

2016

Cours réseau : Adressage IPv4



Donat FUZELLIER

Seo-webranking

02/11/2016

Table des matières

Le modèle O.S.I.	5
Explications du Modèle OSI	7
La couche physique.....	7
La couche liaison de données	7
La couche réseau	7
La couche transport	7
La couche session	8
La couche présentation.....	8
La couche application	8
Le modèle TCP/IP	8
La couche hôte réseau / Accès au réseau	8
La couche internet / Réseau	8
La couche transport	9
La couche application	9
Définitions :	9
IP	9
NAT	9
ICMP	10
OSPF.....	10
EIGRP	10
TCP.....	10
UDP	10
Exercice de contrôle de connaissance	10
Internet of Everything.....	11
Comment est vu une adresse ipv4 au sein des protocoles.....	11
L'adresse binaire	12
Une adresse décimale.....	13
Exemple basique de conversion :	14
Exercices :	17
Le masque de sous réseau	18
Les classes d'adresses	19
Classe A.....	19
Classe B	19
Classe C	19
Classe D.....	19
Classe E	19

L'adressage IP	
Espace d'adressage	20
Le découpage d'une classe en sous-réseaux.....	20
Exemple :	22
Tableau des masques de sous-réseau valides pour un octet IPv4	23
Notation CIDR	23
Adresse réseau	25
Adresse de l'hôte	25
Adresse de diffusion	26
Première adresse d'hôte.....	26
Dernière adresse d'hôte.	27
Masque de sous-réseau IPv4	27
Opération AND	27
Attribution statique	30
Attribution dynamique	31
Le protocole DHCP	31
Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion.....	32
Trafic monodiffusion.....	32
Transmission de diffusion	33
Diffusion dirigée.....	33
Diffusion limitée	33
Transmission multidiffusion.....	33
Adresses de multidiffusion	34
Clients multidiffusion.....	35
Résumé :	35
Les types d'adresses IPv4.....	36
Adresses privées	36
Adresses publiques	37
Adresses réseau et de diffusion	37
Bouclage	38
Adresses link-local	38
Adresses TEST-NET.....	38
Adresses expérimentales	39
Rappel : A titre informatif	39
Blocs d'adresses A.....	39
Blocs d'adresses B.....	39
Blocs d'adresses C.....	39
Limites de l'adressage par classe	40

L'adressage IP

Adressage sans classe	40
IANA et RIR	40
Voici les principaux registres :.....	41
FAI.....	41
Raccordement du FAI à Internet	41
8.1.4.7 Exercice - Adresses IPv4 publiques ou privées	44
Les adresses réseau IPv6.....	44
8.2.1.2 La coexistence des protocoles IPv4 et IPv6	44

Le modèle O.S.I.

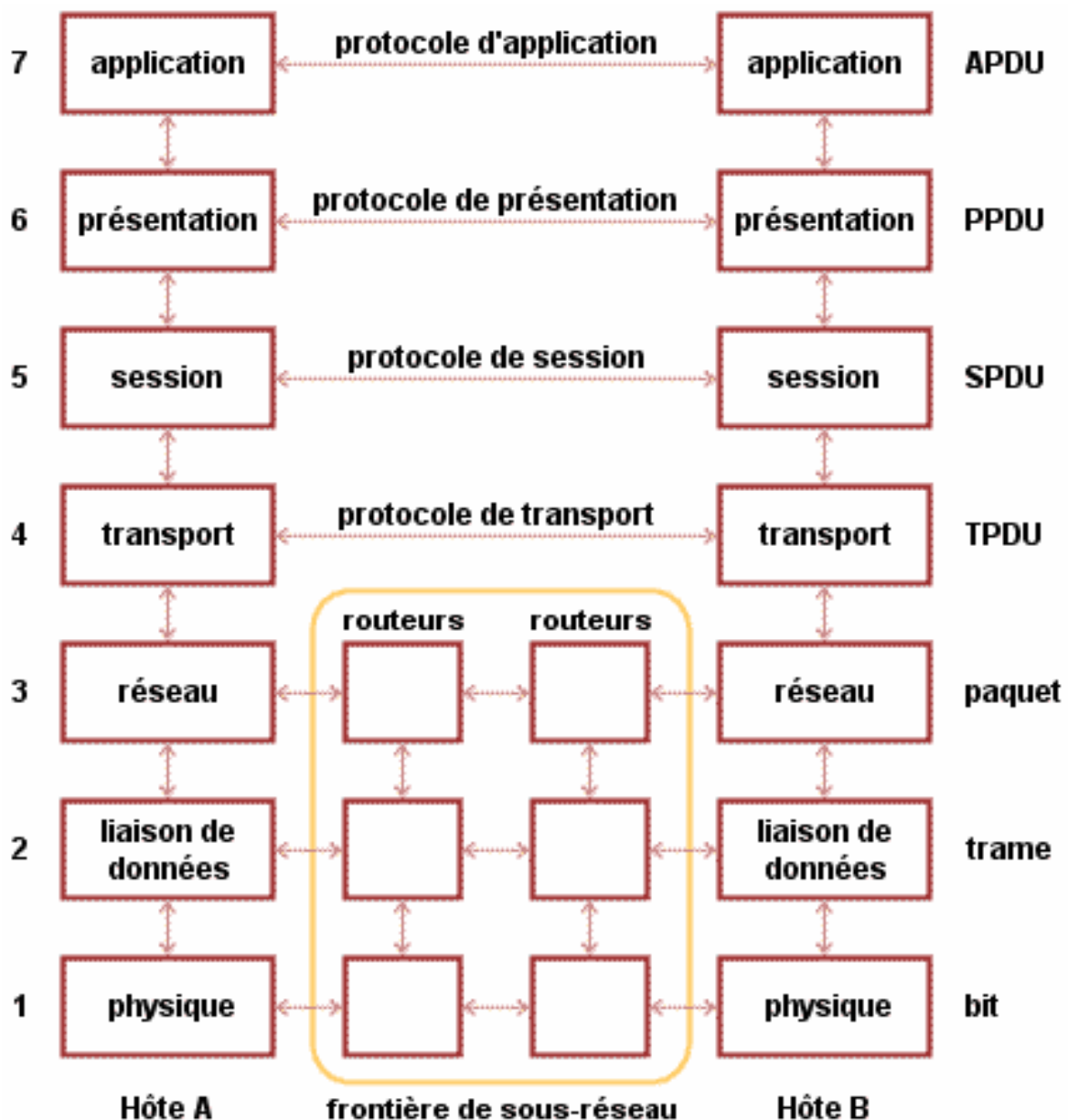
Au sein des couches du modèle O.S.I., l'adressage IP est une des fonctions les plus importantes de la couche réseau.

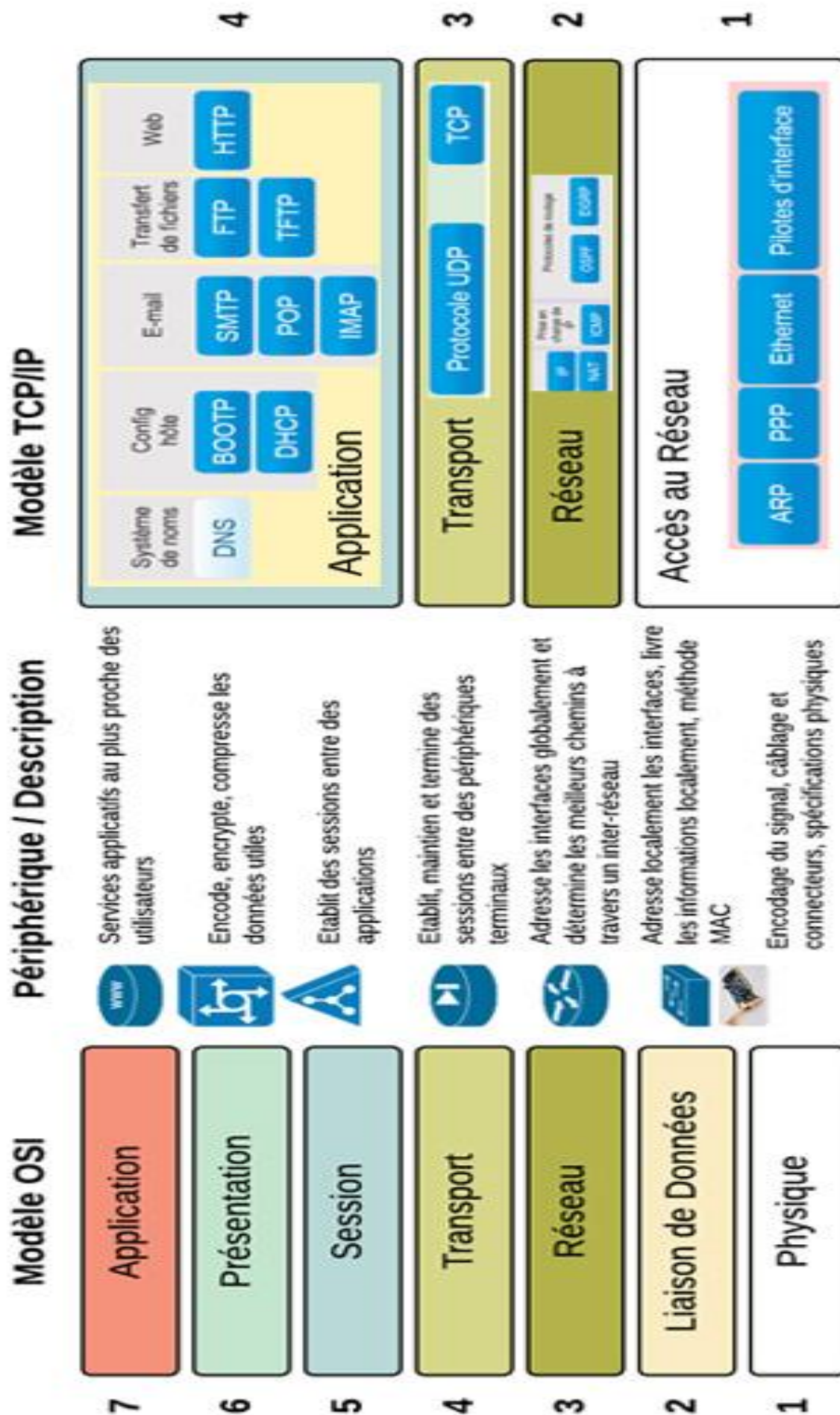
Le **modèle OSI** (de l'[anglais](#) *Open Systems Interconnection*) est un standard de communication, en [réseau](#), de [tous les systèmes informatiques](#). C'est un [modèle](#) de communications entre [ordinateurs](#) proposé par l'[ISO](#) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

Le modèle OSI regroupe sept couches de protocoles permettant la communication en réseau.

Astuce : Apprendre Pour Savoir Toujours Résoudre Les Problèmes. => A.P.S.T.R.L.P.

Au sein de la couche réseau, plusieurs protocoles s'appliquent : IP, NAT, ICMP, OSPF et EIGRP.





Explications du Modèle OSI

Les couches basses (1, 2, 3 et 4) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique.

Les couches 1 à 3 interviennent entre machines voisines, et non entre les machines d'extrémité qui peuvent être séparées par plusieurs routeurs.

Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques.

Les couches 4 à 7 sont des couches qui n'interviennent qu'entre hôtes distants.

La couche physique

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication.

- Elle garantit la transmission des données bits pour bits

La couche liaison de données

La couche de liaison, comme son nom l'indique lie les données.

- Elle transforme et fractionne les données d'entrée de l'émetteur en trames.
- Elle transmet des trames en séquence et gère les trames en réponse renvoyées par le récepteur.
- La couche liaison de données reconnaît les trames et est capable de renvoyer les trames s'il y a eu des problèmes de transmission, ainsi que de corriger les erreurs de la couche physique.
- Elle est chargée de l'adressage physique, de la topologie de réseau et de l'accès au media.

La couche réseau

C'est la couche qui permet de gérer le sous-réseau, ainsi que le routage des paquets et l'interconnexion des différents sous-réseaux entre eux.

- Il crée les requêtes qui garnissent les tables ARP.
- L'unité d'information de la couche réseau est le paquet.

La couche transport

Cette couche est responsable du bon acheminement des messages complets au destinataire.

