Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Hes·so FRIBOURG FREIBURG
Haute Ecole Spécialisée de Suisse occidentale
Fachhochschule Westschweiz

Bachelor of Science HES-SO in Telecommunications
Technologies de l'information et de la communication

Réseaux IP

- Travail pratique -

Introduction aux services TCP/IP : DNS

François Buntschu
francois.buntschu@hefr.ch

Haute école d'ingénierie et d'architecture de Fribourg (HEIA-FR)

HES-SO//Fribourg, 22 novembre 2017, v1.5

Table des matières

1. OBJECTIFS

La suite de protocole Internet, aussi appelée TCP/IP du nom des deux protocoles les plus importants, est actuellement la plus répandue dans les réseaux *informatiques*.

Une gamme de services fait partie de cette suite de protocoles. Parmi eux, les services DHCP [1] (*Dynamic Host Configuration Protocol*) et DNS [2] (*Domain Name Service*) sont particulièrement importants. DNS est le « *bottin téléphonique Internet distribué* » qui permet d'associer une adresse IP à un nom de station.

Les buts principaux de ce travail pratique sont les suivants :

- Installer et configurer un serveur DNS sous linux
- Configurer un domaine « local » : **lte*xx*.ch**
  (avec xx étant votre place de travail, par ex. lte01.ch ou lte06.ch)
- Configurer la résolution inverse pour la/les machine(s) de votre domaine
- Mesurer les messages échangés entre une station client et votre serveur DNS
- Mesurer les messages échangés entre votre serveur DNS et Internet

2. CONFIGURATION D'EXPÉRIENCE

2.1. Schéma du réseau

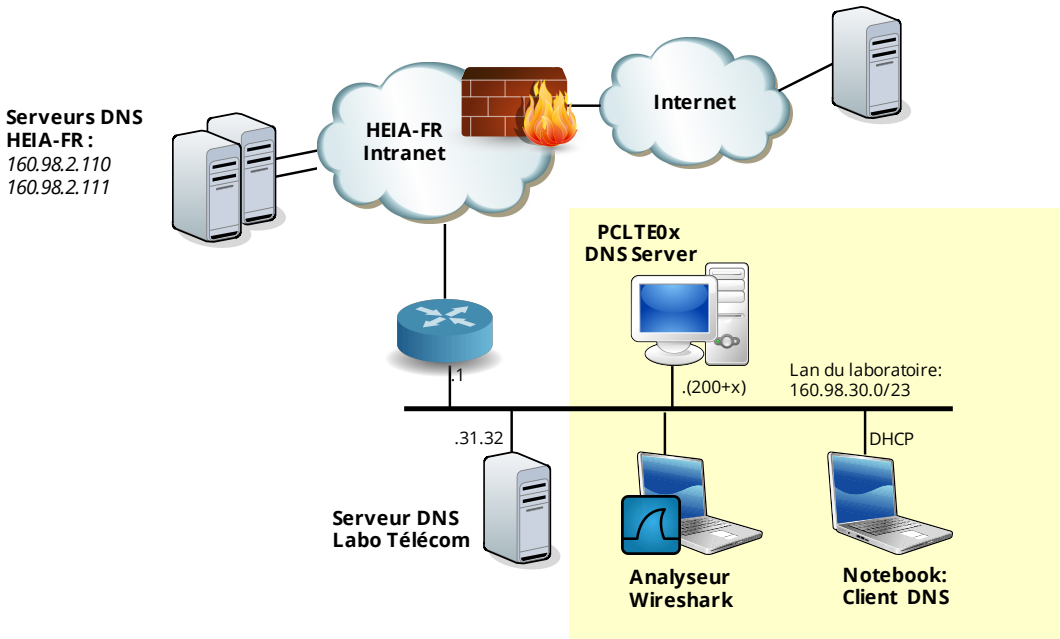

Figure 1 : *Infrastructure du réseau*

2.2. Configuration du PC et de l'analyseur

Le PC de votre place de travail est à connecter à votre notebook et à l'analyseur de protocole au travers d'un HUB ou du Switch avec le port « *mirroir* ».

