Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

CONCOURS EXTERNE
DE TECHNICIEN DE CLASSE NORMALE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2018 -

Mardi 3 avril 2018

Option « infrastructures et réseaux »

Traitement de questions et résolution de cas pratiques, à partir d'un dossier, portant sur l'une des deux options suivantes choisies par le candidat le jour de l'épreuve :

- infrastructures et réseaux,

- solutions logicielles et systèmes d'information.

Cette épreuve permet d'évaluer le niveau de connaissances du candidat, sa capacité à les ordonner pour proposer des solutions techniques pertinentes et à les argumenter.

Le jury tiendra compte de la qualité rédactionnelle ainsi que de la présentation de la copie dans la notation. Un malus pourra être appliqué.

Le dossier ne peut excéder 20 pages.

(Durée : 3 heures – Coefficient 2)

Le dossier documentaire comporte 13 pages.

IMPORTANT

IL EST RAPPELE AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE NI SUR LA COPIE NI SUR LES INTERCALAIRES.

ECRIRE EN NOIR OU EN BLEU - PAS D'AUTRE COULEUR

SUJET

LES QUESTIONS

Les réponses doivent être rédigées. Elles doivent être claires et synthétiques. L'ensemble des questions sera noté sur 10 points.

Question 1 :

Dans un câble croisé RJ45, citer les numéros des paires qui se croisent ?

Question 2 :

Préciser ce qu'est une adresse MAC ?

Question 3 :

Quel protocole utilise le port 110 ?

Question 4 :

Quel protocole peut-on utiliser pour accéder à la configuration d'un serveur distant?

Question 5 :

Quelle est l'utilité d'un pare-feu ?

Question 6 :

Définir le terme « broadcast ». Quelle est la différence avec le multicast ?

Question 7 :

À quoi correspond la norme LTE, définie par le consortium 3GPP ?

Question 8 :

Citer dans l'ordre les couches du modèle OSI en partant des couches matérielles vers les couches hautes.

Question 9 :

Quelle est la différence entre WPA et WPA2 ?

Question 10 :

Reproduire et compléter sur votre copie cette trame IEEE 802.3 avec les éléments suivants :

- Adresse destinataire (6 octets)
- Données (0-1500 octets)
- Préambule (7 octets)
- Contrôle (4 octets)
- Adresse source (6 octets)
- Délimiteur de début de trame (1 octet)
- Longueur de données (2 octets)
- Padding (0 – 46 octets)

LES CAS PRATIQUES

Le cas pratique est scindé en deux parties distinctes. L'ensemble de ces parties sera noté sur 10 points.
Les réponses devront être argumentées et structurées.

Cas 1 :

Vous êtes affecté(e) à la Préfecture de Police de Paris à la direction opérationnelle des services techniques et logistiques (DOSTL). Dans le cadre d'un déménagement, plusieurs services s'installent sur un nouveau site qui vient d'être construit. Vous participez à l'installation, au déploiement et à la configuration du matériel informatique.

Afin d'assurer la cohérence du plan d'adressage de la Préfecture de Police, le sous-réseau affecté à ce site est le 192.168.100.0 /24.

Ce site est prévu pour 110 personnes. Chaque personne est équipée d'un poste de travail composé d'un ordinateur et d'un téléphone VoIP. 40 imprimantes et 5 télévisions sur IP sont également prévues.

Le site est relié au datacenter de la Préfecture de Police, notamment pour que les utilisateurs accèdent à la messagerie, à l'intranet et au système des fichiers de police. Les serveurs qui hébergent ces services sont situés sur un site géographiquement distant.

1. Le plan d'adressage réseau est-il correctement dimensionné ? Justifier votre réponse.

2. Y a-t-il un intérêt à découper le réseau en VLAN ? Justifier votre réponse.

3. Citer 2 points de vigilance au bon fonctionnement de la VoIP.

4. Les utilisateurs se plaignent de ne plus recevoir leurs mails. En tant qu'administrateur réseau, quelle procédure pouvez-vous mettre en œuvre pour qualifier et résoudre la panne ?

Cas 2 :

Vous êtes affecté(e) à la direction des systèmes d'information et de communication (DSIC) du ministère de l'intérieur, dans une équipe de techniciens réseaux.

On considère le réseau, représenté par la Figure 1, où la machine Eqmt 1 souhaite envoyer des données à la machine Eqmt 2. Les deux machines n'étant pas sur le même sous-réseau, les données vont donc devoir être routées via les deux routeurs R1 et R2.
Ce réseau Internet est supporté par trois réseaux physiques Ethernet (3 réseaux IP) dont les adresses Internet, de classe C et de masque 255.255.255.0, sont 193.2.2.0, 193.4.4.0 et 193.6.6.0.

