

TD4 : NAT, DHCP et Couche transport

10 mai 2011

1 DHCP

1. Quel est le service rendu par le protocole DHCP ? A quel niveau opère ce protocole ? Et quel est l'intérêt de ce service ?

DHCP : Dynamic Host Configuration Protocol

Ce protocole permet la configuration automatique de la couche IP d'une machine qui en fait la demande.

Ceci inclut, l'attribution d'une adresse IP mais aussi configurer la table de routage et donner les adresses des serveurs DNS pour la résolution d'adresses symboliques

DHCP opère au niveau application

Intérêt : permet de partager un ensemble d'adresses IP entre un groupe de machines. Mais la principale avantage est de simplifier l'administration des réseaux

2. Que fait une machine pour localiser un serveur DHCP ? Peut-on avoir plusieurs serveurs DHCP sur un même réseau local ? Est-ce obligatoire d'avoir un serveur DHCP par réseau local ?

Envoyer un paquet DHCPDISCOVER en mode diffusion avec l'adresse 255.255.255.255 comme @ destination.

Plusieurs serveurs peuvent co-exister sur un même réseau. Le choix entre plusieurs offres est à faire par la machine qui a initié la demande.

Il est possible aussi de n'avoir pas de serveur DHCP sur un réseau mais d'avoir un relai DHCP : un programme qui se comporte comme un serveur pour les machines et qui contacte un serveur (sur un autre réseau) pour avoir l'information de configuration.

3. Donner le chronogramme d'échange des paquets DHCP lors de la configuration d'une machine. Pour chaque paquet préciser les adresses IP source et destination.

1. Envoi de DHCPDISCOVER de la machine avec @src=0.0.0.0 et @dest= 255.255.255.255 (noter que la machine n'a pas d'adresse à ce stade et ne connaît pas l'adresse du serveur)

2. Le serveur qui reçoit la demande envoie un DHCP OFFER proposant une configuration avec @src= l'adresse du serveur et @dest= 255.255.255.255

Noter que la machine à configurer n'a pas d'adresse et le seul moyen de l'atteindre est par diffusion.

3. La machine reçoit, éventuellement plusieurs offres, et choisit une configuration. Elle envoie un DHCP REQUEST au serveur choisi demandant l'attribution de la configuration proposée. @src= 0.0.0.0 et #dest.= 255.255.255.255

noter que la machine n'a pas encore une adresse, et elle envoie en mode diffusion pour informer en même temps les serveurs non choisis de son choix.

4. Si la proposition est valable toujours, le serveur envoie DHCP ACK pour confirmer avec @src= l'adresse du serveur et @dest = 255.255.255.255 : la machine pourra utiliser l'adresse proposée dès réception de ce message. Sinon le serveur envoie un message DHCP NAK avec une nouvelle proposition de configuration (et on recommence à partir de l'étape 3).

4. Quel est le protocole de transport utilisé pour transporter les paquets DHCP? Justifier.

UDP qui opère en mode déconnecté qui est plus adapté que TCP pour traiter des messages en mode diffusion.

En plus un serveur DHCP se trouve souvent sur le même réseau local ou un réseau voisin avec des taux d'erreurs de transmission qui sont très faibles.

2 Traduction d'adresses

On considère le cas d'un particulier qui possède trois machines et un abonnement d'accès à Internet auprès d'un fournisseur d'accès (FAI). L'accès se fait pas une ligne téléphonique. Le FAI attribue au particulier l'adresse IP fixe suivante : 138.76.29.7/24. Les trois machines sont reliées entre-elles par un réseau local de type 10baseT. Une des machines sert comme une passerelle pour permettre le partage de l'accès à l'Internet entre les trois machines.

1. Combien d'interfaces réseaux doit posséder la passerelle? Quelles sont les types des ces interfaces?

2 interfaces : 1) modem pour connexion avec FAI et 2) ethernet pour communication avec les machines sur le réseau local.

