

# Atelier3 B-1

25/09/2023

*Protocoles DHCP et DNS*

## I. Table des matières

|        |  |    |
|--------|--|----|
| I.     | Table des matières.....  | 2  |
| II.    | Introduction .....   | 3  |
| III.   | Rôle du DNS.....   | 3  |
| IV.    | Nslookup et résolution dns.....  | 4  |
|        | a) Who is DNS : .....  | 5  |
|        | b) Test web .....  | 6  |
| V.     | Pare-feux et ACL : .....   | 7  |
| VI.    | Analyse passive.....   | 8  |
|        | c) RCPBIND.....  | 8  |
| VII.   | Différent type de dns.....   | 11 |
| VIII.  | Test Nslookup.....   | 12 |
|        | d) Nslookup résolution server messagerie : .....                                       | 13 |
|        | e) Définition d'un rcpcbind : .....  | 15 |
| IX.    | Analyse Dns.....   | 15 |
|        | f) Port utilisé par le protocole DNS sur la couche de couche 4 utilisé par DNS ? ..... | 15 |
|        | g) RFC1035 .....   | 15 |
|        | h) Structure des requêtes et des réponses DNS : .....                                  | 16 |
| X.     | Réflexion sur le DNS : .....   | 16 |
|        | i) Windows terminal : .....  | 17 |
| XI.    | Différent outils linux pour l'analyse DNS .....  | 18 |
| XII.   | Outils delv : .....  | 20 |
| XIII.  | Exercice 6 : Analyse approfondie des échanges sous Packet Tracer .....                 | 23 |
|        | j) 2e partie : Inspecter le trafic interréseau au bureau central .....                 | 26 |
| XIV.   | Étude sur le DHCP .....  | 27 |
|        | k) RFC .....   | 28 |
|        | l) Différent type d'allocation : .....   | 28 |
|        | m) Risque DHCP : .....   | 32 |
|        | n) Risque configuration clasic : .....   | 33 |
| XV.    | Création d'un réseaux DHCP : .....   | 34 |
|        | o) Problématique du DHCP : .....   | 36 |
| XVI.   | Mise en situation man in the middle: .....   | 37 |
| XVII.  | Configuration des DNS : .....  | 40 |
| XVIII. | Code Html.....   | 42 |
| XIX.   | Protocoles vus .....   | 44 |

|      |                   |    |
|------|-------------------|----|
| XX.  | Conclusion: ..... | 44 |
| XXI. | Sources .....     | 44 |



## II. Introduction

Cet atelier nous initie à l'utilisation du DNS, aux modes itératif et récursif, et nous aide à comprendre l'importance du DNS dans un réseau. Il nous permet également de découvrir des outils tels que "whois" ou "nslookup", qui s'avéreront particulièrement utiles pour un technicien réseau.

## III. Rôle du DNS

Un DNS, ou [Domain Name System](#) (Système de Noms de Domaine), est un service essentiel sur Internet. Il fonctionne comme un annuaire qui traduit les noms de domaine conviviaux que les gens utilisent en adresses IP, permettant ainsi aux ordinateurs de localiser les ressources en ligne. Voici une explication de son utilité :

- Traduction des noms de domaine en adresses IP : Les utilisateurs d'Internet accèdent aux sites web, aux services en ligne et à d'autres ressources en utilisant des noms de domaine faciles à retenir, tels que " www.icann.org ". Le DNS associe ces noms de domaine à des adresses IP numériques, telles que " IP 192.0.32.7", qui sont utilisées par les ordinateurs et les serveurs pour localiser ces ressources.
- Par exemple, si nous effectuons un ping sur **www.icann.org**, nous pouvons constater que notre requête de ping est couronnée de succès car le DNS associe le nom de domaine **www.icann.org** à l'adresse IP **192.0.32.7**. Le DNS joue un rôle essentiel dans la résolution des noms de domaine en adresses IP, permettant ainsi aux ordinateurs de localiser les ressources en ligne.

```
PS C:\Users\eloha> ping www.icann.org

Envoi d'une requête 'ping' sur www.vip.icann.org [192.0.32.7] avec 32 octets de données :
Réponse de 192.0.32.7 : octets=32 temps=148 ms TTL=242
Réponse de 192.0.32.7 : octets=32 temps=148 ms TTL=242
Réponse de 192.0.32.7 : octets=32 temps=148 ms TTL=242
Réponse de 192.0.32.7 : octets=32 temps=148 ms TTL=242

Statistiques Ping pour 192.0.32.7:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
```

- Facilité d'utilisation : Le DNS simplifie la navigation sur Internet en permettant aux utilisateurs d'utiliser des noms de domaine plus conviviaux au lieu de se souvenir d'adresses IP complexes.
- Évolutivité : Le DNS est un système hiérarchique, ce qui signifie qu'il peut gérer un grand nombre de noms de domaine de manière efficace et évolutive.