Le HUB/Switch sera connecté au LAN du laboratoire (Attention au type de câble utilisé pour cette connexion !)

***Remarque** : Si vous le désirez, vous pouvez utiliser Wireshark sur la machine Linux ou sur votre notebook pour vos mesures.*

Le serveur DNS utilisé dans le cadre de ce laboratoire fonctionnera sous Linux Ubuntu (BIND 9.x).

- Démarrer le PC (ou la machine virtuelle[1]) avec Linux et connectez-vous avec l'utilisateur **lte** et le mot de passe **telecom**.
- Préparer et enclencher votre analyseur.
- Configurer l'adresse IP de l'interface Ethernet de la machine Linux (au travers des menus) ou en lançant l'application suivante depuis un shell :

```
[lte@pcltexx ~]$ sudo nm-connection-editor
```

Assurer que la configuration de la carte réseau est active avec une adresse IP statique : 160.98.30.(200+x)

Après avoir modifié la configuration de la carte réseau, n'oubliez pas de relancer ce service en cliquant sur l'icône 'réseau' de la barre d'outils.

2.3. Configuration du serveur DNS

En principe, le service DNS est installé sur la machine Linux. Afin de le contrôler, effectuer la commande suivante :

```
[lte@pcltexx ~]$ ls /etc/init.d/bind9
```

Si vous obtenez le fichier suivant :

```
/etc/init.d/bind9
```

Cela signifie que le service (serveur) DNS est installé. Si ce n'est pas le cas, appeler le professeur/assistant.

***Remarque** : pour effecturer l'installation du serveur Bind vous-même, avec le PC Linux connecté au réseau du laboratoire (LAN1 ou LAN2), l'installation du package DNS se fait au travers de la commande suivante:*

```
[lte@pcltexx ~]$sudo apt-get install bind9
```

La configuration du serveur DNS se fait au travers des fichiers de configuration suivants :

1) Configuration du serveur : `/etc/bind/named.conf.local`
2) Configuration de votre domaine : `/etc/bind/db.lte`**`xx`**`.ch.zone`
   (avec xx correspondant à votre place de travail, par ex : `db.lte01.ch.zone`)
3) Configuration de la résolution inverse :
   `/etc/bind/db.30.98.160.in-addr.zone`
   - Ces fichiers se trouvent en annexe à la donnée.
   - Copier ces fichiers dans les répertoires ci-dessus et éditer la configuration au moyen d'un éditeur de texte (par exemple gedit) et configurer/modifier les différents paramètres (en gras dans les fichiers en annexe) pour refléter la configuration de la Figure 1 : *Infrastructure du réseau*.

[1] La carte réseau de la machine virtuelle doit être en mode « *bridged* » vers la carte LAN du PC.

- Démarrer (redémarrer) le service DNS au moyen de la commande suivante[1] :

```
[lte@pcltexx ~]$ sudo /etc/init.d/bind9 restart
Stopping named:                                            [  OK  ]
Starting named:                                            [  OK  ]
```

- Le serveur DNS n'est pas (par défaut) autoriser d'effectuer des requêtes récursives pour des clients « inconnus ». Afin de permettre cela, modifiez le fichier `/etc/bind9/named.conf.options` en ajoutant l'entrée suivante :

```
allow-recursion { any; };
```

- Pour permettre la résolution de domaines appartenant à la HEIA-FR (comme par ex. heia-fr.ch, hefr.ch, etc) qui sont sécurisés avec DNSSec, nous devons désactiver cette validation en modifiant le fichier `/etc/bind9/named.conf.options` en modifiant l'entrée suivante :

```
dnssec-validation no
```

2.4. Configuration du notebook

Votre notebook va servir de client DNS et éventuellement d'analyseur.

