

## Chap. III L'adressage IPv4 et IPv6

Toute machine ou équipement IP est identifié par une adresse IP qui contient l'adresse du réseau local et le numéro de la machine dans ce réseau local auquel il est physiquement connecté (Ethernet, liaison série,...). La communication avec d'autres objets du même réseau IP se fait directement grâce au réseau local de niveau 2. La communication avec d'autres objets IP d'autres réseaux IP se fait grâce à des passerelles ou des routeurs qui utilisent l'adresse IP pour déterminer le chemin à suivre (ou router) pour atteindre la destination.

Les protocoles de routage sont un ensemble de règles permettant de router des données à travers des réseaux en utilisant les adresses IP.

### III.1. Adressage IPv4 par classe

Tous les périphériques appartenant à un réseau doivent être identifiés de manière unique. Au niveau de la couche réseau, les paquets de communication doivent être identifiés par les adresses source et de destination. Avec l'adressage IPv4, cela implique que chaque paquet comporte, dans l'en-tête de la couche 3, une adresse source 32 bits et une adresse de destination 32 bits.

Cette adresse est sous la forme **w.x.y.z** où **w**, **x**, **y** et **z** sont des octets.

**Exemple** : 192.168.10.2

Pour chaque adresse, **une partie des bits d'ordre haut représente l'adresse réseau**. Au niveau de la couche 3, un réseau se définit par un groupe d'hôtes dont la partie adresse réseau de l'adresse contient la même configuration binaire.

Bien que l'ensemble des 32 bit défini l'adresse IPv4 d'un hôte, un nombre variable de bits constitue la partie hôte de l'adresse. Le nombre de bits contenus dans la partie hôte détermine le nombre d'hôtes possible sur un réseau.

#### III.1.1 Les différents types d'adresses d'un réseau

Dans la plage d'adresses de chaque réseau, il y a trois types d'adresse :

- **L'adresse réseau** : l'adresse qui fait référence au réseau.

Dans la plage d'adresses d'un réseau, la plus petite adresse est réservée à l'adresse réseau.

Dans la partie hôte, cette adresse comporte un 0 pour chaque bit d'hôte.

**Exemple** : Pour le réseau **192.110.10.0** avec **24** bits (les trois premiers octets) pour l'identificateur réseau, et le dernier octet à **0**.

Pour exprimer une adresse réseau IPv4, nous ajoutons une longueur de **préfixe** à l'adresse réseau. La longueur de préfixe correspond au **nombre de bits de l'adresse qui représentent la partie réseau**.

Par exemple, dans 172.16.4.0 /24, /24 est la longueur de préfixe. Elle nous indique que les 24 premiers bits correspondent à l'adresse réseau. Il reste donc 8 bits (le dernier octet) qui correspondent à la partie hôte.

- **L'adresse de diffusion** : est une adresse spécifique, attribuée à chaque réseau, utilisée pour envoyer les données à tous les hôtes du réseau

Elle permet de transmettre des données à l'ensemble des hôtes d'un réseau. C'est ainsi qu'un hôte peut envoyer un seul paquet adressé à l'adresse de diffusion du réseau.

L'adresse de diffusion correspond à **la plus grande adresse** de la plage d'adresses d'un réseau. Il s'agit de l'adresse dans laquelle les bits de la partie hôte sont tous des « 1 ».

Les paquets de diffusion sont habituellement limités au réseau local. Cette limitation dépend de la configuration de la passerelle et du type de diffusion. Il existe deux types de diffusion : *la diffusion dirigée* et *la diffusion limitée*.

#### ***Diffusion dirigée (broadcast).***

Une diffusion dirigée est envoyée à tous les hôtes d'un réseau particulier. Ce type de diffusion permet l'envoi d'une diffusion à tous les hôtes d'un réseau qui n'est pas local. Par exemple, pour qu'un hôte situé en dehors du réseau 172.16.4.0/24 communique avec tous les hôtes de ce réseau, l'adresse de destination du paquet doit être 172.16.4.255. *Par défaut, les routeurs n'acheminent pas les diffusions dirigées.*

#### ***Diffusion limitée***

La diffusion limitée permet une transmission qui est limitée aux hôtes du réseau local. Ces paquets utilisent toujours l'adresse IPv4 de destination **255.255.255.255**. Les routeurs ne transmettent pas les diffusions limitées. C'est la raison pour laquelle un réseau IPv4 est également appelé « *domaine de diffusion* ». Les routeurs forment les limites d'un domaine de diffusion.