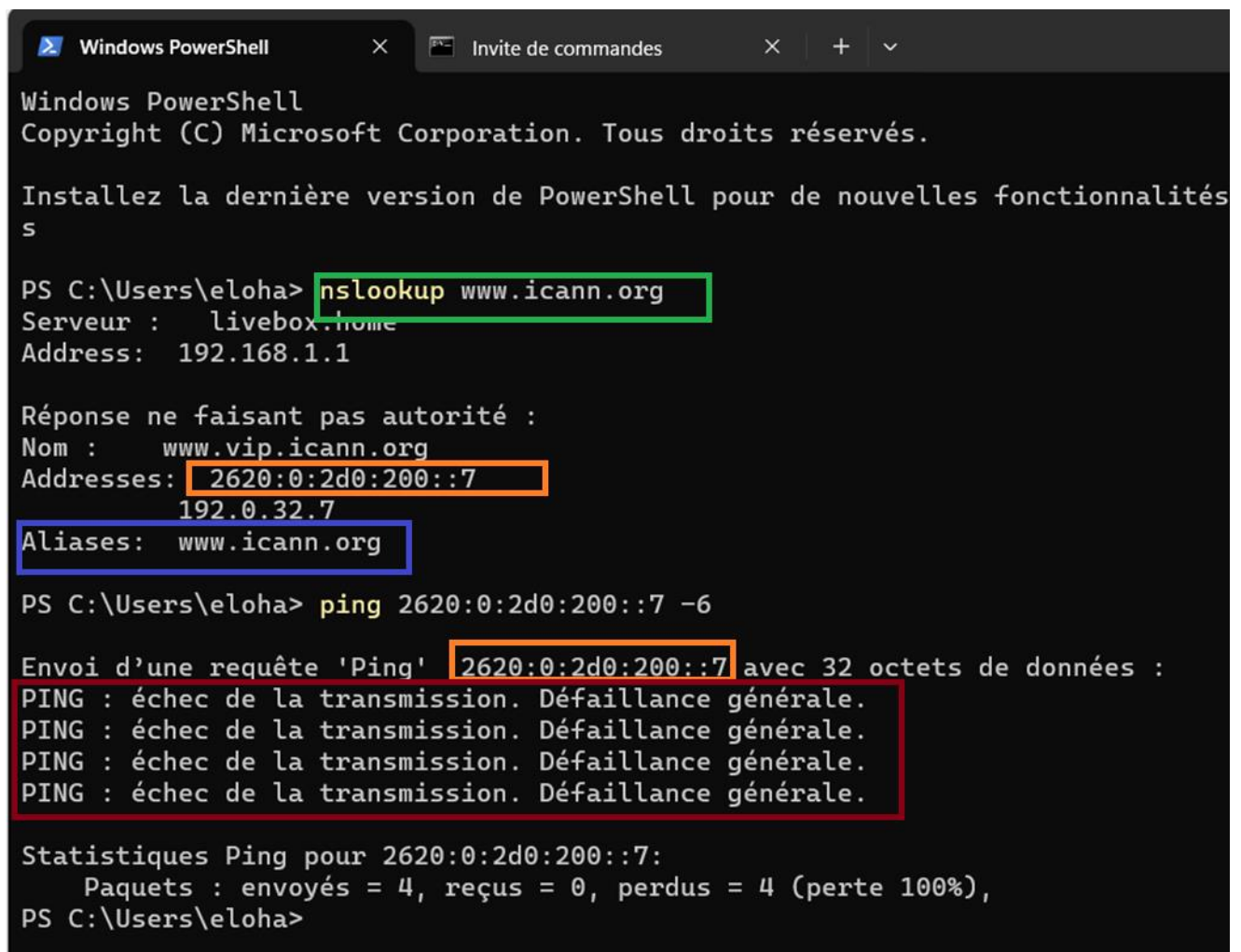
- Redirection et équilibrage de charge : Les systèmes DNS permettent de rediriger les demandes vers les serveurs appropriés, ce qui peut être utilisé pour l'équilibrage de charge, la répartition de trafic, et la résilience.
- Localisation géographique : Le DNS peut être utilisé pour diriger les utilisateurs vers des serveurs ou des services situés géographiquement près de leur emplacement, améliorant ainsi la vitesse et la qualité de service.

En résumé, le DNS joue un rôle essentiel en permettant aux utilisateurs d'accéder aux ressources en ligne de manière conviviale, en garantissant la résolution des noms de domaine en adresses IP, et en facilitant la gestion du trafic Internet à grande échelle.

