heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Labo TIB

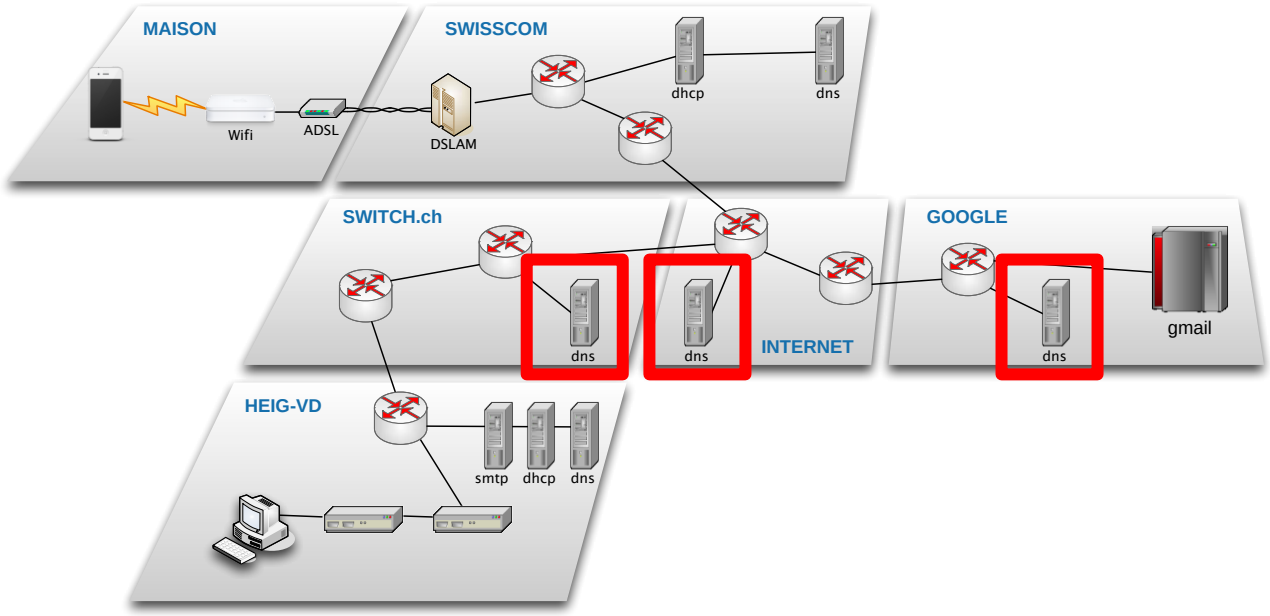
DNS

Objectifs d'apprentissage

1. Comprendre la traduction de noms de domaines en adresse IP.
2. Savoir expliquer le fonctionnement de DNS.
3. Savoir expliquer ce qui est nécessaire pour acheter et configurer un nom de domaine.

Contenu

Dans ce laboratoire, nous allons étudier la traduction de noms de domaines (comme www.heig-vd.ch) en adresses IP.



1. Observer la traduction de noms de domaines en adresses IP
2. Analyser le fonctionnement du système DNS.

Rapport à fournir

Un rapport de 2 pages au maximum avec les éléments suivants :

1. Nom du laboratoire, noms des étudiants, date du laboratoire
2. **Objectif 1 : traduction de noms de domaine en adresse IP**
    - Rappel de l'objectif d'apprentissage et du critère de succès
    - Explication courte du but du protocole DNS
    - Description courte du fonctionnement de DNS (avec diagramme en flèches). Indiquez notamment le serveur DNS qui donne la réponse.
    - Explication : pourquoi certains noms de domaines ont plusieurs adresses IP associées ?
    - Réponse : si vous répétez la requête DNS plusieurs fois, est-ce que l'ordre des adresses IP reste le même ? Donnez une raison.
    - Explication de la signification d'une réponse qui ne fait pas autorité (*non-authoritative answer*) et qui mécanisme derrière.
3. **Objectif 2 : fonctionnement du système DNS**
    - Rappel de l'objectif d'apprentissage et du critère de succès
    - Dessinez un diagramme des serveurs DNS utilisés lors d'une requête DNS pour le nom « fr.wikipedia.org » et des messages échangés entre les serveurs.
    - Expliquez très succinctement le fonctionnement d'une résolution de nom DNS à l'aide de ce diagramme.
    - Que se passerait-il si tous les treize serveurs DNS racine tombent en panne, par exemple à cause d'une attaque ?
4. Auto-évaluation : est-ce que vous avez atteint les objectifs d'apprentissage de la page 1 ?