Elle est responsable de la fiabilité d'une communication réseau entre des nœuds d'extrémité, fournit des mécanismes pour l'établissement, le maintien et la fermeture de circuits virtuels, ainsi que pour la détection des défaillances.

Le rôle principal de la couche transport est de prendre les messages de la couche session et le cas échéant de les découper en unités plus petites, de les transmettre à la couche réseau.

- Elle peut optimiser le réseau
- Elle contrôle le flux.
- C'est l'une des couches les plus importantes
- Elle qui fournit le service de base à l'utilisateur.

L'adressage IP

- Elle qui gère l'ensemble du processus de connexion.
- L'unité d'information de la couche réseau est le message.

La couche session

Cette couche organise et synchronise les échanges entre tâches distantes.

- Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties.
- Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...), c'est la gestion du jeton.
- La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.
- Elle se charge de la livraison des données, de la classe de service et de la signalisation des exceptions

La couche présentation

Cette couche peut convertir les données, les reformater, les crypter et les compresser.

- Elle traite l'information de manière à la rendre compatible entre tâches communicantes.
- Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.
- Elle est chargée des structures de données et de la négociation de la syntaxe de transfert des données

La couche application

Cette couche est le point de contact entre l'utilisateur et le réseau.

Exemple : le transfert de fichier, la messagerie...

- Elle apporte à l'utilisateur les services de base offerts par le réseau.

Cheminement

Les données sont segmentées puis mise en paquet et envoyer en trames sous forme de bits.

Le modèle TCP/IP

La couche hôte réseau / Accès au réseau

Cette couche est assez "étrange".

Elle regroupe les couches physiques et liaison de données du modèle OSI.

- Elle permet, à un hôte, d'envoyer des paquets IP sur le réseau.
- Beaucoup de réseaux locaux utilisent Ethernet;
- Ethernet est une implémentation de la couche hôte-réseau.

La couche internet / Réseau

Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Le point critique de cette couche est le routage.

- Elle réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion.

L'adressage IP

- Elle permet l'injection de paquets dans n'importe quel réseau
- Elle achemine des paquets indépendamment les uns des autres jusqu'à destination.
- On peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.
- Son Protocol officiel : le protocole IP (Internet Protocol).

La couche transport

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Elle utilise le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol).

La couche application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles.

Cette couche contient tous les protocoles de haut niveau.

- Telnet, TFTP (trivial File Transfer Protocol),
- SMTP (Simple Mail Transfer Protocol).
- HTTP (HyperText Transfer Protocol).
- TFTP (surtout utilisé sur réseaux locaux) utilisera UDP
on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée.
- Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP.
- SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs.

Définitions :

IP

Une **adresse IP** (avec IP pour [Internet Protocol](#)) est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque appareil connecté à un [réseau informatique](#) utilisant l'[Internet Protocol](#). L'adresse IP est à la base du système d'acheminement (le routage) des messages sur Internet.

NAT

En [réseau informatique](#), on dit qu'un [routeur](#) fait du **Network Address Translation** (NAT) (« translation d'adresse réseau »¹) lorsqu'il fait correspondre les [adresses IP](#) internes non uniques et souvent non routables d'un [intranet](#) à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur [Internet](#) à toutes les adresses d'un [réseau privé](#), et pallie ainsi l'[épuisement des adresses IPv4](#).

La fonction NAT dans un routeur de service intégré (ISR) traduit une adresse IP source interne en adresse IP globale.

Ce procédé est très largement utilisé par les box internet (ou modem routeur) des fournisseurs d'accès pour cacher nos ordinateurs domestiques derrière une seule identification publique.

ICMP

Internet Control Message Protocol est l'un des [protocoles](#) fondamentaux constituant la [suite des protocoles Internet](#). Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.

ICMP se situe au même niveau que le protocole [IP](#) bien qu'il ne fournisse pas les primitives de service habituellement associées à un protocole de [couche réseau](#). Son utilisation est habituellement transparente du point de vue des applications et des utilisateurs présents sur le [réseau](#).

OSPF

Open Shortest Path First (OSPF) est un [protocole de routage interne IP](#) de type « à état de liens ». Il a été développé au sein de l'[Internet Engineering Task Force](#) (IETF) à partir de 1987. La version actuelle d'OSPFv2 est décrite dans la [RFC 2328](#) en 1997. Une version 3 est définie dans la [RFC 2740](#) et permet l'utilisation d'OSPF dans un réseau [IPv6](#).

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) est un [protocole de routage](#) développé par [Cisco](#) à partir de leur protocole original [IGRP](#). EIGRP est un protocole de routage à vecteur de distance [IP](#), avec une optimisation permettant de minimiser l'instabilité de routage due aussi bien au changement de topologie qu'à l'utilisation de la bande passante et la puissance du processeur du routeur.

TCP

TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet.

- Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet.
- A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial.
- TCP s'occupe également du contrôle de flux de la connexion.

UDP

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là un avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

Exercice de contrôle de connaissance

01-adressage IP - contrôle de connaissance sur l'adressage OSI et TCP-IP

(Expression évoquant un monde où tous les ordinateurs et périphériques pourraient communiquer entre eux)

La prolifération des appareils connectés impose de fait, la solution de L'IPv6, IPv4 étant fortement assuré d'être saturer. Mais pourquoi IPv4 est sature...ou du moins risque-t-il de l'être.

Pour comprendre ceci, il nous faut faire une comparaison entre IPv4 et IPv6. Et en 1^{er} lieu découvrir Ipv4

Comment est vu une adresse ipV4 au sein des protocoles.

Le seul système de calcul qui est utilisé dans un ordinateur est le système binaire, historiquement, les 1er essais de création de machine à calculer reposaient sur les signaux électriques, bien avant l'apparition des 1^{er}s transistors, cet héritage technologique fonctionne toujours sur le principe de la notation binaire en base2

Avec seulement deux chiffres 1 et 0 ou 1 correspond à la présence d'un signal et zéro à son absence.

Mais alors comment est vu une adresse IP par l'ordinateur...

Une adresse IPv4 est constituée de 4 groupes de 8 chiffres, c'est un système en 32 bits.

Un bit pouvant seulement être ou ne pas être, (souvenez vous nous sommes en binaire).

Chaque périphérique d'un réseau doit être identifié par une adresse binaire unique. Dans les réseaux IPv4, cette adresse est représentée par une chaîne de 32 bits (composée de 1 et de 0)

Mais alors comment manipuler les adresses IPv4, il nous faut effectuer des conversions binaires.

Afin de comprendre la conversion binaire, il faut prendre en compte le fait que nous évoluons dans un système dit « a notation pondérée »...

J'en vois déjà qui sont perdu avec, binaire et pondère,

Un système a notation pondérée, c'est un moyen de noter des valeurs avec un seul indicateur, ce qui correspond au système binaire puisque, puisque le binaire, c'est être la ou pas !

Donc imaginez un tableau avec 8 cases, de droite à gauche, on va du plus petit vers le plus grand, et tout cela en base 2

Suivant le domaine d'activité, une puissance de deux se note :

- 2^n
- $2^{\wedge} n$
- $2^{**} n$
- $2 [3] n$
- $2 \uparrow n$
- puissance (2, n)
- $1 << n$
- $H_3(2, n)$
- $2 \rightarrow n \rightarrow 1$

Il existe plusieurs prononciations :

- 2 exposants n
- 2 puissances n
- 2 à la puissance n
- 2 élevé à la puissance n
- nième puissance de 2

Rappel : nous sommes dans un système 8 bits soit de 0 à 7 ...ne faite pas l'erreur de 1 à 8, sinon toute votre réflexion en serai faussé.

Soit 2^0 , 2^1 , 2^2 , 2^3 , 2^4 , 2^5 , 2^6 , 2^7

Ce qui donne, de droite à gauche...

BASE 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
DECIMAL	128	64	32	16	8	4	2	1
Bits	1	1	1	1	1	1	1	1
Valeur	255							

Il nous est plus facile de manipuler des nombres dans le système décimal que dans le système binaire, et ceci n'est pas difficile à comprendre, dans ce système 255 en décimal est égal à 1111 1111 en binaire.

Une adresse IPv4 étant constitué de 4 octets de 8 bits chacun sépare par un point (rappel système 32bits)

L'adresse binaire

11000000 10101000 00001010 00001010

est exprimée en décimale à point de la manière suivante :

192.168.10.10

Le système binaire ne comprenant que 2 chiffres, zéro et un, il nous faut réfléchir étape par étape, case par case, bit par bit...

Imaginez que vous deviez poser des questions à une personne qui ne peut dire que « oui » ou se taire...

L'adressage IP

Afin de progresser dans la conversation il va vous falloir décomposer votre question en espérant avoir une réponse ou pas... et bien pour convertir un nombre décimal en binaire, il va falloir faire de même.

Prenons la valeur décimale de 255, celle-ci correspond aux réponses aux questions suivantes....

On part de droite vers la gauche....

$255 - 1 = 254$ donc le 1bit de droite est actif.

$254 - 2 = 252$ donc le 2eme bit est actif.

$252 - 4 = 248$ donc le 3eme bit est actif.

$248 - 8 = 240$ donc le 4eme bit est actif.

$240 - 16 = 224$ donc le 5eme bit est actif.

$224 - 32 = 192$ donc le 6eme bit est actif.

$192 - 64 = 128$ donc le 7eme bit est actif.

$128 - 128 = 0$ donc le 8eme bit est actif.

Soit

$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255 \Rightarrow \text{CQFD.}$

De même si les bits sont tous sur zéro

Alors

$0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0$

Une combinaison différente de uns et de zéros donne une valeur décimale différente.

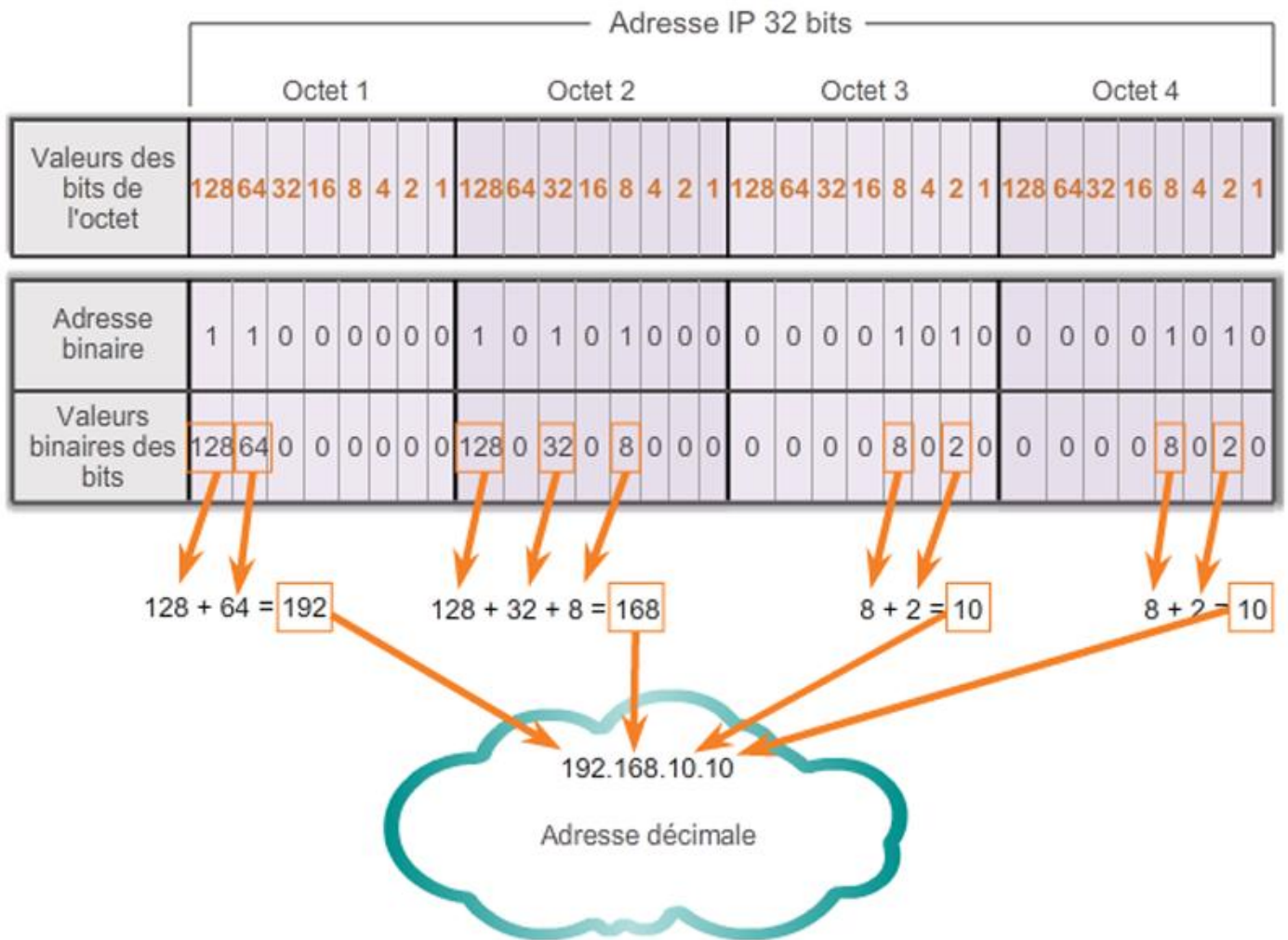
Une adresse décimale

192.168.10.10

Sous forme d'octets

192	168	10	10
1100 0000	1010 1000	0000 1010	0000 1010

Regarder la figure suivante, ceci devrai vous aider a mieux comprendre...