#### IV. Nslookup et résolution dns

```
C:\Users\eloha>ping www.icann.org -6
La requête Ping n'a pas pu trouver l'hôte www.icann.org. Vérifiez le nom et essayez à nouveau.

C:\Users\eloha>ping www.icann.org
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités
s

PS C:\Users\eloha> nslookup www.icann.org
Serveur : livebox.home
Address: 192.168.1.1

Réponse ne faisant pas autorité :
Nom : www.vip.icann.org
Adresses: 2620:0:2d0:200::7
192.0.32.7
Aliases: www.icann.org

PS C:\Users\eloha> ping 2620:0:2d0:200::7 -6

Envoi d'une requête 'Ping' 2620:0:2d0:200::7 avec 32 octets de données :
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.

Statistiques Ping pour 2620:0:2d0:200::7:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
PS C:\Users\eloha>
```

nslookup est un outil de ligne de commande qui permet de **résoudre des noms de domaine** en adresses IP, d'effectuer des résolutions inverses, d'interroger des serveurs

DNS spécifiques et de détecter des problèmes liés au DNS. Il est largement utilisé pour le dépannage et la gestion des systèmes réseau.

Dans notre exemple, en utilisant [nslookup](https://www.icann.org) sur [www.icann.org](https://www.icann.org), nous pouvons récupérer à la fois l'adresse IP version 4 (IPv4) et l'adresse IP version 6 (IPv6) associées au nom de domaine du site.

Maintenant, si nous souhaitons vérifier directement si le site bloque les requêtes "ping" via IPv6, nous pouvons prendre directement l'adresse IPv6 et effectuer notre test. Comme le montre le message d'erreur : "**Échec de la transmission. Défaillance générale**", cela suggère que les pings IPv6 ne sont pas autorisés.

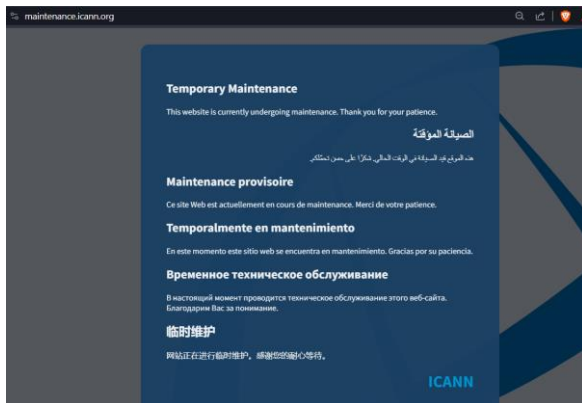
L'indication "**Aliases : [www.icann.org](https://www.icann.org)**" signifie que cette adresse IP est liée au nom de domaine [www.icann.org](https://www.icann.org). Elle permet de faire le lien entre l'adresse IP et le nom de domaine.

#### a) Who is DNS :

Il existe également des outils tels que "who.is" qui permettent d'obtenir des informations sur le DNS. Comme nous pouvons le constater, ces outils fournissent des informations similaires à celles que l'on obtient avec nslookup.

