

8• Gestion des adresses en IP

Exercice 1 : Adressage IPV4 de base (hiérarchisé à deux niveaux).

L'adressage IPV4 a été créé dans sa version de base en distinguant trois classes d'adresses associées à trois classes de réseaux notés A, B et C.

- 1) *Comment est notée l'adresse d'un hôte et l'adresse d'un réseau ?*
- 2) *Comment un ordinateur hôte ou un routeur reconnaissent-il qu'une adresse de destination appartient à l'une des classes ?*
- 3) *Quelle est la proportion relative du nombre d'adresses IPV4 affectées aux différentes classes A, B, C ? En déduire une conséquence si l'utilisation des adresses de classe A (ou B) est inefficace.*
- 4) *Quelle est l'opération effectuée sur une adresse de station pour déterminer son adresse de réseau ?*
- 5) *Comment l'adresse d'un hôte destinataire est elle utilisée pour le routage ?*

On vient de voir que les conventions d'adressage de base IPV4 permettent implicitement la détermination de l'appartenance d'une adresse à l'une des classes A, B, C ainsi que celle de l'adresse du réseau auquel il appartient. Bien que cela ne soit pas nécessaire on souhaite maintenant pour toute adresse IP rendre explicite l'adresse de son réseau d'appartenance en utilisant systématiquement la notation 'adresse/n'. On rappelle que dans cette notation n est la longueur du préfixe définissant le réseau d'appartenance ou le nombre de bits en fort poids du masque.

- 6) *Quelle sont les valeurs de n_1 et n_2 pour les adresses suivantes : 17.234.16.45/ n_1 , 207.12.231.23/ n_2 .*
- 7) *Pourquoi a t'on procédé à un tel découpage et quels en sont les difficultés actuelles ?*

Exercice 2 : Adressage IPV4 de base avec la notion de sous réseau (hiérarchisé à trois niveaux).

L'adressage IPV4 a assez rapidement introduit la possibilité de structurer les adresses d'un réseau IP en sous réseaux. Une entreprise dont l'informatique était basée sur de petites architectures réseaux hétérogènes (Novell, ...) décide de passer à Internet. Après en avoir fait la demande l'entreprise a obtenu l'adresse 193.1.1.0. Compte tenu de l'organisation actuelle de l'entreprise l'ingénieur système doit définir au moins 6 sous-réseaux. Compte tenu de l'évolution prévisible de l'entreprise, l'ingénieur système pense que le sous-réseau le plus important peut comporter à moyen terme 25 hôtes.

Question 1

Quel est le découpage que doit effectuer l'ingénieur système ? En déduire la valeur du masque de sous réseau. On donnera le résultat dans la notation

décimale pointée et dans la notation /n.

Question 2

On considère le 2^{ème} sous réseau dont l'adresse.

Quelle est son adresse complète de sous réseau ?

Quelle est l'adresse de diffusion à tous les hôtes de ce sous réseau ?

Exercice 3 : Adressage en IPV4 avec CIDR

Comme son nom l'indique CIDR ('Classless Inter Domain Routing') est une approche sans classe. On ne considère plus une adresse comme appartenant implicitement à l'une des trois classes A, B ou C. En CIDR on associe explicitement à toute adresse de réseau IP un masque qui définit le préfixe qui caractérise le réseau auquel correspond cette adresse. Les adresses de réseaux sont donc maintenant toujours utilisées avec leur préfixe qui peut être de taille arbitraire (par exemple /8, /17, /21).

Supposons qu'on attribue à une entreprise l'adresse 194.16.0.0 avec le préfixe /21 soit en binaire un masque 11111111 11111111 11111000 0000000000 ou en notation décimale pointée une valeur de masque 255.255.248.0). Cette attribution veut dire que cette entreprise dispose pour son réseau du bloc d'adresse qui s'étend de 194.16.0.0 à 194.16.7.255. Soit l'adresse 194.16.6.23 d'un hôte dans ce réseau à atteindre. En utilisant le masque (défini ici par /21) qui doit toujours être associé à l'adresse on voit que cet hôte doit être atteint au moyen de l'adresse réseau 194.16.0.0. Il faut donc rechercher dans les tables de routage une entrée correspondant à cette adresse de réseau.

Question 1

Considérons l'adresse CIDR d'un réseau qui serait 193.53.32.0/20.

Quelle serait le nombre d'hôtes que comporterait ce réseau ?

Question 2

Dans le réseau précédent 193.53.32.0/20 quelle est l'adresse la plus petite utilisable pour un hôte et quelle est la plus grande ?

Question 3

Supposons qu'un utilisateur restitue une ancienne adresse de classe A, B ou C comme 17.0.0.0 ou 134.15.0.0 ou 194.65.32.0 anciennement attribuées.

Ces adresses n'étant plus jamais utilisées par leurs anciens propriétaires, pourrait-on les attribuer à nouveau selon l'approche CIDR (attribuer par exemple 17.46.64.0/19, 134.15.0.0/20 et 194.65.32.0/21) ?

Question 4

Une entreprise s'adresse à un Prestataire de Service Internet PSI (ISP 'Internet Service Provider') pour obtenir 800 adresses.

Que devait faire le prestataire dans l'adressage par classes A, B, C pour satisfaire son client et avec quels inconvénients ?

Question 5

Nous supposons que le prestataire d'accès Internet a reçu pour exercer son activité le bloc d'adresses CIDR 202.0.64.0/18 avec lequel il a constitué son réseau. Chaque prestataire est libre de découper son espace d'adresse comme il l'entend pour fournir des adresses à ses clients. Les clients peuvent également à leur tour découper l'espace reçu pour le distribuer en interne selon les principes CIDR. Ils pourraient même devenir prestataires d'accès Internet.