2. Afin de partager l'accès à l'Internet, le particulier attribue à ces machines les adresses suivantes : 138.76.29.7, 138.76.29.8 et 138.76.29.9 . Qu'en pensez-vous de cette solution?

LA FAI a attribué une adresse d'une seule machine. Ces autres adresses sont vraisemblablement des adresses allouées à d'autres abonnés. Donc la solution n'est pas correcte.

3. Proposer un plan d'adressage pour le réseau du particulier.

La seule approche possible est d'utiliser des adresses privées.

4. Proposer deux méthodes différentes pour partager l'accès au WEB entre les trois machines.

Le web est une application sur le réseau Internet : on peut envisager de partager l'accès exclusivement au Web (sans les autres services) en utilisant un proxy web. L'autre approche est de partager l'accès à l'internet en utilisant un service de traduction d'adresses. (NAT)

5. A quel niveau opère le service NAT? Que peut-on conclure?

NAT opère au niveau 3 (IP). Le principe est de déguiser des paquets ayant comme adresse source une adresse privée en paquet ayant une adresse publique (la seule disponible dans notre cas)

Pour pouvoir renvoyer la réponse à la machine source le serveur nat maintient une table de correspondance:

<adresse privée, port> --> <adresse publique, nouveau numéro de port>

Puisque NAT opère au niveau 3, le service ne peut pas intervenir pour modifier des informations envoyées dans des couches plus hautes

Par exemple, le protocole FTP, envoie au niveau 7, le numéro de port de connexion. Ce numéro reste inchangé par NAT !! (depuis on pris en compte des cas aussi fréquents que FTP dans le service NAT, pour garantir la cohérence du message : avoir les mêmes numéros de port au niveau 4 et 7)

3 Couche Transport

1. Que représente un numéro de port dans une connexion TCP/IP?

Le numéro SAP de la couche application (adresse de l'application)

2. Donner les informations qui caractérisent une connexion TCP/IP reliant deux applications.

Cinq informations sont requises: @source et destination numéros de ports source et destination, et le protocole de transport employé: UDP ou TCP.

3. Quelle est la taille d'une trame Ethernet qui encapsule un paquet UDP dont le champ de données contient la chaîne « Hello »

On suppose qu'un caractère est codé sur 1 octet.

Paquet UDP: 8 (entête UDP) + 5 (message) + 20 (entête IP)

+ 18 (entête Ethernet) = 51

donc 64 (après ajout de bourrage) + 8 préambule

= 72 octets.

4. Que représente le champ numéro de séquence dans l'en-tête TCP? Quelle est la valeur initiale de ce champ?

C'est le numéro (position) du 1er octet dans le message dans la séquence des octets envoyés par la machine sur la connexion TCP actuelle. On commence par une valeur aléatoire ISN (Initial sequence Number) pour éviter la confusion entre des messages qui arrivent tardivement et qui sont émis lors d'une précédente connexion TCP entre les mêmes deux machines

5. Rappeler les drapeaux de l'en-tête TCP et préciser la signification de chacun.

6 drapeaux qui sont dans l'ordre:

URG: indique, si positionné, que le champ pointeur données urgentes est à prendre en compte.

ACK: indique, si positionné, que le numéro d'acquittement est à prendre en compte

PSH: indique, si positionné, que les données sont à transmettre immédiatement à la couche application (sans attendre le remplissage du buffer)

RST: à positionner en cas de demande de fermeture de la connexion TCP suite à une erreur.

SYN: à positionner lors de la demande d'ouverture de connexion

FIN: à positionner lors de la demande de fermeture de la connexion.

6. Quelle est la taille maximale des données de bourrage qu'on peut avoir dans une trame Ethernet encapsulant un paquet TCP ?

64 - [18 (entête Ethernet) + 20 (Entête IP) + 20 entête (TCP)] = 6 octets

7. On considère une connexion TCP reliant deux applications A et B. Comment A peut-elle demander à B de suspendre l'envoi des données suite à la saturation de sa mémoire ?