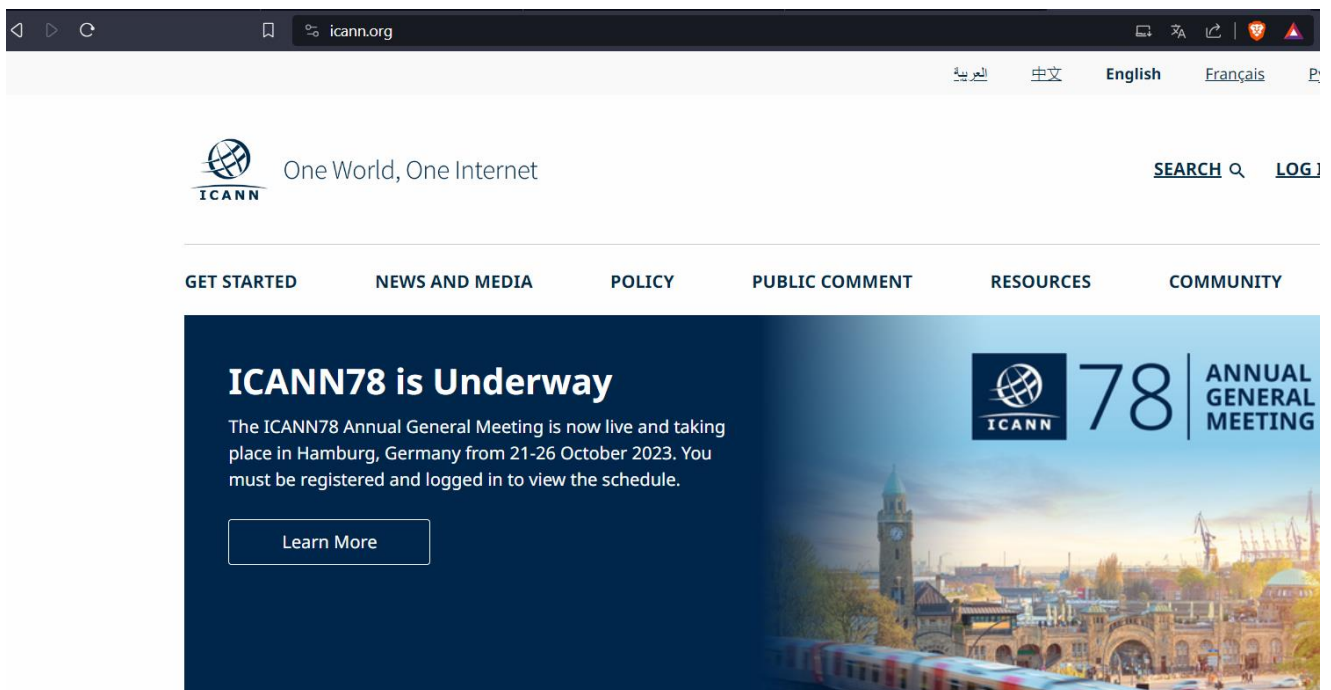
| Hostname      | Type  | TTL   | Priority | Content  |
|---------------|-------|-------|----------|--|
| icann.org     | SOA   | 3600  |          | sns.dns.icann.org noc@dns.icann.org 2023101450 10800 3600 1209600 3600 |
| icann.org     | NS    | 21600 |          | a.icann-servers.net  |
| icann.org     | NS    | 21600 |          | b.icann-servers.net  |
| icann.org     | NS    | 21600 |          | c.icann-servers.net  |
| icann.org     | NS    | 21600 |          | ns.icann.org   |
| icann.org     | A     | 550   |          | 192.0.43.7   |
| icann.org     | AAAA  | 510   |          | 2001:500:88:200::7   |
| icann.org     | MX    | 600   | 10       | pechora1.icann.org   |
| icann.org     | MX    | 600   | 10       | pechora3.icann.org   |
| icann.org     | MX    | 600   | 10       | pechora4.icann.org   |
| icann.org     | MX    | 600   | 10       | pechora5.icann.org   |
| www.icann.org | A     | 29    |          | 192.0.32.7   |
| www.icann.org | AAAA  | 30    |          | 2620:0:2d0:200::7  |
| www.icann.org | CNAME | 3570  |          | www.vip.icann.org  |

## b) Test web

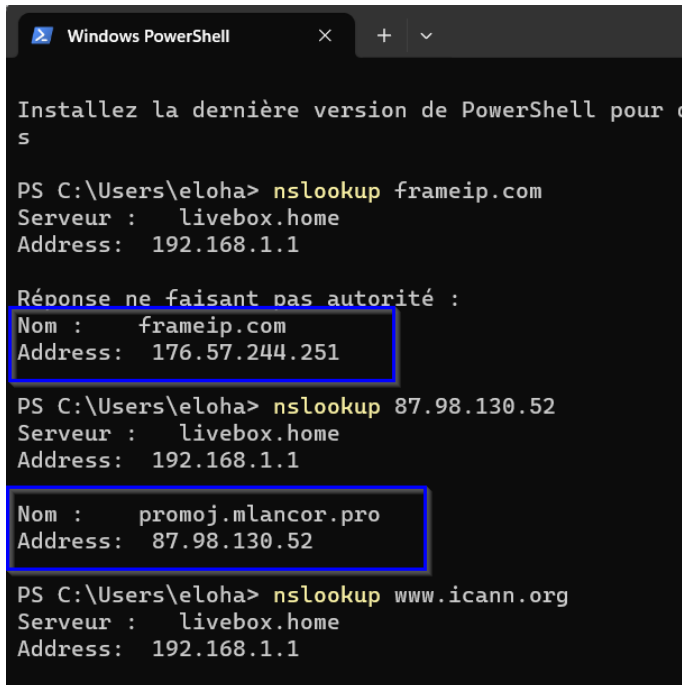


ici on test <https://192.0.32.7> et on tombe sur le site de maintenance de l'icann

Et quand je tape [www.icann.org](https://www.icann.org) je tombe sur ce site :



