Subnetting, NAT, ICMP, ARP, DHCP, DNS – Corrigé

http://perso.ens-lyon.fr/annececile.orgerie/teaching.html

1 Subnetting

1.1 Création de sous-réseaux

✘ **Question 1.1.** *On vient d'attribuer à votre entreprise l'adresse IP* `214.123.155.0`*. Vous devez créer 10 sous-réseaux distincts pour les 10 succursales de l'entreprise, à partir de cette adresse IP. Quelle est la classe de ce réseau ? Quel masque de sous-réseau devez-vous utiliser ? Combien d'adresses IP (machines ou routeurs) pourra recevoir chaque sous- réseau ?*

Correction 214 = 128 + 64 + 16 + 4 + 2 = 11 [010110] ← classe C

Pour avoir 10 sous-réseaux différents, il faut que le réseau utilise 4 bits supplémentaires pour coder les sous-réseaux. – 1 bit ← 2 sous-réseaux – 2 bit ← 4 sous-réseaux – 3 bit ← 8 sous-réseaux – 4 bit ← 16 sous-réseaux Le masque original contenait 24 bits (255.255.255.0). Il doit maintenant en contenir 28 pour chaque succursale d'où le masque : 255.255.255.240 (240 = 128 + 64 + 32 + 16 = 11110000)

Chaque sous-réseau pourra contenir au maximun 14 ($2^4 - 2$) machines

□

✘ **Question 1.2.** *Quelle est l'adresse réseau et de broadcast du 5ième sous-réseau utilisable ?*

Correction Pour des raisons de compatibilité, on évite en général d'utiliser le sous-réseau qui a la même adresse de réseau que le réseau global et celui qui a la même adresse de broadcast. En effet, l'adresse de réseau était utilisée avant pour le broadcast et si un des sous-réseaux a la même adresse de broadcast que le réseau global, il ne sera pas possible de différencier, un broadcast vers toutes les machines du réseau d'un broadcast vers ce sous-réseau particulier. Le 5ième sous-réseau qu'il est conseillé d'utiliser en pratique est donc en fait le 6ième. Son adresse est donc 214.123.155.80 car 80 = 64 + 16 = 0101 0000 et 0101 = 5. Son adresse de broadcast est égale a 214.123.155.95 car 95 = 64 + 16 + 8 + 4 + 2 + 1 = 0101 1111.

□

✘ **Question 1.3.** *Combien d'adresses IP distinctes est-il possible d'utiliser avec un tel masque, tout sous-réseaux possibles confondus ?*

Correction Si l'on utilise pas le premier et le dernier sous-réseau, $14 \times (16 - 2) = 196$ adresses sont disponibles. Sinon, on en a $16 \times (16 - 2) = 224$ les adresses manquantes sont les adresses de réseaux et de broadcast des différents sous-réseaux. □

1.2 Réseau (presque) complet

Des systèmes autonomes identifiés par les numéros 1, 2, 3, 4 sont reliés entre-eux par des liens inter- réseaux pour former le réseau de réseaux ci-dessous (Figure 1).

On suppose que le protocole utilisé a l'intérieur d'un système autonome est de type état de liens comme OSPF. Entre les systèmes autonomes, le protocole utilisé est de type vecteur de chemin comme BGP. Un chemin sera constitué des numéros des systèmes autonomes à traverser pour atteindre un préfixe de réseau donné.

✘ **Question 1.4.** *Quelles seront les adresses listées pour un traceroute de* `1.1.1.1` *vers* `3.1.3.3` *?*

