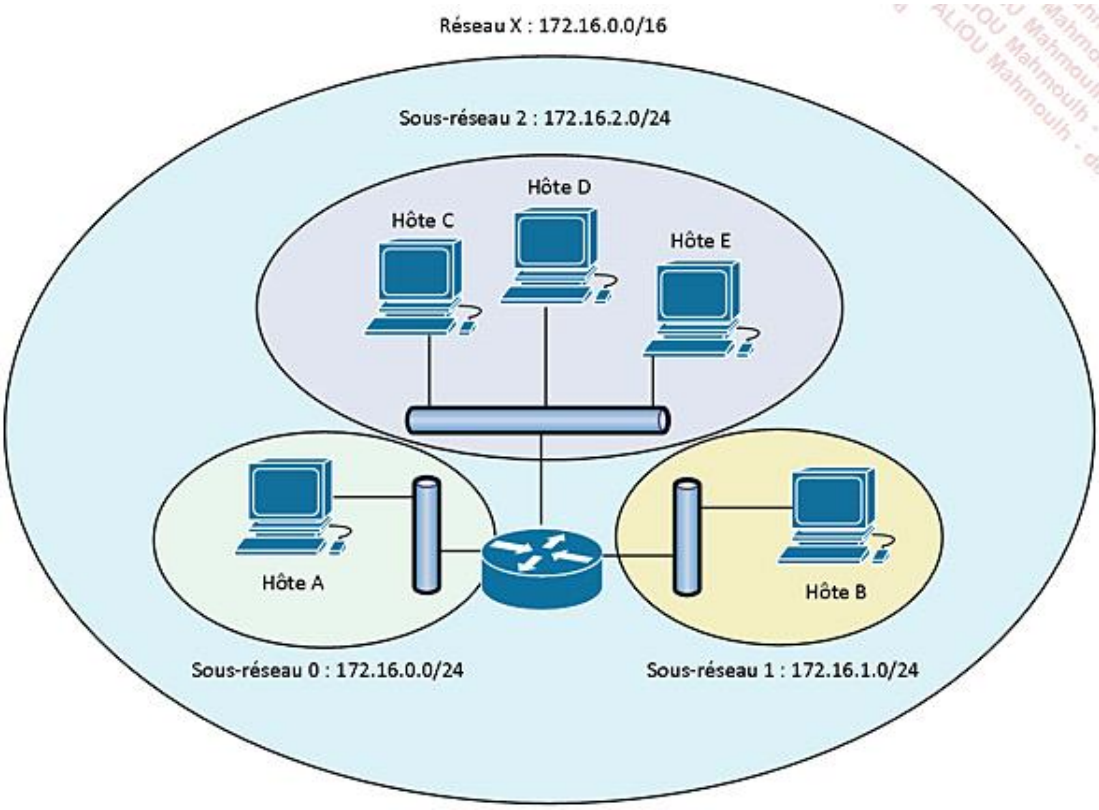
Nouveau préfixe

On peut aussi considérer qu'on possède 16 bits de réseau, 8 bits de sous-réseau et enfin 8 bits d'adressage des hôtes. Les bits de sous-réseau deviennent alors une variable que l'on peut utiliser pour organiser le réseau (par numéro de réseau, par numéro de site, par numéro de région…).

Peu importe le nom qu'on leur donne, ces 8 nouveaux bits font maintenant partie du préfixe réseau, ils peuvent être utilisés pour dénommer le réseau :

- Le sous-réseau 0 a pour adresse 172.16.0.0/24.
- Le sous-réseau 1 a pour adresse 172.16.1.0/24.
- Le sous-réseau 2 a pour adresse 172.16.2.0/24.