Pour un client demandant 800 adresses que va faire le prestataire si au moment de la demande la première adresse réseau qui est libre est 202.0.70.0 ?

Question 6

Comment se passe avec CIDR le routage dans le réseau Internet pour atteindre l'un des hôtes appartenant au réseau du client ayant obtenu les 800 adresses ?

Vous prendrez si nécessaire une adresse à titre d'exemple dans cet ensemble.

Question 7

En résumé montrez en quoi CIDR constitue une amélioration majeure de l'adressage IPV4.

Exercice 4 : Allocation d'adresses IP4 pour les réseaux privés

Dans le cadre du protocole IPV4 on a défini deux types d'adresses IP : les adresses IP publiques (également appelées globales) et les adresses IP privées (également appelées locales). Cette définition apparaît dans la norme RFC 1597 (mars 1994) dont le titre est 'Address allocation for private Internets' (version définitive RFC 1918 février 1996).

Question 1

Quelles sont les adresses IPV4 qui sont définies comme adresses privées (ou locales) et quelles sont les adresses qui sont définies comme publiques ou globales ?

Question 2

Comment sont attribués ces deux types d'adresses ?

Question 3

Comment sont utilisés ces deux types d'adresses (quelles sont les règles mises en oeuvre pour ces adresses dans un routeur d'un réseau IPV4 privé c'est à dire un réseau d'entreprise ou un réseau personnel et dans un routeur du réseau IPV4 global) ?

Question 4

Dans quels buts a-t-on défini ces deux types d'adresses (avec quels avantages et quels inconvénients) ?

Exercice 5 : Traduction d'adresses IPV4 (NAT)

La norme RFC 1631 (mai 1994) ('The IP Network Address Translator'), définit un principe général de traduction d'adresses IP. La dernière version, la plus récente de cette approche RFC 3002 (janvier 2001) améliore différents points.

La traduction d'adresses peut être appliquée par différents types d'appareils dont la caractéristique principale est d'être situés entre un réseau IPV4 privé et le réseau IPV4 global. Typiquement la traduction est effectuée par un routeur, mais on peut aussi appliquer la traduction dans un hôte quelconque ou dans un filtre (pare-feux ou 'firewall').

La traduction au niveau des adresses IP s'applique à l'adresse source d'un datagramme IP en provenance du réseau privé (baptisé encore en NAT réseau interne) et à destination du réseau public (baptisé encore en NAT réseau externe). De manière symétrique, la traduction est effectuée sur les datagrammes en provenance du réseau public (ou externe) vers le réseau privé (ou interne).

La traduction d'adresse peut être réalisée de différentes façons qui sont examinées dans les questions suivantes.

Question 1

Dans le mode NAT statique l'adresse IPV4 source privée est traduite en une adresse IPV4 source publique qui est toujours la même. La correspondance dans ce cas est bijective (biunivoque) c'est-à-dire qu'à une adresse privée est associée de manière statique une adresse publique (selon une table de correspondance statiquement définie par un administrateur réseau).

*Quelle utilisation peut-on faire d'un tel mode de traduction d'adresses IP ?
Quels sont les inconvénients ?*

Question 2

Dans le mode NAT dynamique, la traduction d'une adresse source IPV4 privée est effectuée vers une adresse source IPV4 publique qui est prise dans un bloc d'adresses publiques disponibles. L'adresse publique utilisée n'est donc pas toujours la même. Par exemple si l'on suppose que l'hôte d'adresse 172.20.40.17 émet un datagramme à un instant donné vers l'Internet global, son adresse est traduite dans la première adresse disponible d'un bloc. Par exemple, si l'adresse 212.19.50.63 du bloc disponible 212.19.50.0 à 212.19.50.255 est non utilisée au moment de l'émission du datagramme, on l'utilisera et on traduira 172.20.40.17 en 212.19.50.63. Cette correspondance est enregistrée dans une table. De manière à éviter de bloquer indéfiniment une adresse attribuée dynamiquement, un temporisateur est utilisé pour révoquer l'attribution d'une adresse publique. A l'échéance, on récupère une adresse attribuée et l'on procède à une nouvelle attribution d'adresse si un nouvel échange à lieu (éventuellement on peut reprendre la même adresse pour un autre quantum).

Quel avantage nouveau obtient-on d'un tel mode de traduction d'adresses IP ?

Question 3

Le troisième mode est connu sous différents noms (mode NAT avec surcharge NAT 'overloading' encore appelé NAT with PAT 'Port Address Translation'). Dans ce cas la traduction

d'une adresse source IPV4 privée vers une adresse source IPV4 publique est complétée par la traduction du numéro de port. Le plus souvent, dans ce cas on suppose l'utilisation d'une seule adresse publique (par exemple une adresse publique comme 212.19.50.63 disponible). Si l'on suppose que l'hôte d'adresse 172.20.40.17 émet un datagramme selon le protocole TCP avec le numéro de port source 5032, alors son adresse IP est traduite en l'adresse IP publique (212.19.50.63) et le numéro de port source TCP est également traduit vers un numéro de port non utilisé (par exemple 4097 si ce port n'est pas déjà attribué à une autre communication). Comme dans le cas du NAT dynamique, les attributions sont associées à un temporisateur avec récupération à échéance. Ce mode de fonctionnement est le plus utilisé.