On peut observer que lorsque l'on tape directement l'adresse IP, on est redirigé vers la page de maintenance, tandis que lorsque l'on utilise le nom de domaine, on accède au bon site. Il semble que cela soit dû au fait que la page de maintenance et la page par défaut s'affichent en cas d'erreur de nom de domaine. Étant donné que la plupart des gens utilisent le nom de domaine et que le DNS n'a pas été configuré pour gérer l'accès via l'adresse IP, cela nous conduit à une page qui n'est pas destinée à servir de page d'accueil.



```
Windows PowerShell

Installez la dernière version de PowerShell pour c
s

PS C:\Users\eloha> nslookup frameip.com
Serveur : livebox.home
Address: 192.168.1.1

Réponse ne faisant pas autorité :
Nom : frameip.com
Address: 176.57.244.251

PS C:\Users\eloha> nslookup 87.98.130.52
Serveur : livebox.home
Address: 192.168.1.1

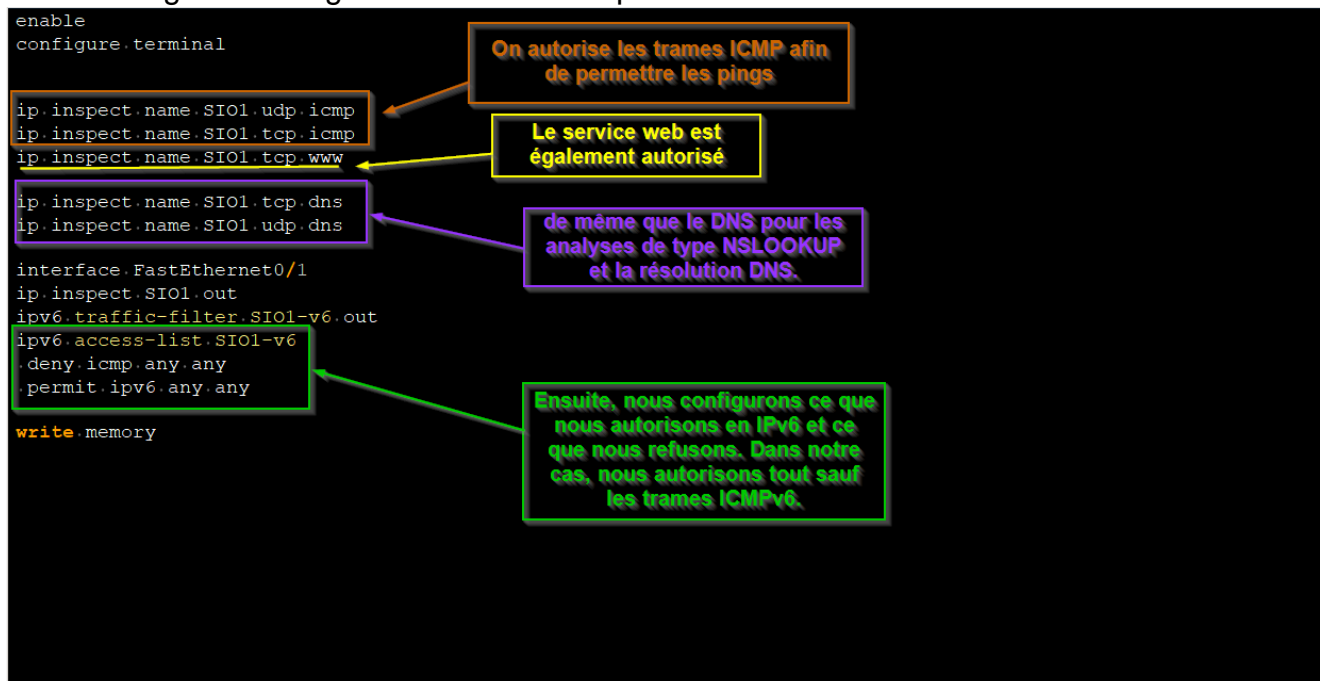
Nom : promoj.mlancor.pro
Address: 87.98.130.52

PS C:\Users\eloha> nslookup www.icann.org
Serveur : livebox.home
Address: 192.168.1.1
```

## V. Pare-feux et ACL :

Pour comprendre pourquoi les pings IPv6 ne sont pas autorisés, j'ai refait un exemple de configuration pare-feu reproduisant la situation que nous avons observée.

