

# - UTC505/USRS4D -

## Couche Réseau IP, Adressage & Architecture

E. Gressier-Soudan

03/10/2021

E. Gressier-Soudan

1



# ADRESSAGE IP

03/10/2021

E. Gressier-Soudan

2



# Adresse IP v4

- Une adresse IP v4 est sur 4 octets (32 bits)
- Elle est composée de 2 parties :
  - Une partie réseau
  - Une partie index d'interface (de communication)
- Pour séparer les deux parties, on utilise un masque :
  - Une suite de 1 puis une suite de 0
  - On fait un **et logique** entre l'adresse IP et le masque
  - La longueur de la partie à 0 doit correspondre à la partie interface/hôte
- Exemple : 163.173.128.60 "et logique" 255.255.252.0 donne le réseau 163.173.128.0... attention, la définition du réseau n'est pas complète au sens strict de la terminologie Internet... cf transparent suivant pour la bonne spécification de l'adresse de réseau

## Avec détails

Soit l'adresse IP d'interface 163.173.128.6

- Ré-écriture de l'adresse quasiment en binaire donne :  
163.173. "1000 0000"."0000 0110"

Soit le masque 255.255.252.0

- Ré-écriture du masque en binaire :  
1111 1111.1111 1111.1111 1100.0000 0000

Application du masque sur l'adresse IP (ET logique) ci-dessus donne :  
163.173.1000 0000.0000 0000

- Soit 163.173.128.0

Le masque peut s'écrire aussi /22 en notation compacte (22 bits consécutifs à 1 à partir de la gauche de l'adresse).

Une adresse de réseau sans masque n'a pas de sens, la bonne formulation du résultat est : 163.173.128.0/22

# Adresse de diffusion d'un réseau

- L'adresse de diffusion : partie interface remplie par des 1
- En reprenant l'adresse de réseau IP précédente :

163.173.1000 0000.0000 0000/22

- On passe à 1 les 10 derniers bits

163.173.1000 0011.1111 1111

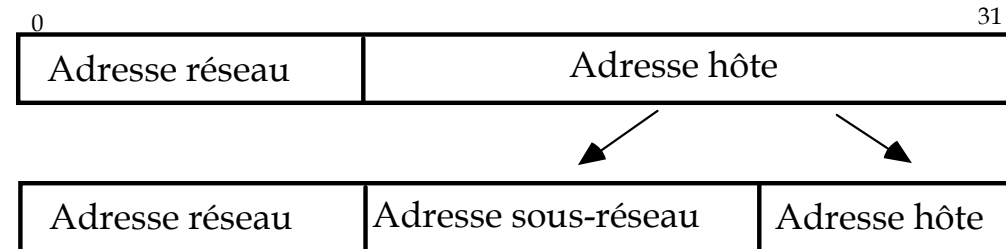
- On obtient comme adresse de broadcast :

163.173.131.255

# Broadcast dirigé et broadcast limité

- Certains auteurs introduisent cette différenciation.
  - Le broadcast dirigé correspond à l'adresse de diffusion sur tout un réseau au sens CIDR, comme dans le transparent précédent : l'adresse 163.173.131.255 du réseau 163.173.128.0/22. Un datagramme avec cette adresse peut traverser plusieurs routeurs avant d'atteindre les interfaces cibles d'un réseau. Cette terminologie est dans la RFC919 (1984)
  - Le broadcast limité correspond à une diffusion qui atteint tous les voisins de l'émetteur mais ne traverse pas de routeur : 255.255.255.255 ou 0.0.0.0 sur certains anciens OS comme de vieux Unix.

# Les sous-réseaux IP V4 : Hiérarchisation à trois niveaux “IP Subnetting” RFC 950 (1985)



- Possibilité offerte de structurer l'espace d'adressage interne à un réseau en **deux niveaux** (voire plus).
- **Problème:** La frontière entre adresse de sous-réseau et adresse d'interface (d'ailleurs on ne devrait pas parler d'hôte) est définie par l'administrateur du réseau selon les besoins de l'entreprise.
- Nécessité de fournir le découpage sur chaque machine/équipement d'un sous-réseau (en particulier routeurs)