Envoyer un message TCP avec le champs fenêtre à 0.
pour reprendre la communication on envoie un autre message TCP avec un champs fenêtre à une valeur > 0

8. Le protocole TCP et le protocole de liaison de données LAPB opèrent tous les deux en mode connecté. Comparer les approches TCP et LAPB en terme de détection de perte de données et en terme de technique de régulation de flux de données.

	TCP	LAPB
Unité d'acquittement	octet	Trame
Durée de temporisateur de garde	Dynamique	Statique
Anticipation	Dynamique (fenêtre)	Statique
Numéro initial	Valeur aléatoire	0

Noter que le protocole LAPB est conçu pour l'échange sur une liaison de données bi-points où le temps de propagations des messages est maîtrisé (et le même pour un débit donné). Ce n'est pas le cas pour TCP où les messages peuvent avoir de délai variable de réception en fonction de l'état du réseau et des chemins empruntés.

9. L'envoi de chaque paquet TCP est gardé par un temporisateur T. Si le temporisateur expire avant la réception d'un acquittement, l'émetteur considère que les données envoyées sont perdues. Il renvoie de nouveau ces données. Que doit être la valeur de T ?

$T >$ temps aller retour : un temps variable à estimer en fonction des temps de réception d'acquittement pour les données déjà envoyées. Soit DAR le délai aller retour actuel. A chaque réception d'un acquittement on calcule RTT, le temps aller retour pour le segment acquitté.
on a :

$$DAR = \alpha DAR + (1 - \alpha)RTT$$

$$\alpha \in [0, 1]$$

T est pris normalement pour être égale à 2 DAR.

10. On considère une connexion TCP reliant deux applications. A envoie à B trois paquets de 30 octets chacun. Donner le chronogramme des paquets échangés entre A et B depuis la demande d'ouverture jusqu'au la fermeture de la connexion.