- **Des adresses d'hôte** : sont des adresses attribuées aux périphériques finaux sur le réseau.

Dans les adresses IPv4, nous attribuons les valeurs situées entre l'adresse réseau et l'adresse de diffusion aux périphériques de ce réseau.

**Exemple** : Pour le réseau **192.110.10.0** avec **24** bits pour l'identificateur réseau ; l'adresse d'un hôte peut être 192.110.10.25

Cette adresse est également désignée sous le nom **d'adresse unicast**.

### III.1.2 Les anciennes classes d'adresses réseau

À l'origine, les plages monodiffusion étaient regroupées selon certaines tailles appelées des adresses de classe A, B et C. Il y a aussi des adresses de classe D (multidiffusion) et de classe E (expérimentales). Les adresses étaient initialement attribuées en fonction de la classe.

#### 1. Blocs d'adresses A

Un bloc d'adresses de classe A a été créé pour prendre en charge les réseaux de très grande taille, comportant plus de 16 millions d'adresses d'hôte. Les adresses de classe A utilisaient un préfixe /8 invariable : le premier octet indiquant l'adresse réseau, les trois octets restants correspondaient aux adresses d'hôte.

Afin de réserver un espace d'adresses aux classes d'adresse restantes, le bit de poids fort de l'octet de valeur supérieure devait être un zéro dans toutes les adresses de classe A.

D'où la plage d'adresse pour la classe A : **0.0.0.0/8 - 127.0.0.0/8.**

#### 2. Blocs d'adresses B

L'espace d'adressage de classe B a été créé pour répondre aux besoins des réseaux de taille moyenne ou de grande taille, comportant plus de 65 000 hôtes. Les adresses IP de classe B utilisent les deux premiers octets pour indiquer l'adresse réseau. Les deux octets suivants correspondent aux adresses d'hôte. Pour les adresses de classe B, les deux bits de poids fort du premier octet étaient '10'.

Cela limitait le bloc d'adresses de la classe B à **128.0.0.0/16 - 191.255.0.0/16**

#### 3. Blocs d'adresses C

Cet espace d'adressage était réservé aux réseaux de petite taille, comportant 254 hôtes au maximum. Les blocs d'adresses de classe C utilisaient le préfixe /24. Ainsi, un réseau de classe C ne pouvait utiliser que le dernier octet pour les adresses d'hôte, les trois premiers octets correspondant à l'adresse réseau.

Le bloc d'adresses de classe C à **192.0.0.0/24 - 223.255.255.0/24**

#### 4. Adresses de multidiffusion (multicast)

Un autre gros bloc d'adresses est réservé à un usage spécifique : il s'agit de la plage d'adresses de multidiffusion, allant de **224.0.0.0 à 239.255.255.255.**

La transmission multidiffusion réduit le volume de trafic en permettant à un hôte d'envoyer un seul paquet à un groupe d'hôtes désigné. Pour atteindre plusieurs hôtes de destination à l'aide d'une transmission de type monodiffusion, un hôte source a besoin d'envoyer un paquet qu'il adresse à chaque hôte. Dans une transmission multidiffusion, l'hôte source peut envoyer un seul paquet, qui parviendra à des milliers d'hôtes de destination.

*Exemples de transmission multidiffusion* : Distribution de contenu vidéo et audio, Échange d'informations de routage entre des protocoles de routage, jeu en ligne.

Les hôtes qui souhaitent recevoir des données multidiffusion spécifiques sont appelés des '**clients multidiffusion**'. Ces clients font appel à des services activés par un programme client pour s'abonner au groupe de multidiffusion.

Chaque groupe de multidiffusion est représenté par une seule adresse de destination multidiffusion. Lorsqu'un hôte s'abonne à un groupe de multidiffusion, il traite les paquets adressés à cette adresse multidiffusion, ainsi que ceux adressés à son adresse monodiffusion (unicast), qui lui a été attribuée.

## 5. Adresses expérimentales

Un important bloc d'adresses est réservé à un usage spécial, il s'agit de la plage d'adresses expérimentales IPv4, allant de **240.0.0.0 à 255.255.255.254**. Actuellement, ces adresses sont répertoriées comme étant réservées pour une utilisation expérimentale et future.