Les valeurs de positions chaque fois qu'un 1 binaire est présent.

- Si, dans un rang, la valeur est 0, n'ajoutez pas de valeur.
- Si les 8 bits sont des 0, 00000000, la valeur de l'octet est 0.
- Si les 8 bits sont des 1, 11111111, la valeur de l'octet est 255 (128+64+32+16+8+4+2+1).
- Si les 8 bits sont mixtes, les valeurs sont ajoutées. Par exemple, l'octet 00100111 a une valeur de 39 (32+4+2+1).

Ainsi, la valeur de chacun des quatre octets peut aller de 0 à 255 au maximum.

Exemple basique de conversion :

Pour l'adresse IP binaire suivante :

Nous avons 32 bits

11000000101010000000101000001010.

Découpons les 32 bits en 4 octets

11000000 10101000 00001010 00001010

L'adressage IP

Convertissons chaque octet en nombre décimal à l'aide d'un tableau.

N'hésitez pas à griffonner sur une feuille, un petit tableau a main levée.

Un OCTET de 8 Bits									Un OCTET de 8 Bits									Un OCTET de 8 Bits									Un OCTET de 8 Bits							
128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0		1	0	1	0	0	1	0	0		0	0	0	0	1	0	1	0		0	0	0	0	1	0	1	0
Quelques petites additions plus tard qui nous donne la somme de chaque bit pour chaque Octet.																																		
192								.	168								.	10								.	10							

Convertissez le nombre binaire en décimal !

- 1) 01011011 = 91.
- 2) 01001000 = 72.
- 3) 11010000 = 208
- 4) 01010111 = 87

Vu que nous travaillons avec des adresses IPv4 en décimal

Il nous faut régulièrement effectuer ce genre de conversions.

Il nous faut dans un 1^{er} temps, vérifier si la valeur décimale est comprise entre 0 et 255.

Le bit le plus à gauche d'un octet est désigné par l'appellation de « bit fort », en effet c'est bien la valeur la plus haute de notre série de 8 nombres.

L'adressage IP

Ce qui donne comme réflexion, par exemple pour 168

Quelle valeur a le bit de plus fort d'un octet ?

Réponse : 128

168 est-il supérieur ou égal au bit fort ?

Réponse : oui

Ce qui donne 1XXX XXXX

Donc $168 - 128 = 40$

On passe ensuite à bit de droite

Est-ce que 40 est \geq à 64

Réponse : Non,

Le 2ème bit est donc à zéro,

Nous passons au suivant...

Ce qui donne 10XX XXXX

$40 \geq$ à 32, oui

Le 3ème bit est actif.

$40 - 32 = 8$

Ce qui donne 101X XXXX

$8 \geq 16$, non

Ce qui donne 1010 XXXX

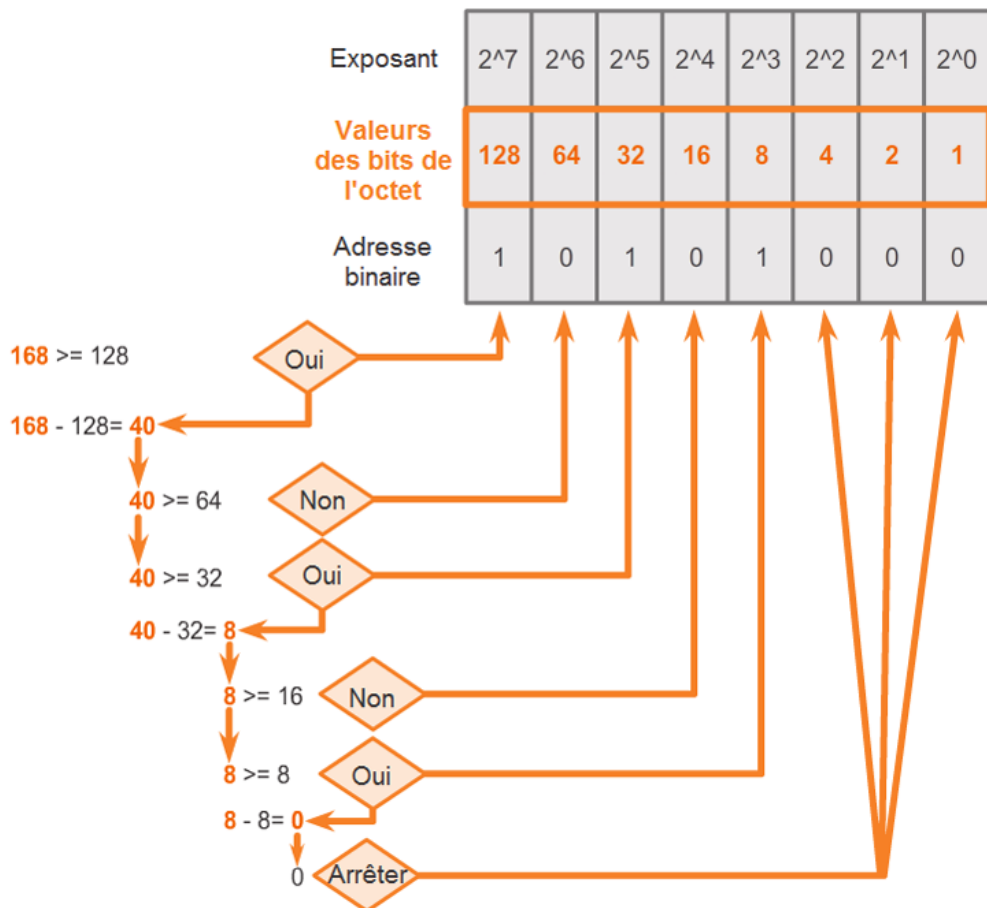
$16 - 8 = 8$

$8 \geq 8$, oui

Ce qui donne 1010 1XXX

$8 - 8 = 0$, tous les bits restant sont à zéro

Ce qui donne « 1010 1000 », La conversion de 168 en binaire est donc 10101000.





Adresse IPv4 binaire

Exercices :

En suivant les exemples suivant, convertissez ...

Valeur décimale	131							
Base	2	2	2	2	2	2	2	2
Exposant	7	6	5	4	3	2	1	0
Position	128	64	32	16	8	4	2	1
Bit	1	0	0	0	0	0	1	1

207 = 1100 1111

83 = 0101 0011

54 = 00110110

Le masque de sous réseau

A ce stade, vous devez avoir compris le principe de bits dans une adresse IPv4.

Maintenant, il nous faut comprendre que l'on distingue 2 parties dans une adresse Ipv4

Et c'est la conversion binaire d'une adresse IP qui vous permettra de dire si deux hôtes sont sur le même réseau

Il y a 2 parties dans une adresse réseau, respectivement, une partie réseau, et une partie hôtes.

Voyez cela comme un nom de famille et un prénom.

Dans le flux de 32 bits, une partie des bits constitue la partie réseau et une autre partie des bits compose la partie hôte.

Afin de déterminer la partie réseau d'une adresse IPv4, il nous faut connaître le masque de sous-réseau.

Mais qu'est-ce donc que le masque de sous réseau.

Alors pour la petite histoire, lors de la création des protocoles internet, certaines petites erreurs ont été commises, notamment dans l'attribution des adresses IPv4. Ce qui a été solutionné avec la création des masques de sous réseaux.

Lisez la partie suivante sur les classes d'adresses...

Sources : <http://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.class.html>

Les classes d'adresses

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement (ou le *routing*) des paquets entre les différents réseaux. Ces groupes ont été baptisés **classes d'adresses IP**. Ces classes correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum.

Classe A



Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

Classe B



Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

Classe C



Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

Classe D



Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits de poids fort égaux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (*host groups*).

Classe E

Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

Chacune de ses classes a de fait un nombre d'hôtes, restreint, et ce en fonction du nombre de bits encore disponible pour chaque octets, ce qui nous donne un espace d'adressage réseaux.

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques	adresses uniques
E	non défini	240.0.0.0 - 255.255.255.255	adresses uniques	adresses uniques

Le tableau ci-dessus montre que la distribution de l'espace d'adressage est mal répartie.

On ne dispose pas de classe intermédiaire entre A et B alors que l'écart entre les valeurs du nombre d'hôte par réseau est énorme. La répartition en pourcentages de l'espace total d'adressage IP est :

- Classe A - 50%
- Classe B - 25%
- Classe C - 12.5%
- Classe D - 6.25%
- Classe E - 6.25%

À cette mauvaise distribution de l'espace d'adressage, il faut ajouter les nombreuses critiques sur la façon dont les attributions de classes IP ont été gérées dans les premières années de l'Internet. Comme les classes ont souvent été attribuées sur simple demande sans corrélation avec les besoins effectifs, on parle d'un grand «gaspillage».

Au cours des années, plusieurs générations de solutions ont été apportées pour tenter de compenser les problèmes de distribution de l'espace d'adressage. Les sections suivantes présentent ces solutions dans l'ordre chronologique.

Le découpage d'une classe en sous-réseaux

Pour compenser les problèmes de distribution de l'espace d'adressage IP, la première solution utilisée a consisté à découper une classe d'adresses IP A, B ou C en sous-réseaux. Cette technique appelée *subnetting* a été formalisée en 1985 avec le document [RFC950](#).

Si cette technique est ancienne, elle n'en est pas moins efficace face aux problèmes d'exploitation des réseaux contemporains. Il ne faut jamais oublier que le découpage en réseaux ou sous-réseaux permet de cloisonner les domaines de diffusion.

Les avantages de ce cloisonnement de la diffusion réseau sont multiples.

- Au quotidien, on évite l'engorgement des liens en limitant géographiquement les annonces de services faites par les serveurs de fichiers.
- Les services Microsoft™ basés sur netBT sont particulièrement gourmands en diffusion réseau.

En effet, bon nombre de tâches transparentes pour les utilisateurs supposent que les services travaillent à partir d'annonces générales sur le réseau.

L'adressage IP

Sans ces annonces par diffusion, l'utilisateur doit désigner explicitement le service à utiliser. Le service d'impression est un bon exemple.

- Il existe quantité de vers et/ou virus dont les mécanismes de propagation se basent sur une reconnaissance des cibles par diffusion.

Le ver *Sasser* en est un exemple caractéristique. Voir <https://fr.wikipedia.org/wiki/Sasser>

En segmentant un réseau en plusieurs domaines de diffusion, on limite naturellement la propagation de code malveillant.

Le **subnetting** devient alors un élément de la panoplie des outils de sécurité.

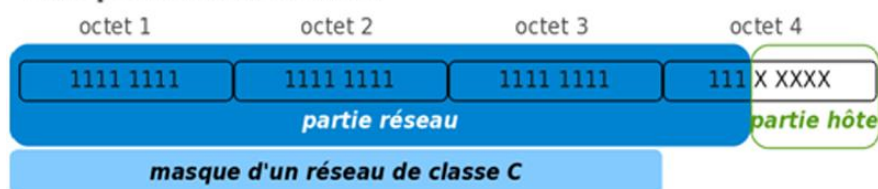
Pour illustrer le fonctionnement du découpage en sous-réseaux, on utilise un exemple pratique. On reprend l'exemple de la classe C 192.168.1.0 dont le masque réseau est par définition 255.255.255.0.