Délai

Le fichier PDF du rapport doit être envoyé à l'adresse labo.tib.heig@gmail.com **avant le début du prochain laboratoire**.

1 Introduction

Lors des laboratoires précédents nous avons étudié la communication à l'intérieur de notre réseau LAN. En particulier, nous avons observé

- le protocole DHCP qui permet à un PC d'acquérir une adresse IP,
- que la communication à l'intérieur de notre LAN utilise Ethernet et des adresses MAC,
- que le protocole ARP effectue la traduction d'une adresse IP locale en adresse MAC.

Nous avons aussi déjà étudié la structure d'Internet comme interconnexion de réseau. Internet est donc un réseau décentralisé, sans un organisme de contrôle central.

Mais pour envoyer un ping sur smtp.gmail.com, votre PC a besoin de l'adresse IP du destinataire. Comment peut-il apprendre l'adresse IP qui correspond à smtp.gmail.com ? C'est le système DNS qui permet ça. Nous allons étudier DNS dans ce laboratoire.

2 Matériel

Utilisez la VM Ubuntu TIB pour les manipulations.

Objectif 1 : traduction de noms de domaine en IP

Le premier objectif est de comprendre la traduction d'un nom de domaine en adresse IP.

L'objectif est atteint si vous savez expliquer

- le but du protocole DNS et
- le fonctionnement du protocole DNS.

Procédez par les étapes suivantes :

1. Lancez Wireshark sur le PC1, avec le filtre d'affichage « dns ».
2. Depuis le PC1, effectuez un ping sur smtp.gmail.com.
3. Analysez les paquets DNS capturés.
4. Dessinez un diagramme en flèches (avec adresses IP src et dst) pour illustrer les paquets échangés.

La commande nslookup

La commande nslookup permet de facilement effectuer des requêtes DNS.

1. Effectuez une requête DNS avec la commande *`nslookup smtp.gmail.com`*.
2. Effectuez des requêtes DNS pour www.24heures.ch, www.epfl.ch et www.heig-vd.ch.
    a. Pourquoi y a-t-il plusieurs adresses IP pour certains noms de domaine ?
    b. Si vous répétez la requête plusieurs fois (attendez 20-30 secondes entre les requêtes), est-ce que l'ordre des adresses IP reste le même ? Donnez une raison.
3. Effectuez plusieurs requêtes pour le nom de domaine « www.google.ch ». Nslookup affiche qu'il s'agit de d'une réponse « non-authoritative ». Expliquez ce que cela veut dire.

Objectifs 2 : fonctionnement du système DNS

Le deuxième objectif est de comprendre la collaboration entre les différents serveurs DNS pour trouver une adresse IP.

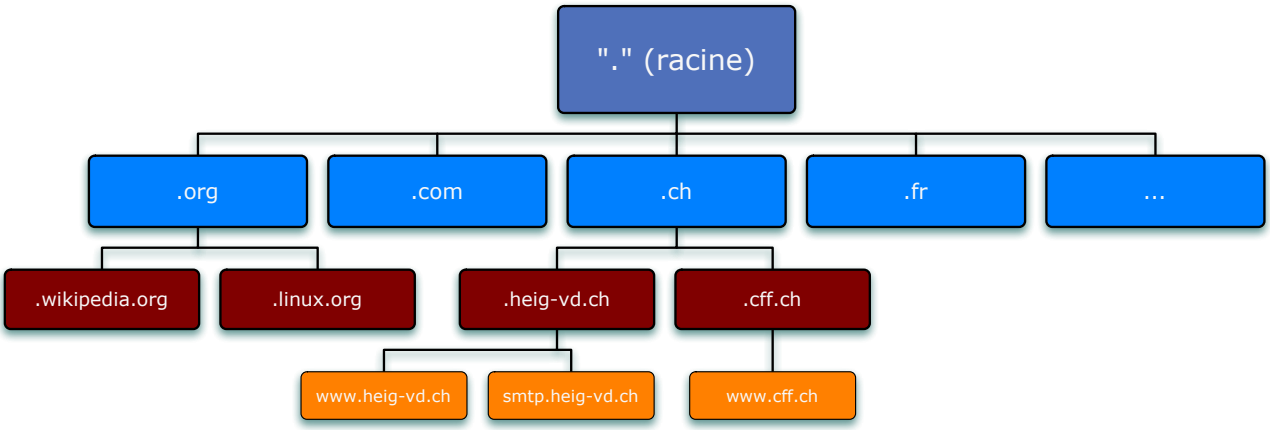
L'objectif est atteint si vous êtes capable de dessiner un diagramme qui montre les différents serveurs DNS et les communications entre eux lors d'une requête DNS.