- Configurer la carte réseau du notebook en DHCP

> Laisser la configuration IP de votre machine **Linux** par défaut, soit en statique avec l'adresse mentionnée précédemment, avec les DNS par défaut, soit 160.98.2.110 et 160.98.2.111

- Modifier la configuration DNS de votre notebook avec uniquement le DNS suivant :
  - 160.98.30.(200+x) → **Votre** serveur DNS

    (x= votre place de travail)

Questions :

P1: Documenter et valider le bon fonctionnement de votre maquette. Pour cela, utiliser les commandes 'nslookup'[2] et 'ping' sur votre notebook.

P2: Décrivez les différents paramètres de configurations utilisés dans *db.pcltexx.ch.zone* et dans *db.30.98.160.in-addr.zone*

P3: Quels sont les paramètres qu'il faut configurer ***au minimun*** lorsque vous voulez gérer et configurer un domaine.

P4: Quels est l'organisme qui gère les domaines .ch ? Comment obtenez-vous cette information ?

P5: A quoi sert le fichier /etc/bind/db.root ?

[1] En cas de problème, vous pouvez visualiser les erreurs en affichant le fichier `/var/log/syslog` au moyen de la commande `tail -25 /var/log/syslog`

[2] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/nslookup.mspx?mfr=true

3. PROTOCOLE DNS

Commentaire

Le protocole DNS est du type client-serveur. Il permet à une station, à partir d'un nom Internet (par exemple www.admin.ch) d'obtenir l'adresse IP correspondante. L'adresse du serveur DNS est un paramètre de configuration du PC. Plusieurs adresses peuvent être configurées. Le protocole DNS peut fonctionner de manière directe ou récursive (le serveur DNS demande de lui-même à un autre serveur DNS si il ne connaît pas la réponse). Le serveur DNS peut aussi fournir un nom IP correspondant à une adresse IP s'il est configuré pour le faire.

Tâches générales (pour toutes les expériences/mesures de ce TP):

- Décrire vos conditions de mesures.
- Décrire vos observations, en particulier donner les adresses IP et les numéros de port (TCP ou UDP) utilisés (source et destination).
- Identifier et essayer d'expliquer les messages échangés les plus importants d'après vous.
- Donner une synthèse des résultats des mesures.

- Sur votre analyseur, configurer un filtre de protocole IP de type DNS pour ne retenir que les échanges DNS.
- Effacer la cache DNS de votre notebook
  - Sous Windows : en utilisant la commande « **`ipconfig /flushdns`** » dans un invité de commande.
  - Sous OSX : en utilisant la commande « **`sudo killall -HUP mDNSResponder`** » dans une fenêtre terminale
- Démarrez la mesure avec la fenêtre de décodage complet. Faites ensuite une requête www.admin.ch au moyen d'un browser. Arrêtez la mesure.

Windows est très loquace, il risque d'y avoir d'autres messages DNS provenant de votre notebook qui n'ont rien à voir avec la requête ci-dessus. A vous de trier !

3.1. Analyse des protocoles observés

Questions :

P6: Quels sont les protocoles de couche 2, 3 et 4 utilisés pour l'échange DNS ? Indiquez le champ dans chacune des couches qui vous permet de définir le protocole qui est transporté.

P7: Quels sont les interlocuteurs de votre notebook et de la machine Linux pour les dialogues DNS ? Quelles sont leurs adresses IP ? Combien de trames provenant et à destination de votre notebook avez-vous enregistrées ? Commentez !

3.2. Analyse des échanges DNS

Questions :

P8: Quels sont les types de message DNS observés ?

P9: Dessinez les échanges observés entre le client (votre notebook), le serveur DNS et Internet en fonction du temps (diagramme en flèche), commentez !

P10: Où se trouve l'information demandée ? Quelles sont les réponses du serveur DNS ?

3.3. Requêtes inverses

- Démarrer la mesure avec la fenêtre de décodage complet. Envoyez ensuite la commande « **`nslookup 160.98.30.(200+x)`** » (sans les parenthèses et avec x étant le n° de votre place de travail) à partir d'un invité de commande de votre notebook.

Questions :

P11: Quels sont les types de message DNS observés ?
P12: Où se trouve l'information demandée ? Quelles sont les réponses du serveur DNS ?