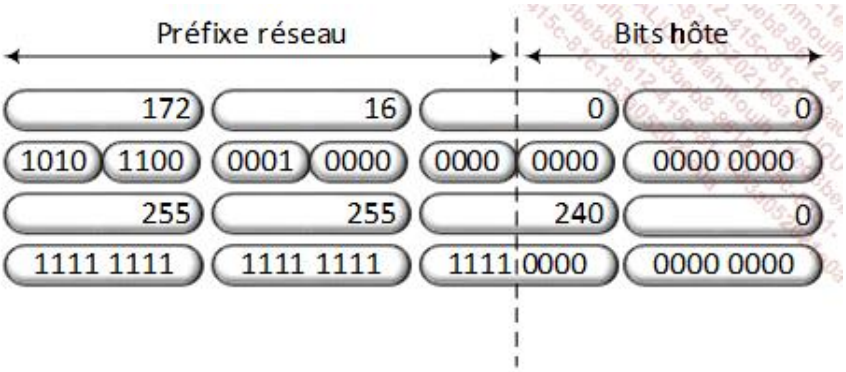
La nouvelle organisation du réseau peut être représentée de cette manière :



Sous-réseaux IP

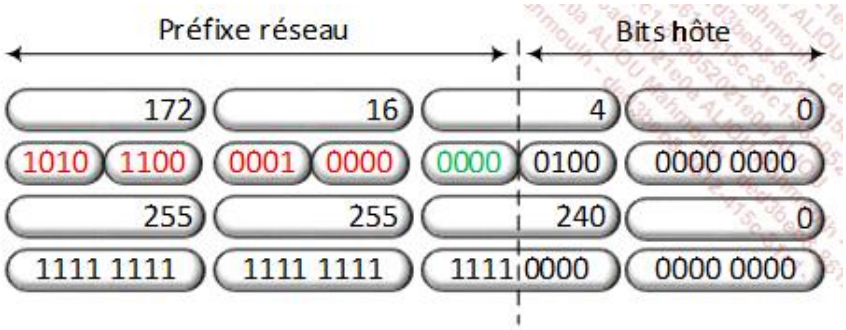
Si moins d'hôtes sont nécessaires, il est possible d'effectuer la même opération avec des sous-réseaux qui ont une autre taille, par exemple avec des réseaux qui doivent comporter au maximum 4 000 hôtes. Le tableau précédent montre que 20 bits permettent d'héberger 4 096 hôtes ce qui signifie qu'il faut prendre 4 bits de plus au masque existant.

Cet exemple pose un problème de plus car le découpage ne tombe pas entre 2 octets, l'adresse réseau doit donc être choisie en respectant le découpage.