# Notion de masque ou de préfixe étendu ("Subnet Mask")

- Le masque se formalise, il permet le filtrage des adresses destination pour trouver l'adresse du sous-réseau d'appartenance.
- On le note autrement : comme on a une suite de 1 à partir de la gauche, on peut compter le nombre de 1
- Exemple un réseau : 135.28/16 correspond à 135.28.0.0 avec un masque 255.255.0.0
- Exemples : On souhaite une partie réseau sur 16 bits
  - puis une adresse de sous-réseau sur 8 bits et 8 bits pour la partie interface :  
Valeur du masque (notation décimale pointée):
    - **255.255.255.0**
    - (0xFFFFF00 en hexadécimal)
    - Valeur du préfixe étendu : **/24**
  - Autre possibilité de découpage 10 bits sous-réseau + 6 bits interface :
    - **255.255.255.192** ou **/26**



# Les adresses particulières (RFC 1340)

## Adresse 0/8: l'hôte courant

- **0.0.0.0 ou 0.x.y.z**
- 0.0.0.0 : l'adresse **source** d'une station qui ne connaît pas son adresse (utilisable également 0.x.y.z adresse x.y.z dans le réseau courant).
- l'adresse **destination** par défaut.

## Adresse 127/8: rebouclage "Loopback"

- Pour permettre à deux utilisateurs sur le même site de communiquer par IP (toutes les adresses "127.x.y.z" sont affectées à cette fonction).
- Exemple 127.0.0.1 ("localhost").

## Adresse destination: 255.255.255.255

- Idée au départ : diffusion à tout l'internet.
- En fait diffusion limitée au sous-réseau local (non routé hors du sous-réseau).

## Adresses destination: net.111...111/lgnet :

- Diffusion limitée à toutes les interfaces du réseau d'appartenance, principe qui est généralisé lorsqu'on utilise un masque de longueur variable.

# Conception d'un plan d'adressage avec sous-réseaux

1. Combien de sous-réseaux doit-on déployer aujourd'hui ?
2. Combien de sous-réseaux devront être déployés dans le futur ?
3. Combien d'hôtes au maximum vont se trouver dans un sous-réseau actuel ?
4. Combien d'hôtes au maximum vont se trouver dans un sous-réseau dans le futur ?
5. Un problème d'Urbanisation ou d'Assistance à la maîtrise d'ouvrage :
  - Choisir un découpage qui doit permettre au nombre souhaité de sous-réseaux d'avoir le nombre souhaité d'hôtes.
  - Ce découpage devrait permettre d'accompagner le développement futur du réseau suffisamment longtemps.

# Bilan IP V4 et les sous-réseaux

## Avantages

- Les tables de routage de l'Internet ne peuvent croître en taille à l'infini. Seuls les routeurs internes doivent connaître les sous-réseaux.
- L'espace d'adressage privé est mieux géré. Lors de la création de nouveaux réseaux on évite de demander des adresses.
- Si un réseau modifie sa structure interne, il n'est pas nécessaire de modifier les routes dans l'Internet  
⇒ problème de "route-flapping".

## Inconvénients

- Il faut gérer le masque en plus de l'adresse.
- On ne définit qu'une seule façon de hiérarchiser l'espace d'adresses d'une entreprise/campus/organisme/habitat/...

# Masques de sous-réseaux : VLSM 'Variable Length Subnet Masks' RFC1009... sous-partie de CIDR RFC4632

- Hiérarchisation complète des adresses IPv4 : Une façon pour utiliser dans un même réseau **plusieurs masques** de sous réseaux différents (**plusieurs préfixes étendus**).

## Exemple

- Le réseau classe 135.8.0.0/16 est découpé par le masque 255.255.254.0 ou le préfixe /23 (soit  $2^7 = 128$  sous-réseaux de  $2^9 - 2 = 510$  interfaces).
- Il se crée un nouveau sous-réseau de 15 interfaces (extension prévisible à 50).
  - Si on lui attribue une adresse de sous-réseau /23 on va perdre environ 500 adresses.
  - Il serait par contre très intéressant de lui attribuer une adresse /26 d'un sous-réseau de  $64 - 2 = 62$  hôtes.

# Problèmes de déploiement d'un réseau VLSM (1/2)

**Le protocole de routage interne doit utiliser les préfixes étendus pour les sous-réseaux.**

- Déterminer correctement le numéro de réseau et d'hôte quel que soit le découpage.
- => RIPv2 ('Routing Information Protocol' RFC2453) permet de déployer VLSM.