Sans découpage, le nombre d'hôtes maximum de ce réseau est de 254. Considérant qu'un domaine de diffusion unique pour 254 hôtes est trop important, on choisit de diviser l'espace d'adressage de cette adresse de classe C.

On *réserve* 3 bits supplémentaires du 4ème octet en complétant le masque réseau.

De cette façon on augmente la partie réseau de l'adresse IP et on diminue la partie hôte.

Masque réseau étendu



Adresse 192.168.1.0 avec *subnetting* sur 3 bits

Adresse réseau	192.168. 1. 0	Plage d'adresses utilisables	Adresse de diffusion
Masque de réseau	255.255.255.224		
Sous-réseau 0	192.168. 1. 0	192.168.1. 1 - 192.168.1. 30	192.168.1. 31
Sous-réseau 1	192.168. 1. 32	192.168.1. 33 - 192.168.1. 62	192.168.1. 63
Sous-réseau 2	192.168. 1. 64	192.168.1. 65 - 192.168.1. 94	192.168.1. 95
Sous-réseau 3	192.168. 1. 96	192.168.1. 97 - 192.168.1.126	192.168.1.127
Sous-réseau 4	192.168. 1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
Sous-réseau 5	192.168. 1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
Sous-réseau 6	192.168. 1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
Sous-réseau 7	192.168. 1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

L'adressage IP

Selon les termes du document [RFC950](#), les sous-réseaux dont les bits de masque sont tous à 0 ou tous à 1 ne devaient pas être utilisés pour éviter les erreurs d'interprétation par les protocoles de routage dits *classful*.

Comme RIPv1. En effet, ces protocoles de routages de «première génération» ne véhiculaient aucune information sur le masque sachant que celui-ci était déterminé à partir de l'octet le plus à gauche.

Dans notre exemple ci-dessus, il y avait confusion aux niveaux de l'adresse de réseau et de diffusion.

- L'adresse du sous-réseau 192.168.1.0 peut être considérée comme l'adresse réseau de 2 réseaux différents : celui avec le masque de classe C (255.255.255.0) et celui avec le masque complet après découpage en sous-réseaux (255.255.255.224).
- De la même façon, l'adresse de diffusion 192.168.1.255 est la même pour 2 réseaux différents : 192.168.1.0 ou 192.168.1.224.

Depuis la publication du document [RFC950](#), en 1985, les protocoles de routage qui servent à échanger les tables d'adresses de réseaux connectés entre routeurs ont évolué. Tous les protocoles contemporains sont conformes aux règles de routage inter-domaine sans classe (CIDR).

Les protocoles tels que RIPv2, OSPF et BGP intègrent le traitement des masques de sous-réseaux. Ils peuvent même regrouper ces sous-réseaux pour optimiser le nombre des entrées des tables de routage.

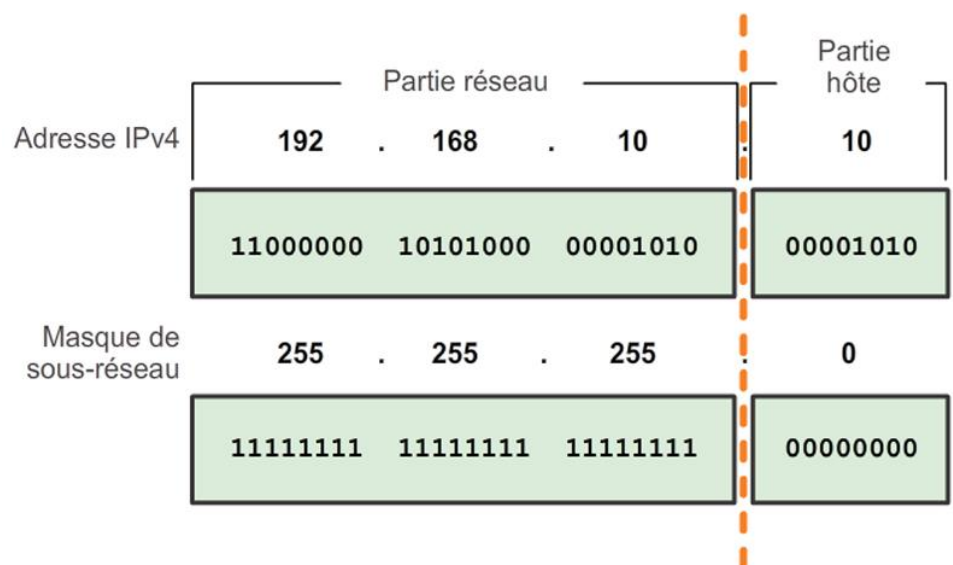
Pour appuyer cet argument, le document [RFC1878](#) de 1995 spécifie clairement que la pratique d'exclusion des sous-réseaux *all-zeros* et *all-ones* est obsolète.

Donc, afin de connaître la partie hôtes de notre IPv4, le masque de sous-réseau est indispensable.

Exemple :

Adresse IPv4 :
192.168.10.10 - Masque
de sous-réseau :
255.255.255.0

Afin de différencier la
partie réseau et hôtes de
l'adresse
IPv4 192.168.10.10.



Il nous faut de nouveau convertir en binaire chaque octets du masque et les octets à zéro nous indiqueront la partie hôtes.

Reste ensuite à indiquer à l'hôte, son masque de sous-réseau, ainsi celui-ci saura à quel réseau il appartient.

Tableau des masques de sous-réseau valides pour un octet IPv4

Valeur du masque de sous-réseau	Valeur du bit							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Notre couple IPv4 et netmask (masque de sous réseau) devient donc évident.

Il nous est possible de noter le masque de sous réseau en fonction de son nombre de Bits.

On dit que l'on indique la longueur du préfixe

Ce qui donne pour :

IPv4 : 192.168.10.10 sur 32 bits

Netmask : 255.255.255.0 sur 24bits

Ce qui peut aussi se noter 192.168.10.10/24

Notation CIDR

La valeur située après le « / » ou « slash » (barre oblique) indiquant le nombre de bits étant à « 1 » dans le masque, soit ici 24 bits.

un bloc est défini par le préfixe (par exemple 192.168.0.0) suivi de / puis du nombre de bits représentant la taille du bloc.

par exemple /20 indiquera que les 20 premiers bits de gauche représentent la taille du bloc d'adresses ou bien le masque réseau.

La taille du bloc sera en fait de $2^{(32-n)}$:

L'adressage IP

Dans le cas de /20 le bloc fera 2^{12} soit 4096 adresses ip .

En fonction du nombre d'hôtes voulu le masque devra être adapté afin de ne pas diffuser sur une trop large plage d'IPv4. Nous verrons cela par la suite.

En regardant la figure suivante, nous pouvons remarquer que l'adresse réseau peut rester inchangée, mais que la plage d'hôtes et l'adresse de diffusion varient selon les longueurs de préfixe.

Nous pouvons voir que le nombre d'hôtes accessibles sur le réseau varie lui aussi.

Décimale à point		Bits significatifs affichés en binaire
Adresse réseau	10.1.1.0/24	10.1.1.00000000
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.254	10.1.1.11111110
Adresse de diffusion	10.1.1.255	10.1.1.11111111
Nombre d'hôtes: $2^8 - 2 = 254$ hôtes		

Adresse réseau	10.1.1.025	10.1.1.00000000
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.126	10.1.1.01111110
Adresse de diffusion	10.1.1.127	10.1.1.01111111
Nombre d'hôtes: $2^7 - 2 = 126$ hôtes		

Adresse réseau	10.1.1.026	10.1.1.00000000
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.62	10.1.1.00111110
Adresse de diffusion	10.1.1.63	10.1.1.00111111
Nombre d'hôtes: $2^6 - 2 = 62$ hôtes		

Adresse réseau	10.1.1.027	10.1.1.00000000
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.30	10.1.1.00111110
Adresse de diffusion	10.1.1.31	10.1.1.00111111
Nombre d'hôtes: $2^5 - 2 = 30$ hôtes		

Adresse réseau	10.1.1.028	10.1.1.00000000
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.14	10.1.1.00001110
Adresse de diffusion	10.1.1.15	10.1.1.00001111
Nombre d'hôtes: $2^4 - 2 = 14$ hôtes		

L'adressage IP

Nous savons maintenant qu'une adresse IPv4 est constituée de 2 parties, et que la partie réseau est connu grâce au masque de sous réseau.

- Que ceci se démontre en effectuant la conversion en binaire et
- En fonction du masque de sous réseau choisis nous obtenons un nombre d'hôtes précis.

Et bien sachez qu'il existe trois sortes d'adresse comprises dans la plage d'adresses de chaque réseau IPv4 :

- Adresse réseau
- Adresses d'hôte
- Adresse de diffusion

Adresse réseau

L'adresse réseau est généralement utilisée pour faire référence à un réseau.

Le masque de sous-réseau ou la longueur du préfixe peuvent aussi être utilisés pour décrire une adresse réseau.

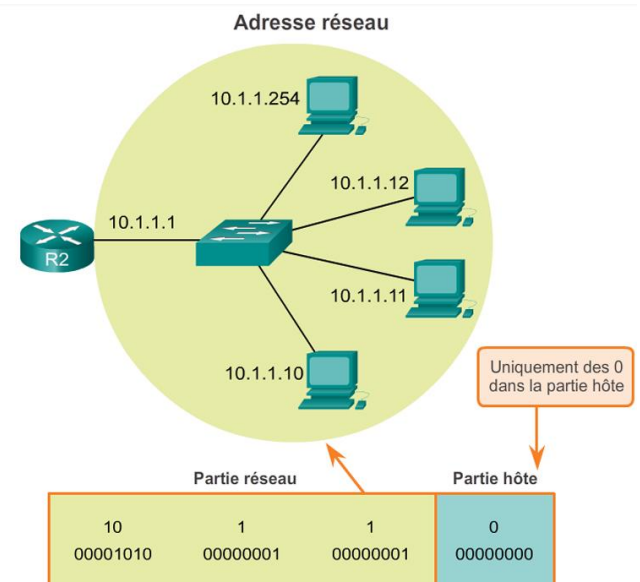
Par exemple, le réseau présente ici, peut être appelé le réseau 10.1.1.0, le réseau 10.1.1.0 255.255.255.0 ou le réseau 10.1.1.0/24.

Tous les hôtes du réseau 10.1.1.0/24 auront la même partie réseau.

Dans la plage d'adresses IPv4 d'un réseau, la première adresse est réservée à l'adresse réseau.

La partie adresse de cette adresse comprend uniquement des 0.

Tous les hôtes du réseau partagent la même adresse réseau.

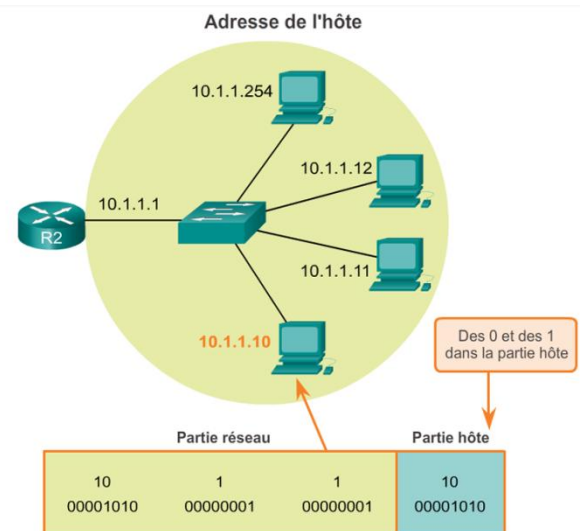


Adresse de l'hôte

Chaque périphérique final nécessite une adresse unique pour communiquer sur le réseau.

Avec les adresses IPv4, les valeurs comprises entre l'adresse réseau et l'adresse de diffusion peuvent être attribuées aux périphériques finaux d'un réseau.

Comme ici, la partie hôte de cette adresse est composée de n'importe quelle combinaison de bits 0 et 1, mais ne peut pas contenir uniquement des bits 0 ou 1.



Adresse de diffusion

L'adresse de diffusion IPv4 est une adresse spécifique, attribuée à chaque réseau.