Quels en sont les avantages et les inconvénients ?

Exercice 7 : Utilitaire ping et adresses IPV6

L'utilitaire ping créé pour le protocole IPV4 a été adapté à IPV6. Il s'appelle alors ping6. Sur une machine, l'exécution de la commande ping6, donne une liste résultat de la forme suivante :

```
$ ping6 2001:660:3003:1D05::1:1

PING ping6 2001:660:3003:1D05::1:1: 56 data bytes

64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=0 time=43.1 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=1 time=40.0 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=2 time=44.2 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=3 time=43.7 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=4 time=38.9 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=5 time=41.2 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=6 time=39.1 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=7 time=42.1 ms

- - - 2001:660:3003:1D05::1:1 ping statistics - - -

 9 packets transmitted, 9 packets received, 0% packet loss

round-trip min/avg/max = 38.9/41.3/44.2 ms
```

Question 1

Comment fonctionne l'utilitaire ping. Que peut-on déduire du résultat de l'exécution de cette commande?

Question 2

L'adresse IPV6 utilisée en paramètre de la commande ping6 est l'adresse 2001:660:3003:1D05::1:1 . Il s'agit d'une adresse notée sous une forme compacte (avec des raccourcis).

Quelles sont les règles définies pour compacter une adresse IPV6. Comment se note l'adresse 2001:660:3003:1D05::1:1 sous une forme développée (notation complète d'une adresse IPV6) ?

Question 3

A quelle catégorie (à quel plan d'adressage) appartient l'adresse 2001:660:3003:1D05::1:1 (selon son préfixe est-ce une adresse prestataire, agrégée ou géographique). Même question pour l'adresse: 5F0D:E900:80DF:E000:0001:0060:3E0B:3010 ?

Question 4

Commentez la valeur des temps d'aller retour (round trip time) (que pouvez vous dire à la lecture de ces chiffres) ?

Exercice 8 : Mobilité avec IP en version 4

Les appareils portables (comme les ordinateurs portables, les téléphones IP, les organisateurs...) qui utilisent les protocoles de l'Internet, posent le problème du déplacement d'un hôte IPV4 à l'intérieur de l'Internet. L'objectif de la norme 'IP Mobility' (RFC 3344 dernière version en 2002) encore connue sous le sigle MIP4 (pour 'Mobile IP' en version 4) est de permettre à un hôte dans un réseau IP de changer de point de rattachement au réseau Internet en conservant toujours la même adresse IP.

L'adressage IPV4 fait que tout appareil doit posséder une adresse IP qui permet de le localiser dans un réseau auquel il est rattaché. IP mobile en V4 a donc comme objectif de permettre à un hôte de communiquer avec d'autres hôtes dans le réseau Internet même après un changement de point d'attachement sans avoir à reconfigurer manuellement cet hôte. La norme IP mobile suppose donc qu'un ordinateur mobile (un nœud mobile ou 'mobile node' en anglais) possède une adresse IP principale fixe qui appartient à son réseau d'origine (son réseau 'home network'). C'est avec cette adresse IP qu'il doit continuer de pouvoir être accessible en toutes circonstances qu'il soit connecté dans son réseau d'origine ou qu'il se soit déplacé dans un réseau étranger ('foreign network').

Pour les besoins de la mobilité, IP mobile en version 4 fait l'hypothèse qu'un hôte mobile doit être modifié pour supporter un ensemble de logiciels réseaux spécifiques lui permettant d'être mobile (en particulier la couche IP est modifiée). Nous allons voir que certains routeurs doivent également subir des modifications en vue de la mobilité. Par contre un hôte habituel de l'Internet qui communique avec un mobile (en anglais 'correspondent node') doit rester un hôte quelconque de l'Internet c'est-à-dire qu'il ne doit pas avoir à subir de modifications de ses logiciels réseaux Internet.

Pour assurer la mobilité en IP, une première solution consisterait à utiliser le routage IP. Il faudrait définir dans les tables de routage, des routes vers des hôtes (en anglais 'host specific route') de sorte qu'un hôte mobile dans le réseau Internet pourrait conserver toujours la même adresse IP tout en restant accessible n'importe où dans l'Internet grâce au routage IP.

Question 1

Etudiez la solution de mobilité en IP par l'utilisation de routes conduisant vers un hôte unique. Quelles seraient les conséquences d'une telle approche de la mobilité sur le fonctionnement de l'Internet?

Indications : vous examinerez les avantages et les inconvénients de cette solution en considérant principalement les problèmes de performances des opérations à réaliser que sont la commutation d'un datagramme dans un routeur et la mise à jour des routes par les protocoles de routages dynamiques compte tenu de l'existence de routes vers les hôtes uniques.

Question 2

On se place maintenant dans l'hypothèse ou lorsqu'un mobile arrive dans un réseau étranger, il communique en IP en utilisant une adresse IP dans ce réseau. En IP mobile cette nouvelle adresse est baptisée 'care-of address'. Citez toutes les techniques que vous connaissez permettant à un hôte, d'obtenir dynamiquement une adresse IP dans un réseau ?

Lorsqu'un mobile est arrivé dans un réseau étranger nous supposons qu'il dispose d'un moyen pour s'apercevoir qu'il a changé de réseau. Par exemple, en interrogeant un serveur sur la valeur du préfixe réseau courant il peut déterminer s'il a changé de réseau. Nous supposons que le mobile demande alors et obtient une adresse IP dans ce réseau par l'un des moyens listés à la question précédente.