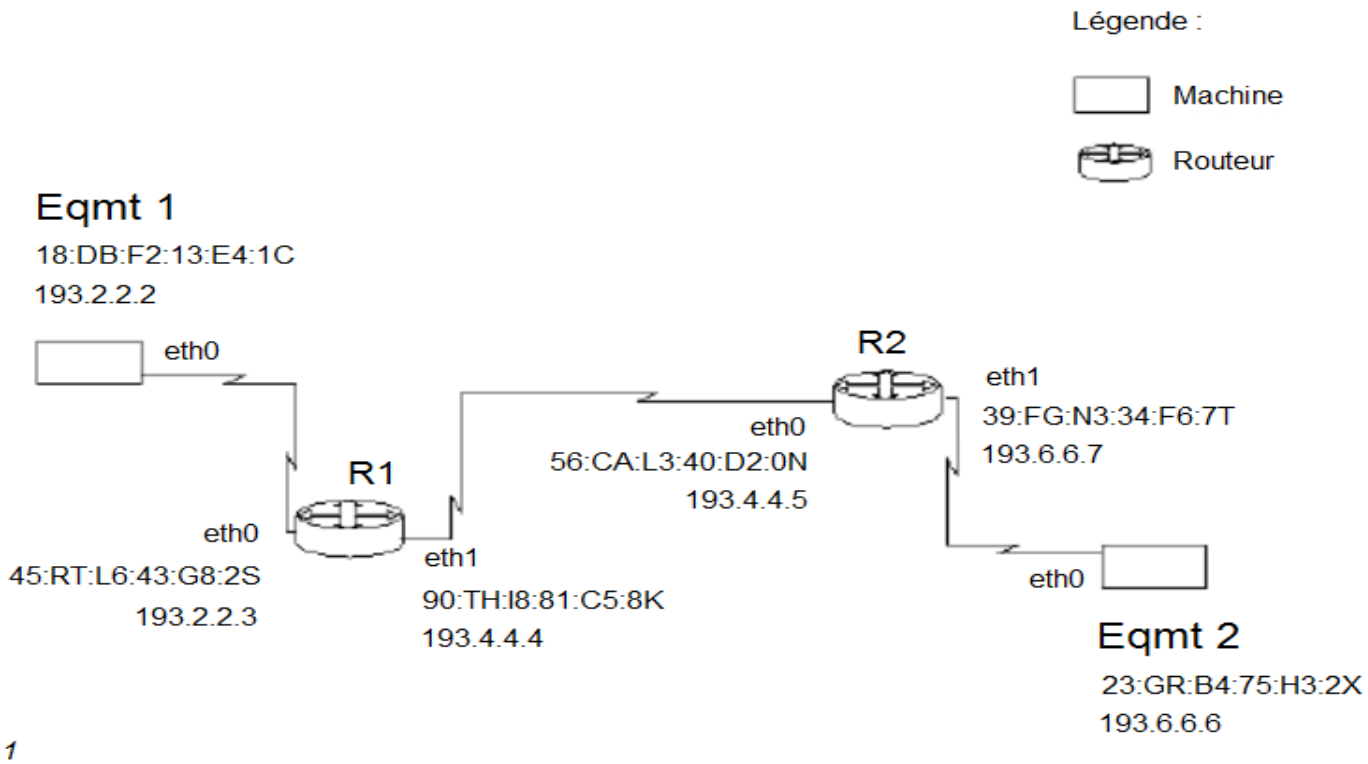


Figure 1

1. Donner les adresses IP source et destination du paquet prêt à être envoyé de Eqmt 1.

2. Donner les tables de routage initiales les plus simples (minimales), sur chaque machine (Eqmt 1, R1, R2 et Eqmt 2), permettant l'acheminement du paquet de Eqmt 1 vers Eqmt 2.

3. Donner les étapes successives nécessaires à cet acheminement, en précisant les adresses utilisées dans les en-têtes des trames Ethernet envoyées pour transporter le paquet ci-dessus.

Dossier documentaire :

Document 1	Pourquoi créer des VLAN ? *https://blog.devensys.com/pourquoi-creer-des-vlans/* 15 février 2015, Léo Gonzales	pages 1 à 3
Document 2	Les tables de routage *http://www.linux-france.org/prj/edu/archinet/systeme/ch06s03.html* 2004	pages 4 à 6
Document 3	Routeur (Equipement réseau) *http://www.commentcamarche.net › Encyclopédie › Réseaux / Internet › Réseaux locaux*	pages 7 à 8
Document 4	Réseaux TCP/IP/Adressage IP v4 *https://fr.wikibooks.org/wiki/R%C3%A9seaux_TCP/IP/Adressage_IP_v4* Dernière modification faite le 31 janvier 2018 à 18:39	pages 9 à 13

Pourquoi créer des VLANs ?

Vous n'avez jamais entendu parler de Vlan ? Le concept vous parait obscur ? Vous ne comprenez pas l'intérêt ? Alors cet article est fait pour vous ! En effet, nous allons tenter de vous expliquer, d'une part ce qu'est un VLAN, et de l'autre pourquoi faire des VLANS.

Qu'est-ce qu'un VLAN ?

Par VLAN comprenez Virtual Local Area Network. Du coup, pour comprendre ce qu'est un VLAN il faut comprendre ce qu'est un LAN (Local Area Network).
Un LAN est un réseau où tous les périphériques sont dans le même domaine de broadcast (adresse de diffusion vers tous les périphériques d'un réseau). Dans un LAN, chaque élément du réseau peut communiquer avec l'ensemble du réseau sans passer par un routeur.
Sans VLAN un switch considère toutes ses interfaces comme étant dans le même LAN et donc dans le même domaine de broadcast. Alors qu'avec les VLANS, un switch peut mettre certaines de ses interfaces dans un domaine de broadcast et d'autres dans un autre domaine de broadcast. Un même switch a alors plusieurs domaines de broadcast. Soit plusieurs séparations logiques sur un même support physique.

Schéma 1 :

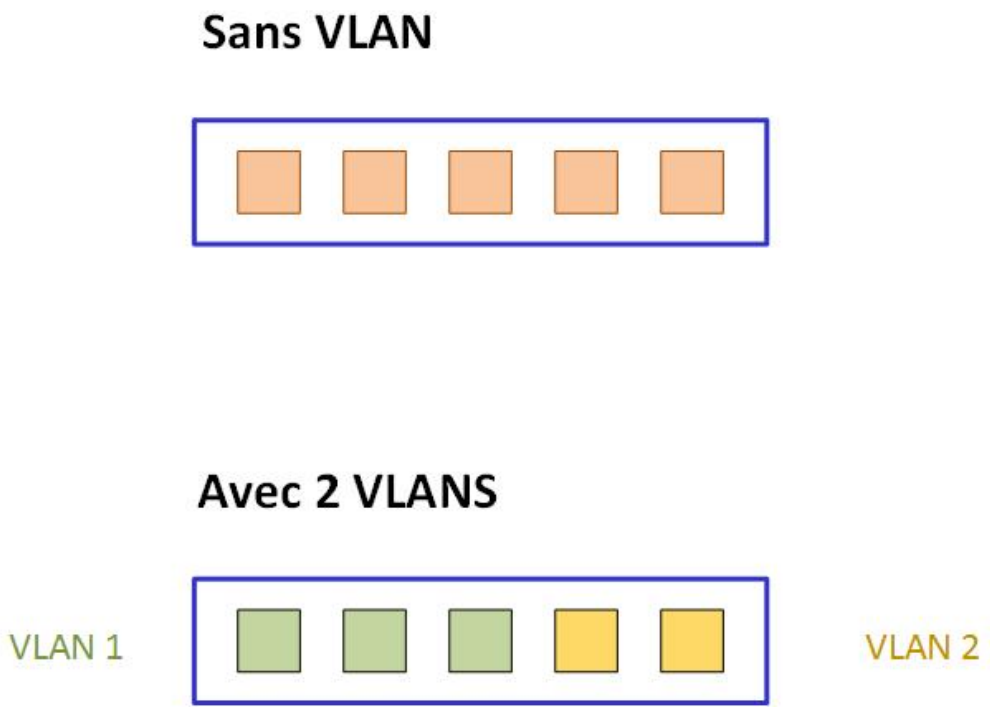
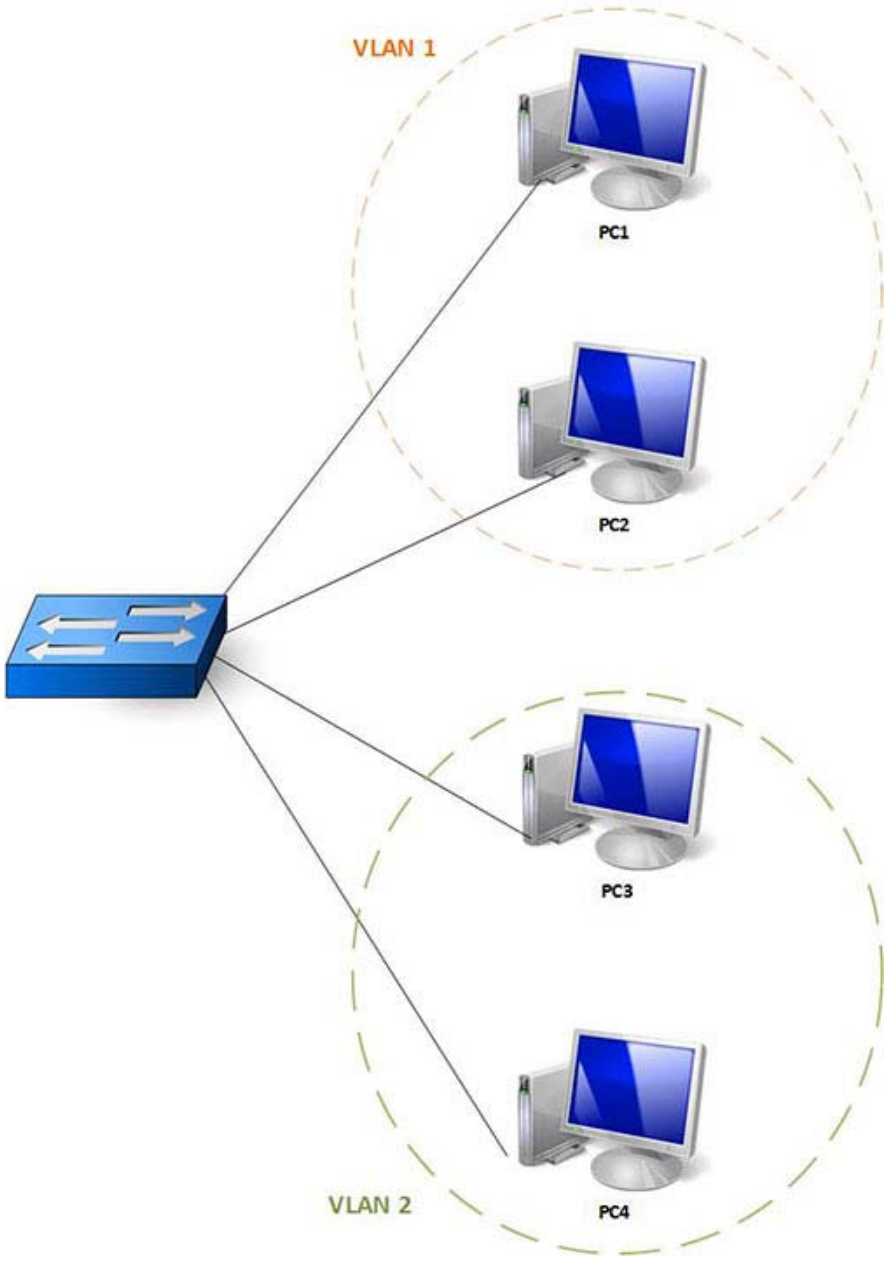