Voici les règles à configurer sur un routeur/pare-feu :



```
enable
configure terminal

ip inspect name SIO1 udp icmp
ip inspect name SIO1 tcp icmp
ip inspect name SIO1 tcp www

ip inspect name SIO1 tcp dns
ip inspect name SIO1 udp dns

interface FastEthernet0/1
ip inspect SIO1 out
ipv6 traffic-filter SIO1-v6 out
ipv6 access-list SIO1-v6
deny icmp any any
permit ipv6 any any

write memory
```

On autorise les trames ICMP afin de permettre les pings

Le service web est également autorisé

de même que le DNS pour les analyses de type NSLOOKUP et la résolution DNS

Ensuite, nous configurons ce que nous autorisons en IPv6 et ce que nous refusons. Dans notre cas, nous autorisons tout sauf les trames ICMPv6

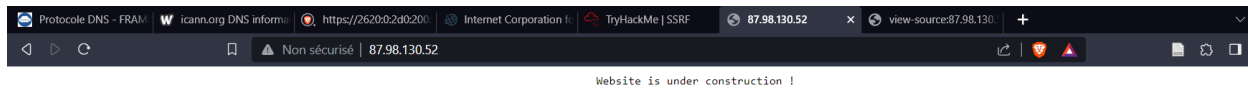
On peut aussi configurer un pare-feu pour bloquer un individu malveillant sur un ou certains ports. Pour cela, j'ai réalisé une vidéo démonstrative que vous trouverez ci-dessous :

<https://youtu.be/eM6d6Mhavy4>



## VI. Analyse passive

En saisissant l'adresse IP dans le navigateur, nous sommes automatiquement redirigés vers cette page. Par curiosité, j'ai donc effectué une analyse avec Nmap sur cette adresse :



Nmap, abréviation de "Network Mapper," est un outil informatique utilisé pour explorer et analyser les réseaux. Il permet de scanner un réseau informatique pour découvrir quels appareils sont connectés, quels ports réseau sont ouverts sur ces appareils, et quelles sont les services qui fonctionnent sur ces ports. En somme, Nmap aide à cartographier et à évaluer les dispositifs et les services d'un réseau, ce qui est précieux pour la gestion de la sécurité et la configuration des réseaux informatiques.

```
root@ip-10-10-2-170:~# nmap 87.98.130.52

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-26 22:07 BST
Nmap scan report for promo.j.mlanco.r.pro (87.98.130.52)
Host is up (0.015s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
30/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
```

Potential faille de sécurité

Intéressant pour un red hat

L'analyse Nmap révèle la présence de plusieurs ports ouverts. Le **port SSH**, par exemple, est utilisé pour une connexion sécurisée à une machine.

Il y a également un port HTTP, sur lequel je me suis connecté par défaut en entrant l'adresse IPv4. Le DNS a associé la connexion à ce port.

De plus, un port HTTPS est ouvert, renforçant la sécurité des communications.

**Enfin, j'ai identifié un port "rpcbind" dont je n'avais pas connaissance. J'ai donc effectué des recherches pour en savoir davantage sur ce protocole :**