Question 3

Quelles sont les possibilités de communications Internet qui sont offertes au mobile au moyen de cette nouvelle adresse (l'adresse dans le réseau étranger)?

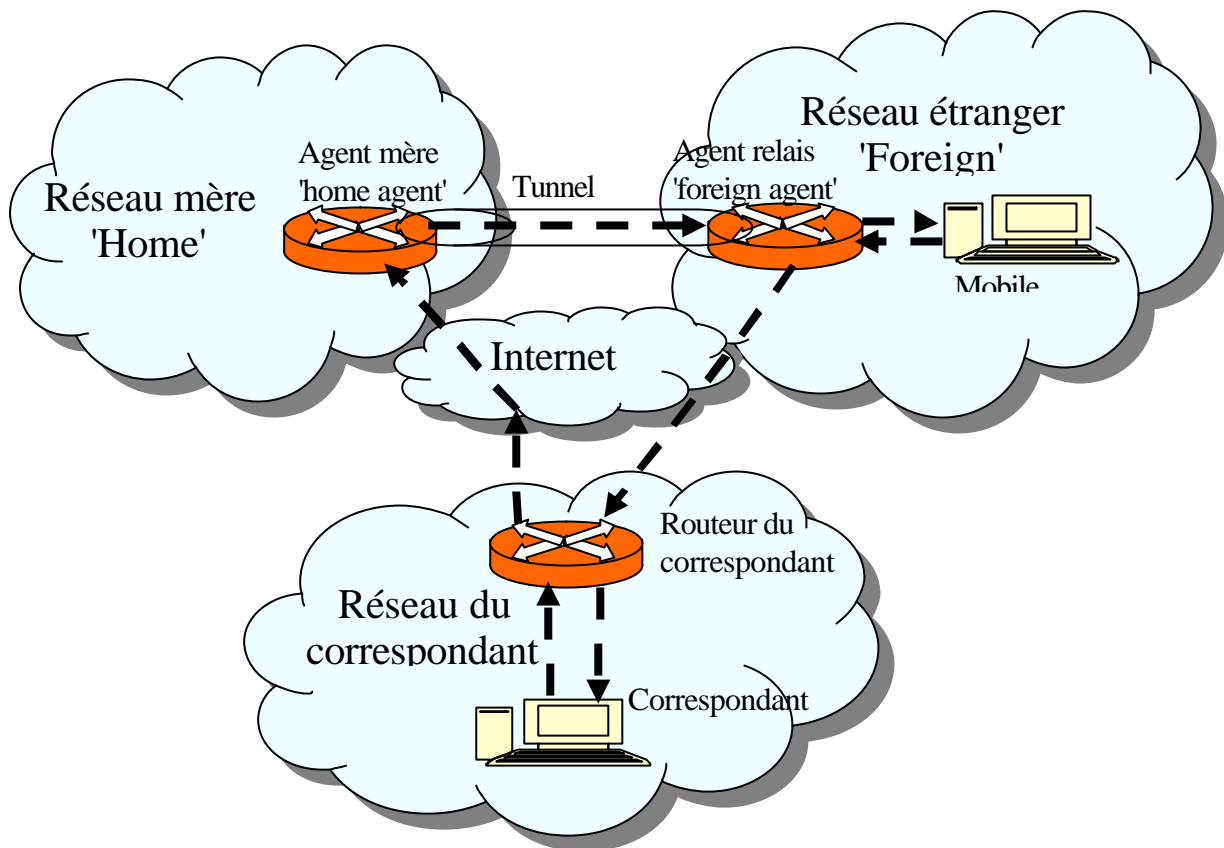
Indications : peut-il appeler un nouveau correspondant ? Peut-il continuer une communication qui était en cours avec un correspondant malgré le changement d'adresse (justifiez votre réponse en particulier si le transport utilisé est TCP) ? Peut-il être appelé par un nouveau correspondant ?

Pour permettre à un correspondant d'envoyer des datagrammes vers un mobile, IP mobile suppose l'existence de deux systèmes informatiques jouant des rôles particuliers. Le plus souvent il s'agit d'extensions logicielles en vue de la mobilité qui sont installées dans des routeurs.

L'agent mère (traduction la plus fréquemment constatée de 'home agent') est situé dans le réseau mère c'est-à-dire le réseau d'origine du mobile ('home network'). C'est très souvent le réseau de l'entreprise où travaille la personne qui utilise un mobile de façon professionnelle. Le rôle de l'agent mère ('home agent') est de remplacer un mobile dans son réseau d'origine lorsque celui-ci est absent. L'agent mère reçoit les datagrammes IP adressés au mobile sur son adresse IP principale et les réexpédie vers le mobile dans un autre réseau où celui-ci s'est déplacé.

L'agent relais ('foreign agent') est situé dans le réseau étranger visité par le nœud mobile (en anglais le 'foreign network'). Il doit enregistrer la présence du mobile et sa nouvelle adresse IP lorsqu'il vient d'arriver dans le réseau étranger. Mais son rôle est principalement de recevoir les datagrammes retransmis par l'agent mère et de les relayer pour les délivrer à destination du mobile. Il lui faut aussi signaler à l'agent mère son adresse d'agent relais pour que l'agent mère puisse lui réexpédier les datagrammes arrivés pour le mobile. Dans le sens inverse, le mobile répond aux datagrammes qui sont envoyés par un correspondant en s'adressant directement à ce correspondant.