Elle permet de transmettre des données à l'ensemble des hôtes d'un réseau.

Pour envoyer les données à tous les hôtes d'un réseau en une seule fois, un hôte peut envoyer un paquet adressé à l'adresse de diffusion du réseau : chaque hôte du réseau qui recevra ce paquet en traitera le contenu.

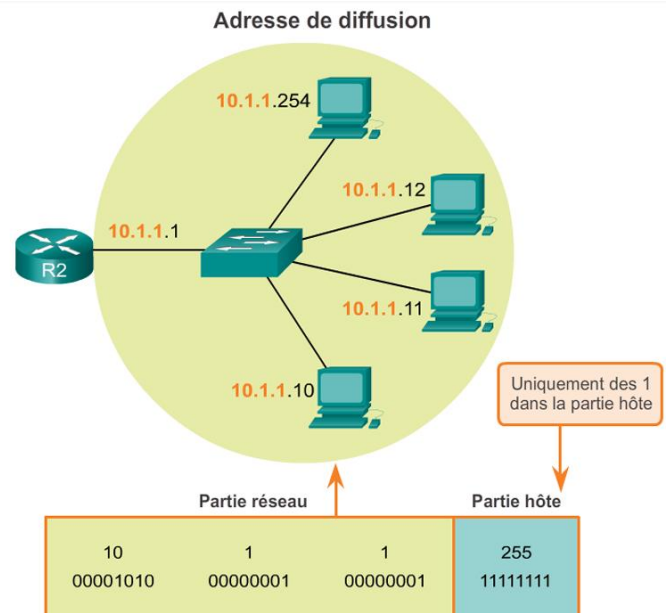
L'adresse de diffusion correspond à la plus grande adresse de la plage d'adresses d'un réseau.

Il s'agit de l'adresse dans laquelle les bits de la partie hôte sont tous à « 1 ».

Un octet au format binaire ne comportant que des 1 correspond au nombre 255 en notation décimale. Par conséquent, pour le réseau 10.1.1.0/24, dans lequel le dernier octet est utilisé pour la partie hôte, l'adresse de diffusion serait 10.1.1.255.

ATTENTION : la partie hôte n'est pas toujours un octet entier !

Cette adresse est également désignée sous le nom de diffusion dirigée.

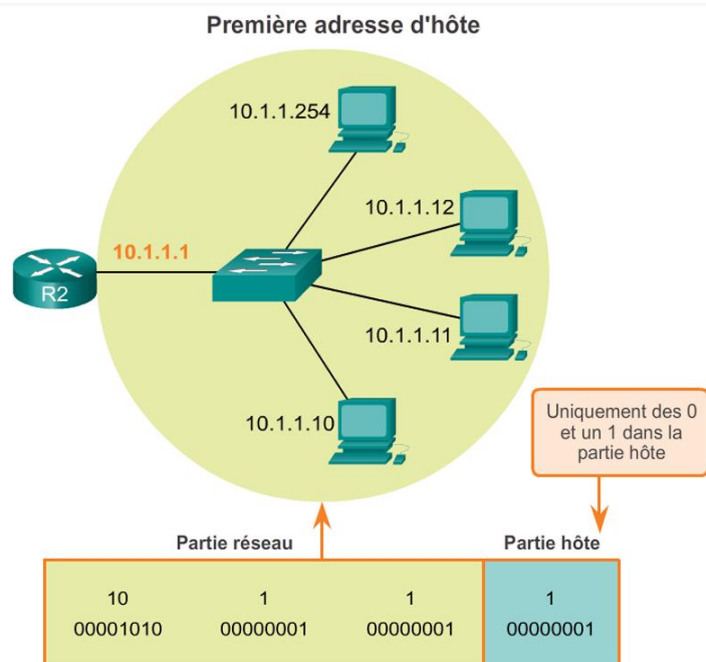
**Première adresse d'hôte.**

Maintenant que nous avons un masque de sous réseau, il nous faut définir la plage d'IPv4 de sous réseau.

Cette plage va de la 1^{ère} IPv4 à la dernière du réseau. Les hôtes du réseau se verront attribuer des adresses IPv4 dans cette plage.

La première adresse de la plage est toujours supérieur de 1 à la partie réseau et correspond toujours au bit le plus faible de la partie hôte.

Soit pour le réseau 10.1.1.0/24, 10.1.1 Pour la partie réseau et 1 pour la partie hôte, donc la première IPv4 de la plage est : 10.1.1.1. De nombreux schémas d'adressage utilisent la première adresse d'hôte pour le routeur ou la passerelle par défaut.

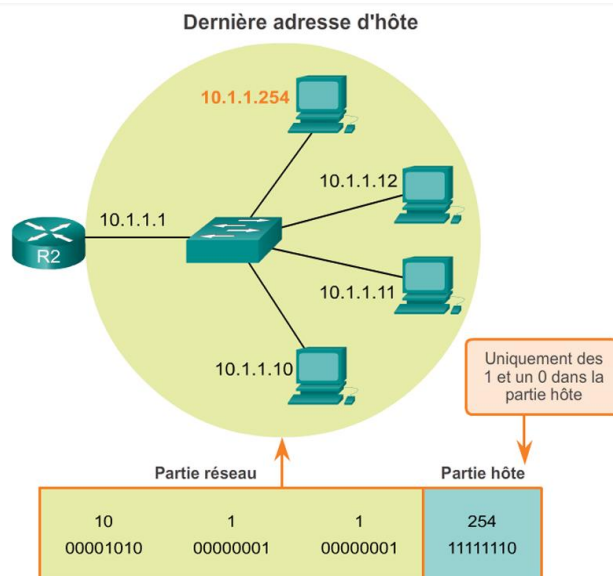


Dernière adresse d'hôte.

Le masque étant sur 24 bits, la dernière IPv4 sera égal à tous les bits restant à « 1 » de la partie hôte.

Attention, on tient compte de la première IPv4 du réseau.

Le bit le plus faible étant utilisé celui-ci ne sera pas disponible dans la dernière IPv4. Ce qui nous donne 10.1.1.254



Masque de sous-réseau IPv4

Si un périphérique ce voit attribuer une adresse IPv4, il utilisera le masque de sous-réseau pour résoudre et découvrir l'adresse réseau.

Lors de l'envoi de donnée sur le réseau, le périphérique va déduire si l'adresse IP de destination fait partie de son réseau ou non en effectuant une opération en comparant son masque de sous réseau avec celui de la destination. Si les bits de réseau correspondent, l'hôte source et l'hôte de destination sont sur le même réseau, et le paquet peut être transmis localement, sinon il enverra vers la passerelle par défaut qui gérera l'envoi vers l'autre réseau.

Cette résolution s'effectue en binaire, par l'intermédiaire de opération AND.

Opération AND

Il s'agit de l'une des trois opérations binaires de base, appliquées en logique numérique.

Les deux autres sont les opérations OR (OU) et NOT (NON). Bien que les trois soient utilisées dans les réseaux de données, l'opération AND permet de déterminer l'adresse réseau.

De ce fait, nous aborderons uniquement l'opération logique AND.

L'opération logique AND consiste à comparer deux bits, ce qui donne le résultat suivant :

Rappeler vous, nous sommes en système binaire, il n'y a donc que deux valeurs disponibles, 0 ou 1

1 AND 1 = 1, 0 AND 1 = 0, 0 AND 0 = 0, 1 AND 0 = 0. Seul 1 AND 1 retourne 1, c'est assez simple à calculer.

Si l'adresse IPv4 est			
Binaire		Décimal	
Partie réseau	Partie hôte	Partie réseau	Partie hôte
1100 0000 1010 1000 0000 1010	0000 1010	192.160.10	10
Et que le masque est			
1111 1111 1111 1111 1111 1111 0000 0000		255.255.255.0	
Alors on applique AND pour obtenir l'adresse réseau			
1100 0000 1010 1000 0000 1010 0000 0000		192.168.10.0	

L'adressage IP

Nota ; dans une adresse IPv4, La partie hôte de l'adresse réseau ne sera alors composée que de 0.

Pour une adresse IP spécifique et son sous-réseau, l'opération AND permet de déterminer à quel sous-réseau l'adresse appartient, ainsi que les adresses appartenant au même sous-réseau.

N'oubliez pas que si deux adresses se trouvent sur le même réseau ou sous-réseau, elles sont considérées comme locales et peuvent donc communiquer directement entre elles.

Les adresses qui ne sont pas sur le même réseau ou sous-réseau sont considérées comme distantes et doivent donc avoir un périphérique de couche 3 (voir le model OSI) (tel qu'un routeur ou un commutateur de couche 3) entre elles pour communiquer.

En cas de vérification réseau ou de recherche de panne réseau, chose que vous aurez à faire régulièrement, il faut souvent déterminer si deux hôtes sont sur le même réseau local.

Cela n'est possible que si l'on se pose dans la perspective des périphériques réseau.

Suite à une mauvaise configuration, un hôte peut s'identifier sur un réseau qui n'était pas celui prévu à l'origine.

Cela peut créer un fonctionnement imprévisible, sauf si le problème est identifié en examinant les processus d'opération AND utilisés par l'hôte.

Exercice de base avec la calculatrice Windows...

01-adressage IP - 8.1.2.7 Lab - Using the Windows Calculator with Network Addresses – ILM

01-adressage IP - 8.1.2.8 Lab - Converting IPv4 Addresses to Binary – ILM

	10	61	74	246
Adresse de l'hôte	10	61	74	246
Masque de sous-réseau	255	255	240	0
Adresse de l'hôte en notation binaire	00001010	00111101	01001010	11110110
Masque de sous-réseau (format binaire)	11111111	11111111	11110000	00000000
Adresse réseau en notation binaire	00001010	00111101	01000000	00000000
Adresse du réseau (format décimal)	10	61	64	0

	10	161	113	33
Adresse de l'hôte	10	161	113	33
Masque de sous-réseau	255	255	255	240
Adresse de l'hôte en notation binaire	00001010	10100001	01110001	00100001
Masque de sous-réseau (format binaire)	11111111	11111111	11111111	11110000
Adresse réseau en notation binaire	00001010	10100001	01110001	00100000
Adresse du réseau (format décimal)	10	161	113	32

	10	223	219	125
Adresse de l'hôte	10	223	219	125
Masque de sous-réseau	255	255	252	0
Adresse de l'hôte en notation binaire	00001010	11011111	11011011	01111101
Masque de sous-réseau (format binaire)	11111111	11111111	11111100	00000000
Adresse réseau en notation binaire	00001010	11011111	11011000	00000000
Adresse du réseau (format décimal)	10	223	216	0

	10	218	197	218
Adresse de l'hôte	10	218	197	218
Masque de sous-réseau	255	255	255	240
Adresse de l'hôte en notation binaire	00001010	11011010	11000101	11011010
Masque de sous-réseau (format binaire)	11111111	11111111	11111111	11110000
Adresse réseau en notation binaire	00001010	11011010	11000101	11010000
Adresse du réseau (format décimal)	10	218	197	208

Adresse de l'hôte	10	86	216	163
Masque de sous-réseau	255	255	255	128
Adresse de l'hôte en notation binaire	00001010	01010110	11011000	10100011
Masque de sous-réseau (format binaire)	11111111	11111111	11111111	10000000
Adresse réseau en notation binaire	00001010	01010110	11011000	10000000
Adresse du réseau (format décimal)	10	86	216	128

Comme vous le constaterai par la suite, la plupart des hôtes d'un réseau sont des périphériques finaux :

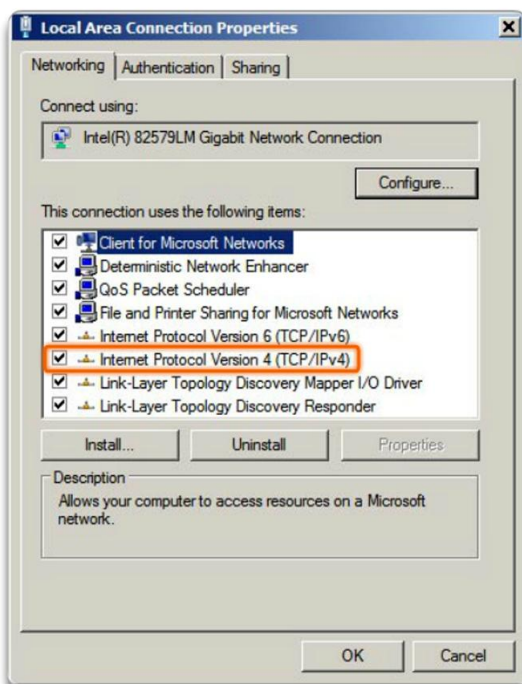
- Ordinateurs.
- Téléphones IP.
- Imprimantes.
- Tablettes.
- Smartphones.