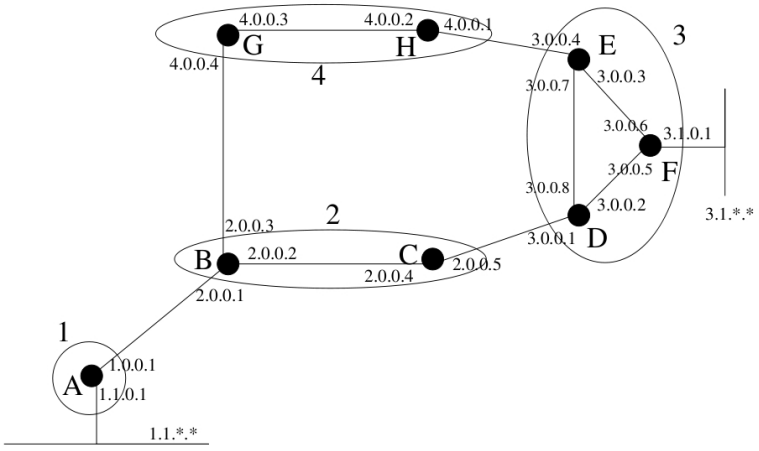

FIG. 1 – Réseau

Correction Un traceroute consiste à envoyer vers une destination des PINGs de TTL 0, 1, 2,... jusqu'à réception du PONG. La liste des adresses des routeurs intermédiaires qui répondent est alors établie.

On ne voit qu'une seule interface par routeur, celle de la route retour : 1.1.0.1 2.0.0.1 2.0.0.4 3.0.0.1 3.0.0.5 3.1.3.3 □

✘ **Question 1.5.** *Pour chaque nœud sur la route de* `1.1.1.1` *à* `3.1.3.3` *(source et destinations incluses), indiquez l'entrée dans la table de routage qui a permis de choisir le nœud suivant (next hop) sur la route, et indiquez les mécanismes qui ont conduit à insérer cette entrée dans la table (on précisera en particulier le protocole de routage qui a inséré l'entrée).*

Correction
- 1.1.1.1 : routage par défaut vers la passerelle, entrée configurée manuellement ou par DHCP
- A : entrée pour 3.*.*.* vers B d'après BGP
- B : entrée pour 3.*.*.* vers C d'après OSPF
- C : entrée pour 3.*.*.* vers D d'après BGP
- D : entrée pour 3.1.*.* vers F d'après OSPF
- F : entrée pour 3.1.*.* vers lien ethernet configuré manuellement
- 3.1.3.3 : le paquet est arrivé le nœud a obtenu son adresse soit par configuration manuelle soit par DHCP

□

✘ **Question 1.6.** *Quelles seraient les adresses listées pour un traceroute de* `1.1.1.1` *vers* `3.1.3.3` *après rupture du lien entre C et D (et après convergence des protocoles de routage) ?*

Correction
- 1.1.0.1
- 2.0.0.1
- 4.0.0.4
- 4.0.0.2
- 3.0.0.4
- 3.0.0.6
- 3.1.3.3

□

✘ **Question 1.7.** *On suppose que le lien CD se rétablit mais que C n'a pa encore fait passer l'information à B alors que D a informé E et F. Quelles seraient alors les adresses listées pour un traceroute de* `1.1.1.1` *vers* `3.1.3.3` *?*

Correction Les ICMP de E et F reviennent par DC :
- 1.1.0.1
- 2.0.0.1
- 4.0.0.4
- 4.0.0.2
- 3.0.0.7
- 3.0.0.5
- 3.1.3.3

□

✘ **Question 1.8.** *Expliquez comment le problème du comptage à l'infini sera évité si les liens CD puis EH cassent.*

Correction Quand CD casse, les routeurs de 2 utilisent 2 - 4 - 3 pour atteindre 3.*.*.*. Quand EH casse, les routeurs de 4 n'essayeront pas de passer par 2 puisque leur chemin contient 4. Ils annoncent donc une distance infinie et les routeurs de 2 feront alors de même. □

2 NAT, ICMP, DHCP, DNS

2.1 NAT

✘ **Question 2.1.** *Qu'est-ce que la traduction d'adresse réseaux (NAT = Network Adress Translation) ? A quoi cela sert-il ? Quel problèmes liés à IP cela permet-il de résoudre ?*

Correction On dit qu'un routeur fait du Network Address Translation (NAT) lorsqu'il fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi la carence d'adresses IPv4 d'Internet.

De plus, cela permet à l'administrateur d'un réseau local de ne gérer qu'une adresse publique. Il a donc une gestion plus facile de ces adresses puisqu'elles sont privées. Cela permet par exemple aux abonnés ADSL de connecter plusieurs ordinateurs sur une ligne unique.

Le NAT masquant l'adresse IP de la machine interne, participe ainsi à la sécurité du site.

