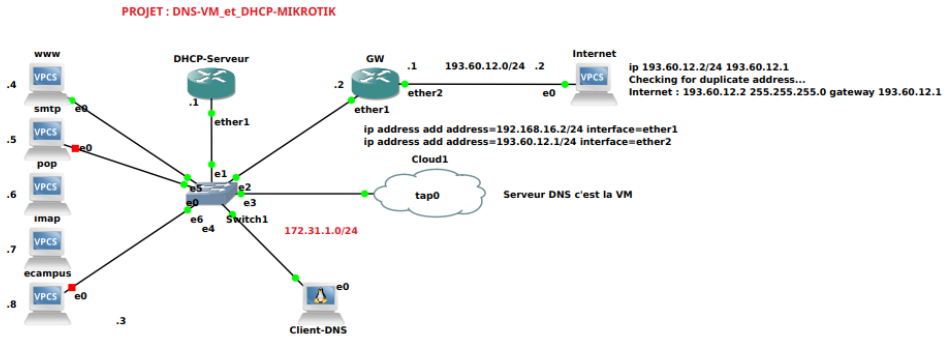
UNIVERSITÉ CAEN NORMANDIE

TP DNS

20.01.2023

Des URL deviennent IP... ☺

Auteur : Pascal Fougeray



Source : Moi ☺

1 Préambule

— Nous allons voir
  — Les adresses IP privées et publiques
  — Ce qu'est le protocole DNS avec Wireshark
  — Ce qu'est un client DNS
  — À quoi sert un serveur DNS
  — Nous allons utiliser les 2 connexions de la salle 406,
    1. l'interface **enp0s31f6** qui doit être sur le réseau de la FAC 10.38.16.0/22
    2. l'interface **BR0** qui doit être sur le second réseau **192.168.128.0/22**
  — Ce TP à 2 parties
    1. **Client** (Nous allons l'être plusieurs fois) pour l'étude du protocole, des principes et des commandes vues au CM.
    2. **Serveur** en installant un : **dnsmasq**
— **Câblez** le câble rouge entre l'interface **BR0** du HOST et la table et **vérifiez** que vous avez une IP ! ! !
— **Prenez des notes sur ce que vous comprenez, ces notes vous y aurez le droit de les avoir avec vous au CT !**

2 Introduction

Dans ce TP, je vous propose de voir le principe du DNS
Nous allons voir
— Les IP dynamiques
— **Installer** un serveur DNS, le **configurer** et le **lancer**
— **Capturer** des paquets de types DNS
— Voir le port 53
— Voir la relation entre le serveur DNS et le serveur DHCP
— etc...

3 Théorie, rappels

1. Quelle est la principale information qu'un serveur DNS de base doit donner ?
2. Sur quelle couche transport le DNS s'appuie-t'il ?
3. Si on n'avait pas de serveur DNS que se passerait-il ?
4. Sous Linux, quelles sont les 3 commandes qui permettent d'interroger un serveur DNS ?

4 Pratique

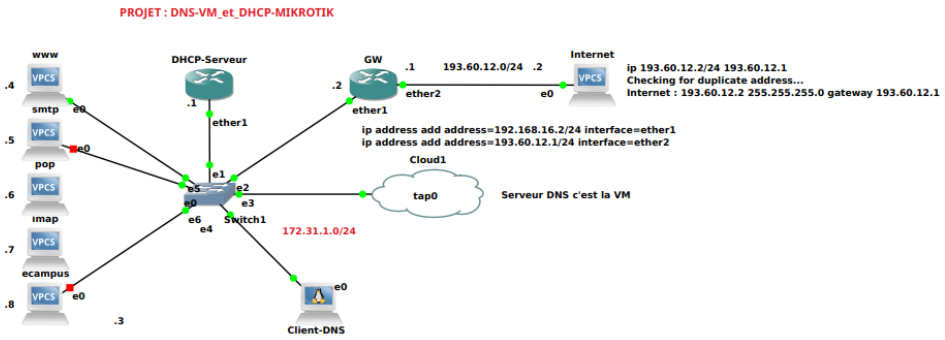
4.1 Première partie : En tant que client

1. Sur le HOST, **lancez** la commande ***nslookup www.unicaen.fr***
   Quel type d'@IP obtient-on ?
   Quel est l'@IP du serveur de nom ?
   Est-ce logique par rapport au contenu du fichier **/etc/resolv.conf** ?
2. **Branchez** le câble rouge sur **BR0**
3. **Lancez** la VM et **loguez** vous dessus
4. **Lancez** la commande ***nslookup www.unicaen.fr***
   Quel type d'IP obtient-on ?
   Quel est l'@IP du serveur de nom ?
   Est-ce logique par rapport au contenu du fichier **/etc/resolv.conf** ?
5. **Lancez** la commande ***ip route ls*** *quelle est la* ***route par défaut*** *ou bien la* ***Passerelle ?***

   Il faut maintenant que la route par défaut soit par le réseau **192.168.128.0/22**
6. **Passez** root
   (a) **Faites** tomber cette route par défaut ***ifdown enp0s3***,
   (b) on pourrait aussi retirer l'interface sur le NAT dans la configuration de la VM dans virtualbox
   (c) **Lancez** la commande ***dhclient -r enp0s3***
   (d) **Lancez** la commande ***dhclient enp0s9***
7. **Vérifiez** que c'est bon en lançant la commande ***ip route ls*** et en visualisant le fichier **/etc/resolv.conf**
   C'est bon ?
8. **Lancez** la commande ***nslookup www.unicaen.fr***
   Quel type d'IP obtient-on ?
   Quel est l'@IP du serveur de nom ?
   Est-ce logique par rapport au contenu du fichier **/etc/resolv.conf** ?
9. **Concluez** sur cette partie.