On attribue le plus grand nombres d'adresses IPv4 de la plage IP du réseau aux hôtes du réseau.

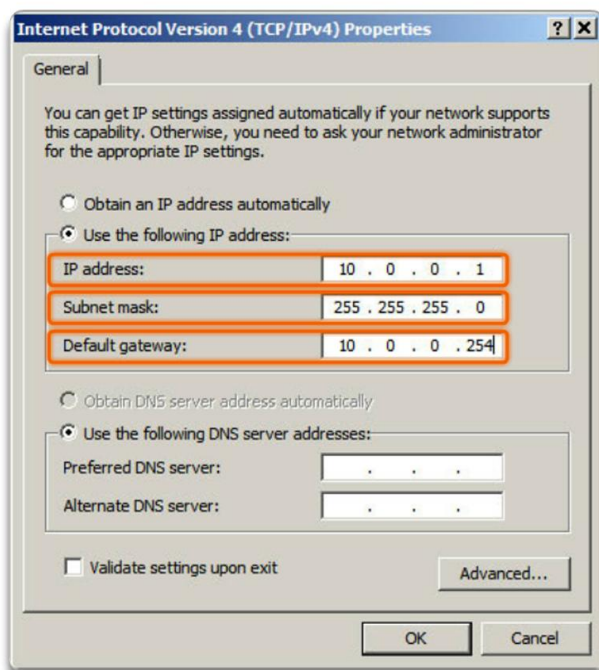
Les adresses IP peuvent être attribuées de manière statique ou de manière dynamique.

Attribution statique

Propriétés d'interface LAN



Configuration d'une adresse IPv4 statique



Lors de la configuration d'une adresse Ip statique, vous devez configurer manuellement les informations requise

- L'adresse IP.
- Le masque de sous reseau.
- La passerelle par défaut.

IL est indispensable de configurer une adresse IP statique sur certains périphériques , comme par exemple un serveur , une imprimante et les périphériques réseau qui ne sont pas amené a ce déplacer.

Les principaux avantages a configurer une adresse IP statique sur un poste hôte, est dans le fait que :

- Vous éliminer l'erreur possible de DHCP.
- Vous identifier formellement ce peripherique sur le reseau
- Vous tenez une liste precise et a jour des peripheriques du réseau.

Attribution dynamique

Sur les réseaux locaux, il n'est pas rare que les utilisateurs changent fréquemment.

Les nouveaux utilisateurs arrivent avec des ordinateurs portables et ont besoin d'une connexion. D'autres disposent de nouvelles stations de travail ou d'autres périphériques réseau, tels que des smartphones, qui doivent être connectés.

Plutôt que de demander à l'administrateur réseau d'attribuer des adresses IP à chaque station de travail, il est plus facile d'attribuer ces adresses automatiquement.

Le protocole DHCP (Dynamic Host Configuration Protocol

Le protocole DHCP permet l'attribution automatique des informations d'adressage, telles que l'adresse IP, le masque de sous-réseau, la passerelle par défaut et d'autres paramètres.

La configuration du serveur DHCP nécessite qu'un bloc d'adresses, appelé pool d'adresses, soit utilisé pour l'attribution aux clients DHCP d'un réseau. Les adresses attribuées à ce pool doivent être définies de manière à exclure toutes les adresses statiques utilisées par d'autres périphériques.

Le protocole DHCP est généralement la méthode d'attribution d'adresses IPv4 privilégiée pour les réseaux de grande taille, car le personnel de support du réseau est dégagé de cette tâche et le risque d'erreur de saisie est presque éliminé.

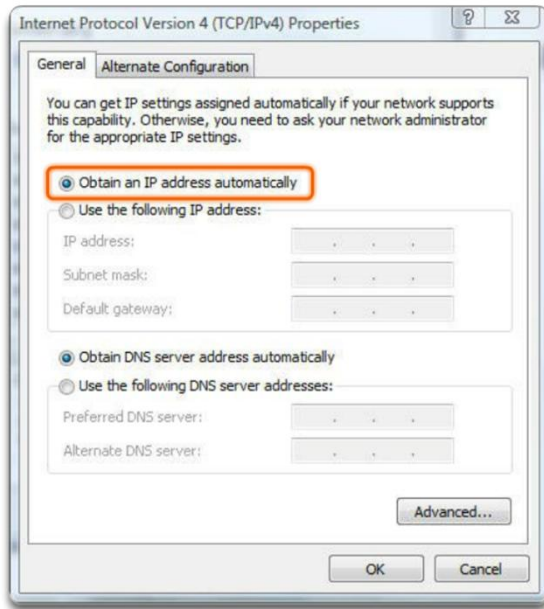
L'autre avantage de l'attribution dynamique réside dans le fait que les adresses ne sont pas permanentes pour les hôtes, elles sont uniquement « louées » pour une certaine durée. Si l'hôte est mis hors tension ou retiré du réseau, l'adresse est retournée au pool pour être réutilisée. Cela est particulièrement intéressant pour les utilisateurs mobiles qui se connectent et se déconnectent d'un réseau.

DHCP, est un protocole applicatif, il utilise UDP au niveau de la couche transport.

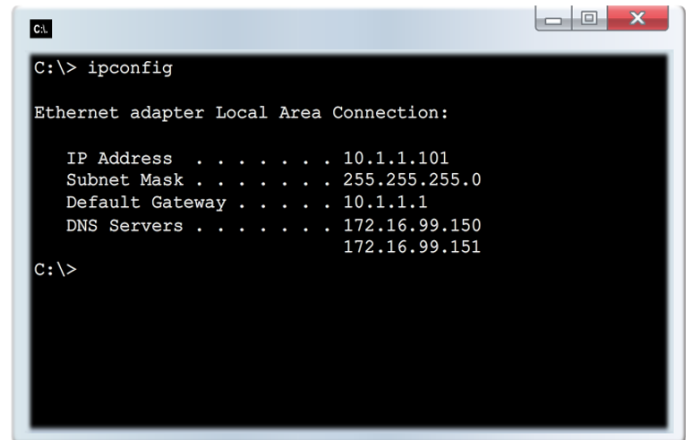
L'adressage IP

Si le protocole DHCP est activé sur un périphérique hôte, la commande **ipconfig** peut être utilisée pour afficher les informations sur l'adresse IP attribuée par le serveur DHCP, comme illustré à la Figure 2.

Attribution d'une adresse IPv4 dynamique



Vérification d'une adresse IPv4 dynamique



Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

Au sein d'un réseau IPv4, il existe trois façons de communiquer.

- **Monodiffusion** : processus consistant à envoyer un paquet d'un hôte à un autre hôte spécifique.
- **Diffusion** : processus consistant à envoyer un paquet d'un hôte à tous les hôtes du réseau.
- **Multidiffusion** : processus consistant à envoyer un paquet d'un hôte à un groupe d'hôtes en particulier (qui peuvent se trouver sur différents réseaux).

Trafic monodiffusion

- La monodiffusion est utilisée dans les communications normales d'hôte à hôte, que cela soit entre client et serveur, ou encore dans un réseau peer-to-peer. Les paquets de type monodiffusion utilisent les adresses de périphérique de destination comme adresses de destination et peuvent être routés sur un interréseau.

Dans un réseau en monodiffusion, l'adresse IP de la source et celle de la destination sont encapsulées dans le message.

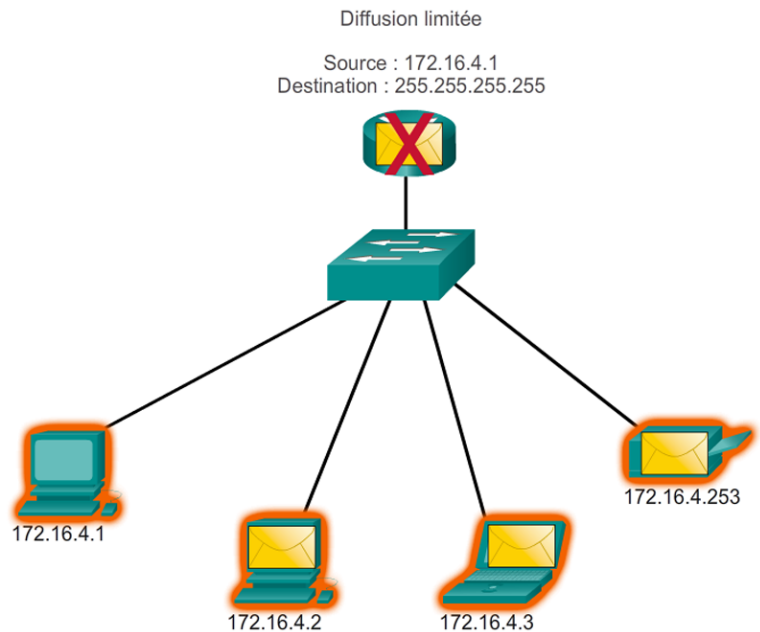
L'hôte source place dans l'en-tête du paquet monodiffusion son adresse IPv4 comme adresse source et l'adresse IPv4 de l'hôte de destination comme adresse de destination. Même si la destination spécifiée dans un paquet est une monodiffusion, une diffusion ou une multidiffusion, l'adresse source d'un paquet est toujours l'adresse de monodiffusion de l'hôte d'origine.

Transmission de diffusion

Le trafic de diffusion est utilisé pour envoyer des paquets à tous les hôtes du réseau grâce à l'adresse de diffusion du réseau. Avec une diffusion, le paquet contient une adresse IP de destination avec uniquement des un (1) dans la partie hôte. Cela signifie que tous les hôtes se trouvant sur ce réseau local (domaine de diffusion) recevront le paquet et le regarderont. De nombreux protocoles réseau, tels que DHCP, utilisent les diffusions. Lorsqu'un hôte reçoit un paquet envoyé à l'adresse de diffusion du réseau, il traite le paquet comme il le ferait pour un paquet adressé à son adresse de monodiffusion.

Voici quelques cas d'utilisation des transmissions de diffusion :

- Mappage des adresses d'une couche supérieure à des adresses d'une couche inférieure
- Demande d'une adresse
- Contrairement à une transmission de type monodiffusion où les paquets peuvent être routés via l'inter-réseau, 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

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. Bien que, par défaut, les routeurs n'acheminent pas les diffusions dirigées, ils peuvent être configurés de manière à le faire.

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.

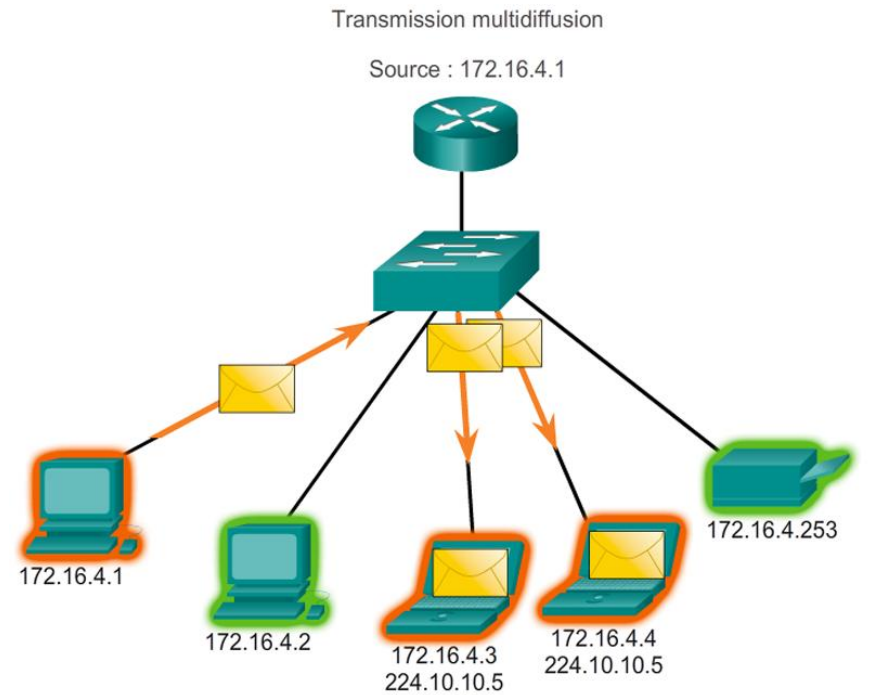
Transmission multidiffusion

L'adressage IP

La transmission multidiffusion permet de conserver la bande passante d'un réseau IPv4. Elle réduit le trafic en permettant à un hôte d'envoyer un paquet à un groupe d'hôtes spécifiques qui font partie d'un groupe de multidiffusion.