**Les routeurs réalisent une recherche de "correspondance la plus longue"**

- ('Longest Match based forwarding algorithm')
- En cas de plusieurs routes dans une table, la route de plus long préfixe est la plus précise

=> elle doit être sélectionnée et utilisée.

**Exemple :**

Soit un datagramme vers 136.1.6.5 (1000 1000.0000 0001.0000 0110.0000 0101)  
avec 3 préfixes dans la table

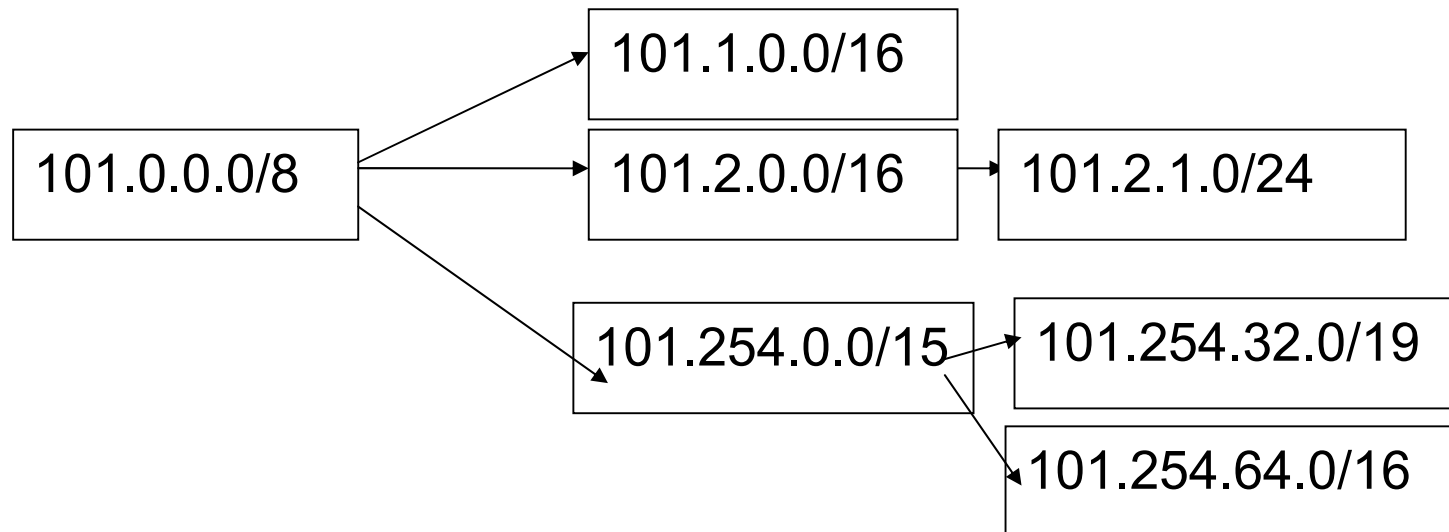
136.1.0.0/16 : 1000 1000.0000 0001.

136.1.4.0/21 : 1000 1000.0000 0001.0000 0

136.1.6.0/24 : 1000 1000.0000 0001.0000 0110.

Le routeur choisit la route 136.1.6.0/24.

# Agrégation en une seule route



# Problèmes de déploiement d'un réseau VLSM (2/2)

- **Pour l'agrégation des routes les adresses doivent être assignées 'topologiquement'.**
- L'adressage doit être associée à la topologie du réseau.
- On réduit la quantité d'information de routage en prenant un bloc d'adresses VLSM assigné à une certaine région de la topologie.
- On peut alors agréger en une seule route, les routes pour l'ensemble des adresses d'une région.

# Bilan IP V4 avec VLSM

## Avantages

- L'utilisation de plusieurs masques permet un usage plus efficace de l'espace d'adressage attribué à une organisation : il n'est plus nécessaire de se conformer à la taille unique des sous-réseaux.
- On réduit le volume d'informations nécessaire au routage au niveau dorsal ('backbone') d'une organisation.

## Inconvénients

- Nécessite l'adaptation des protocoles de routage pour échanger les masques: par exemple RIP-1 ('Routing Information Protocol' version 1) n'autorise qu'un seul masque de sous réseau par réseau.