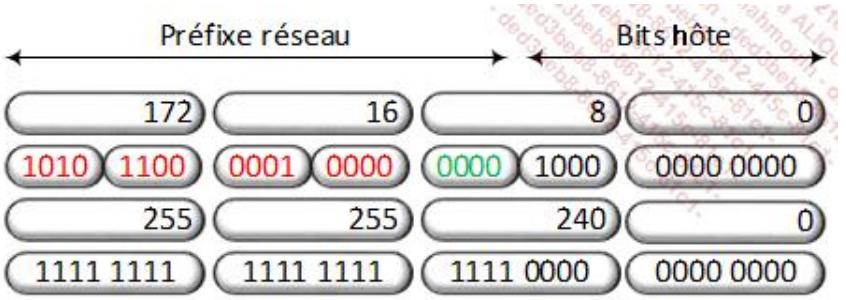


Adresse de réseau

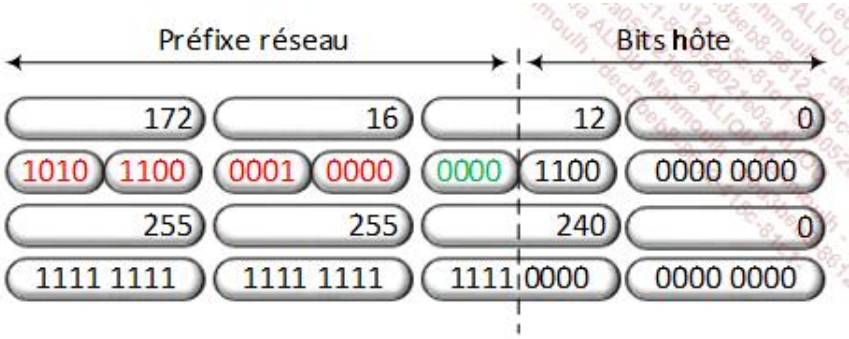
Cela veut dire que tant qu'un réseau a les 20 premiers bits égaux, les adresses suivantes font donc toutes partie du même réseau :



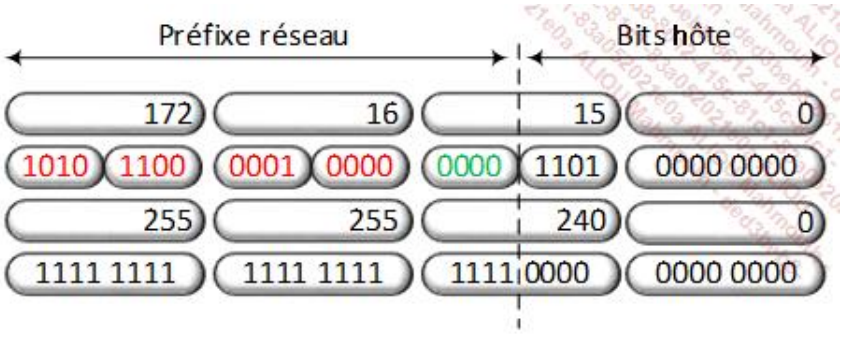
Première machine



Seconde machine



Troisième machine

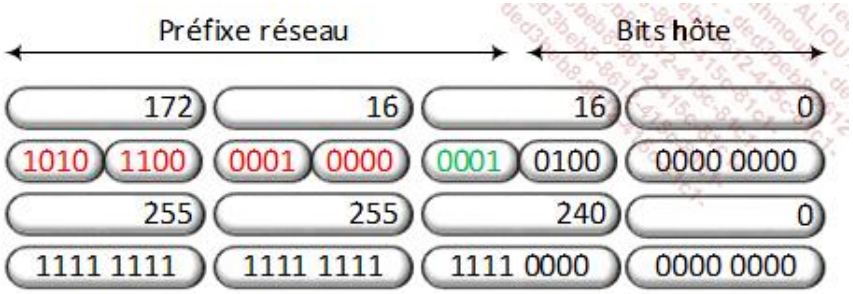


Quatrième machine

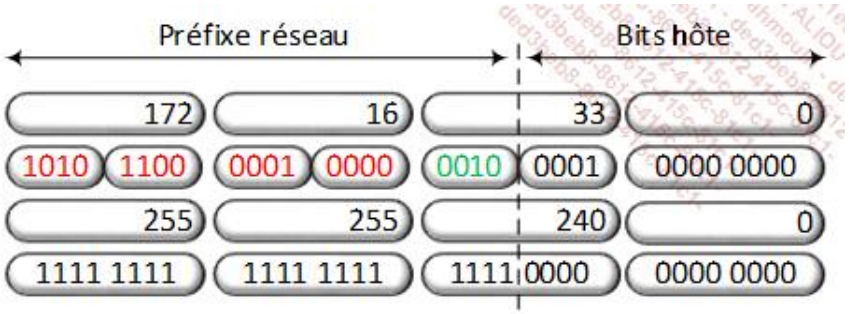
Si toutes ces adresses font partie du même réseau, cela signifie qu'il s'agit en réalité de machines différentes au sein du même réseau !

Il faut noter que même si le dernier octet ne comporte que des 0, cela n'en reste pas moins une adresse de machine valable car le dernier octet ne détermine pas à lui seul la partie hôte.