Schéma 2 :

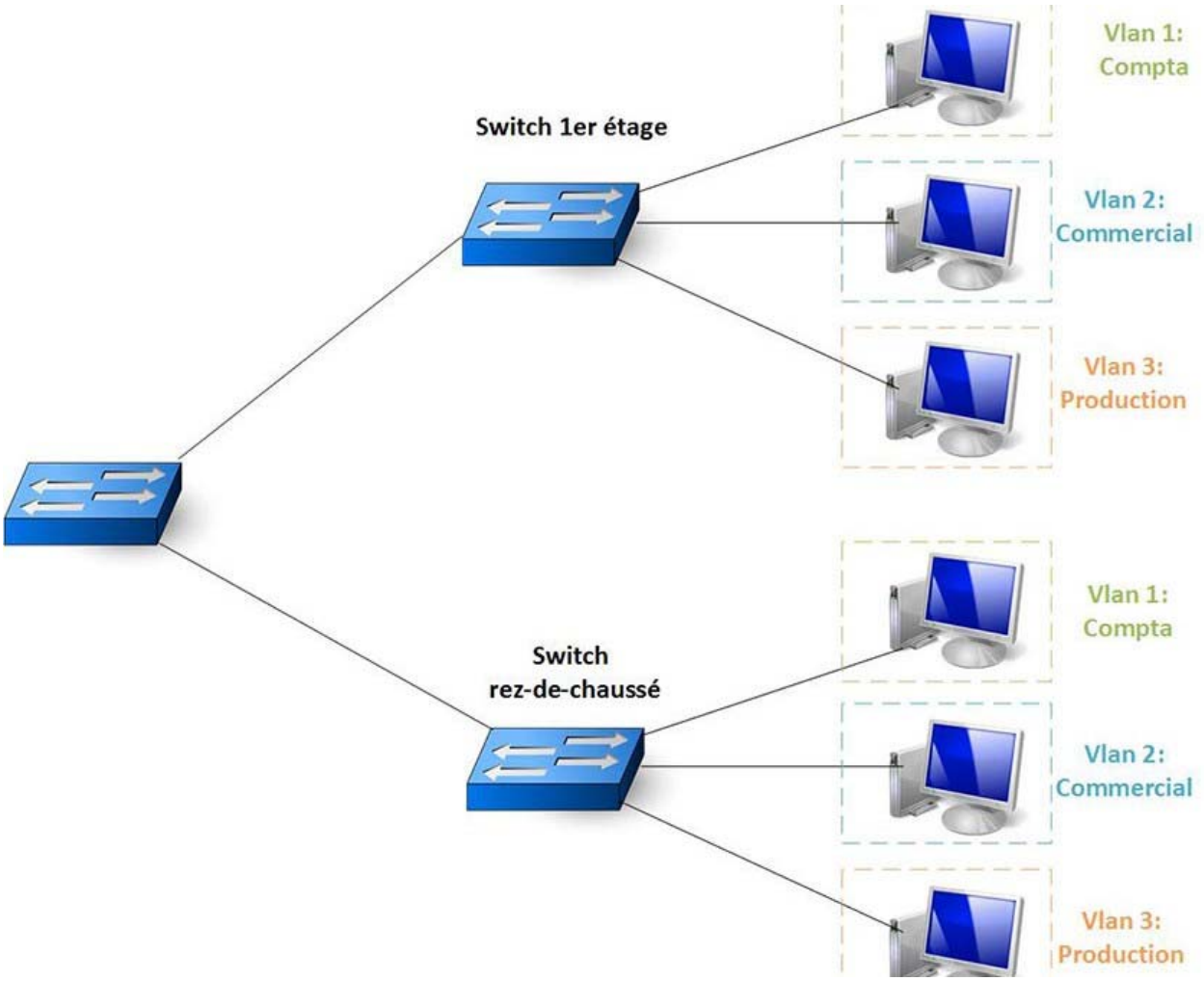


Si PC1 envoie un message en broadcast, PC2 le recevra, mais PC3 et PC4 ne le recevront pas. Autrement dit, VLAN1 est un domaine de broadcast et VLAN2 est un autre domaine de broadcast, pourtant les 4 PC sont tous branchés sur le même switch.

Pourquoi créer des VLANS ?