En raison de l'existence de ces trois entités essentielles au fonctionnement du routage IP mobile (un correspondant avec son routeur de rattachement, un agent mère dans le réseau mère et un agent relais dans le réseau étranger) le routage d'un datagramme en IP mobile est baptisé routage triangulaire. La figure suivante traduit la circulation des datagrammes IP du correspondant vers le mobile et du mobile vers le correspondant. On peut voir une grande analogie entre ce fonctionnement pour les datagrammes et la réexpédition du courrier postal.



Question 4

On rappelle qu'avec IP mobile, un mobile est toujours atteint au moyen de son adresse IP de rattachement dans son réseau mère (son réseau principal d'accueil 'home'). Comment l'agent mère peut-il faire pour remplacer un mobile IP quand celui-ci est absent de ce réseau d'origine ?

Indications : Recherchez le protocole permettant à un hôte d'un réseau IP de se déclarer destinataire des messages à destination d'une certaine adresse IP.

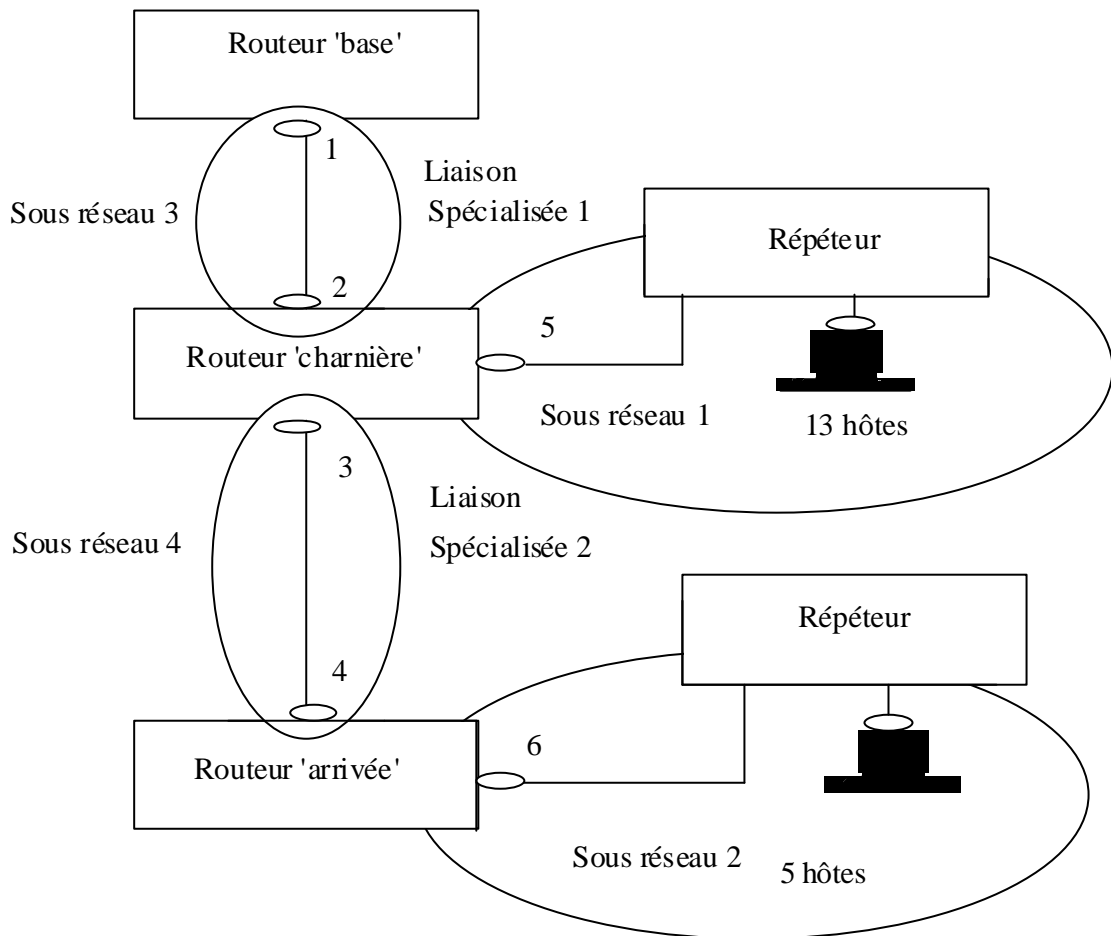
L'agent mère ayant récupéré tous les datagrammes à destination du mobile, doit les retransmettre au mobile qui se trouve dans le réseau étranger par l'intermédiaire de l'agent relais. Mobile IP impose que la communication entre l'agent mère dans le réseau mère et l'agent relais dans le réseau étranger s'effectue en mode tunnel. Utiliser un tunnel signifie que le datagramme IP qui avait été transmis d'un correspondant vers le mobile est encapsulé dans un nouveau datagramme IP. On conserve donc toute l'entête d'origine et toute la charge utile du datagramme original en considérant le tout comme la charge utile d'un nouveau datagramme avec une nouvelle entête IP entre agent mère et agent relais. L'agent relais peut donc récupérer en sortie du tunnel, le datagramme transmis initialement par le correspondant et c'est ce datagramme qui est utilisé pour la délivrance au mobile dans le réseau étranger.

Question 5

Pourquoi procède t'on ainsi ?