### III.1.3 Adresses publiques et privées

#### 1. Adresses privées

Bien que la majorité des adresses d'hôte soient des adresses publiques utilisées dans les réseaux accessibles sur Internet, d'autres blocs d'adresses sont attribués à des réseaux qui ne nécessitent pas d'accès à Internet, ou uniquement un accès limité. Ces adresses sont appelées des **adresses privées**.

Voici ces plages d'adresses privées :

<b>10.0.0.0</b>	<b>à</b>	<b>10.255.255.255</b>	<b>(10.0.0.0 /8)</b>
<b>172.16.0.0</b>	<b>à</b>	<b>172.31.255.255</b>	<b>(172.16.0.0 /12)</b>
<b>192.168.0.0</b>	<b>à</b>	<b>192.168.255.255</b>	<b>(192.168.0.0 /16)</b>

Les blocs d'adresses d'espace privé, sont réservés aux réseaux privés. En règle générale, les hôtes qui ne nécessitent pas d'accès à Internet peuvent utiliser les adresses privées sans limitation. Plusieurs hôtes de réseaux différents peuvent utiliser les mêmes adresses d'espace privé. *Les paquets qui utilisent ces adresses comme source ou destination ne doivent pas être visibles sur Internet.* Le routeur ou le périphérique pare-feu, en périphérie de ces réseaux privés, doivent bloquer ou traduire ces adresses.

#### 2. Adresses publiques

Ces adresses sont attribuées à des hôtes publiquement accessibles depuis Internet. Toutefois, même dans cette plage, de nombreuses adresses sont déjà réservées à un usage spécial.

#### 3. Traduction d'adresses de réseau (NAT)

Grâce à des services qui traduisent les adresses privées en adresses publiques, les hôtes d'un réseau privé peuvent accéder aux ressources présentes sur Internet. Appelés NAT (Network Address Translation), ces services peuvent être mis en œuvre sur un périphérique situé en périphérie du réseau privé. Les services NAT permettent aux hôtes du réseau « d'emprunter » une adresse publique pour communiquer avec des réseaux externes.

#### 4. Bouclage (Adresses réservées)

L'adresse de bouclage IPv4 **127.0.0.1** est une autre adresse réservée. Il s'agit d'une adresse spéciale que les hôtes utilisent pour diriger le trafic vers eux-mêmes. L'adresse de bouclage crée un moyen rapide, pour les applications et les services TCP/IP actifs sur le même périphérique, de communiquer entre eux. En utilisant l'adresse de bouclage à la place de l'adresse d'hôte IPv4 attribuée, deux services actifs sur le même hôte peuvent contourner les couches les plus basses de la pile TCP/IP. Vous pouvez également envoyer une requête *ping* à l'adresse de bouclage afin de tester la configuration TCP/IP de l'hôte local.

**Remarque :** Bien que seule l'adresse **127.0.0.1** soit utilisée, les adresses de la plage **127.0.0.0 - 127.255.255.255** sont réservées. Toutes les adresses de cette plage sont envoyées en boucle sur l'hôte local. Aucune des adresses de cette plage ne devrait jamais apparaître sur un réseau quel qu'il soit.

5. L'adresse **0.0.0.0** est réservée au **routing par défaut**.

#### 6. Adresses link-local

Les adresses IPv4 du bloc d'adresses **169.254.0.0 à 169.254.255.255 (169.254.0.0/16)** sont conçues comme des *adresses link-local*. Elles peuvent être automatiquement attribuées à l'hôte local par le système d'exploitation, dans les environnements où aucune configuration IP n'est disponible. Elles peuvent être utilisées dans un réseau peer-to-peer restreint ou pour un hôte qui ne parviendrait pas à obtenir automatiquement une adresse auprès d'un serveur DHCP.

Les transmissions basées sur des adresses IPv4 link-local ne conviennent que dans le cadre d'une communication avec d'autres périphériques connectés au même réseau. Un hôte ne peut pas envoyer de paquet avec une adresse de destination IPv4 link-local à un routeur pour qu'il soit acheminé. Les adresses link-local ne fournissent pas de services en dehors du réseau local.