Les VLANs comprenant beaucoup de périphériques engendrent un grand domaine de broadcast. Les périphériques sont donc exposés à un plus grand nombre de messages de broadcast. Or ces derniers nécessitent un temps de processus important. Autrement dit, dans un VLAN très encombré (exemple : un VLAN de 500 utilisateurs), les périphériques seront plus lent que dans un petit VLAN (exemple : un VLAN de 10 utilisateurs). De plus, ces nombreux messages de broadcast peuvent entrainer une surcharge des liens et la perte de paquets. Il est donc important de considérer le dimensionnement de son réseau afin de garantir des performances optimales.
Les VLANs vous permettent également de séparer logiquement des départements ou des groupes de travail sans pour autant qu'ils soient séparés physiquement. Ainsi on pourra avoir le département comptabilité sur un Vlan, le département commercial sur un autre et de même pour le département production et le département direction. Evidement ce n'est qu'un exemple, le réseau peut être divisé avec n'importe quelle logique voulue.

Schéma 3 :



En outre, les VLANs entrainent un certain niveau de sécurité. En effet, les attaques utilisant le broadcast sont contenues au sein d'un VLAN (ARP cache poisoning, DHCP spoofing, attaque smurf, MAC table overflow…). De plus, des règles de sécurité pourront être ajoutées sur les communications entre les VLANs permettant ainsi d'apporter une nouvelle couche de sécurité à la défense en profondeur de l'entreprise.
La QoS (Quality of Service) est également simplifiée avec la création de VLANs. Par exemple, si tous les téléphones IP sont dans le même VLAN appelé VoIP, on pourra favoriser le flux venant de ce VLAN.

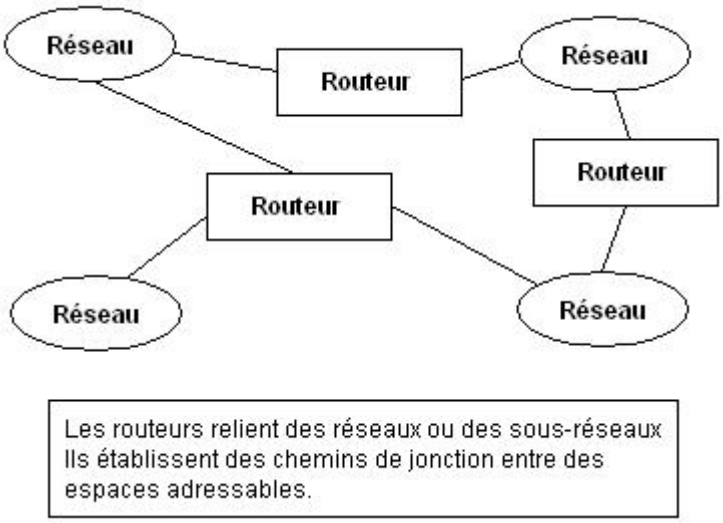
Conclusion

Les VLANS sont des configurations essentielles dans un réseau d'entreprise. En effet les VLANs optimisent le réseau et permettent d'implémenter de la sécurité et de la QoS.

Les tables de routage

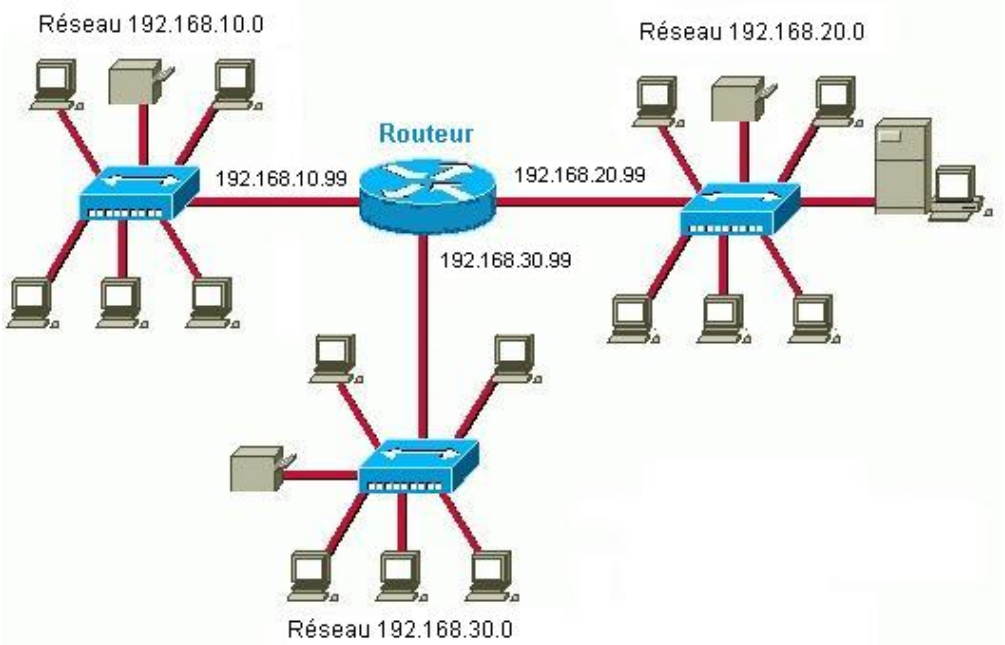
Les réseaux IP sont interconnectés par des routeurs IP de niveau 3 (appelés abusivement en terminologie IP des gateways ou passerelles).

Figure 1. routeurs interconnectés



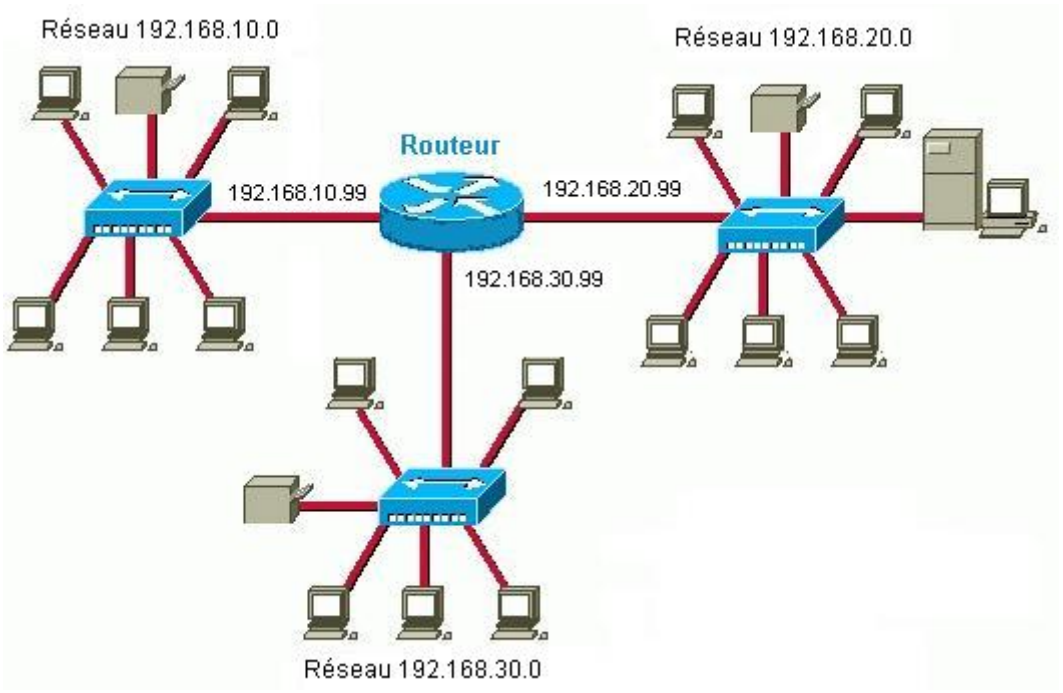
Chaque hôte IP doit connaître le routeur par lequel il faut sortir pour pouvoir atteindre un réseau extérieur, c'est-à-dire avoir en mémoire une table des réseaux et des routeurs. Pour cela il contient une table de routage locale.
Dans une configuration de **routage statique**, une table de correspondance entre adresses de destination et adresses de routeurs intermédiaires est complétée « à la main » par l'administrateur, on parle de **table de routage**.