10• Déploiement de réseaux IP

Un ingénieur réseau doit installer un nouveau sous-réseau Internet dans son entreprise. L'organisation administrative et géographique des ordinateurs à raccorder est telle qu'il apparaît naturel de créer deux groupes de 5 et 13 hôtes. Chaque groupe de postes est interconnecté au moyen d'un réseau ethernet partagé. On utilise pour cela un répéteur (par exemple de standard 10 BaseT). On associe aux deux groupes, deux sous-réseaux IP et on interconnecte les deux sous-réseaux au moyen de routeurs. Un routeur existant dans l'entreprise baptisé dans la figure suivante routeur 'base' sert à connecter le nouvel ensemble au reste du réseau d'entreprise. Chaque sous-réseau dispose d'un routeur. Ces routeurs sont baptisés 'charnière' pour le groupe de 13 hôtes et 'arrivée' pour le groupe de 5 hôtes. Les routeurs sont connectés au moyen de deux liaisons spécialisées point à point notées Liaison spécialisée 1 et 2.



Exercice 1 : Choix des adresses

Pour réaliser l'installation IP de ce nouvel ensemble, l'ingénieur réseau souhaite d'une part économiser les adresses IP mais aussi minimiser le nombre des entrées à placer dans les tables de routage pour atteindre le nouvel ensemble (agréger les routes). Pour cela l'ingénieur considère comme indispensable que le nouvel ensemble à installer forme un unique réseau IP, comprenant différentes adresses elles-mêmes organisées en sous réseaux (selon la figure).

Détaillons maintenant toutes les adresses à fournir. Sur le dessin les points qui doivent recevoir une adresse IP sont marqués par de petits ovales.

L'ingénieur réseau doit attribuer des adresses IP pour le sous-réseau 1, c'est à dire pour chacun des 13 hôtes qui constituent ce sous réseau IP, mais aussi pour le port du routeur 'charnière' qui dessert le sous-réseau 1. Ce port est indiqué par le numéro 5 sur la figure.

De même le sous réseau 2 doit comprendre 5 adresses d'hôtes et une adresse pour le port d'accès à partir du routeur 'arrivée'. Ce port est indiqué par le numéro 6 sur la figure.

Les routeurs utilisés ne gèrent pas les liaisons dénumérotées. On rappelle que de nombreux routeurs en appliquant la RFC 1812 permettent d'utiliser des liaisons spécialisées (LS) sans adresses IP. Dans ce cas, moyennant des directives de configuration des routeurs, deux routeurs reliés par une liaison spécialisée forment en fait du point de vue du routage un seul routeur virtuel. La liaison spécialisée est cachée et gérée par le logiciel du routeur. Dans l'exemple traité ici, selon les principes de base de l'adressage IP, il faut attribuer des adresses IP aux deux extrémités d'une liaison spécialisée pour pouvoir l'utiliser dans le cadre du routage. Ces adresses doivent appartenir au même sous réseau IP. Les deux LS forment donc deux petits sous réseaux baptisés 3 et 4. Ces deux sous réseaux ont besoin seulement de deux adresses IP.

L'ingénieur réseau a un bloc d'adresses IP non utilisées dans le cadre d'un adressage de type IPV4 CIDR à partir de l'adresse 193.137.1.0.

Question 1

Pour le nouvel ensemble l'ingénieur pense pouvoir utiliser seulement un bloc de 32 adresses libres parmi celles dont ils dispose.

Pourquoi ?

Quelle adresse de réseau choisit-il pour la totalité des adresses du nouvel ensemble (donner l'adresse de réseau et son masque en notation /n)?

Question 2

L'ingénieur attribue pour commencer les adresses d'extrémité de la liaison spécialisée 1 (adresses du sous-réseau 3). Il doit donc créer un sous réseau avec deux adresses IPV4.

Quelle est l'adresse de réseau du sous-réseau 3 (l'adresse et le masque du plus petit réseau IPV4 possédant au moins deux adresses utilisables à partir de la première adresse libre) ?

Question 3

L'ingénieur attribue la première adresse IP utilisable du réseau déterminé à la question 2 (la plus petite) à l'extrémité 1 sur le dessin (port du routeur 'base') et la seconde (la plus grande) à l'extrémité 2 (port du routeur 'charnière').

Quelles sont les deux adresses attribuées ?

Question 4

L'ingénieur attribue ensuite les adresses IP d'extrémités de la liaison spécialisée 2 (adresses IP du sous réseau 4).

Quelle est l'adresse de réseau retenue pour ce nouveau bloc de deux adresses si l'on attribue les adresses immédiatement disponibles après l'attribution du sous réseau 3 ?

Question 5

Si l'on attribue la plus petite adresse utilisable de ce sous réseau à l'extrémité 3 (port du routeur 'charnière') et la plus grande adresse à l'extrémité 4 (port du routeur 'arrivée'), quelles sont les deux adresses retenues ?

Question 6

L'ingénieur doit ensuite attribuer des adresses de sous réseaux pour les sous réseaux 1 et 2 qui correspondent à 13+1 soit 14 adresses et 5+1 soient 6 adresses.

Quelle est maintenant la première adresse disponible ?

De manière à optimiser l'utilisation des adresses dans quel ordre doit-il attribuer les deux demandes ?

Question 7

Quelle est alors l'adresse de sous réseau attribuée pour le sous réseau 1.

Si l'on prend la plus petite adresse disponible dans ce sous réseau, quelle est l'adresse attribuée au port du routeur 'charnière' indiquée 5 sur le dessin ?

Question 8

Quelle est l'adresse de sous réseau attribuée pour le sous réseau 2 ?

Si l'on prend la plus petite adresse disponible dans ce sous réseau, quelle est l'adresse attribuée au port du routeur 'arrivée' indiquée 6 sur le dessin ?

