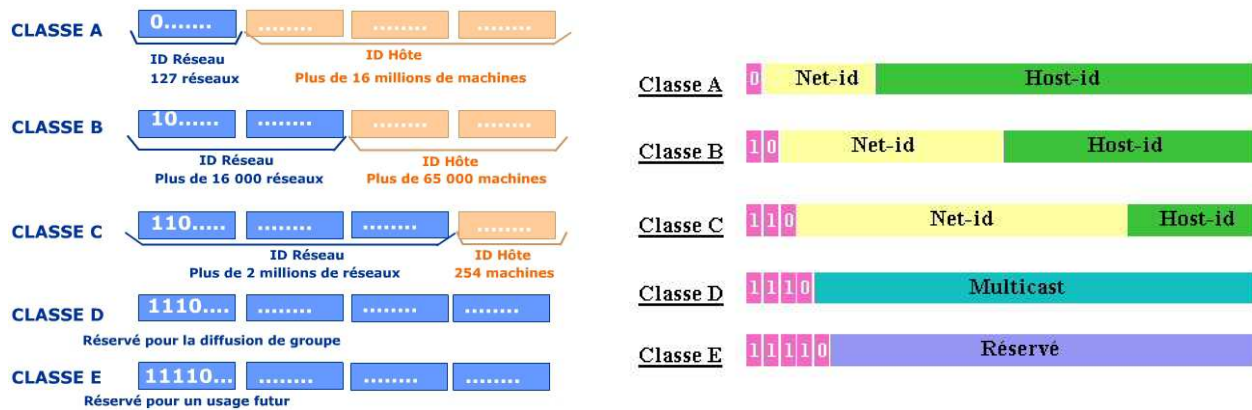


LES CLASSES DE RESEAUX ET LE DECOUPAGE EN SOUS-RESEAUX



Objectifs du COURS :

Ce cours traitera essentiellement les points suivants :

- les classes d'adresses IPv4
- les classes de réseaux
- le découpage d'une classe en sous-réseaux
- l'espace d'adressage privé
- exercices d'application

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement (ou le routage) 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.

LES CLASSES D'ADRESSES IPV4

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 (NetID) et les 3 autres correspondent à l'adresse de l'hôte (HostID).

Remarques :

L'adresse réseau 0.0.0.0 n'existe pas et le NetID « 127 » est réservée pour les communications en boucle locale (loopback).

127.0.0.0 = machine
locale (LocalHost)

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 4 bits de poids fort égaux à 1110. Il s'agit d'une zone d'adresses dédiées aux services de multi-diffusion (multicast) vers des groupes d'hôtes (host groups).

CLASSE : E

Le premier octet a une valeur comprise entre 240 et 255 ; soit 4 bits de poids fort égaux à 1111. Il s'agit d'une zone d'adresses réservées à des opérations de maintenance et d'expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

LES CLASSES DE RÉSEAUX

Classe	Masque de sous réseau par défaut	Adresse réseau	Nombre de réseaux	Nombre d'hôtes
A	255.0.0.0	1.0.0.0 à 126.0.0.0	126 (= $2^7 - 2$)	16 777 214
B	255.255.0.0	128.0.0.0 à 191.255.0.0	16 384 (= 2^{14})	65 534
C	255.255.255.0	192.0.0.0 à 223.255.255.0	2 097 152 (= 2^{21})	254
D	Non défini	224.0.0.0 à 239.255.255.0		
E	Non défini	240.0.0.0 à 255.255.255.0		

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.

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.

LES CLASSES DE RESEAUX ET LE DECOUPAGE EN SOUS RESEAUX

Au quotidien, on évite l'engorgement des liens en limitant géographiquement les annonces de services faites par les serveurs de fichiers. Les services Microsoft 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. 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. 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, nous allons utiliser un exemple pratique. On reprend l'exemple de la classe C : 192.168.1.0 dont le masque de sous-réseau par défaut est 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 4^{eme} octet en complétant le masque de sous-réseau. De cette façon on augmente la partie réseau de l'adresse IP et on diminue la partie hôte.