4.2 Seconde partie : En tant que serveur

On va travailler sur la structure suivante :



Elle représente le LAN d'une petite organisation.
Quelques petites informations pour le bon déroulement du TP
— On est en LAN sur un réseau 172.31.1.0/24
— Le routeur nommé DHCP-Serveur sert de serveur DHCP comme dans le TP DHCP, il a @IP **172.31.1.1**
— Le routeur nommé GW est la passerelle pour pouvoir quitter le LAN et aller sur Internet, elle a @IP **172.31.1.2**
— La machine VPCS nommée Internet représente Internet
— Les machines VPCS WWW, SMTP, POP, IMAP et eCampus sont des serveurs avec des IP Fixes **172.31.1.4 à .8**
— Le nuage est connecté sur l'interface TAP0 de la VM (Comment ? On s'en moque ! ! !), elle a @IP **172.31.1.254**
— La machine MicroLinux nommée Client-DNS ne connaît rien au démarrage

4.3 Sans serveur DNS

1. **Récupérez** sur ecampus le projet nommé DNS-VM_et_DHCP-Mikrotik
2. **Ouvrez** le projet avec GNS3
3. **Lancez** que la machine MicroLinux nommée Client-DNS
   (a) Quelle est son IP ?
   (b) Peut-on faire un ping ?
   NON !
4. **Lancez** le routeur nommé DHCP-Serveur et **attendez** quelques minutes
5. **Relevez** l'**@IP** et le **masque** de l'interface **eth0** de la machine MicroLinux nommée Client-DNS ainsi que sa **passerelle** et le contenu du fichier **/etc/resolv.conf**
   Est-ce Logique ?
   Qui a donné ces informations à la machine MicroLinux nommée Client-DNS ?
6. **Connectez** vous sur le routeur nommé DHCP-Serveur.
   Je rappelle login : **admin** et pas de MDP ! ! !
7. **Lancez** la commande ***/export***
8. **Lisez** la conf du routeur, la partie DHCP serveur
   Est-ce conforme à ce que l'on a relevé précédemment ?
9. Sur le câble reliant la machine MicroLinux nommée Client-DNS et le switch, **mettez** une sonde wireshark en sélectionnant le protocole **DNS**
10. Sur la machine MicroLinux nommée Client-DNS, **lancez** la commande ***nslookup www.unicaen.fr***
    Que se passe-t-il ? Pourquoi ?
11. Que **voyez**-vous sur la sonde wireshark ?
12. **Concluez** sur cette partie sans DNS !

4.4 Avec un serveur DNS

Nous allons **installer** et **paramétrer** un serveur DNS.
ATTENTION : soyez rigoureux !
Nous allons utiliser la version **dnsmasq**.

1. **Passez** root sur la VM
2. **Lancez** la commande ***netstat -lunp4***
   Le port DNS est-il ouvert ?
   Non ? Alors il faut l'ouvrir en installant un serveur DNS
3. **Lancez** la commande ***apt install dnsmaq***
4. **Lancez** la commande ***netstat -lunp4***
   Le port DNS est-il ouvert ?
   Oui ? Alors il faut configurer le serveur DNS

5. **Sauvegardez** le fichier ***/etc/dnsmasq.conf : mv dnsmasq.conf dnsmasq.conf-original***
6. **Mettez** cela dans le fichier ***dnsmasq.conf***

   #### DNS ####
   domain-needed
   bogus-priv
   # Ficher des forwarders
   resolv-file=**/etc/dnsmasq-dns.conf**
   strict-order
   user=root
   group=root
   # Fichier des enregistrements A et AAAA
   addn-hosts=**/etc/dnsmasq-hosts.conf**
   expand-hosts
   domain=**unicaen.fr**
   # LOG DNS
   log-queries
   #L'interface TAP0
   listen-address=**172.31.1.254**
7. **Expliquez** ce que vous avez compris dans ces différentes lignes.
8. **Lancez** la commande ***systemctl status dnsmasq.service***

   Qu'est-ce qui ne va pas ?

   Est-ce logique ?
9. **Mettez** cela dans le fichier ***dnsmasq-hots.conf***

   172.31.1.4 www www.unicaen.fr
   172.31.1.5 smtp smtp.unicaen.fr
   172.31.1.6 pop pop.unicaen.fr
   172.31.1.7 imap imap.unicaen.fr
   172.31.1.8 ecampus ecampus.unicaen.fr
10. **Lancez** la commande ***systemctl restart dnsmasq.service*** *puis* ***systemctl status dnsmasq.service***

    Est-ce que tout va ?

    Est-ce logique ?
11. Sur la machine MicroLinux nommée Client-DNS, **lancez** la commande ***nslookup www.unicaen.fr***

    Que se passe-t-il ? Pourquoi ?
12. Que **voyez**-vous sur la sonde wireshark ?
13. **Concluez** sur cette partie avec DNS !

5 Conclusion

À partir de maintenant vous savez ce qu'est
— Le protocole DNS
— Un client DNS
— Un serveur DNS, l'information qu'il donne :

N'oubliez pas de faire une synthèse ! ! ! !