Prénom :
Nom :
Groupe TD :
Date :

Programmation répartie

M4102

François Merciol, Didier Lesage

DUT Informatique – 2nd année

Vannes – 2020/2021

Support de cours **étudiant**

http://m4102.merciol.fr/

(page gauche vide)

Table des matières

Table des figures

Liste des tableaux

Listings

1 TD-TP 6 & 7 : Gestion de DNS dynamique

Nous entamons la dernière série. Oui les meilleures choses ont une fin. Voici les 2 derniers TP qui vont de pair. Il s'agit d'assurer la mise à jour d'une entrée dynamique de DNS. Nous procéderons en 2 étapes :

- La récupération de notre adresse IP
- La déclaration de notre adresse provisoire auprès d'un servuer DNS dynamic.

Rappels :

- n'oubliez pas qu'il y a un contrôle de présence. Les absences sont remontées et gérés par le secrétariat. Les retards seront comptabilisés pour être intégrés dans la note de contrôle continue.
- Vous rendrez votre résultat vendredi de la dernière semaine. Il comptera pour votre note de contrôle terminal. Veillez à le soigner particulièrement.

1.1 DNS dynamique ?

Un DNS dynamique est une méthode pour mettre à jour les enregistrements gérés par un système de noms de domaine.

Ces enregistrements permettent principalement d'attribuer un nom de domaine à une adresse IP. Dans un DNS, un *fully qualified domain name* (FQDN, ou nom de domaine pleinement qualifié) est un nom qui révèle la position d'un nœud dans une arborescence DNS en précisant tous les domaines de niveau supérieur jusqu'à la racine.

Aussi, un nom de type *FQDN* caractérise généralement un équipement sur un réseau.

```
1 | www.devoirs.univ-ubs.fr
```

Les serveurs DNS assurent donc la gestion de tables de correspondance entre noms et adresses IP. Celles-ci sont élaborées sous la forme de fichiers texte présentant généralement une *zone* et son contenu.

server1	IN	A	10.0.0.1
www	IN	CNAME	server1

Si les enregistrements ci-dessus sont associés à l'espace de nommage **domaine.fr**, ils décrivent...

- **server1.domaine.fr**, associé à l'adresse IP **10.0.0.1**
- **www.domaine.fr**, alias de *server1.domaine.fr*, associé à l'adresse **10.0.0.1**

1.2 Revenons à la notion de « dynamique »

Lorsque votre *smartphone* ou votre box internet se connecte sur le réseau, une adresse IP lui est attribuée. Cette adresse, « piochée » dans un « pool » spécifique, reste généralement invariable le temps de l'établissement de la liaison. Souvent, des connexions consécutives permettent d'obtenir une même adresse IP pour un même périphérique. Généralement, une adresse est attribuée pour une durée maximale de 12 ou 24 heures.

On parle alors d'attribution d'adresse *IP dynamique*.

Un serveur auquel une adresse IP dynamique est attribuée est difficilement adressable, et les services qu'il pourrait publier (HTTP, FTP...) sont alors difficilement accessibles depuis n'importe quel point d'accès à Internet. L'attribution d'un nom d'hôte à ce serveur et la gestion dynamique d'une correspondance avec une adresse IP, gérée par un serveur DNS, permettent alors une meilleure accessibilité.

Imaginons un serveur HTTP, équipé d'un modem ADSL, permettant une connexion sur le réseau Internet à l'aide des services d'un fournisseur d'accès (Orange, Free, SFR...). A chaque connexion au réseau, le modem se voit attribué une adresse IP qui peut être différente de la précédente. Cette adresse IP attribuée est une adresse IP publique, adressable depuis tout le réseau Internet.

L'installation, sur ce serveur, d'un logiciel surveillant les changements d'adresse IP publique permettrait, lorsque cela est nécessaire, de transmettre l'information à un serveur DNS gérant l'espace d'adressage de notre serveur, et ainsi de mettre à jour l'adresse IP associée au nom d'hôte choisi pour adresser le serveur.