Classe C avec « subnetting » sur 3 bits				2 ³ = 8 sous-réseaux
NetID				HostID
1111 1111	1111 1111	1111 1111	111	0 0000
255	255	255	224	
octet 1	octet 2	octet 3	octet 4	

Sous réseau	Masque	@ réseau	Plage d'@ utilisables	@ de diffusion
0	255.255.255.224	192.168.1.0	192.168.1.1 192.168.1.30	192.168.1.31
1		192.168.1.32	192.168.1.33 192.168.1.62	192.168.1.63
2		192.168.1.64	192.168.1.65 192.168.1.94	192.168.1.95
3		192.168.1.96	192.168.1.97 192.168.1.126	192.168.1.127
4		192.168.1.128	192.168.1.129 192.168.1.158	192.168.1.159
5		192.168.1.160	192.168.1.161 192.168.1.190	192.168.1.191
6		192.168.1.192	192.168.1.193 192.168.1.222	192.168.1.223
7		192.168.1.224	192.168.1.225 192.168.1.254	192.168.1.255

Nbre de s/réseaux = nombre de bits attribués en plus au netID²

On peut remarquer que le nombre maximum d'adresses d'hôtes disponibles correspond à l'espace d'adressage du sous-réseau moins deux. C'est parce que la première adresse désigne le réseau et que la dernière est l'adresse de diffusion (broadcast) vers tous les hôtes du sous-réseau.

L'ESPACE D'ADRESSAGE PRIVÉ

Pour chaque classe, il y a un pool d'adresses réservées pour l'utilisation de réseaux privés. Ces adresses ne sont pas routées sur internet. Il faut obligatoirement utiliser ces adresses sur un réseau local privé.

Classe	Plage d'adresse
A	10.0.0.1 à 10.255.255.254
B	172.16.0.0 à 172.31.255.254
C	192.168.0.0 à 192.168.255.254

EXERCICES D'APPLICATION

Pour configurer l'interface d'un hôte qui doit se connecter à un réseau existant, on nous donne l'adresse **172.16.19.40/21**.

Question 1 :

Quel est le masque réseau de cette adresse ?

La notation /21 indique que le netID occupe 21 bits. On décompose ces 21 bits en 8 bits + 8 bits + 5 bits ; ce qui donne : 255.255.248.0.

Question 2 :

Combien de bits ont été réservés pour les sous-réseaux privés ?

La valeur du premier octet de l'adresse étant comprise entre 128 et 192, il s'agit d'une adresse de classe B. Le masque réseau par défaut d'une classe B étant 255.255.0.0, 5 bits (1111 1000) ont été réservés sur le troisième octet pour constituer des sous-réseaux.

Question 3 :

Combien de sous-réseaux privés sont disponibles ?

RFC = Request For
Comments

Le nombre de valeurs codées sur 5 bits est de 2^5 soit 32. Suivant la génération du protocole de routage utilisé, on applique deux règles différentes.

Historiquement, on devait exclure le premier (all-zeros) et le dernier (all-ones) sous-réseau conformément au document RFC950 de 1985. Cette règle suppose que les protocoles de routage utilisent uniquement la classe du réseau routée sans tenir compte de son masque et donc de sa longueur variable.

Dans ce cas, le nombre de sous-réseaux utilisables est 30.

Dans les réseaux contemporains, on peut retenir l'ensemble des sous-réseaux sachant que les protocoles de routage véhiculent les masques de longueurs variables dans chaque entrée de table de routage. Cette règle est applicable depuis la publication des documents standards relatifs au routage inter-domaine sans classe (CIDR) notamment le RFC1878 de 1995.

Dans ce cas, le nombre de sous-réseaux utilisables est 32.

Question 4 :

Quelle est l'adresse du sous-réseau de l'exemple ?

Les deux premiers octets étant compris dans la partie réseau, ils restent inchangés. Le quatrième octet (40) étant compris dans la partie hôte, il suffit de le remplacer par 0. Le troisième octet (19) est partagé entre partie réseau et partie hôte. Si on le convertit en binaire, on obtient : 00010011. En faisant un ET logique avec la valeur binaire correspondante 5 bits réseau (11111000) on obtient : 00010000 ; soit 16 en décimal. L'adresse du sous-réseau est donc 172.16.16.0.

Question 5 :

Quelle est l'adresse de diffusion du sous-réseau de l'exemple ?

Les deux premiers octets étant compris dans la partie réseau, ils restent inchangés. Le quatrième octet (40) étant compris dans la partie hôte, il suffit de le remplacer par 255. Le troisième octet (19) est partagé entre partie réseau et partie hôte. Si on le convertit en binaire, on obtient : 00010011. On effectue cette fois-ci un OU logique avec la valeur binaire correspondant aux 3 bits d'hôtes à un (00000111). On obtient : 00010111 ; soit 23 en décimal. L'adresse de diffusion du sous-réseau est donc 172.16.23.255.