3.4. Requêtes itératives

- Démarrer la mesure avec la fenêtre de décodage complet. Envoyez ensuite la commande « **`nslookup www.tic.ac.uk`** » à partir du DOS shell de votre notebook.
- Mesurer les échanges DNS de votre notebook vers votre serveur DNS, et depuis votre serveur DNS vers Internet

Questions :

P13: Dessiner le diagramme en flèches des échanges observés.
P14: Combien de requêtes effectue votre serveur DNS pour résoudre la requête ci-dessus ?

4. RÉFÉRENCES / DOCUMENTATIONS

[1] RFC 1541 (DHCP), 2132 (DHCP options)
[2] RFC 1035 (DNS)
[3] D. Comer, TCP/IP vol. 1. Prentice-Hall.
[4] F. Buntschu/T. Martinson, Notes de cours Réseaux IP

5. TEMPS À DISPOSITION ET RAPPORT

La séance dure 4 périodes. Un rapport contenant mesures et explications doit être rendu au plus tard 7 jours après la réalisation du TP. Le rapport insistera plus sur ce qui a été observé que sur l'exactitude absolue des réponses.

6. ANNEXE A : FICHIERS DE CONFIGURATION DU SERVEUR DNS

6.1. named.conf.local (bind9 sur Ubuntu)

```
// Haute ecole d'ingenierie et d'architecture de Fribourg
// Reseaux IP
// ------------------------------------------------------------------------------
// TP DNS - Filename= /etc/bind/named.conf.local
// ------------------------------------------------------------------------------
// (c) F.Buntschu
// Version 1.4
// ------------------------------------------------------------------------------

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your organization
// include "/etc/bind/zones.rfc1918";


// A ajouter / completer pour le TP
// *********************************
zone "ltexx.ch." IN {
        type master;
        file "/etc/bind/db.ltexx.ch.zone";
        allow-update {
                none;
                };
        notify yes;
};

zone "30.98.160.in-addr.arpa." IN {
        type master;
        file "/etc/bind/db.30.98.160.in-addr.zone";
        allow-update { none; };
};
```

6.2. db.ltexx.ch.zone

```
// Haute ecole d'ingenierie et d'architecture de Fribourg
// Reseaux IP
// ------------------------------------------------------------------------------
// TP DNS - Filename= ltexx.ch.zone
// ------------------------------------------------------------------------------
// (c) F. Buntschu
//
// Version 1.4
//  ------------------------------------------------------------------------------

$ORIGIN ltexx.ch.
$TTL 86400
@       IN      SOA     ltexx.ch. root.ltexx.ch. (
                        2015111601
                        3600
                        900
                        604800
                        86400 )

// Descriptions of names servers for this domain (primary and secondary)
                        IN      NS      ourpc.ltexx.ch.
                        IN      NS      tlabs.tic.eia-fr.ch.

// List of known hosts in this domain
ourpc                   IN      A       160.98.30.<b>[1]

www                     IN      CNAME   ourpc

smtp                    IN      CNAME   ourpc
pop                     IN      CNAME   ourpc
ltexx.ch.               IN      MX      10 pop.ltexx.ch.
```

6.3. db.30.98.160.in-addr.zone

```
// Haute ecole d'ingenierie et d'architecture de Fribourg
// Reseaux IP
// ------------------------------------------------------------------------------
// TP DNS - Filename= 30.98.160.in-addr.zone
// ------------------------------------------------------------------------------
// (c) F. Buntschu
//
// Version 1.4
// ------------------------------------------------------------------------------


$TTL 86400
@       IN      SOA     ourpc.ltexx.ch. root.ltexx.ch. (
                        2015111701
                        3600
                        900
                        604800
                        86400 )

; Descriptions of names servers for this domain
                 IN      NS      ourpc.ltexx.ch.
                 IN      NS      tlabs.tic.eia-fr.ch.


; List of known hosts in this domain

<b>[2]            IN      PTR     ourpc.ltexx.ch.
```

[1] <b> représente l'adresse IP du PC de votre place de travail

[2] Pour ce fichier il faut uniquement mentionner le <b> et non pas 160.98.30.<b> !