1.3 Mais comment obtenir notre adresse publique ?

Nous avons vu que le protocole TCP permettait d'identifier les deux points d'une communication, généralement un client et un serveur.

Ainsi, pour connaître son adresse IP publique (adresse IP sur le réseau Internet), il suffit de contacter un serveur et de lui demander de nous retourner l'adresse IP associée à la partie distante du *socket* caractérisant la connexion établie.

Il existe, sur Internet, des services permettant d'obtenir, sous la forme d'une réponse à une requête HTTP, un message fournissant l'adresse IP à l'origine de la requête...

```
https://api.ipify.org
http://checkip.amazonaws.com
http://icanhazip.com
http://checkip.dyndns.org
```

1.4 Il faut donc un client pour notre serveur...

Pour que notre serveur soit accessible au travers de son nom d'hôte, il faut donc développer un client dont les fonctionnalités principales sont :

- La détection de l'adresse IP publique courante
- En cas de besoin, la mise à jour du serveur DNS de gestion de notre nom d'hôte

Nous allons assurer la conception de ce client. Les contraintes de fonctionnement du réseau de l'IUT nous obligerons à dialoguer avec des serveurs un peu *particuliers* (accessibles sur le réseau local de l'établissement), tout en respectant parfaitement la logique du réseau public Internet.

1.5 Obtention de l'adresse IP publique

Au cours de ce TP, vous allez développer la première partie du logiciel client de gestion de DNS dynamique : l'obtention de l'adresse IP attribuée à votre passerelle publique.

Pour réaliser cette fonctionnalité, vous développerez un client HTTP qui aura simplement à demander la fourniture d'une page d'un site dont l'adresse vous sera communiquée au début du TP.

La page, au format HTML, qui sera retournée par le serveur, contiendra un message intégrant la présentation de l'adresse IP de l'émetteur de la requête d'origine. Celle-ci sera peut-être *décorée* à l'aide de textes de présentation et de balises HTML de mise en forme. Dans tous les cas, la page ne contiendra qu'une seule chaîne de caractères de la forme **W.X.Y.Z** caractérisant l'adresse IP retournée.

L'application devra contacter le serveur très régulièrement (toutes les 30 secondes) afin de constater un éventuel changement d'adresse IP publique.

Après chaque requête, l'application devra éventuellement signaler (message sur la sortie standard) le changement d'adresse IP.

```
Requête HTTP à émettre : GET /tp6/ HTTP/1.1
```

Pour qu'une requête respecte le format HTTP/1.1, elle doit fournir un header indiquant le nom du serveur sollicité. Ainsi, l'utilisation de l'URL **http ://checkip.dyndns.org** génère la requête HTTP suivante :

```
GET / HTTP/1.1
Host: checkip.dyndns.org
```

Par défaut, la plupart des serveurs maintiennent les connexions établies par les clients après émission d'une réponse à la requête initiale. Pour faciliter la lecture de données dans le flux d'entrée du socket client en évitant une lecture bloquée après réception de la réponse, il est possible de demander au serveur de ne pas maintenir la connexion après traitement de la requête. Pour cela, ajouter le header suivant dans la requête émise au serveur :

```
Connection: close
```

1.6 Travail à réaliser cette semaine

Dans un premier temps, il faut récupéere notre adresse IP. Pour cela vous vous connecterez sur l'adresse suivante : http://www.zandolite.com/TP6/.

Ce serveur vous donnera une adresse fictive. C'est logique, puisque nous devons simuler le fait qu'elle évolue avec le temps. Or il est peu probable que cela soit le cas durant un TP. Il faut donc tricher un peu.

Au cas où vous pourriez utiliser les machine de l'IUT (le pire n'est jamais sûr), nous devons envisager que plusieurs PC est en réalité à même adresse (celle du mandataire de l'IUT) face au serveur de simulation.

Dans ce cas, tout est prévu. Il suffit d'ajouter un argument à votre demande en choisisant un identifiant qui vous est propre (votre nom, vos initiles ou celles de votre grand-mère). Nous vous donnons l'exemple en choisisant "MonId" (ce qui est un très mauvais choix, évidemment). Cela nous donnerait : http://www.zandolite.com/TP6/?id=MonId.