#### 7. Adresses TEST-NET

Le bloc d'adresses **192.0.2.0 à 192.0.2.255 (192.0.2.0/24)** est réservé à des fins pédagogiques. Ces adresses peuvent être utilisées dans la documentation et dans des exemples de réseau. Contrairement aux adresses expérimentales, les périphériques réseau accepteront ces adresses dans leur configuration. Les adresses de cette plage ne doivent pas être visibles sur Internet.

### III.1.4 Limites de l'adressage par classe

Les besoins de certaines entreprises ou organisations n'étaient pas toujours couverts par les classes A, B et C. L'attribution par classe des adresses IP gaspille souvent de nombreuses adresses, ce qui épuise la disponibilité des adresses IPv4. Par exemple, une entreprise avec un réseau de 260 hôtes se voit attribuer une adresse de classe B avec plus de 65 000 adresses.

**Remarque :** Le lundi 31 janvier 2011, l'IANA (Internet Assigned Numbers Authority) a attribué les deux derniers blocs d'adresses IPv4 /8 aux *organismes d'enregistrement Internet locaux* (Regional Internet Registry : RIR). Les différentes prévisions indiquent que les cinq RIR auront épuisé les adresses IPv4 entre 2015 et 2020.

**Liste des RIR :**

- **RIPE-NCC** (Réseaux IP Européens, créé en 1992) pour l'Europe et le Moyen-Orient ;
- **APNIC** (*Asia Pacific Network Information Center*, créé en 1993) pour l'Asie et le Pacifique ;
- **ARIN** (*American Registry for Internet Numbers*, créé en 1997) pour l'Amérique du Nord (entre 1993 et 1997, ce rôle était attribué à InterNIC) ;
- **LACNIC** (*Latin America and Caribbean Network Information Center*, créé en 1999) pour l'Amérique latine et les îles des Caraïbes ;
- **AfriNIC** (*African Network Information Center*, créé en 2005) pour l'Afrique.

## III.2 Adressage classique de sous-réseaux

La création de sous-réseaux permet de créer plusieurs réseaux logiques à partir d'un seul bloc d'adresses.

### III.2.1 Masques de sous réseau : définition des parties réseau et hôte

Une adresse IPv4 est divisée en deux parties : une partie réseau et une partie hôte. Le nombre de bits qui correspond à la partie réseau s'appelle *la longueur de préfixe*. Pour définir les parties réseau et hôte d'une adresse, les périphériques utilisent une configuration de 32 bits appelée *masque de sous-réseau*. Le masque de sous-réseau est exprimé dans le même format décimal à point que celui de l'adresse IPv4. Ce masque est créé en plaçant le nombre binaire 1 dans chaque position de bit qui représente la partie réseau et en plaçant le nombre binaire 0 dans chaque position de bit qui représente la partie hôte.

**Le préfixe et le masque de sous-réseau constituent des moyens distincts de représenter la même chose : la partie réseau d'une adresse.**

Le masque de sous-réseau est configuré sur l'hôte en conjonction avec l'adresse pour définir la partie réseau de cette adresse.

Exemple l'hôte 172.16.20.35/27 a pour :

**Adresse hôte :** 172.16.20.35 en binaire : **10101100.00010000.00010100.00100011**  
**Masque de sous-réseau :** 255.255.255.224 en binaire : **11111111.11111111.11111111.11100000**  
**Adresse réseau :** 172.16.20.32 en binaire : **10101100.00010000.00010100.00100000**

**Masque de sous-réseau :** 255.255.255.224 notation en décimale à point  
/27 au format avec barre oblique

Dans la mesure où les bits de poids fort des masques de sous-réseau sont des 1 contigus, il y a un nombre limité de valeurs de sous-réseau dans un octet. Ces configurations sont les suivantes:

<u>Binaire : décimale</u>	<u>Binaire : décimale</u>
00000000 = 0	11111000 = 248
10000000 = 128	11111100 = 252
11000000 = 192	11111110 = 254
11100000 = 224	11111111 = 255
11110000 = 240	

Si le masque de sous-réseau d'un octet est représenté par 255, tous les bits équivalents de cet octet de l'adresse sont des bits réseau. De même, si le masque de sous-réseau d'un octet est représenté par un 0, tous les bits équivalents de cet octet de l'adresse sont des bits d'hôte.