Figure 2. schéma de routage



La table de routage d'un routeur comporte les adresses des réseaux de destination, le masque, les adresses des passerelles (routeurs intermédiaires) permettant de les atteindre, l'adresse de la carte réseau (interface) par laquelle le paquet doit sortir du routeur.
La commande **Route** permet d'afficher et de manipuler le contenu de la table de routage.
Considérons le schéma de réseau suivant :

Figure 3. schéma de réseau 1

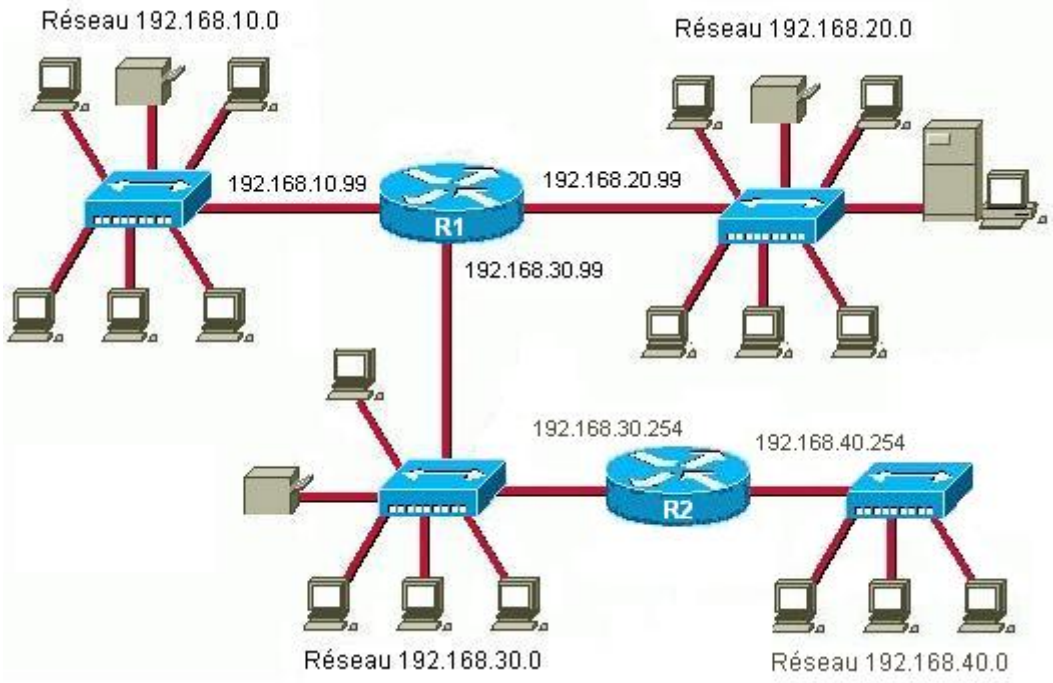


La table de routage du routeur sera :

Destination	*Masque de Sous réseau*	*Passerelle*	*Interface*	
192.168.10.0	255.255.255.0	192.168.10.99	192.168.10.99	sortie de la passerelle vers le sous-réseau 10
192.168.20.0	255.255.255.0	192.168.20.99	192.168.20.99	sortie de la passerelle vers le sous-réseau 20
192.168.30.0	255.255.255.0	192.168.30.99	192.168.30.99	sortie de la passerelle vers le sous-réseau 30

Ce réseau local est maintenant relié via un autre routeur à un 4ème réseau, le schéma devient :

Figure 4. schéma de réseau 2



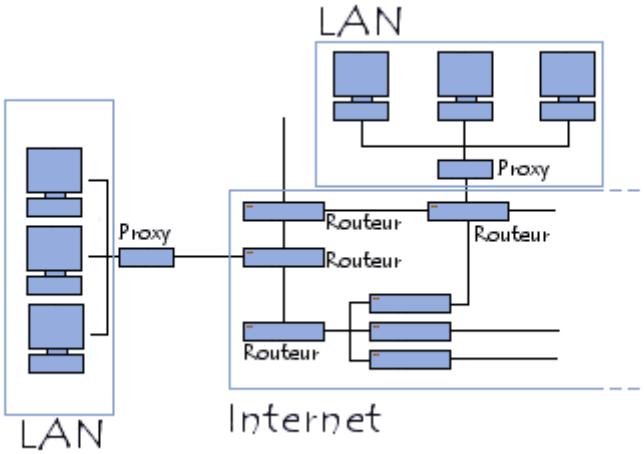
La nouvelle entrée à ajouter dans **la table de routage du routeur R1** sera :

Destination	*Masque de Sous réseau*	*Passerelle*	*Interface*	
192.168.40.0	255.255.255.0	192.168.30.254	192.168.30.99	sortie de la passerelle vers le sous-réseau 40 via le routeur 192.168.30.254

Routeur (Equipement réseau)

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.
Lorsqu'un utilisateur appelle une URL, le client Web (navigateur) interroge le serveur de noms, qui lui indique en retour l'adresse IP de la machine visée.

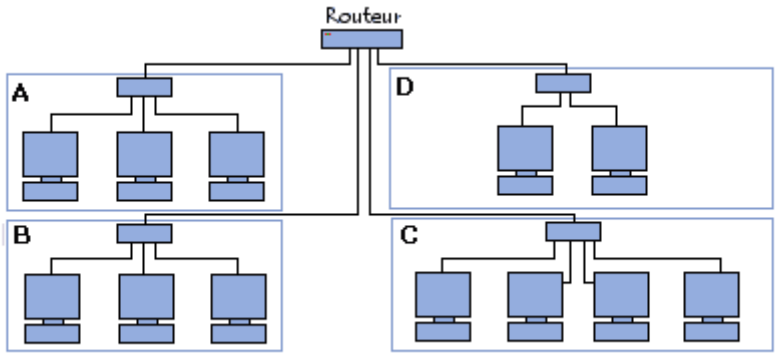
Son poste de travail envoie la requête au routeur le plus proche, c'est-à-dire à la passerelle par défaut du réseau sur lequel il se trouve. Ce routeur va ainsi déterminer la prochaine machine à laquelle les données vont être acheminées de manière à ce que le chemin choisi soit le meilleur.
Pour y parvenir, les routeurs tiennent à jour des tables de routage, véritable cartographie des itinéraires à suivre en fonction de l'adresse visée. Il existe de nombreux protocoles dédiés à cette tâche.