Exercice 2 : Construction de tables de routage statiques

Dans les questions qui suivent on s'intéresse à la construction des routes dans le cadre d'un routage statique (d'initialisation des tables de routage) pour atteindre les différentes composantes du nouvel ensemble (réseaux, stations, liaisons spécialisées). Pour construire le routage, il peut être très pratique de reporter toutes les adresses définies dans le premier exercice sur la figure qui représente la topologie du réseau pour avoir une vue d'ensemble du plan d'adressage.

Question 1

Dans la table de routage d'un hôte d'un réseau IP on définit en général trois routes.

Définir les trois entrées nécessaires au routage pour l'une des stations du sous réseau 1.

Pour chaque entrée on définira au moins la destination de la route, le masque de cette destination (en notation /n) et le prochain saut ('next hop' ou 'gateway' définissant le prochain routeur ou la station visité).

Question 2

Définir les entrées concernant le nouvel ensemble, pour la table de routage du routeur 'base'.

Pour chaque route on précisera la destination, le masque de la destination, le prochain saut ('next hop' ou 'gateway' définissant le prochain routeur ou la station visité) et le type de la route. Le type est soit local s

les paquets sont délivrés à leur destinataire directement, soit distant si les paquets doivent être relayés par le prochain routeur avant d'être délivré. Pour construire la réponse, on doit définir d'abord la route pour atteindre tout le nouvel ensemble à partir du routeur 'base'. On définira aussi une route qui dessert localement la liaison spécialisée numéro 1. Comme on a créé ce sous réseau IP numéro 1, l'accès à ces adresses doit être possible à toutes fins utiles comme l'envoi de paquets de tests ou de paquets d'administration de réseau SNMP (IP ne sert pas uniquement pour délivrer des messages TCP ou UDP à des hôtes). Cet accès est-il à réaliser par le routeur 'base' via le port numéroté 1 ?

Question 3

Définir les entrées concernant le nouvel ensemble, pour la table de routage du routeur 'charnière'.

Pour chaque route on précisera comme précédemment la destination, le masque de la destination, le prochain routeur et le type de la route (ne pas oublier les liaisons spécialisées).

Question 4

Définir les entrées concernant le nouvel ensemble, pour la table de routage du routeur 'arrivée'.

Question 5

Est ce que le plan d'adressage précédent est satisfaisant ?

On examinera le critère de l'utilisation des adresses IP. On examinera ensuite le critère de l'agrégation des routes (de la minimisation du nombre de routes à créer).

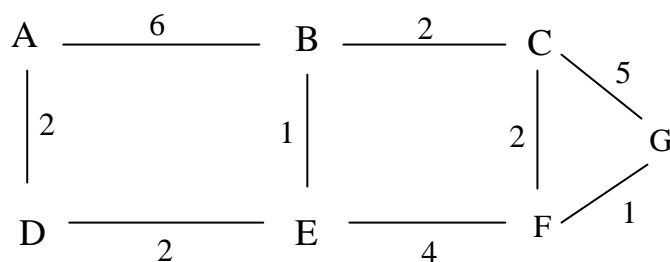
De combien d'entrées a-t-on besoin dans une table de routage pour accéder au nouvel ensemble des deux sous réseaux ou à chacun des sous réseaux ?

11•Routage OSPF

("Open Shortest Path First")

Le but de ce problème est d'étudier le protocole internet OSPF. C'est un protocole de routage réparti dans lequel chaque routeur gère une base de données de l'ensemble des liaisons d'un réseau (topologie du réseau) et calcule à partir de cette base les plus courts chemins par l'algorithme de Dijkstra. Cette base de donnée est mise à jour par diffusion en inondation par chaque routeur de l'état de ses liaisons aux autres routeurs. Il entre dans la classe des protocoles baptisés "à état des liaisons" ou "linkstate".

Par exemple soit un réseau de 7 routeurs A, B, C, D, E, F, G dont la topologie est la suivante (les coûts de transit pour chaque liaison sont supposés égaux dans chaque direction et sont mentionnés sur l'arc représentant la liaison).



La base de données (topologie ou carte du réseau) qui doit être connue de chaque routeur donne principalement les coûts en point à point pour chaque liaison. D'autres informations sont également stockées dans cette table. Certaines de ces informations seront introduites dans la suite.

La base de données (topologie ou carte du réseau) qui doit être connue de chaque routeur donne principalement les coûts en point à point pour chaque liaison. D'autres informations sont également stockées dans cette table. Certaines de ces informations seront introduites dans la suite.

De	Vers	Coût
A	B	6
A	D	2
B	A	6
B	C	2
B	E	1
C	B	2
C	F	2
C	G	5
D	A	2
D	E	2
E	B	1
E	D	2
E	F	4
F	C	2
F	E	4
F	G	1
G	C	5
G	F	1

Cette base de données est construite par échange d'informations entre les routeurs. Pour cela le protocole suivant est effectué. Son déclenchement peut répondre à différentes stratégies de mise à jour :

- périodiquement
- lorsqu'un routeur nouveau s'initialise
- lorsqu'un routeur s'aperçoit qu'il a un nouveau voisin
- lorsque le coût d'une liaison avec un voisin a changé

• Étape 1 :

Chaque routeur construit un paquet appelé "paquet d'état des liaisons" ou LSP ("Link State Packet") qui contient des coûts de liaison que le routeur souhaite faire connaître. Un LSP comporte principalement une liste de noms de routeurs (voisins d'un routeur) et les coûts pour les atteindre. Les LSP émis par un même routeur sont numérotés au moyen d'un numéro de séquence. Pour simplifier on ne se préoccupe pas du retour à zéro des compteurs utilisés trop longtemps.