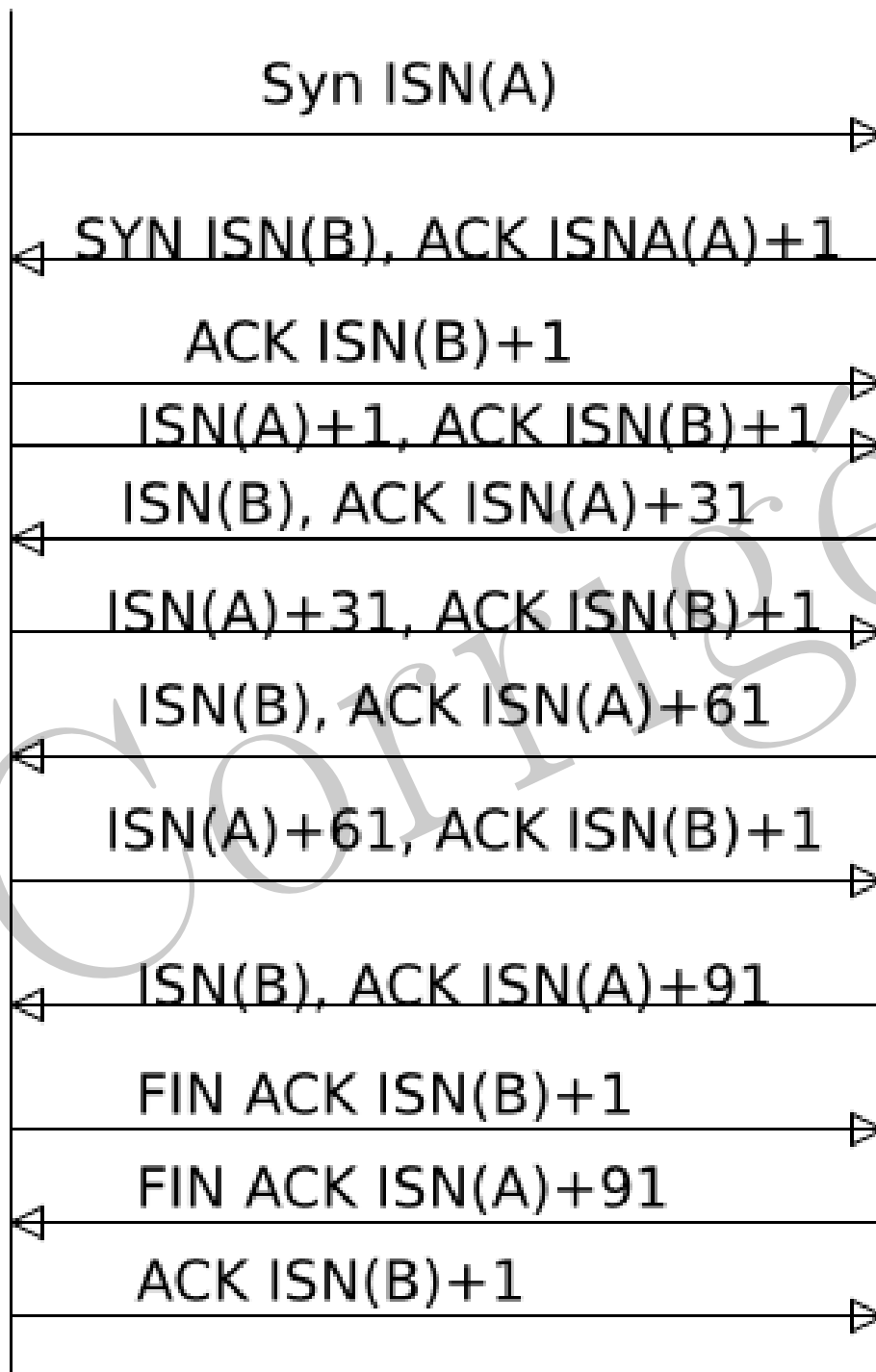


FIGURE 1 – réponse question 10

11. On considère une connexion TCP reliant deux applications A et B. La taille maximale des segments TCP qu'on peut envoyer sur la connexion est de 800 octets. A envoie à B trois segments dont les tailles sont respectivement 750, 350 et 10 octets. Le premier segment se perd dans le réseau. Donner le chronogramme d'échange des paquets TCP sur cette connexion.
12. On considère deux stations A et B connectées sur un réseau local 10baseT. On exécute sur les deux machines une application d'échange de messages textes utilisant le protocole TCP. La taille maximale d'un message texte est fixée à 33 caractères. Un caractère est codé sur 1 octet. La taille de la fenêtre TCP est fixée à 33 octets.
- Quel est le taux de l'utilisation du réseau si on considère une session d'échange de x messages de taille maximale.
- La fenêtre est égale à la taille max du message alors la machine source ne peut envoyer un message avant de recevoir l'acquittement du précédent.

pour envoyer x messages il faut échanger :

- 3 segments TCP pour demande de connexion
- X segments pour l'envoi de messages
- X segments pour les acquittements
- 3 segments pour pour déconnexion.

Tous les segments (sauf ceux transportant les messages) ont la taille minimale : 20 (entête TCP) + 20 (entête IP) donc les trames qui les encapsulent ont la taille 72 octets.

Les trames encapsulant les segments de messages ont la taille suivant:
 $33+20+20+18+8 = 99$ octets.

$$\text{Taux} = \frac{33 \times X}{6 \times 72 + X \times (72 + 99)}$$

- Recalculer la taux de l'utilisation dans le cas de l'utilisation d'UDP à la place de TCP.

En cas d'utilisation de UDP pas de connexion et de déconnexion.

On a X messages :

Les trames ont comme taille : $33+8+20+18+8 = 87$ octets (la trame)

$$\text{taux} = \frac{33}{87}$$

- Calculer le temps d'exécution d'une session d'échange de 10 messages textes de taille maximale chacun (cas TCP) $\text{temps} = \frac{((6+X) \times 72) + X \times 99}{10^7} \times 8$