### III.2.2 Opération AND

À l'intérieur des périphériques de réseau de données, une logique numérique est appliquée pour interpréter les adresses. Lorsqu'un paquet est créé ou transmis, **l'adresse réseau** de destination doit être extraite de l'adresse de destination. Cela est possible par le biais de l'opérateur logique AND (ET). L'adresse d'hôte est logiquement ajoutée par une opération AND à son masque de sous-réseau pour déterminer l'adresse à laquelle l'hôte est associée. Lorsque cette opération AND est appliquée entre l'adresse et le masque de sous-réseau, le résultat obtenu est l'adresse réseau.

**Exemple :** Adresse hôte : 172.16.20.35 en binaire : 10101100.00010000.00010100.00100011

Masque de sous-réseau : 255.255.255.224 en binaire : 11111111.11111111.11111111.11100000

En appliquant l'opération AND entre l'adresse hôte et le masque ; on obtient :

Adresse réseau : 172.16.20.32 en binaire : **10101100.00010000.00010100.00100000**

### III.2.3 Notions de base sur la création de sous-réseaux

La création de sous-réseaux permet de créer plusieurs réseaux logiques à partir d'un seul bloc d'adresses. Puisque nous utilisons un routeur pour interconnecter ces réseaux, chaque interface du routeur doit disposer d'un identificateur réseau unique. Tous les nœuds de cette liaison se trouvent sur le même réseau.

Nous créons les sous-réseaux au moyen d'un ou de plusieurs bits d'hôte en tant que bits réseau. Pour cela, il convient de développer le masque pour emprunter quelques bits de la partie hôte de l'adresse et créer d'autres bits réseau. Plus les bits d'hôte utilisés sont nombreux, plus le nombre de sous-réseaux qui peuvent être définis est important. Pour chaque bit emprunté, il faut doubler le nombre de sous-réseaux disponibles.

**Nombre de sous-réseaux :**  $2^m$  où  $m$  est le nombre de bits empruntés  
**Le nombre d'hôtes :**  $2^n - 2$  où  $n$  est le nombre de bits laissés pour les hôtes.

Exemple : Si on emprunte un bit, nous obtenons :

$$2^1 = 2 \text{ sous-réseaux}$$

$$2^7 - 2 = 126 : \text{on déduit que chacun de ces sous-réseaux peut avoir 126 hôtes.}$$

### Exemple d'adressage classique de sous-réseaux :

Une seule adresse réseau est disponible : 192.168.1.0 (/24), Masque : 255.255.255.0

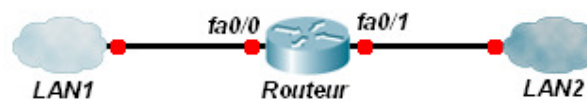


Figure III.1 Un réseau formé de deux sous-réseau (LAN1 et LAN2)

**Adresse :** 11000000.10101000000000001.00000000

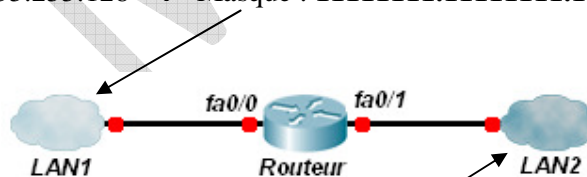
**Masque :** 11111111.11111111.11111111.00000000

Le routeur, a deux interfaces pour interconnecter deux réseaux (LAN1 et LAN2). Avec un bloc d'adresses de 192.168.1.0 /24, nous créons deux sous-réseaux. Nous empruntons un bit de la partie hôte en utilisant le masque de sous-réseau 255.255.255.128, à la place du masque d'origine 255.255.255.0. Le bit le plus significatif du dernier octet est utilisé pour distinguer les deux sous-réseaux. Pour l'un des sous-réseaux, ce bit est un **0** (LAN1) et pour l'autre, un **1** (LAN2).