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. L'inter-réseau doit répliquer des flux de multidiffusion de façon efficace, afin qu'ils atteignent uniquement les destinataires visés.



Voici quelques exemples de transmission multidiffusion :

- Diffusions vidéo et audio
- Échange d'informations de routage entre des protocoles de routage
- Distribution de logiciels
- Jeu en ligne

Adresses de multidiffusion

L'IPv4 utilise un bloc d'adresses réservées pour s'adresser à des groupes de multidiffusion.

Cette plage d'adresses va de 224.0.0.0 à 239.255.255.255.

La plage d'adresses de multidiffusion est divisée en différents types d'adresse :

- les adresses link-local réservées
- les adresses d'étendue globale.

Il existe un autre type d'adresse de multidiffusion, dit adresses d'étendue administrative ou d'étendue limitée.

Les adresses de multidiffusion IPv4 du bloc 224.0.0.0 - 224.0.0.255 sont des adresses de liaison locales réservées.

Ces adresses s'appliquent aux groupes de multidiffusion d'un réseau local.

Un routeur connecté au réseau local sait que les paquets sont adressés à un groupe de multidiffusion link-local et ne transmet jamais ces paquets.

L'adressage IP

Les adresses link-local réservées s'appliquent principalement aux protocoles de routage qui utilisent le type de transmission multidiffusion pour échanger des informations de routage.

Les adresses d'étendue globale vont de 224.0.1.0 à 238.255.255.255.

Elles peuvent aussi être utilisées dans la multidiffusion de données sur Internet.

Par exemple, 224.0.1.1 est une adresse réservée au protocole NTP (Network Time Protocol) pour synchroniser les horloges des périphériques réseau.

Clients multidiffusion

Les hôtes qui reçoivent des données de multidiffusion spécifiques sont appelés des « clients multidiffusion ». Ces clients font appel à des services demandés par un programme client pour s'abonner au groupe de multidiffusion.

Chaque groupe de multidiffusion est représenté par une seule adresse de destination multidiffusion IPv4.

Lorsqu'un hôte IPv4 s'abonne à un groupe de multidiffusion, il traite les paquets adressés à cette adresse de multidiffusion, ainsi que ceux adressés à son adresse de monodiffusion, qui a été attribuée à lui seul.

Adresse/préfixe donné de **190.11.199.133/22**

Type d'adresse	Saisissez le dernier octet du préfixe de réseau en notation binaire	Entrez le DERNIER octet en notation décimale	Entrez l'adresse complète en notation décimale
Réseau	00000000	0	190.11.196.0
Diffusion	11111111	255	190.11.199.255
Première adresse d'hôte utilisable	00000001	1	190.11.196.1
Dernière adresse d'hôte utilisable	11111110	254	190.11.199.254

Contrôler

Réinitialiser

Nouvelles valeurs

Démonstration

Résumé :

- Le paquet de monodiffusion se déplace sur le réseau destiné à un périphérique spécifique
- Le paquet de diffusion est envoyé à chaque périphérique du réseau local.
- Le paquet de multidiffusion est envoyé à tous les périphériques, mais n'est traité que par ceux qui font partie du groupe de multidiffusion.

Plus d'info en ligne : <https://fr.wikipedia.org/wiki/Multicast>.

Rappel et précisions :

Les types d'adresses IPv4

Bien que la majorité des adresses d'hôte IPv4 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.

Adresses privées

Voici ces plages d'adresses privées :

10.0.0.0 à 10.255.255.255 (10.0.0.0/8)

172.16.0.0 à 172.31.255.255 (172.16.0.0/12)

192.168.0.0 à 192.168.255.255 (192.168.0.0/16)

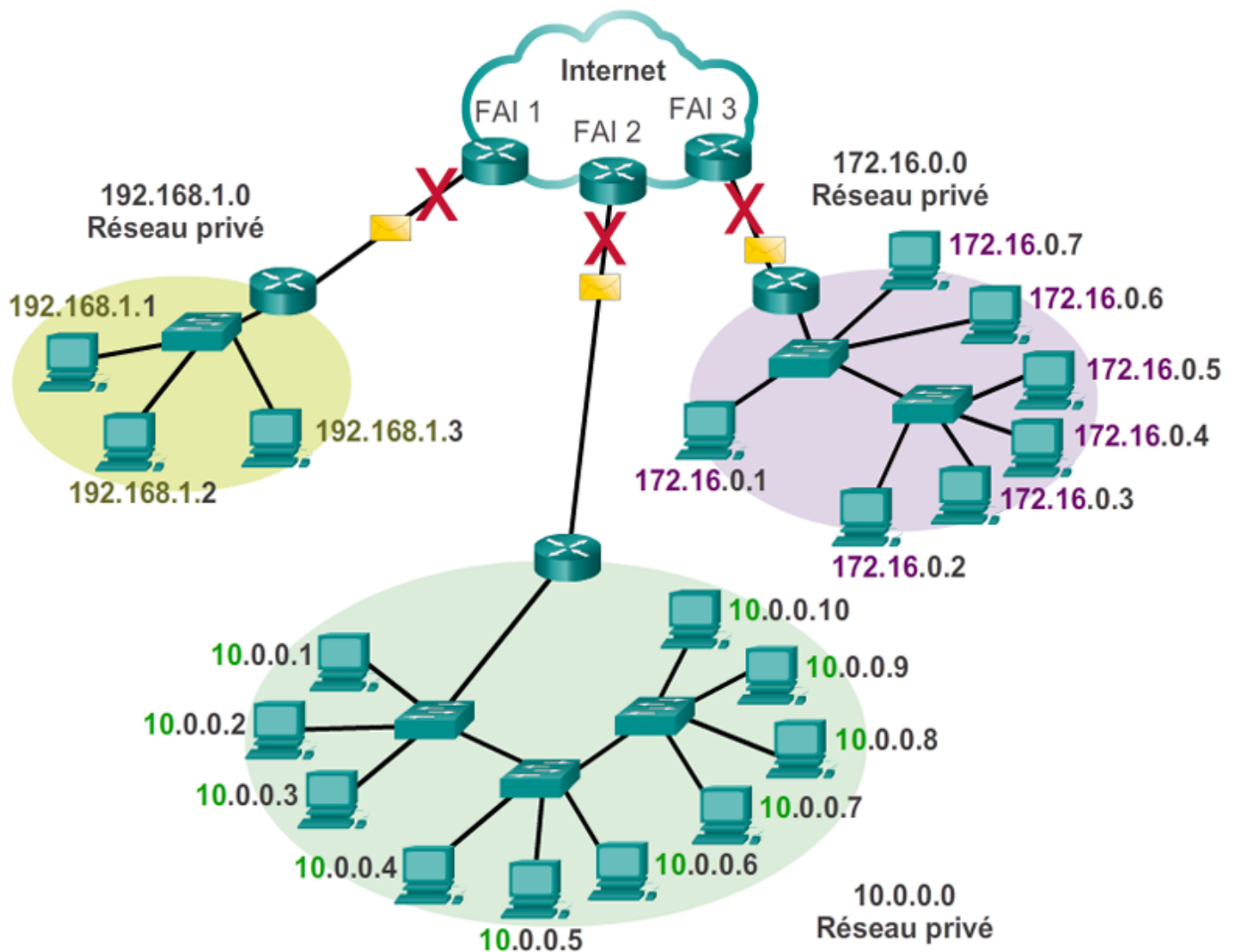
Les adresses privées sont définies dans le RFC 1918, « **Address Allocation for Private Internets** » et sont parfois appelées adresses RFC 1918.

Les blocs d'adresses d'espace privé, comme l'illustre la figure, sont utilisés dans les réseaux privés. Les hôtes qui n'ont pas besoin d'accéder à Internet peuvent utiliser des adresses privées. Cependant, au sein du réseau privé, les hôtes ont toujours besoin d'adresses IP uniques dans l'espace privé.

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. Même si ces paquets parvenaient sur Internet, les routeurs ne disposeraient pas de routes pour les acheminer vers le réseau privé en question.

Dans le RFC 6598, l'IANA a réservé un autre groupe d'adresses connu sous le nom d'espace d'adressage partagé. Comme avec l'espace d'adressage privé du RFC 1918, les adresses partagées de l'espace d'adressage ne sont pas globalement routables. Toutefois, ces adresses sont conçues uniquement pour les réseaux de fournisseurs de services. Le bloc d'adresses partagé est 100.64.0.0/10.

Les adresses privées ne peuvent pas être routées sur Internet.



Adresses publiques

La grande majorité des adresses de la plage d'hôtes multidiffusion IPv4 sont des adresses publiques. Ces adresses sont normalement attribuées à des hôtes publiquement accessibles depuis Internet. Même dans ces blocs d'adresses IPv4, de nombreuses adresses sont réservées à des usages particuliers.

Adresses réseau et de diffusion

Comme nous l'avons vu, dans chaque réseau, la première et la dernière adresse ne peuvent pas être attribuées à des hôtes.

Il s'agit respectivement de l'**adresse réseau** et de l'**adresse de diffusion**.

Bouclage

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.

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 ce bloc 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.

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, comme indiqué dans la figure. Un hôte ne peut pas envoyer de paquet avec une adresse de destination IPv4 link-local à un autre routeur pour qu'il soit acheminé. De plus, sur l'hôte, le paramètre IPv4 de durée de vie (TTL) doit être défini sur 1 pour ces paquets.

Les adresses link-local ne fournissent pas de services en dehors du réseau local. Toutefois, de nombreuses applications client/serveur et peer to peer fonctionneront correctement avec des adresses link-local IPv4.

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. Ces adresses apparaissent souvent avec des noms de domaine exemple.com ou exemple.net dans les requêtes pour commentaires et la documentation de fournisseur et de protocole. Les adresses de cette plage ne doivent pas être visibles sur Internet.

Adresses expérimentales

Les adresses du bloc **240.0.0.0 à 255.255.255.254** sont répertoriées comme étant réservées pour une utilisation future (RFC 3330).

Actuellement, ces adresses ne peuvent être utilisées qu'à des fins de recherche ou d'expérimentation, mais ne peuvent pas être utilisées dans un réseau IPv4.

Cependant, selon le RFC 3330, elles peuvent techniquement être converties en adresses utilisables dans le futur.

Rappel : A titre informatif

À l'origine, le RFC 1700, « Assigned Numbers », regroupait les plages monodiffusion selon différentes tailles, appelées des adresses de classe A, B et C. Il établissait également des adresses de classe D (multidiffusion) et de classe E (expérimentales), comme nous l'avons déjà vu. Les classes d'adresses de monodiffusion A, B et C définissaient des réseaux de taille spécifique et des blocs d'adresses spécifiques pour ces réseaux. Une entreprise ou une organisation se voyait attribuer un réseau entier de bloc d'adresses de classe A, B ou C. L'utilisation de l'espace d'adressage s'appelait adressage par classe.

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 IPv4 de classe A utilisaient un préfixe /8 invariable, le premier octet indiquant l'adresse réseau. Les trois octets restants correspondaient aux adresses d'hôte. Toutes les adresses de classe A nécessitaient que le bit de poids fort du premier octet soit un zéro. Cela implique qu'il n'y avait que 128 réseaux de classe A disponibles, de 0.0.0.0/8 à 127.0.0.0/8. Même si les adresses de classe A réservaient la moitié de l'espace d'adressage, elles ne pouvaient être attribuées qu'à 120 entreprises ou organisations, en raison de leur limite de 128 réseaux.