# CIDR 'Classless Inter Domain Routing'

RFC1517, 1518, 1519, 1520, 4632 (2006)

- **Problème constant en IP v4:**  
**saturation de l'espace d'adressage et croissance de la taille des tables de routage au niveau dorsal**
- L'approche VLSM étendue à tout l'espace d'adressage de l'Internet permet de faire durer l'adressage IP V4.
- En améliorant l'utilisation des adresses encore disponibles.
- En diminuant le volume des tables de routage par agrégation des routes.

# Contraintes pour le déploiement de CIDR

- **Les hôtes et routeurs doivent supporter l'environnement CIDR.**
- Les adresses de réseaux doivent être échangées par les protocoles de routage avec leur préfixe qui peut être de taille quelconque : /11, /13 ...
- Les routeurs doivent implanter un algorithme de "correspondance la plus longue",
- Les adresses doivent être distribuées sur une base topologique pour agréger les routes

# Bilan IPV4 avec CIDR

## Avantages CIDR

- CIDR alloue efficacement les adresses IPv4
- CIDR permet de coller assez finement aux demandes avec peu de gaspillage.
- Les adresses peuvent être d'anciennes adresses A, B ou C récupérées (cf annexe en fin de support).

Exemple 129.6.0.0/22 ou 198.60.32.0/22 donnent 1024 - 2 adresses.

- Un prestataire Internet 'ISP est libre d'assigner ses adresses à ses clients. Le découpage est récursif et peut opérer à tous les niveaux
- **CIDR permet d'agréger les routes à tous les niveaux**
  - Contrôle de la taille des tables de routage.
  - Facilite l'administration des routeurs.

## Inconvénients CIDR

- CIDR étant une approche topologique fortement hiérarchisée présente les inconvénients de la hiérarchisation.
- Si une organisation souhaite changer de prestataire sans changer d'adresse on doit créer une route d'exception ce qui est coûteux.

# Il faut continuer les économies d'adresses IP

- Adresses locales non routables
- Traduction d'adresses NAT
- DHCP
- Liaisons dénumérotées
- Nouvelle stratégie d'allocation des adresses

# L'utilisation d'adresses locales/privées

## RFC 1918

Les organisations qui veulent créer un Internet privé peuvent utiliser sans demande les adresses réservées (privées) suivantes:

- 10/8 (10.0.0.0 à 10.255.255.254)
- 172.16/12 (172.16.0.0 à 172.31.255.254)
- 192.168/16 (192.168.0.0 à 192.168.255.254)

Ces adresses ne sont pas routées hors du domaine de routage.

On évite ainsi beaucoup de demandes d'adresses sans courir aucun risque.

# Utilisation d'un routeur traducteur d'adresses

- RFC2663 (base), RFC3022 et bien d'autres
- Une organisation ayant créé un Internet privé (RFC 1918) mais souhaitant néanmoins avoir un accès à l'Internet mondial peut utiliser un routeur traducteur d'adresses IP (NAT, 'Network Address Translator').
- Il n'est pas nécessaire d'avoir un ensemble d'adresses globales pour une correspondance bijective :

Adresses privées <-> Adresses globales

- Quelques adresses IP suffisent (une seule ?).
- S'il y a ambiguïté le routeur NAT différencie les communications au niveau UDP/TCP en modifiant l'adresse de transport (N° de port).

# Routeur de traduction NAT

- L'utilisation du NAT pose un certain de problèmes à tous les équipements de l'Internet qui utilisent l'adresse IP à l'intérieur du contenu acheminé... protocoles IPSEC, et, protocoles de Tunnel par exemple
- La complexité qu'implique NAT est regroupée sous l'expression NAT Traversal qui est l'objet d'une partie du cours à part entière.

# Attribution dynamique d'adresses

- DHCP 'Dynamic Host Configuration Protocol' (RFC 2131)
- Un hôte n'a pas d'adresse IP fixe mais au moyen de DHCP reçoit sur demande une adresse prise dans un ensemble d'adresses disponibles.
  - Une même adresse peut servir à désigner des hôtes différents dans le temps.
  - Il n'est pas nécessaire d'avoir autant d'adresses que d'abonnés si tous les abonnés ne se connectent pas en même temps.
- DHCP et NAT se combinent pour "empoisonner" la vie des développeurs d'applications... mais cela devrait rester imperceptible pour eux.