En plus de leur fonction de routage, les routeurs permettent de manipuler les données circulant sous forme de datagrammes afin d'assurer le passage d'un type de réseau à un autre. Or, dans la mesure où les réseaux n'ont pas les mêmes capacités en terme de taille de paquets de données, les routeurs sont chargés de fragmenter les paquets de données pour permettre leur libre circulation.

Aspect d'un routeur

Les premiers routeurs étaient de simples ordinateurs ayant plusieurs cartes réseau, dont chacune était reliée à un réseau différent. Les routeurs actuels sont pour la plupart des matériels dédiés à la tâche de routage, se présentant généralement sous la forme de serveurs 1U.



Un routeur possède plusieurs interfaces réseau, chacune connectée sur un réseau différent. Il possède ainsi autant d'adresses IP que de réseaux différents sur lesquels il est connecté.

Routeur sans fil

Le principe d'un routeur sans fil est le même que celui d'un routeur classique, si ce n'est qu'il permet à des dispositifs sans-fil (stations WiFi par exemple) de se connecter aux réseaux auxquels le routeur est connecté par des liaisons filaires (généralement Ethernet).

Algorithmes de routage

On distingue généralement deux types d'algorithme de routage :

- Les routeurs de type vecteur de distance (distance vector) établissent une table de routage
- recensant en calculant le « coût » (en terme de nombre de sauts) de chacune des routes puis transmettent cette table aux routeurs voisins. A chaque demande de connexion le routeur choisit la route la moins coûteuse.
- Les routeurs de type link state (link state routing) écoutent le réseau en continu afin de recenser les différents éléments qui l'entourent. A partir de ces informations chaque routeur calcule le plus court chemin (en temps) vers les routeurs voisins et diffuse cette information sous forme de paquets de mise à jour. Chaque routeur construit enfin sa table de routage en calculant les plus courts chemins vers tous les autres routeurs (à l'aide de l'algorithme de Dijkstra).

Réseaux TCP/IP/Adressage IP v4

Une adresse IP est un entier écrit sur quatre octets, elle peut donc prendre des valeurs entre 0 et 2^{32} - 1. Pour plus de commodité, on note les adresses en donnant les valeurs de chaque octet séparés par des points ; par exemple, 11000000101010000000000100001101 s'écrit : 11000000 10101000 00000001 00001101. devient 192.168.1.13.
Une adresse IP est constituée de deux parties : l'adresse du réseau et l'adresse de la machine, elle permet donc de distinguer une machine sur un réseau. Deux machines se trouvant sur un même réseau possèdent la même adresse réseau mais pas la même adresse machine.

Masques réseau

Ce découpage en deux parties est effectué en attribuant certains bits d'une adresse à la partie réseau et le reste à la partie machine. Il est représenté en utilisant un « masque réseau » où sont placé à 1 les bits de la partie réseau et à 0 ceux de la partie machine.
Par exemple 207.142.131.245 est une adresse IP (celle de Wikilivres, en fait) et 255.255.255.0 un masque réseau indiquant que les trois premiers octet (les 24 premiers bits) sont utilisés pour adresser le réseau et le dernier octet (les 8 derniers bits) pour la machine. 207.142.131.245/255.255.255.0 désigne donc la machine d'adresse 245 sur le réseau d'adresse 207.142.131.0.
Lorsque les bits du masque réseau sont contigus, on utilise une notation plus courte : IP/nombre de bits à 1. 207.142.131.245/255.255.255.0 peut donc aussi se noter 207.142.131.245/24.

Classes d'adresses

Il existe différents découpages possible que l'on appelle « classes d'adresses ». À chacune de ces classes correspond un masque réseau différent :

classe	premiers bits	premier octet	masque
A	0	0-127	255.0.0.0
B	10	128-191	255.255.0.0
C	110	192-223	255.255.255.0
D	1110	224-239	
E	1111	240-255	

Les adresses de classe A permettent donc de créer des réseaux avec plus de machines, par contre, il y a beaucoup plus de réseaux de classe C possibles que de réseaux de classe A ou B.
La classe D est une classe utilisée pour le « multicast » (envoie à plusieurs destinataires) et la classe E est réservée.

Adresses réseaux et adresses de diffusion

Une adresse réseau est une adresse IP qui désigne un réseau et non pas une machine de ce réseau. Elle est obtenue en plaçant tous les bits de la partie machine à zéro.
Une adresse de diffusion (« broadcast » en anglais) est une adresse permettant de désigner toutes les machines d'un réseau, elle est obtenue en plaçant tous les bits de la partie machine à un.
Par exemple :

IP (classe)	masque	adresse réseau	adresse de diffusion
10.10.10.10 (A)	255.0.0.0	10.0.0.0	10.255.255.255
192.168.150.35 (C)	255.255.255.0	192.168.150.0	192.168.150.255

Adresses déconseillées et réseaux privés

Pour éviter les ambiguïtés avec les adresses de réseau et les adresses de diffusion, les adresses « tout à zéro » et « tout à un » sont déconseillées pour désigner des machines sur un réseau.
Dans chaque classe d'adresses, certaines adresses réseaux sont réservées aux réseaux privés.

classe	réseau privé
A	10.0.0.0
A	127.0.0.0
B	de 172.16.0.0 à 172.31.0.0
C	de 192.168.0.0 à 192.168.255.0

Le cas du réseau 127.0.0.1 est particulier : il désigne la boucle locale.

Sous-réseaux

Il est possible de découper un réseau en sous-réseaux en utilisant un masque de sous-réseau. Un masque de sous-réseau permet d'attribuer des bits supplémentaires à la partie réseau d'une adresse IP.
Supposons que l'on dispose d'une adresse de classe C, elle permet normalement d'adresser 254 machines avec le masque 255.255.255.0. Il est possible de découper ce réseau en deux sous réseaux de 126 machines avec le masque 255.255.255.128 ($128 = 10000000_2$).

Le cours sur l'adressage IP

Le protocole IP

Le protocole IP (Internet Protocol) est un des protocoles majeurs de la pile TCP/IP. Il s'agit d'un protocole réseau (niveau 3 dans le modèle OSI). Il n'est pas orienté connexion, c'est a dire qu'il n'est pas fiable.C'est la couche transport qui peut le rendre fiable.