La commande nslookup indique l'adresse IP du serveur qui a envoyé la réponse DNS. De quel serveur s'agit-il ? Est-ce que ce serveur connaît tous les noms de domaines de l'Internet entier ? Faites une requête par exemple pour le site Web de la capitale du Mail (www.bamako.ml).

Evidemment, ce serveur DNS ne peut pas connaître toutes les adresses IP du monde. Mais alors, qui les connaît ?

La réponse est : personne ! DNS est un système distribué hiérarchique, basé sur la hiérarchie des noms de domaines.

La structure des noms de domaines est montrée ci-dessous.



1. Un PC qui cherche l'adresse IP pour fr.wikipedia.org va envoyer une requête DNS à son serveur DNS local.
2. Celui-ci ne connaît pas la réponse et va contacter un des 13 serveurs DNS racine d'Internet.
3. Le serveur racine connaît tous les serveurs DNS responsable des domaines de premier niveau, comme « .org », « .ch », … Il peut donc demander à un des serveurs qui est responsable pour le domaine « .org ».
4. Ce serveur connaît les serveurs DNS qui sont responsables pour le domaine « wikipedia.org » et va le contacter.

5. Le serveur DNS responsable pour « wikipedia.org » enfin connaît l'adresse IP pour le nom de domaine pour « fr.wikipedia.org » et peut donc fournir la réponse en retour.
6. La réponse se propagent le long du chemin inverse et arrive ainsi au serveur DNS local qui la met dans son cache et qui la transmet au PC.

La commande « dig » permet d'analyser la hiérarchie des serveurs DNS.

Si la commande n'est pas encore disponible dans la VM Ubuntu, vous pouvez installer le paquetage *dnsutils*.

Procédez par les étapes suivantes :

1. Utilisez la commande[1] *dig @ns01.heig-vd.ch +trace fr.wikipedia.org*
2. Quels sont les noms
    a. des 13 serveurs DNS racine
    b. des serveurs DNS responsables pour le domaine « .org »
    c. des serveurs DNS responsables pour le domaine « wikipedia.org » et
    d. Quel est le vrai nom de la machine fr.wikipedia.org, ce dernier n'étant qu'un alias simplifié.
3. Utilisez de nouveau la commande dig pour identifier les serveurs DNS pour le domaine « .ch » ainsi que les serveurs DNS de la HEIG-VD.

Objectif 3 : Savoir utiliser la commande whois

Le dernier objectif de ce labo est de savoir utiliser la commande whois.

Lorsqu'on achète un nom de domaine, le nouveau propriétaire doit enregistrer son nom et son adresse. La commande *whois* permet consulte les serveurs Whois qui sont similaires aux serveurs DNS. Elle permet d'obtenir le nom du propriétaire d'un nom de domaine.

Procédez par les étapes suivantes :

1. Tapez la commande whois heig-vd.ch
    a. Qui est le propriétaire du nom de domaine heig-vd.ch ?
2. Qui est le propriétaire du site nom de domaine nimportequoi.ch ?

[1] Le "@ns01.heig-vd.ch" indique le serveur DNS à utiliser. Normalement ce paramètre n'est pas nécessaire. Mais beaucoup de distributions Linux utilisent le système *systemd* qui fait la résolution DNS en local. La commande dig n'affiche plus la trace complète dans ce cas. Il faut donc instruire dig à ne pas utiliser la résolution locale.

3 Exercices avancés

***Les exercices de cette section ne sont pas obligatoires**. Ils ne seront pas considérés pour la note.*

Mais si vous avez de l'intérêt et du temps, je vous encourage à les faire, afin d'approfondir vos connaissances et apprendre encore d'avantage sur les technologies des réseaux. Dans ce cas vous pouvez joindre vos réponses aux exercices avancés au rapport de laboratoire.

Achat d'un nom de domaine en Suisse

Supposons que vous voulez acheter le nom de domaine « monsiteweb.ch ».

- Où est-ce que vous pouvez l'acheter ?
- Il faudra ensuite avoir des serveurs DNS qui sont responsables pour ce domaine, donc qui connaissent l'adresse IP par exemple de « www.monsiteweb.ch ». Combien de serveurs faut-il ?
- A qui devez-vous communiquer les adresses IP de ces serveurs ?
- Quels serveurs DNS vont contacter vos serveurs DNS lors d'une requête DNS ?