# Politique d'allocation des adresses IP

- **Restitution d'adresses** : il est demandé de rendre les adresses inutilisées.
- **Renumérotation** : problème important ....  
Définition de la stratégie en cas de renumérotation.
- **Propriété d'adresses** : une organisation reçoit et conserve indéfiniment si elle le souhaite une adresse IP. En changeant de prestataire elle peut conserver son adresse.

# Conclusion Adressage IPv4

- **Les problèmes de l'adressage IPv4 ont reçu des solutions partielles qui permettent à IPV4 de durer.**
  - Tarissement des adresses.
  - Grossissement des tables de routage.
  - Trop grande centralisation de distribution.  
En fait trop faible hiérarchisation.
  - Pays sous dotés (Chine, Inde, continent asiatique ou africain) qui passent à IPv6
- **Le plan d'adressage Internet IPv4 devrait néanmoins tôt ou tard arriver à saturation**
  - Incertitude très grande sur la date effective de cet événement (on disait 2005 ?... On a dit janvier 2011 ! ... le basculement total n'a pas encore eu lieu).
  - L'incertitude est liée au développement des services Internet consommateurs d'adresses et à la façon de régler les problèmes d'adressage dans ces cas (téléphonie fixe, mobile, commerce, internet des objets...)
  - Emergence de l'Internet des Objets
- **Ces difficultés (et d'autres) ont amené à spécifier une version nouvelle IPV6 qui se déploie aujourd'hui.**

# Conclusion

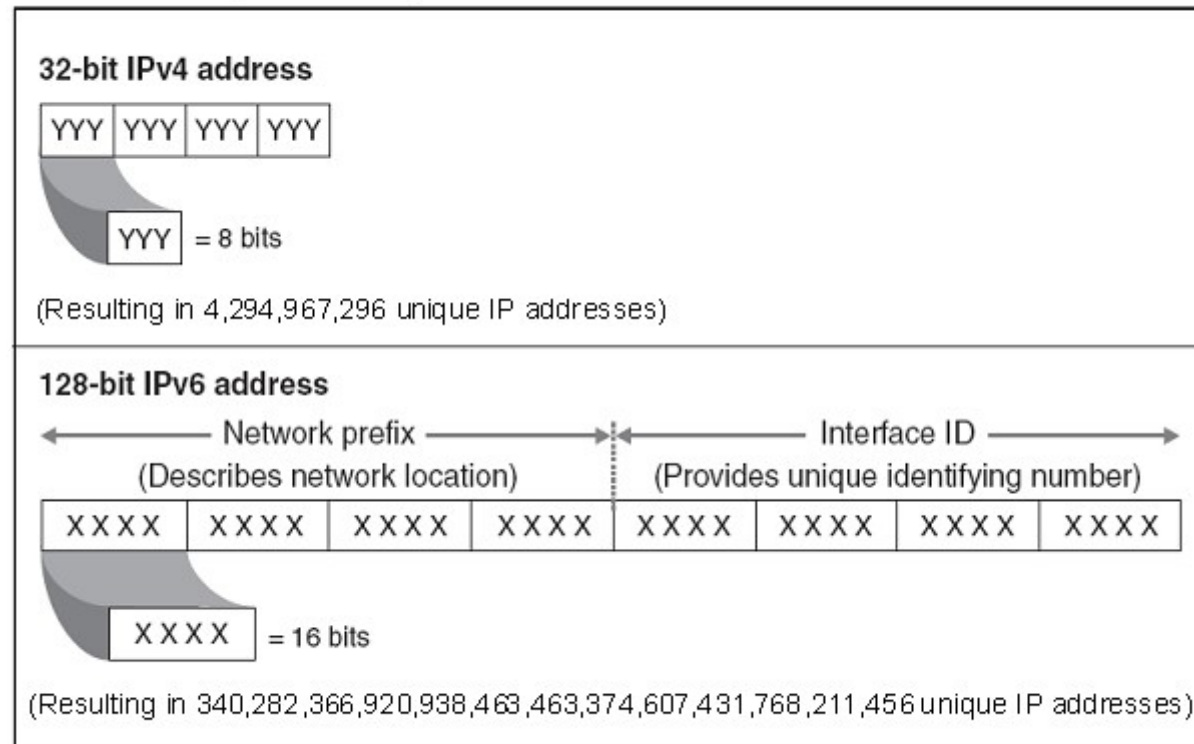
- La couche IP est le ciment de l'Internet, et les routeurs en sont la clef de voûte
  - C'est à cet endroit que tous les efforts d'amélioration vont porter : mise en place de la QoS, optimisation de la gestion des ressources
  - Les adresses forment un système de nommage des interfaces, elles assemblent désignation et localisation des interfaces
  - C'est une glue au-dessus de tous les types de liaisons, et à ce titre IP pourrait être considéré comme une forme de middleware si on compare l'Internet à un bus logiciel