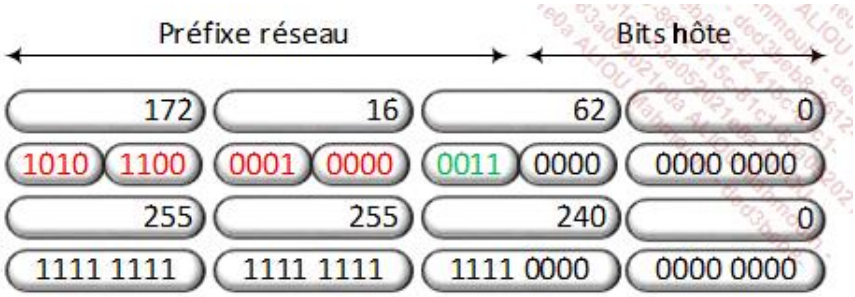
En revanche les adresses suivantes font partie d'un réseau différent car l'un des bits du préfixe est différent :



Réseau différent 1



Réseau différent 2



Réseau différent 3

Il peut paraître laborieux de devoir comparer les bits des adresses pour savoir si oui ou non elles appartiennent au même sous-réseau. Par chance des raccourcis existent et ils font appel aux connaissances fondamentales sur le binaire.

Les méthodes qui suivent sont des méthodes utilisées pour faire ce genre de calcul.

Combien d'hôtes possibles sur un réseau ?

Le nombre d'hôtes possibles sur un réseau dépend du nombre de bits disponibles pour les adresser. Une adresse comprend 32 bits et la différence entre le masque et le nombre total de bits indique le nombre de bits disponibles

pour la partie hôte.

Dans l'exemple précédent, un /20 a été choisi. 32-20 = 12.

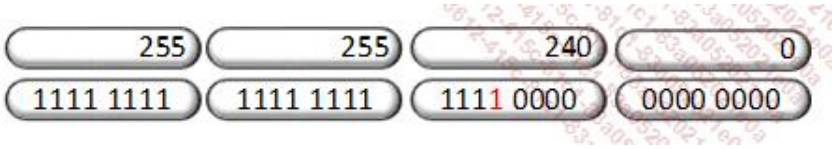
Le nombre de bits pour la partie hôte est égal à 12 bits.

En élevant 2 à la puissance de 12 puis en retranchant 2, on obtient : 4 094 hôtes possibles.

Quels sont les réseaux disponibles ?

Il faut ici trouver la valeur numérique du dernier bit à 1 de l'adresse, au sein de son octet. Cette valeur peut être appelée le "pas".

Dans l'exemple, le dernier bit à 1 est le quatrième bit du troisième octet.



Calcul du pas

Sa valeur numérique est 16 au sein de l'octet.