La création de sous réseaux permet de disposer de deux adresses réseaux :

192.168.1.0 (/25) → Adresse : 11000000.10101000000000001.00000000

255.255.255.128 → Masque : 11111111.11111111.11111111.10000000



192.168.1.128 (/25) → Adresse : 11000000.10101000000000001.10000000

255.255.255.128 → Masque : 11111111.11111111.11111111.10000000

Figure III.2 Deux sous-réseaux

Pour chaque sous-réseau, examinons le dernier octet dans sa forme binaire. Les valeurs de cet octet pour les deux réseaux sont les suivantes :



**Sous-réseau LAN1 : 00000000 = 0**

**Sous-réseau LAN2 : 10000000 = 128**

Schéma d'adressage correspondant à ce réseau :

Pour le sous-réseau **LAN1** :

**Adresse réseau** : 192.168.1.0/25

**Plages d'hôtes** : [192.168.1.1 - 192.168.1.126]

**Adresse de diffusion** : 192.168.1.127

Pour le sous-réseau **LAN2** :

**Adresse réseau** : 192.168.1.128/25

**Plages d'hôtes** : [192.168.1.129 - 192.168.1.254]

**Adresse de diffusion** : 192.168.1.255

Les deux sous-réseaux ont reçus un même nombre d'adresses hôtes : 126.

### III.3 Adressage sans classe VLSM (Variable Length Subnet Mask)

Le système que nous utilisons aujourd'hui est *l'adressage sans classe*. Avec ce type d'adressage, des blocs d'adresses correspondant au nombre d'hôtes *nécessaires* sont attribués aux entreprises.

Le découpage d'un sous-réseau, qui revient à utiliser un masque de sous-réseau de longueur variable VLSM permet d'optimiser l'efficacité de l'adressage. Dans le cadre de la création classique de sous-réseaux, pour déterminer le nombre total d'hôtes, il est nécessaire d'attribuer le même nombre d'adresses à chaque sous-réseau. Si tous les sous-réseaux ont besoin d'un même nombre d'hôtes, l'utilisation de blocs d'adresses de taille fixe est intéressante. Mais, bien souvent, ce n'est pas le cas.

Par exemple, la topologie de la figure III.3 démontre qu'un réseau a besoin de sept sous-réseaux, un pour chacun des quatre réseaux locaux (LAN1, LAN2, LAN3 et LAN4) et un autre pour chacun des trois réseaux étendus (point à point).

Avec l'adresse 192.168.15.0, nous devons emprunter 3 des bits d'hôte du dernier octet (avec l'adressage classique) afin de créer sept sous-réseaux pour le réseau. Ces bits sont empruntés en redéfinissant les bits du masque de sous-réseau correspondant, à des 1, pour qu'ils soient utilisés comme bits réseau. Le dernier octet du masque est donc représenté au format binaire par 11100000, ce qui correspond au nombre 224. Le nouveau masque 255.255.255.224 est représenté avec la notation /27 pour indiquer un total de 27 bits alloués au réseau.

La forme binaire de ce masque de sous-réseau est la suivante:

**11111111.11111111.11111111.11100000**

Après avoir emprunté trois des bits d'hôte pour les bits réseau, il nous reste cinq bits d'hôtes. Ils permettent d'obtenir 30 hôtes par sous-réseau.