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 jusqu'à 65 000 hôtes. Les adresses IP de classe B utilisaient les deux premiers octets pour indiquer l'adresse réseau. Les deux octets suivants correspondaient aux adresses d'hôte. Comme avec la classe A, l'espace d'adressage pour les classes d'adresses restantes devait être réservé. Pour les adresses de classe B, les deux bits de poids fort du premier octet étaient 10. Cela limitait le bloc d'adresses de classe B de 128.0.0.0/16 à 191.255.0.0/16. La classe B attribuait les adresses plus efficacement que la classe A, car elle répartissait de manière équitable 25 % de l'espace d'adressage IPv4 total sur environ 16 000 réseaux.

Blocs d'adresses C

L'espace d'adressage de la classe C était le plus disponible des anciennes classes d'adresses. 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'adressage IP

l'adresse réseau. Les blocs d'adresses de classe C réservaient l'espace d'adressage à l'aide d'une valeur fixe de 110 pour les trois bits de poids fort du premier octet. Cela limitait le bloc d'adresses de classe C de 192.0.0.0/24 à 223.255.255.0/24. Bien qu'il occupait seulement 12,5 % de l'espace d'adressage IPv4, il pouvait attribuer des adresses à 2 millions de réseaux.

Limites de l'adressage par classe

Les besoins de certaines entreprises ou organisations sont couverts par ces trois classes. L'attribution par classe des adresses IP gaspillait souvent de nombreuses adresses, ce qui épuisait la disponibilité des adresses IPv4. Par exemple, une entreprise avec un réseau de 260 hôtes devait se voir attribuer une adresse de classe B avec plus de 65 000 adresses.

Bien que ce système par classe ait été abandonné à la fin des années 90, il n'a pas entièrement disparu dans certains des réseaux modernes. Par exemple, lorsque vous attribuez une adresse IPv4 à un ordinateur, le système d'exploitation examine l'adresse en question pour déterminer si elle est de classe A, B ou C. Le système d'exploitation déduit ensuite le préfixe utilisé par cette classe et effectue l'attribution du masque de sous-réseau par défaut.

Adressage sans classe

Le système utilisé aujourd'hui porte le nom d'adressage sans classe. Son nom formel est le routage CIDR (Classless Inter-Domain Routing, routage interdomaine sans classe). L'attribution par classe d'adresses IPv4 était inefficace, car elle permettait uniquement l'utilisation de longueurs de préfixe /8, /16 ou /24, chacune d'un espace d'adresses distinct. En 1993, l'IETF a créé un nouvel ensemble de normes permettant aux fournisseurs de services d'attribuer des adresses IPv4 sur n'importe quelle limite binaire (longueur de préfixe) au lieu d'utiliser uniquement les classes A, B ou C.

L'IETF savait que le CIDR était uniquement une solution temporaire et qu'un nouveau protocole IP devait être développé pour s'adapter à la croissance rapide du nombre d'utilisateurs d'Internet. En 1994, l'IETF a commencé à chercher un successeur à l'IPv4, à savoir le futur protocole IPv6.

Pour que les hôtes réseau (par exemple les serveurs Web) des entreprises ou des organisations soient accessibles depuis Internet, les organisations et entreprises en question doivent disposer d'un bloc d'adresses publiques. N'oubliez pas que les adresses publiques doivent être uniques et que l'utilisation des adresses publiques est régulée et dépend de chaque organisation. Cela vaut pour les adresses IPv4 et IPv6.

IANA et RIR

L'IANA (Internet Assigned Numbers Authority, <http://www.iana.org>) gère l'attribution des adresses IPv4 et IPv6. Jusque dans le milieu des années 1990, l'ensemble de l'espace d'adressage IPv4 était géré directement par l'IANA. À cette époque, la gestion de l'espace d'adressage IPv4 restant était répartie entre différents autres registres, selon le type d'utilisation ou la zone géographique. Ces sociétés d'enregistrement s'appellent des registres Internet régionaux, comme présenté dans la figure.

Voici les principaux registres :

AfriNIC (African Network Information Centre) - Région Afrique <http://www.afrinic.net>

APNIC (Asia Pacific Network Information Centre) - Région Asie/Pacifique <http://www.apnic.net>

ARIN (American Registry for Internet Numbers) - Région Amérique du Nord <http://www.arin.net>

LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Amérique du Sud et certaines îles des Caraïbes <http://www.lacnic.net>

RIPE NCC (Réseaux IP européens) - Europe, Moyen Orient, Asie centrale <http://www.ripe.net>

FAI

Les RIR sont chargés d'attribuer des adresses IP aux FAI. La plupart des entreprises ou organisations obtiennent leur bloc d'adresses IPv4 auprès d'un FAI. Le FAI fournit généralement un petit nombre d'adresses IPv4 utilisables (6 ou 14) à leurs clients, dans le cadre des services d'accès qu'ils offrent. Il est possible d'obtenir, pour un coût supplémentaire, de plus grands blocs d'adresses sur base de justificatifs des besoins.

En quelque sorte, le FAI prête ou loue ces adresses. Lorsque nous changeons de FAI, le nouveau FAI nous fournit des adresses à partir des blocs d'adresses qui lui ont été attribués. L'ancien FAI retourne les blocs qu'il nous a prêtés à leur pool d'adresses, pour qu'un autre client puisse les emprunter.

Les adresses IPv6 peuvent être obtenues à partir du FAI ou, dans certains cas, directement à partir du RIR. La taille des adresses IPv6 et des blocs d'adresse standard sera abordée dans un autre cours.

Source : https://fr.wikipedia.org/wiki/Fournisseur_d'accès_à_Internet

Raccordement du FAI à Internet

Article détaillé : Maillage de l'infrastructure Internet en France.

À la différence d'un abonné, qui se raccorde à Internet via un prestataire de services (le fournisseur d'accès), le fournisseur d'accès lui-même procède de manière différente.

Dans le cas général, il est un maillon du réseau, transportant ses propres données (pour simplifier, le trafic de ses abonnés), mais aussi potentiellement les données d'autres opérateurs.

Le raccordement qui relie deux opérateurs est fondamentalement différent de celui qui relie un abonné à son fournisseur d'accès.

Les routeurs des deux opérateurs vont en effet échanger, non pas une seule route (qui se résume à « la sortie, c'est par là ») mais plusieurs centaines de milliers de routes, indiquant comment joindre tous les autres opérateurs.

Ainsi, quand un opérateur est relié à 3 autres, il a appris, de 3 sources différentes, toutes les routes que chacun de ces opérateurs connaissait.

Il pourra alors choisir la route qu'il jugera la plus efficace.

Ce mode de raccordement entre opérateur, appelé du transit, est en général facturé (par le plus gros au plus petit, le plus souvent).

Une alternative à ce mode de connexion est, sur la même base technique, de n'échanger que quelques routes (typiquement celles menant à son propre réseau).

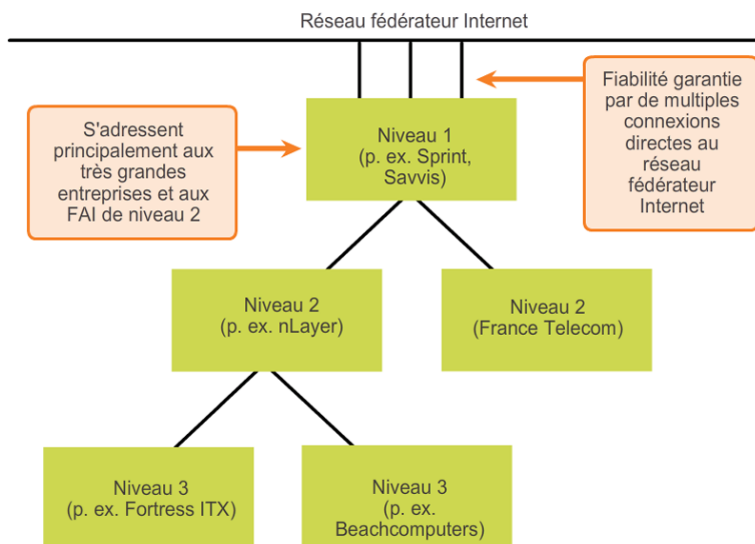
On parle alors d'accord de **peering** (échange entre pairs).

Ce procédé technique de raccordement, sensiblement plus complexe que celui utilisé pour raccorder un abonné à son fournisseur, permet à l'opérateur de changer à tout moment ses accords de peering, ou ses contrats de transit, sans impact notable pour les utilisateurs finaux.

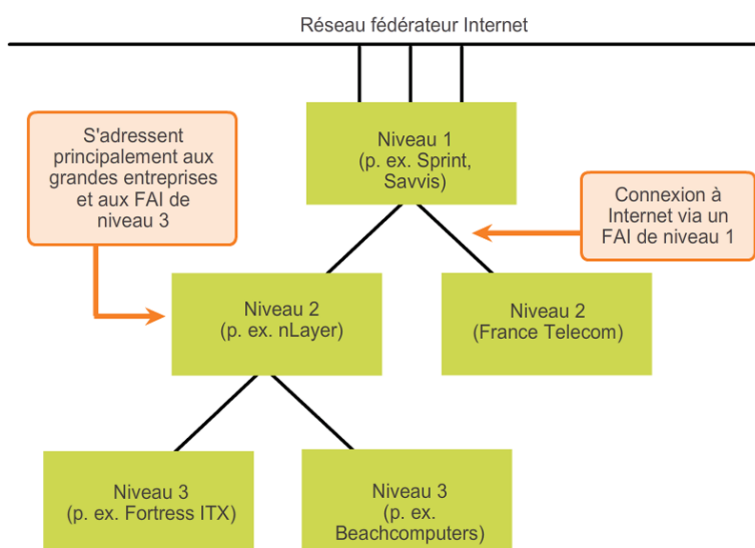
Un opérateur, même de faible envergure, dispose en général de plusieurs contrats de transit, et de plusieurs dizaines, voire centaines, d'accord de **peering**.

C'est l'ensemble des opérateurs, échangeant entre eux des centaines de milliers de routes, qui forment Internet. Certains opérateurs ne s'occupent quasiment que de transport de données. D'autres proposent, contre paiement, un raccordement à des utilisateurs finaux, ce sont les fournisseurs d'accès à Internet.

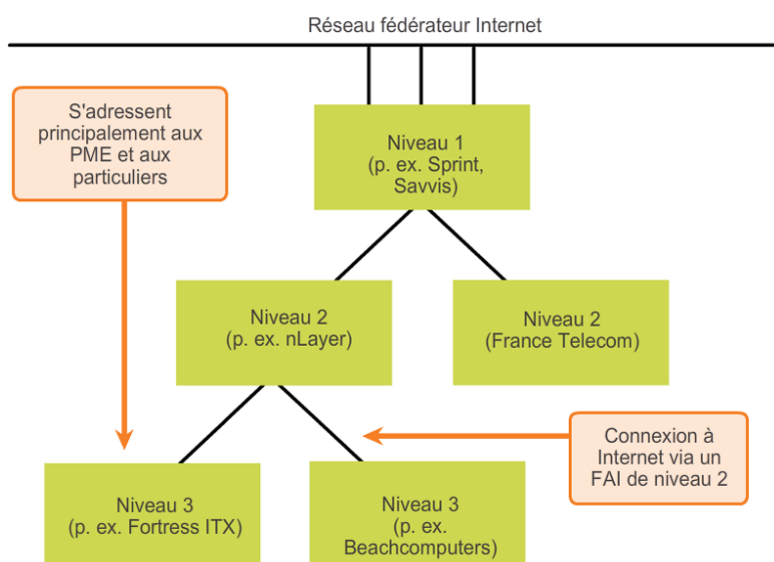
Les trois niveaux de FAI - niveau 1




Les trois niveaux de FAI - niveau 2



Les trois niveaux de FAI - niveau 3




8.1.4.7 Exercice - Adresses IPv4 publiques ou privées



Public

- ✓ 117.22.10.10
- ✓ 198.172.17.7
- ✓ 200.0.0.1
- ✓ 192.255.255.255
- ✓ 127.255.255.255
-
-
-



Privé

- ✓ 172.16.5.9
- ✓ 192.168.33.33
- ✓ 172.16.255.255
-
-
-
-

Les adresses réseau IPv6

8.2.1.2 La coexistence des protocoles IPv4 et IPv6

Ceci fera l'objet d'un autre cours...

Assimilez, en premier lieu, les notions des adresses IPv4.... A suivre...