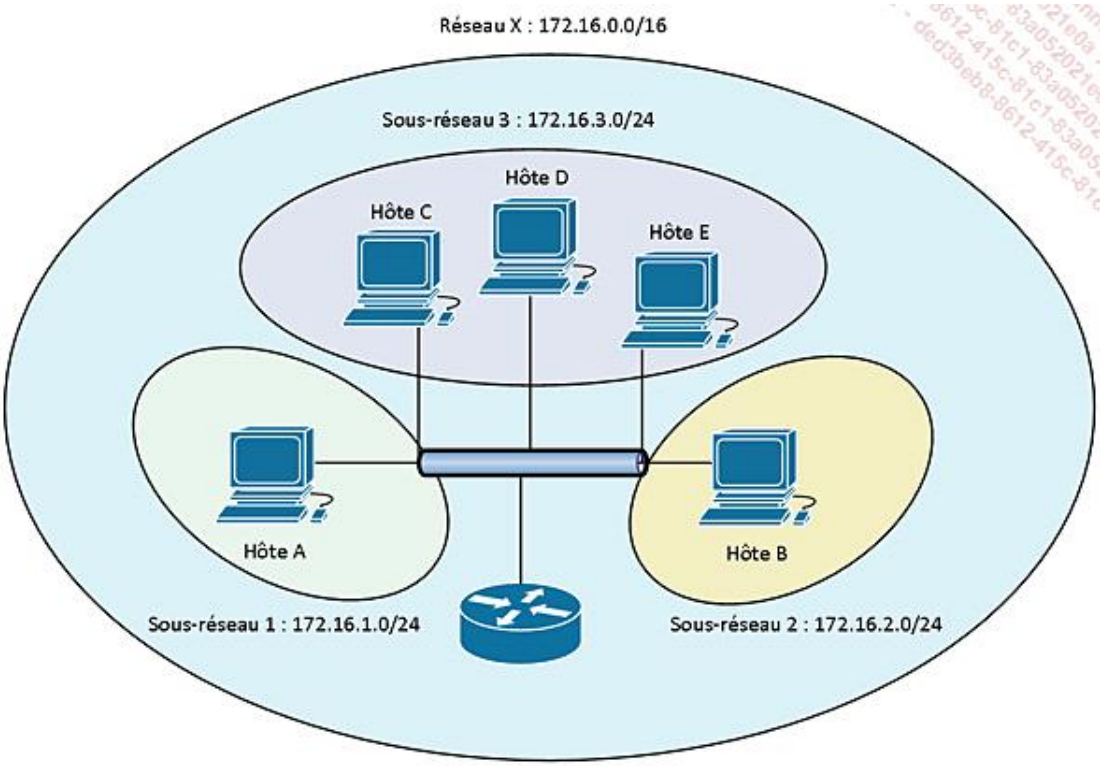
On liste les réseaux en utilisant un intervalle égal au "pas", c'est-à-dire la valeur numérique précédemment obtenue.

Sous la forme d'un tableau en utilisant l'adresse de départ, le résultat est le suivant :

Préfixe 172.16.0.0	
Premier réseau	172.16.0.0
Deuxième réseau	172.16.16.0
Troisième réseau	172.16.32.0
Quatrième réseau	172.16.48.0
Cinquième réseau	172.16.64.0
Sixième réseau	172.16.80.0
…	…

De cette manière on obtient les réseaux qu'on peut utiliser. Chacun des réseaux peut ainsi contenir 4 094 hôtes.

La nouvelle représentation du réseau est la suivante :



Réseau réparti en subnets égaux

Quels hôtes appartiennent à quels réseaux ?

Complétons le tableau précédemment créé avec les adresses Broadcast, la première adresse d'hôte disponible et la dernière adresse d'hôte disponible.

	Adresse réseau	Premier hôte	Dernier hôte	Broadcast
Premier réseau	172.16.0.0	172.16.0.1	172.16.15.254	172.16.15.255
Deuxième réseau	172.16.16.0	172.16.16.1	172.16.31.254	172.16.31.255
Troisième réseau	172.16.32.0	172.16.32.1	172.16.47.254	172.16.47.255
Quatrième réseau	172.16.48.0	172.16.48.1	172.16.63.254	172.16.63.255
Cinquième réseau	172.16.64.0	172.16.64.1	172.16.79.254	172.16.79.255
Sixième réseau	172.16.80.0	172.16.80.1	172.16.95.254	172.16.95.255
...	...	...	...	...

Le tableau qui récapitule le nombre d'hôtes possibles en fonction du masque n'est pas toujours à disposition.

Pour trouver la valeur qui est recherchée, il faut :

- Soit trouver le bit dont la valeur numérique est immédiatement inférieure à celle recherchée.
- Soit apprendre toutes les puissances par cœur.