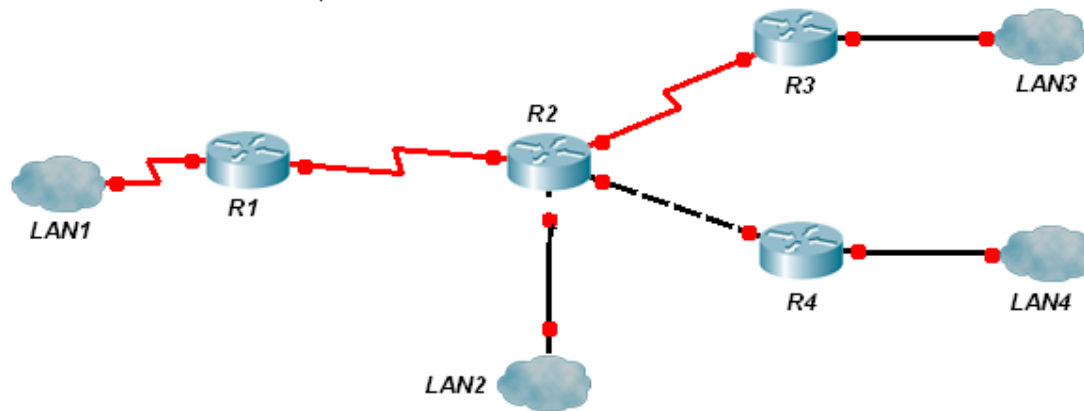


Figure III. 3 Réseau d'entreprise

Bien que nous ayons réussi à diviser le réseau en un nombre adéquat de sous-réseaux, nous avons gaspillé un nombre important d'adresses. Par exemple, seules deux adresses sont nécessaires dans chaque sous-réseau des liaisons de réseau étendu (point à point). Vingt-huit adresses n'ont pas été utilisées dans chacun des trois sous-réseaux du réseau étendu et sont bloquées dans ces blocs d'adresses. De plus, ce schéma ne laisse aucune place à un développement futur, puisqu'il réduit le nombre total de sous-réseaux disponibles. **Ce gaspillage d'adresses est spécifique à l'adressage par classe.**

Comment le découpage d'un sous-réseau peut être utilisé pour optimiser l'attribution d'adresses ?

Les administrateurs réseau doivent développer un schéma d'adressage inter-réseau de façon à pouvoir accueillir le nombre maximal d'hôtes pour chaque sous-réseau.

Pour cela, il faut calculer d'abord le nombre total d'hôtes dont a besoin l'inter-réseau entier de l'entreprise. Vous devez utiliser un bloc d'adresses suffisamment grand pour accueillir tous les périphériques de tous les réseaux de l'entreprise. Ces périphériques sont notamment des périphériques d'utilisateurs, des serveurs, des périphériques intermédiaires et des interfaces de routeur.

**Exemple :** Soit les besoins suivants d'une entreprise (figure III.3)

LAN1 : 58 adresses d'hôte

LAN2 : 26 adresses d'hôte

LAN3 : 10 adresses d'hôte

LAN4 : 10 adresses d'hôte

Trois (03) liaisons WAN (point à point) : 02 adresses d'hôte chacune.

Avec de tels besoins, il est évident que l'utilisation d'un schéma de création de sous-réseaux standard serait inefficace. Dans cet inter-réseau, la création de sous-réseaux standards nécessite que chaque sous-réseau ait des blocs fixes de 62 hôtes, ce qui implique que de nombreuses adresses potentielles seront gaspillées (le réseau LAN2 prend en charge 26 utilisateurs, et les réseaux LAN3 et LAN4 ne prennent en charge que 10 utilisateurs chacun).

Alors, avec le bloc d'adresses 192.168.15.0 /24, nous allons créer un schéma d'adressage à la fois pour répondre aux besoins et ne pas gaspiller d'adresses potentielles.

Lorsque vous créez un schéma d'adressage, commencez toujours par le besoin le plus important.

Commençons par créer des sous-réseaux pour le bloc d'adresses initial 192.168.15.0 /24. En appliquant la formule ***Nombre d'hôtes utilisables =  $2^n - 2$*** , nous déterminons que 6 bits d'hôte permettent d'obtenir 62 hôtes dans le sous-réseau. Ces 62 hôtes répondent au besoin de 58 hôtes du LAN1. Dans notre scénario, le réseau LAN1, avec 58 utilisateurs, représente le besoin le plus important. Nous avons besoin de 6 bits d'hôtes pour accueillir 58 hôtes, ce qui nous laisse 2 bits supplémentaires pour la partie réseau. Le préfixe de ce réseau serait /26 et le masque de sous-réseau 255.255.255.192

### **1. Attribution du réseau LAN1**

Calcul d'un sous-réseau à partir du bloc 192.168.15.0 /24 initial pour accueillir le plus grand réseau local, c'est-à-dire le LAN1 comportant 58 hôtes. Pour cela, il faut emprunter deux bits d'hôte afin d'utiliser un masque de bit /26.

Adresse : 192.168.15.0

Sous forme binaire : 11000000.10101000.00001111.00000000

Masque : 255.255.255.192

/26 bits en binaire : 11111111.11111111.11111111.11000000

Au lieu de poursuivre en utilisant le sous-réseau suivant, nous devons nous assurer que la taille de chaque sous-réseau correspond aux besoins en hôtes.