Private Address	Private Port	External Address	External Port	NAT Port	Protocol Used
10.0.0.5	21023	128.10.19.20	80	14003	tcp
10.0.0.1	386	128.10.19.20	80	14010	tcp
10.0.2.6	26600	207.200.75.200	21	14012	tcp
10.0.0.3	1274	128.210.1.5	80	14007	tcp

FIG. 2 – Exemple NAT

□

✘ **Question 2.2.** *Joe veut jouer avec Bob à un jeu en réseau. Comment peuvent-ils faire dans le cas 1 ? Et dans le cas 2 ?*

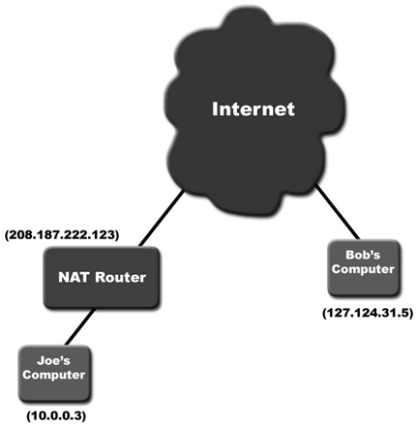

FIG. 3 – Cas 1

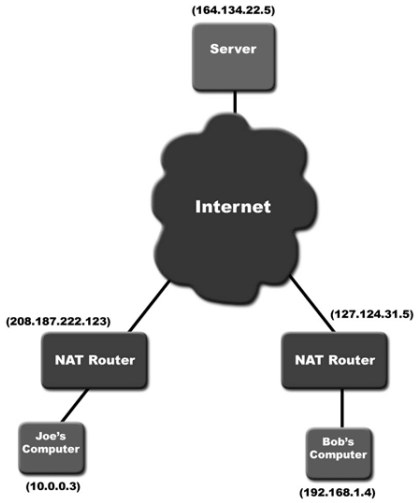

FIG. 4 – Cas 2

Correction 1er cas : le problème vient du fait que Joe ne connaît pas son adresse publique. Donc soit Bob initie le jeu (Joe se connecte à lui), soit Joe envoie un message à Bob pour lui demander son adresse (Bob voit l'adresse de l'expéditeur).

2e cas : Bob et Joe ont le même problème. Ils ne peuvent pas s'envoyer de messages car ils ne connaissent pas leurs adresses respectives. Solution : ils envoient tous les deux un message à un serveur distant dont ils connaissent l'adresse pour lui demander leurs adresses. □

2.2 ICMP

✘ **Question 2.3.** *À quoi sert le protocole ICMP ? Donnez des exemples d'utilisation.*

Correction Internet Control Message Protocol

Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour l'Internet, par exemple lorsqu'un service ou un hôte est inaccessible. Lorsqu'un routeur/station ne peut transmettre / délivrer un paquet vers sa destination, il doit informer la source du paquet du problème rencontré. □

✘ **Question 2.4.** *Donnez une façon simple d'implémenter un ping.*

Correction On utilise ICMP avec le message d'echo. □

✘ **Question 2.5.** *Donnez une façon simple d'implémenter un traceroute.*

Correction On envoie un paquet vide avec un TTL = 1, puis on en envoie un second avec un TTL = 2, etc. □

2.3 DHCP

✘ **Question 2.6.** *Quel est le rôle du protocole DHCP ? À quels inconvénients du modèle TCP/IP original apporte-il une solution ? Quel protocole de transport utilise-t-il ?*

Correction Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui assignant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS.

DHCP apporte une solution à ces inconvénients (pb des IPs statiques et de la config statique) :
- Seuls les ordinateurs en service utilisent une adresse de l'espace d'adressage ;
- Toute modification des paramètres (adresse de la passerelle, des serveurs de noms) est répercutée sur les stations lors du redémarrage ;
- La modification de ces paramètres est centralisée sur les serveurs DHCP.

DHCP suit le concept de client-serveur (serveur DHCP fournit l'information requise quand il reçoit une demande du client (machine)).