Adresse IP

Dans un réseau IP, chaque interface possède une adresse IP fixée par l'administrateur du réseau ou attribuée de façon dynamique via des protocoles comme DHCP. Par extension, pour une machine simple, un PC, avec une seule interface Ethernet, on dira que cette machine a une adresse IP. Il est déconseillé de donner la même adresse à 2 machines différentes sous peine de problèmes (collisions).
Une adresse IP (IPv4 pour être précis) est une suite de 32 bits notée en général a.b.c.d avec a, b, c, et d des entiers entre 0 et 255. Chaque valeur a, b, c ou d représente dans ce cas une suite de 8 bits.
Exemple : une machine a comme adresse IP 134.214.80.12. a vaut 134 soit (1000 0110) en binaire. b vaut 214 soit (1101 0110) en binaire. c vaut 80 soit (0101 0000) et d vaut 12 vaut (0000 1100). En binaire, l'adresse IP s'écrit donc 1000 0110 1101 0110 0101 0000 0000 1100.

Taille des réseaux IP

Un réseau IP peut avoir une taille très variable :

- une entreprise moyenne aura un réseau comportant une centaine de machines.
- un campus universitaire aura un réseau comportant de quelques milliers à quelques dizaines de milliers de machines.
- un grand fournisseur d'accès peut raccorder des millions de postes.
- tous ces différents réseaux peuvent être interconnectés.

Les numéros de réseau (net-id) et de station (host-id)

Au sein d'un même réseau IP, toutes les adresses IP commencent par la même suite de bits. L'adresse IP d'une machine va en conséquence être composée de 2 parties : le net-id (la partie fixe) et le host-id (la partie variable).

Masque d'un réseau IP

Le masque du réseau permet de connaître le nombre de bits du net-id. On appelle N ce nombre. Il s'agit d'une suite de 32 bits composée en binaire de N bits à 1 suivis de 32-N bits à 0.

- Exemple de masque Classe A

Le réseau d'une multinationale comprend toutes les adresses IP commençant par 5 (ici 5 n'est évidemment donné qu'à valeur informative). Une adresse IP sera du type 5.*.*.*. Le net-id comporte 8 bits et le host-id comporte 24 bits. Le masque s'écrira donc en binaire 8 bits à 1 suivi de 24 bits à 0 soit 1111 1111 0000 0000 0000 0000 0000 0000. Le masque sera donc 255.0.0.0 Un tel réseau peut comporter 2^{24} machines soit 16 millions environ.

- Exemple de masque Classe B

Le réseau d'un campus universitaire comprend toutes les adresses IP commençant par 134.214. Une adresse IP sera du type 134.214.*.*. Le net-id comporte 16 bits et le host-id comporte 16 bits. Le masque s'écrira donc en binaire 16 bits à 1 suivi de 16 bits à 0 soit 1111 1111 1111 1111 0000 0000 0000 0000. Le masque sera donc 255.255.0.0. Un tel réseau peut contenir au maximum 2^{16} machines soit 65536 machines.

- Exemple de masque Classe C

le réseau d'une PME comprend toutes les adresses IP commençant par 200.150.17. Une adresse IP sera du type 200.150.17.* Le net-id comporte 24 bits et le host-id comporte 8 bits. Le masque s'écrira donc en binaire 24 bits à 1 suivi de 8 bits à 0 soit 1111 1111 1111 1111 1111 1111 0000 0000. Le masque sera donc 255.255.255.0. Un tel réseau peut contenir au maximum 2^8 machines soit 256 machines.

Adresse réseau

Chaque réseau IP a une adresse qui est celle obtenue en mettant tous les bits de l'host-id à 0. Le réseau de l'exemple 3 a comme adresse réseau 200.150.17.0. Un réseau IP est complètement défini par son adresse de réseau et son masque de réseau.

Notation CIDR

La notation CIDR, pour Classless Inter-Domain Routing, est historiquement introduite après la notion de classe d'adresse IP (cf. section sur les classes). Elle s'inscrit dans une intention d'outrepasser la limite implicitement fixée par la notion de classe en termes de plages d'adresses disponibles dans les réseaux IPv4.
La notation initiale non CIDR considère pour un réseau donné le couple formé par l'adresse et le masque dudit réseau. En notation CIDR, une forme d'adressage équivalente est construite – ou obtenue, si l'on part de l'adresse en notation initiale non CIDR – par l'association de l'adresse du réseau (à l'instar de la notation initiale) et de la longueur du préfixe binaire déterminant ledit réseau. Le préfixe binaire de la notation CIDR correspond au nombre des premiers bits à 1 dans la forme binaire du masque du réseau de la notation initiale non CIDR.
En adressage IPv4, cela se concrétise par une forme décimale de 4 octets suivie d'un entier compris entre 0 et 32. En pratique, cette plage peut s'étendre de 1 à 31 afin de permettre un adressage des hôtes (host-id) par les bits différentiels (en effectif non nul).

- Exemples
  - On considère le réseau d'adresse (décimale) 150.89.0.0 et de masque (décimal) 255.255.0.0 en notation initiale non CIDR. Ledit masque comporte 16 bits à 1 ; ces 16 bits sont les 16 premiers bits du masque. En notation CIDR, ce réseau est identifié par la forme décimale suivante : 150.89.0.0/16.
  - De la même manière, le réseau d'adresse (décimale) 200.89.67.0 et de masque (décimal) 255.255.255.0 pourra être identifié par la notation CIDR 200.89.67.0/24.
  - Pour un réseau d'adresse (décimale) 192.168.144.0 et de masque (décimal) 255.255.240.0, la notation CIDR sera 192.168.144.0/20.

Adresse de diffusion (broadcast)

Cette adresse permet à une machine d'envoyer un datagramme à toutes les machines d'un réseau. Cette adresse est celle obtenue en mettant tous les bits de l'host-id à 1. Le réseau de l'exemple 3 a comme adresse de broadcast 200.150.17.255.

Deux adresses interdites

Il est interdit d'attribuer à une machine d'un réseau IP, l'adresse du réseau et l'adresse de broadcast.
Ce qui, pour le réseau 192.168.1.0/24, nous donne :

- adresse du réseau : 192.168.1.0
- adresse de broadcast : 192.168.1.255

Les classes A, B et C (obsolète)

Historiquement, le réseau Internet était découpé en classes d'adresses :