### c) **RPCBIND**

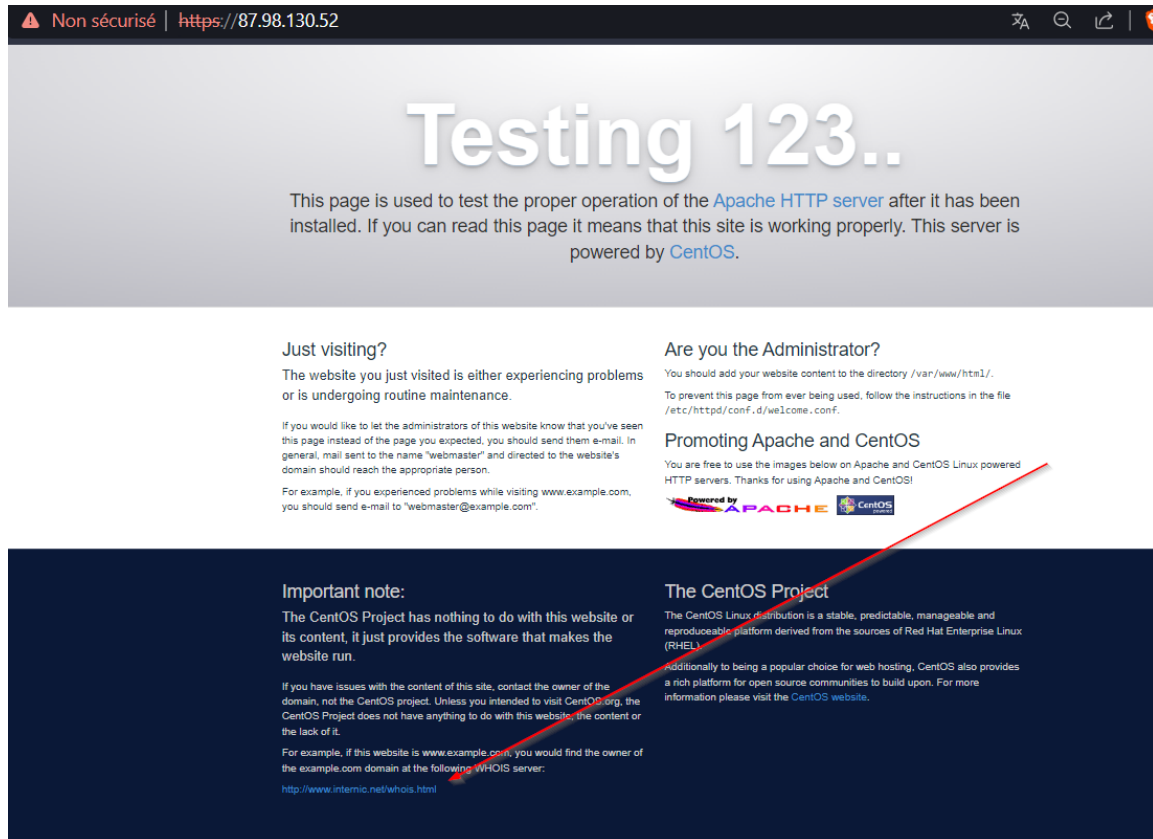
RPCBIND, abréviation de Remote Procedure Call Binding, est un utilitaire qui joue un rôle essentiel dans les systèmes Unix et Linux. Il sert de pont entre les services RPC (Remote Procedure Call) et les ports auxquels ils écoutent. Lorsqu'un processus RPC démarre, il communique avec RPCBIND pour enregistrer le port auquel il écoute ainsi que les numéros de programme RPC qu'il prévoit de fournir. Ensuite, lorsqu'un client souhaite accéder à un service RPC spécifique, il contacte RPCBIND sur le serveur. RPCBIND redirige alors le client vers le port approprié, permettant ainsi la communication avec le service requis.

Ce processus de liaison des services RPC aux ports est essentiel, car il garantit que les clients peuvent accéder aux services de manière transparente. RPCBIND doit être



disponible avant le démarrage des services RPC, car ces derniers dépendent de cette liaison pour fonctionner correctement. De plus, RPCBIND utilise des enveloppes TCP pour le contrôle d'accès, ce qui a un impact sur tous les services RPC. Il est possible de spécifier des règles de contrôle d'accès pour chaque démon RPC NFS, ce qui ajoute une couche de sécurité à ces services.

J'ai tenté de me connecter via HTTPS, et cela a résulté en l'apparition d'un nouveau site :



Un nouveau site est apparu, affichant le message suivant : "Cette page est utilisée pour tester le bon fonctionnement du serveur Apache HTTP après son installation. Si vous pouvez lire cette page, cela signifie que ce site fonctionne correctement. Ce serveur est propulsé par CentOS."

Il y a également un lien vers un service "Whois ICANN". Un site Whois est précisément lié au cours car il permet d'analyser un DNS de manière similaire à un NSLookup.

The screenshot shows the ICANN Lookup website in a browser. The address bar displays 'lookup.icann.org/en'. The page has a dark blue header with the 'ICANN | LOOKUP' logo. Below the header, the main content area is light gray and titled 'Registration data lookup tool'. It includes a search input field with the placeholder 'Enter a value' and a blue 'Lookup' button. Above the input field, there is a link to 'Frequently Asked Questions (FAQ)'. Below the input field, a disclaimer states: 'By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy, and agree to abide by the website Terms of Service and the registration data lookup tool Terms of Use.'