# Adresses IPv6

- Une adresse 128 bits/16 octets/32 nombres hexadecimaux découpés par tranches de 4 séparées par « : » avec un préfixe qui fonctionne sur le principe CIDR, la possibilité de faire des sous-réseaux et identifiant une interface possiblement avec une EUI sur 64 bits
- La taille et la valeur des préfixes définissent des familles d'adresses

# Adresses IPv4 & IPv6

Figure 1: Comparison of IPv6 and IPv4 Address Scheme



Source: GAO.

<https://www.fcc.gov/consumers/guides/internet-protocol-version-6-ipv6-consumers> (16/03/2021)

03/10/2021

E. Gressier-Soudan

29

# Structuration d'une adresse IPv6

## Breakdown of IPv6



Elle peut être compactée en enlevant certains 0 suivant leur place dans l'adresse, compression ci-dessus : 2001:DB8:234:AB00:123:4567:8901:1BCD

Une suite consécutive de :0000:0000: peut être ré-écrite ::, attention, on ne peut le faire qu'une seule fois dans une adresse IPv6



# Merci pour votre attention !!!

# Annexe – musée des adresses IPv4

- CIDR, **Classless Inter-Domain Routing** , est en mis en œuvre depuis 1993 !!!
- Les classes d'adresses pour le routage, Classfull, c'est bien fini aujourd'hui...
- IPv6 devient de plus en plus visible d'ailleurs et il est conforme CIDR par nature



# Musée des adresses IP : les classes d'adresses (1/2)

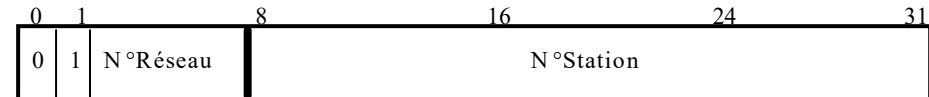
## Adresses Uniques Universelles :

A . B . C . D

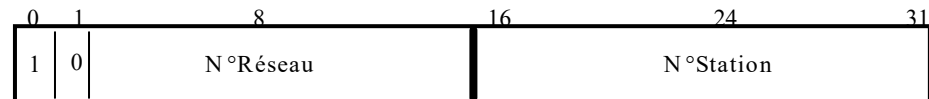
(N°Réseau, N°d'interface)

# Musée des adresses IP : les classes d'adresses (2/2)

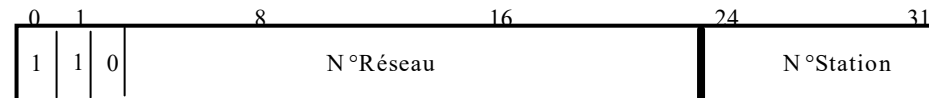
- **Classe A** : Peu de Réseaux, de nombreuses Stations par Réseau
  - N°de Réseau : 1-126, **127** adresse de **rebouclage en local**



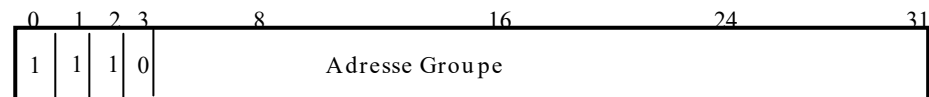
- **Classe B** :
  - N°de Réseau : 128.1 - 191.254



- **Classe C** : Beaucoup de Réseaux, Peu de Stations par Réseau
  - **La classe la plus répandue**
  - N°de Réseau : 192.0.1 - 223.255.254
  - N°de Station : 1 - 254
  - **Broadcast** : **255** dans le champ **N° de Station**