Petite coqueterie, le serveur est d'humeur espiègle. Il ne vous donnera pas toujours la réponse sont le même format. Vous pourez avoir des réponses du genre :

- Une bonne adresse IP v4 est de la forme W.X.Y.Z. La vôtre est... 124.137.195.139... voilà qui devrait vous convenir...
- Nous avons détecté que l'adresse 111.183.115.181 est à l'origine de votre requête...
- Current IP Address : 161.103.119.107

Vous allez devoir reconnaître les 4 chiffres dans le flot de caractère qui vous revient.

C'est à vous de jouer : ✍

C'est la semaine de tout les dangers. C'est cette semaine que vous rendez votre ultime travail !

Rappels :

- n'oubliez pas qu'il y a un contrôle de présence. Les absences sont remontées et gérés par le secrétariat. Les retards seront comptabilisés pour être intégrés dans la note de contrôle continue.
- Vérifiez que votre PC est à l'heure (le serveur lance un défi à 3 minutes près).
- Pour le rendu pensez
  - à fournir tous les éléments qui vous identifi.
  - à donner une archine qui contient votre nom et votre groupe.
  - à donner une archive avec un sous-répertoire qui ne se mélange pas aux autres (avec votre nom).
  - à donner tous les fichiers sources nécessaires.
  - à donner des exemples de vos tests motrant que cela fonctionne pour vous.

1.7 Mise à jour du DNS dynamique

La mise à jour du serveur DNS est réalisée à l'aide d'une requête HTTP respectant le protocole **DynDNS2**. Il s'agit d'un format de requête/réponse exploité par la plupart des fournisseurs de services de DNS dynamiques.

Type de requête
: GET

URI
: /dynDNS

Paramètres

hostname	Nom de l'hôte à mettre à jour sur le serveur DNS
myip	Adresse IP à associer à l'hôte précisé

Une authentification http simple sera à assurer (*Basic authentication*). Celle-ci consiste à transmettre, dans l'entête de la requête HTTP, un champ **Authorization**. Celui-ci doit contenir la méthode utilisée (**Basic**) suivie de la représentation en Base 64 du nom de l'utilisateur et du mot de passe séparés par le caractère « : ». Exemple :

```
1 | Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

Pour que votre client s'authentifie, vous utilisez un nom d'utilisateur quelconque (votre première connexion au service vous enregistrera sur le service), et, comme mot de passe, l'heure courante exprimée sous la forme du nombre de millisecondes écoulées depuis le 1er janvier 1970 minuit.

Le serveur transmettra une réponse « texte » à toute requête émise...

good
: Indique que la mise à jour a été correctement réalisée

nochg
: Précise que la requête a été acceptée mais qu'aucune mise à jour de DNS n'était nécessaire

badauth
: Indique une erreur dans la requête. L'authentification a échoué.

nohost
: Indique une erreur dans la requête. Le nom de l'hôte est incorrect ou non précisé.

noip
: Indique une erreur dans la requête. L'adresse IP fournie est incorrecte ou non précisée.

abuse
: Trop de requêtes infondées de demande de mise à jour ont été émises. Le compte est suspendu temporairement.

Il est nécessaire de contacter le serveur **au moins toutes les 3 minutes** pour qu'une entrée soit maintenue sur le serveur DNS.

Les requêtes de mise à jour ne fournissant pas une nouvelle adresse IP doivent être émises avec plus de 60 secondes d'intervalle, sous peine d'être comptabilisé comme des « requêtes infondées ».

Requête HTTP à émettre :

```
GET /tp6/dynDNS?xxxxxxx HTTP/1.1
```

Vous pouvez vérifier votre succès en consultant la page `http://www.zandolite.com/TP6/index.html`. La fimousse qui va du vert au rouge est également un bon indicateur de votre travail.

Appliquez-vous pour ce dernier rendu : ✍