Il utilise UDP encapsulé dans IP. □

✘ **Question 2.7.** *Donnez un scénario typique d'utilisation de DHCP. Donnez l'enchaînement des messages DHCP utilisés. Que se passe-t-il si 2 serveurs DHCP répondent ?*

Correction C'est un protocole qui permet à une machine d'avoir l'information nécessaire, pour communiquer, au moment de son démarrage : adresse IP, mask, durée de validité, adresse du routeur pour accéder à Internet, adresse d'un serveur de nom (DNS), etc.

Comment le serveur va communiquer avec le client ? Le client n'a pas encore d'adresse.

Le client diffuse sa demande en utilisant l'adresse "broadcast" (255.255.255.255). Il utilise 0.0.0.0 comme adresse source.

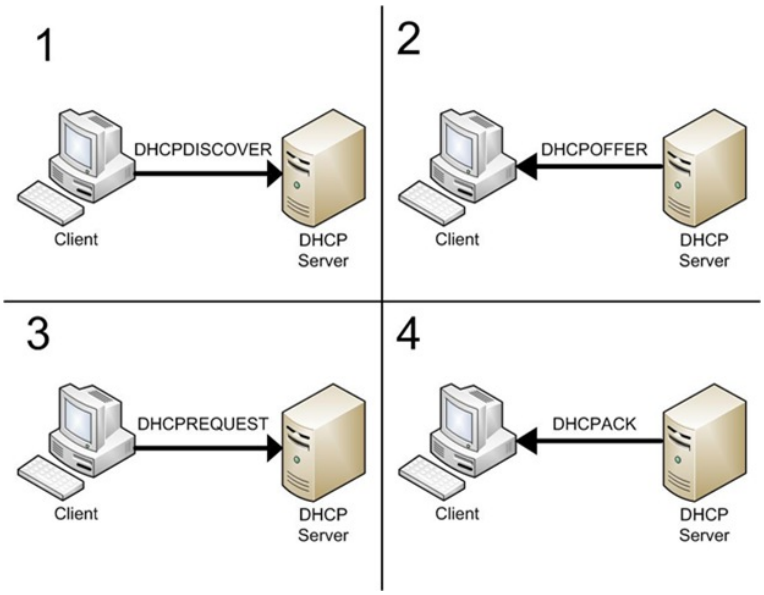

FIG. 5 – Exemple DHCP

1. DHCPDISCOVER source 0.0.0.0, destination 255.255.255.255
2. DHCPOFFER destination 255.255.255.255 Lifetime 3600 secondes
3. DHCPREQUEST Le client broadcaste son DHCPREQUEST ainsi les serveurs qui avaient fait des offres se rendent compte qu'ils n'ont pas été choisis.
4. DHCPACK du serveur au client qui obtient ainsi son IP.
5. DHCREQUEST pour se 're-lier' à un serveur.
6. DHCPACK pour confirmer l'extension du bail

7. DHCPRELEASE quand on part.

□

2.4 DNS

✘ **Question 2.8.** *À quoi sert le protocole DNS ? Comment fonctionne-t-il ?*

Correction Le Domain Name System (ou DNS, système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.

Quand un utilisateur souhaite accéder à un serveur web, par exemple celui de fr.wikipedia.org, son ordinateur émet une requête spéciale à un serveur DNS, demandant 'Quelle est l'adresse de fr.wikipedia.org ?'. Le serveur répond en retournant l'adresse IP du serveur, qui est dans ce cas-ci, 91.198.174.2. □

✘ **Question 2.9.** *IPv6 utilise des adresses sur 16 octets. Si un bloc de 1 million d'adresses est alloué à chaque picoseconde, combien de temps la réserve d'adresses durera-t-elle ?*

Correction 16 octets, cela représente 2^{128} ou $3,4 \times 10^{38}$ adresses. Si l'on attribue ces adresses à la vitesse de 10^{18} adresses par seconde, cela prendra 10^{13} années pour les affecter toutes, ce qui correspond à 1 000 fois l'âge de l'univers. Bien sûr, toutes les adresses ne sont pas envisageables, certaines sont réservées, d'autres inaccessibles. Elles ne sont pas non plus allouées de façon linéaire. Toutefois, en ne considérant qu'un espace réduit à $1/1\,000$ (soit 0,1% de l'espace), le nombre d'adresses disponibles est toujours très important. □