• Étape 2 :

Le paquet LSP est transmis à tous les routeurs voisins et chaque routeur enregistre les informations du LSP généré le plus récemment. Plus précisément chaque voisin effectue le traitement suivant:

- Recevoir le paquet LSP.
- Consulter la base existante.
- Si l'entrée (la liaison et son coût) n'est pas présente, ajouter cette entrée et diffuser l'information à tous les voisins sauf l'émetteur du LSP.
- Si l'entrée est présente et si le numéro de séquence du LSP est plus grand que celui correspondant à l'entrée modifier l'entrée et diffuser l'information à tous les voisins sauf le ré-émetteur du LSP.
- Si l'entrée est présente et si le numéro de séquence du LSP est plus petit ou égal à celui correspondant à l'entrée: ne rien faire.

Question 1

Les protocoles de routage de type vecteurs de distance dont l'exemple type est le protocole Internet RIP ("Routing Information Protocol") se distinguent des protocoles de type Internet OSPF (à état de liaison).

Rappeler en quelques lignes l'algorithme que doit suivre chaque routeur pour le protocole RIP.

Question 2

A quoi pourrait servir la retransmission du LSP à son émetteur ?

Pourquoi un paquet LSP n'est-il pas renvoyé à son émetteur ?

Question 3

A quoi sert le Numéro de Séquence émetteur du point de vue du réseau internet qui est à datagramme ?

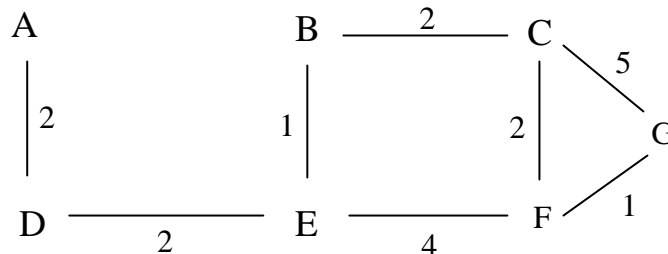
A quoi sert le Numéro de Séquence émetteur du point de vue du protocole de diffusion des informations d'état de liaison ?

En plus du Numéro de Séquence, chaque information concernant une liaison possède une date de péremption (variable baptisée dans OSPF "age") qui apparaît aussi bien dans les paquets LSP échangés que dans les bases de données. Toute information dépassant sa date est systématiquement détruite.

Citer plusieurs types de problèmes qu'une telle datation solutionne.

Question 4

On suppose que la liaison de A vers B est coupée. On a alors le réseau :



A ayant détecté la coupure, A prépare un LSP de la forme : "de A à B, coût = infini , numéro de séquence,"

On suppose que ce LSP est le premier généré (au début il est le seul).

Indiquer ce qui se passe alors dans le réseau. Quelle est la base de données obtenue par les différents noeuds à la fin du processus d'inondation ?

On suppose qu'ensuite B prépare et transmet son LSP concernant A-B.

Quelle est la base de données obtenue ?

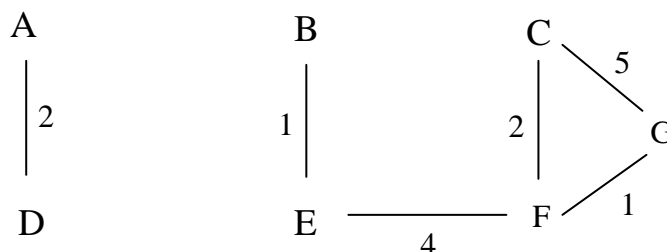
Question 5

On suppose que la liaison de D à E tombe en panne (on suppose que les 2 noeuds D et E se sont aperçus de cette rupture et envoient les LSP correspondants).

Indiquer la (ou les) bases de données obtenues à l'issue de l'algorithme distribué de transmission de l'état des liaisons par chacun des noeuds.

Question 6

A partir des bases de données trouvées à la question précédente et du réseau suivant on suppose que la liaison de B à C tombe en panne et amène au réseau :

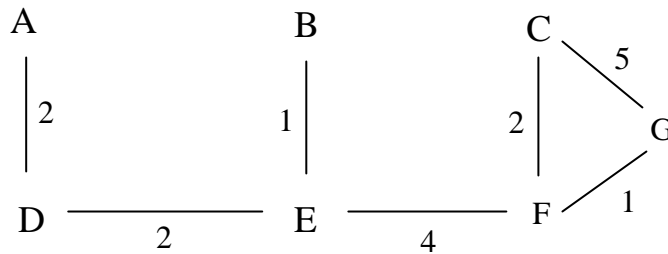


Indiquer les bases de données obtenues par chaque routeur.

Question 7

Par la suite la liaison de D à E est rétablie avec un coût de 2 rendant de nouveau le réseau connexe. On obtient alors le réseau ci-dessous.

On exécute l'algorithme de diffusion en supposant que D et E informent le réseau du rétablissement de cette connexion.



Quelle est la valeur du coût de la liaison de B à C pour les sites A, D et pour les sites B, C, E, F ?

Quel est le risque encouru dans cette situation ?

Comment détecter efficacement la situation ? Sur quel type de site ? (on suggère une utilisation du numéro de séquence)

Comment faire pour mettre en oeuvre une solution de "réconciliation" basée sur le numéro de séquence ?

Question 8

La technique de diffusion par inondation de l'état des liaisons est inconcevable telle que pour le réseau Internet. Pourquoi ?

Que fait-on pour appliquer quand même OSPF à l'internet ?