- Classe A :
  - Le premier bit de ces adresses IP est à 0.
  - Le masque décimal associé est 255.0.0.0, soit les 8 premiers bits à 1.
  - Les adresses de ces réseaux ont la forme décimale a.0.0.0 avec a variant 0 à (2^7-1 =) 127.
  - Cette classe détermine ainsi (127 - 0 + 1 =) 128 réseaux.
  - Le nombre de bits restant pour l'adressage des hôtes est de (32 - 8 =) 24.
  - Chaque réseau de cette classe peut donc contenir jusqu'à 2^{24}-2 = 16 777 214 machines.
- Classe B :
  - Les 2 premiers bits de ces adresses IP sont à 1 et 0 respectivement.
  - Le masque décimal associé est 255.255.0.0, soit les 16 premiers bits à 1.
  - Les adresses de ces réseaux ont la forme décimale a.b.0.0 avec a variant de (2^7 =) 128 à (2^7 + 2^6-1 =) 191 et b variant de 0 à 255.
  - Cette classe détermine ainsi ((191 - 128 + 1) × (255 - 0 + 1) =) 16 384 réseaux.
  - Le nombre de bits restant pour l'adressage des hôtes est de (32 - 16 =) 16.
  - Chaque réseau de cette classe peut donc contenir jusqu'à 2^{16}-2 = 65 534 machines.
- Classe C :
  - Les 3 premiers bits de ces adresses IP sont à 1, 1 et 0 respectivement.
  - Le masque décimal associé est 255.255.255.0, soit les 24 premiers bits à 1.
  - Les adresses de ces réseaux ont la forme décimale a.b.c.0 avec a variant de (2^7 + 2^6 =) 192 à (2^7 + 2^6 + 2^5-1 =) 223, b et c variant de 0 et 255 chacun.
  - Cette classe détermine ainsi ((223 - 192 + 1) × (255 - 0 + 1) × (255 - 0 + 1) =) 2 097 152 réseaux.
  - Le nombre de bits restant pour l'adressage des hôtes est de (32 - 24 =) 8.
  - Chaque réseau de cette classe peut donc contenir jusqu'à 2^8-2 = 254 machines.
- Classe D :
  - Les 4 premiers bits de ces adresses IP sont à 1, 1, 1 et 0 respectivement.
  - Le masque décimal associé par défaut est 224.0.0.0, soit les 3 premiers bits à 1.
  - Les adresses de cette classe ont la forme décimale a.b.c.d avec a variant de (2^7 + 2^6 + 2^5 =) 224 à (2^7 + 2^6 + 2^5 + 2^4-1 =) 239, b, c et d variant de 0 et 255 chacun.
  - Cette classe est spéciale : elle est réservée à l'adressage de groupes de diffusion multicast.
- Classe E :
  - Les 4 premiers bits de ces adresses IP sont (tous) à 1.
  - Le masque décimal associé par défaut est 240.0.0.0, soit les 4 premiers bits à 1.
  - Les adresses de cette classe ont la forme décimale a.b.c.d avec a variant de (2^7 + 2^6 + 2^5 + 2^4 =) 240 à (2^8-1 =) 255, b, c et d variant de 0 et 255 chacun.
  - Cette classe est également spéciale : elle est actuellement réservée à un adressage de réseaux de recherche.

La notion de classe d'adresses a été rendue obsolète pour l'adressage des nœuds du réseau Internet car elle induisait une restriction notable des adresses IP affectables par l'utilisation de masques spécifiques. Les documents RFC 1518[1] et RFC 1519[2] publiés en 1993 spécifient une nouvelle norme : l'adressage CIDR (cf. supra). Ce nouvel adressage précise qu'il est possible d'utiliser un masque quelconque appliqué à une adresse quelconque. Il organise par ailleurs le regroupement géographique des adresses IP pour diminuer la taille des tables de routage des principaux routeurs du réseau Internet.

Exemple

Une machine possède l'adresse IP 134.214.80.12 : elle appartient au réseau de classe B 134.214.0.0 de masque 255.255.0.0. Dans ce réseau, une machine peut avoir une adresse IP comprise entre 134.214.0.1 et 134.214.255.254. L'adresse de broadcast est 134.214.255.255.

Adresses privées (non routables sur l'Internet)

Un certain nombre de ces adresses IP sont réservées pour un usage interne aux entreprises (RFC 1918[3]) Elles ne doivent pas être utilisées sur l'internet où elles ne seront de toute façon pas routées. Il s'agit des adresses :

- de 10.0.0.0 à 10.255.255.255
- de 172.16.0.0 à 172.31.255.255
- de 192.168.0.0 à 192.168.255.255
- les adresses de 127.0.0.0 à 127.255.255.255 sont également interdites.

Les adresses 127.0.0.0 à 127.255.255.255 s'appelle l'adresse de boucle locale (loopback en anglais) et désigne la machine locale (localhost).

Distribution des adresses IP

Sur l'internet, l'organisme IANA est chargé de la distribution des adresses IP. IANA a délégué la zone européenne à un organisme : le RIPE NCC. Cet organisme distribue les adresses IP aux fournisseurs d'accès à l'internet.

Découpage d'un réseau IP

Un réseau IP de classe A, B ou C peut être découpé en sous-réseaux. Lors d'un découpage le nombre de sous-réseaux est une puissance de 2 : 4, 8, 16, 32… ce qui est naturel si l'on pense à la représentation binaire d'une adresse IP. Chaque sous-réseau peut être découpé en sous-sous-réseaux et ainsi de suite On parle indifféremment de réseau IP pour désigner un réseau, un sous-réseau, … Chaque sous-réseau sera défini par un masque et une adresse IP.

Exemple de découpage

On considère le réseau d'adresse 134.214.0.0 et de masque 255.255.0.0. On veut découper ce réseau en 8 sous-réseaux. Pour chaque sous-réseau, on veut obtenir le masque et l'adresse.

- Calcul du masque

On veut découper le réseau en 8. Or $8 = 2^3$. En conséquence, le masque de chaque sous-réseau est obtenu en ajoutant 3 bits à 1 au masque initial. L'ancien masque 255.255.0.0 comprend 16 bits à 1 suivis de 16 bits à 0. Le nouveau masque comprendra donc 16 + 3 = 19 bits à 1 suivis de 13 bits à 0. Il correspond à 255.255.224.0.

- Calcul du net-id de chaque sous réseau

Le net-id de chaque sous-réseau sera constitué de 19 bits :

  - Les 16 premiers bits seront ceux de l'écriture binaire du préfixe d'adresse 134.214 ;
  - Les 3 bits suivants seront constitués du numéro du sous-réseau : 000 (0), 001 (1), 010 (2), 011 (3), 100 (4), 101 (5), 110 (6) ou 111 (7).

- Calcul de l'adresse de chaque sous-réseau

Pour obtenir l'adresse réseau, tous les bits du host-id sont positionnés à 0. On obtient donc comme adresse pour chaque sous-réseau :

  - 134.214.(000 00000).0 soit 134.214.0.0
  - 134.214.(001 00000).0 soit 134.214.32.0
  - 134.214.(010 00000).0 soit 134.214.64.0
  - 134.214.(011 00000).0 soit 134.214.96.0
  - 134.214.(100 00000).0 soit 134.214.128.0
  - 134.214.(101 00000).0 soit 134.214.160.0
  - 134.214.(110 00000).0 soit 134.214.192.0
  - 134.214.(111 00000).0 soit 134.214.224.0.

- Obtention des adresses de broadcast

Pour obtenir l'adresse de broadcast, on met à 1 tous les bits du host-id. Les adresses de broadcast sont donc :

  - 134.214.(000 11111).255 soit 134.214.31.255
  - 134.214.(001 11111).255 soit 134.214.63.255
  - 134.214.(010 11111).255 soit 134.214.95.255
  - 134.214.(011 11111).255 soit 134.214.127.255
  - 134.214.(100 11111).255 soit 134.214.159.255
  - 134.214.(101 11111).255 soit 134.214.191.255
  - 134.214.(110 11111).255 soit 134.214.223.255
  - 134.214.(111 11111).255 soit 134.214.255.255.