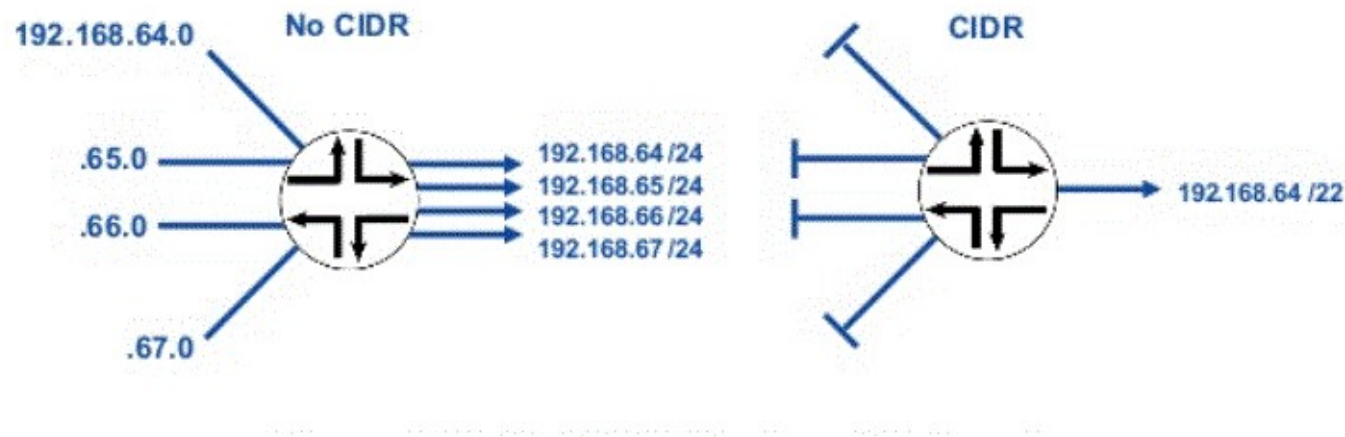


- **Classe D** : Adresses de Groupes de Diffusion (Multicast)
  - N°de Réseau : 225.0.0.0 - 239.255.255.255 (224.0.0.x réservée pour les protocoles de routage)



# CIDR vs CFDR

Une route par adresse de réseau vs Agrégation de routes



Source : Juniper routing 2003 <https://www.slideshare.net/NamNguyen5/junos-routing-overview-from-juniper>

# Conclusion adressage IP V4 par classes: les limitations

- L'espace d'adressage paraissant très suffisant au départ, les adresses ont été distribuées sans soin.  
**=> Gaspillage d'adresses**
- Les besoins exprimés par les entreprises moyennes sont souvent supérieurs à la classe C sans justifier la classe B.

**=> Attribution de plusieurs classes C.**

**=> Gonflement des tables de routage.**

- Des adresses avec classes existent toujours mais elles sont gérées comme des adresses sans classe.

L'adressage sur 32 bits (4 294 967 296 adresses) **est en fait insuffisant.**

# Utilisation des adresses de classe C restantes de l'Internet

Les adresses de classe C constituent une réserve d'adresses.

Solution d'administration et de routage: séparer les adresses de classe C en quatre catégories administrées par chaque continent (plus une réserve).

- 194.0.0.0 - 195.255.255.255 Europe
- 198.0.0.0 - 199.255.255.255 Amérique nord
- 200.0.0.0 - 201.255.255.255 Amérique sud
- 202.0.0.0 - 203.255.255.255 Asie Pacifique
- Quid de l'Afrique ?
- Les distributions sont indépendantes.

Possibilité d'agrégation de routes sur une base continentale :

- Une adresse 194.x.y.z doit être envoyée sur un routeur européen.

# Construction de réseaux sans classe par attribution d'adresses par blocs

**Exemple :** On souhaite construire un réseau IP pour 2048 adresses potentielles ( $2^{11}$ ).

- Par classes on aurait du lui attribuer 8 adresses classe C (8 entrées dans les tables).
- Supposons comme première adresse libre : 194.16.40.0
  - ⇒ On attribue le réseau 194.16.40.0/21
  - ⇒ Première adresse 194.16.40.1
  - 11000010 00010000 00101000 00000001
  - ⇒ Dernière adresse 194.16.47.254
  - 11000010 00010000 00101111 11111110
- Si un paquet est destiné à un hôte de ce bloc (de ce réseau) il faut filtrer l'adresse destinataire avec le masque 255.255.248.0 soit encore le préfixe /21 :
  - 11111111 11111111 11111000 00000000
- On sait que l'on doit router vers le réseau : 194.16.40.0/21.