### **2. Attribution du réseau LAN2**

Nous nous intéressons aux besoins du plus grand sous-réseau suivant. Il s'agit du réseau LAN2 qui nécessite 26 adresses d'hôte, y compris pour l'interface du routeur. Nous devons commencer par l'adresse disponible suivante : 192.168.15.64 afin de créer un bloc d'adresses pour ce sous-réseau. En empruntant un bit supplémentaire, nous pouvons répondre aux besoins du LAN2 tout en minimisant le gaspillage d'adresses. Le bit emprunté fournit le masque /27 avec la plage d'adresses suivante :

192.168.15.64 /27, plage d'adresses d'hôte : 192.168.15.65 à 192.168.15.94

Ce bloc d'adresses fournit 30 adresses, ce qui permet de satisfaire le besoin de 28 hôtes et prévoit de la place pour le développement de ce sous-réseau.

### 3. Attribution du LAN3 et du LAN4

Les réseaux LAN3 et LAN4 nécessitent tous les deux 10 adresses d'hôte. Cette création de sous-réseaux nous permet d'emprunter un autre bit pour développer le masque jusqu'à /28. En commençant par l'adresse 192.168.15.96, nous obtenons les blocs d'adresses suivants, qui fournissent 14 adresses :

Sous-réseau 0 (LAN3) : 192.168.15.96 /28 plage d'adresses d'hôte : .97 à .110  
 Sous-réseau 1 (LAN4) : 192.168.15.112 /28 plage d'adresses d'hôte : .113 à .126

### 4. Attribution des WAN

Dans ces liaisons WAN (point à point), seules deux adresses sont nécessaires. Pour satisfaire ce besoin, nous empruntons 2 autres bits pour utiliser le masque /30. Avec les adresses disponibles suivantes, nous obtenons les blocs d'adresses suivants :

Sous-réseau 0 (R1-R2) : 192.168.15.128 /30 plage d'adresses d'hôte : .129 à .130  
 Sous-réseau 1 (R2-R3) : 192.168.15.132 /30 plage d'adresses d'hôte : .133 à .134  
 Sous-réseau 2 (R2-R4) : 192.168.15.136 /30 plage d'adresses d'hôte : .137 à .138

En résumé :

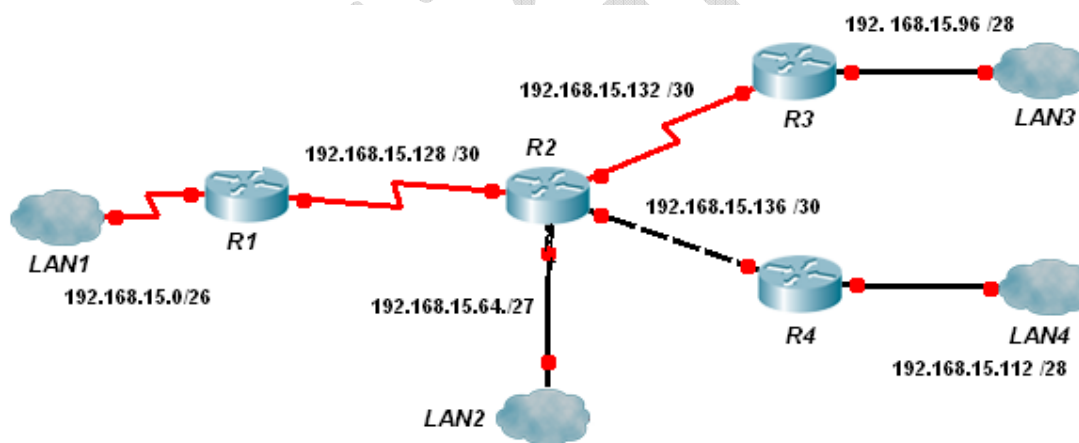


Figure III.4 Adressage VLSM

**Remarque :** En comparaison, l'adressage suivant montre comment 192.168.15.0 serait découpé en sous-réseaux à l'aide d'un adressage de blocs fixes pour fournir suffisamment de blocs d'adresses :

Sous-réseau 0 : 192.168.15.0 /26 plage d'adresses d'hôte : 1 à 62  
 Sous-réseau 1 : 192.168.15.64 /26 plage d'adresses d'hôte : 65 à 126  
 Sous-réseau 2 : 192.168.15.128 /26 plage d'adresses d'hôte : 129 à 190  
 Sous-réseau 3 : 192.168.15.192 /26 plage d'adresses d'hôte : 193 à 254

Les blocs fixes permettent d'obtenir seulement quatre sous-réseaux, c'est-à-dire un nombre insuffisant de blocs d'adresses pour cet inter réseau.