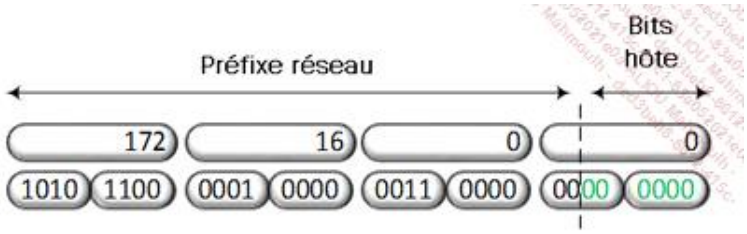
Lorsque ce bit est trouvé, on dispose alors du nombre de bits qui doivent être réservés dans la partie d'identification des hôtes.

Toujours avec le préfixe initial 172.16.0.0/16, si 40 hôtes sont requis par subnet :

Bits	1	2	3	4	5	**6**	7	8
Valeur numérique	1	2	4	8	16	**32**	64	128
Puissance	2	4	8	16	32	**64**	128	256

Bits	9	10	11	12	13	14	15	16
Valeur	256	512	1024	2048	4096	8192	16384	32768
Puissance	512	1024	2048	4096	8192	16384	32768	65536

Le bit dont la valeur est immédiatement inférieure à 40 est le sixième bit, il faut donc en réserver autant dans la partie hôte :



Réservation de bits

On dispose ainsi du masque qui est égal à 32-6 = 26 bits. Soit le masque 255.255.255.192. Les réseaux se décomposent ainsi en suivant la méthode précédemment décrite :

- 172.16.0.0/26
- 172.16.0.64/26
- 172.16.0.128/26
- 172.16.0.192/26
- 172.16.1.0/26
- 172.16.1.64/26
- Etc.

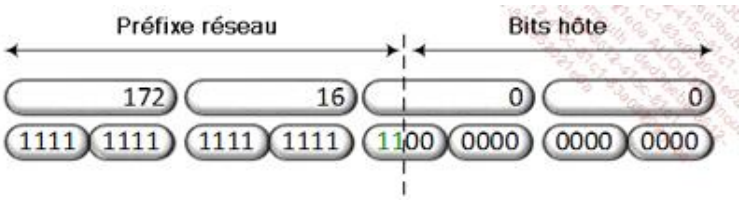
Attention aux nombres d'hôtes qui correspondent parfaitement à la valeur numérique d'un bit. Si 64 hôtes sont nécessaires, il faut sélectionner le bit supérieur car deux adresses ne sont pas utilisables.

4. Le nombre de sous-réseaux dans un réseau

L'approche contraire est également possible, c'est-à-dire de décider à l'avance du nombre de sous-réseaux qui seront nécessaires.

Pour définir un nombre de sous-réseaux, la procédure est inversée : il faut conserver un certain nombre de bits pour la partie préfixe réseau dans le but de les utiliser dans une démarche de subnetting.

En continuant à travailler sur le préfixe 172.16.0.0/16, il est demandé quatre sous-réseaux. La valeur immédiatement inférieure correspond au deuxième bit ce qui signifie qu'il faut réserver 2 bits.



Réservation de bits 2

Le dernier bit à 1 du masque vaut 64 sur le troisième octet et cela indique le pas. Les quatre réseaux possibles sont donc :

- 172.16.0.0
- 172.16.64.0
- 172.16.128.0
- 172.16.192.0

Il reste donc 14 bits disponibles ce qui signifie que 16 382 hôtes par subnet peuvent être hébergés. L'idéal à présent est de recréer un tableau complet afin de disposer de toutes les informations sur tous les réseaux :

	Adresse réseau	Premier hôte	Dernier hôte	Broadcast
Premier réseau	172.16.0.0	172.16.0.1	172.16.63.254	172.16.63.255
Deuxième réseau	172.16.64.0	172.16.64.1	172.16.127.254	172.16.127.255
Troisième réseau	172.16.128.0	172.16.128.1	172.16.191.254	172.16.41.255
Quatrième réseau	172.16.192.0	172.16.192.1	172.16.255.254	172.16.255.255