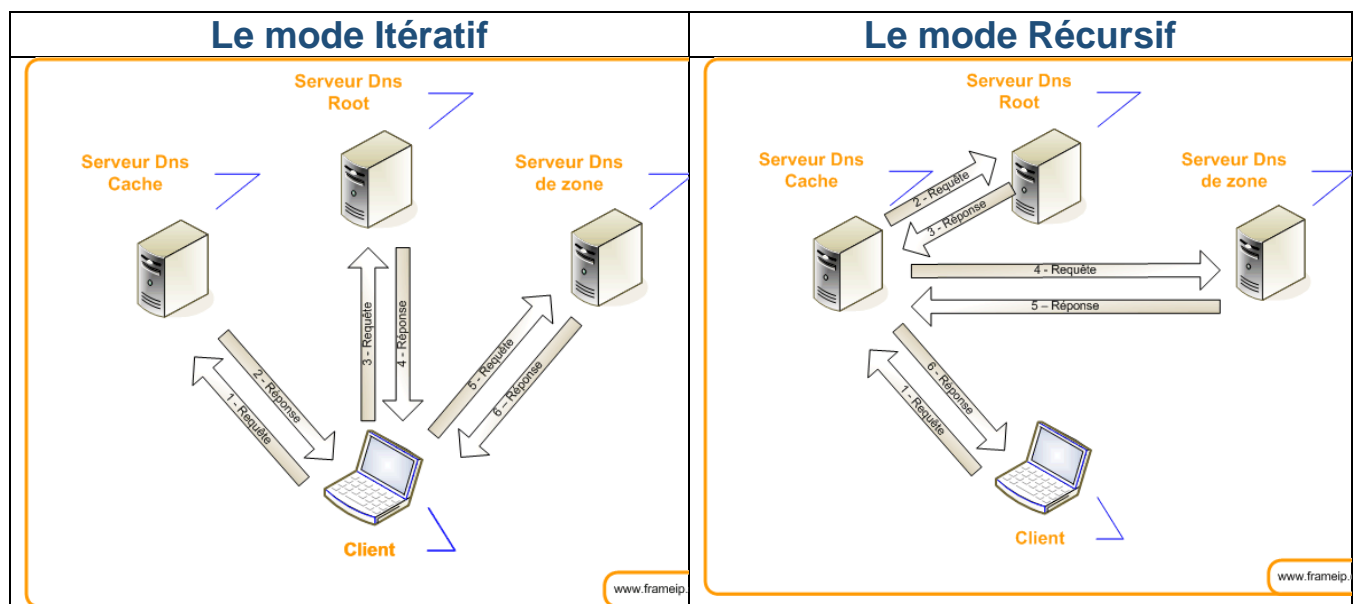
### About ICANN's registration data lookup tool

The ICANN registration data lookup tool gives you the ability to look up the current registration data for domain names and Internet number resources. The tool uses the Registration Data Access Protocol (RDAP) which was created as a replacement of the WHOIS (port 43) protocol. RDAP was developed by the technical community in the [Internet Engineering Task Force](#) (IETF).

RDAP has several advantages over the WHOIS protocol, including more secure access to data, a standardized and user-friendly format, support for internationalization, and the ability to provide differentiated access to registration data. More information can be found [here](#). For additional information on registration data, please visit the [Registration Data at ICANN page](#).

## VII. Différent type de dns

Le DNS (Domain Name System) est un système essentiel qui traduit les noms de domaine en adresses IP, permettant ainsi aux ordinateurs de localiser les serveurs correspondants sur Internet. Les modes itératif et récursif sont deux méthodes utilisées dans le processus de résolution DNS pour obtenir cette correspondance entre les noms de domaine et les adresses IP. Voici les différences entre ces deux modes :



**Mode Itératif :** Ce mode est le plus simple du point de vue du serveur. Les serveurs répondent directement à la requête sur la base seule de ses informations locales. La réponse peut contenir la réponse demandée, ou bien donne la référence d'un autre serveur qui sera « plus susceptible » de disposer de l'information demandée. Il est important que tous les serveurs de noms puissent implémenter ce mode itératif et désactive la fonction de récursivité.

**Le mode Récursif :** Le mode récursif est plus simple du point de vue du client. Dans ce mode, le premier serveur prend le rôle de résolveur.

L'utilisation du mode récursif est limitée aux cas qui résultent d'un accord négocié entre le client et le serveur. Cet accord est négocié par l'utilisation de deux bits particuliers des messages de requête et de réponse :

Le bit Ra (Récursion admissible), est marqué ou non par le serveur dans toutes les réponses. Ce bit est marqué si le serveur accepte à priori de fournir le service récursif au client, que ce dernier l'ait demandé ou non. Autrement dit, le bit RA signale la disponibilité du service plutôt que son utilisation.

VIII. Test Nslookup

| Linux mint   | Windows terminal  |
|--|---|
| <pre>nslookup &gt; set type=NS &gt; server 8.8.8.8 Default server: 8.8.8.8 Address: 8.8.8.8#53 &gt; education.fr ;; communications error to 8.8.8.8#53: timed out Server:      8.8.8.8 Address:     8.8.8.8#53  Non-authoritative answer: education.fr  nameserver = ate-ns02.ate.info education.fr  nameserver = ate-ns04.ate.info education.fr  nameserver = ate-ns01.ate.info education.fr  nameserver = ate-ns03.ate.info  Authoritative answers can be found from: &gt;</pre> | <pre>&gt; nslookup Serveur : AL-DC-01.sio.local Address: 172.31.1.4  *** AL-DC-01.sio.local ne parvient pas à trouver nslookup : &gt; set type=NS &gt; server 8.8.8.8 Serveur par défaut : dns.google Address: 8.8.8.8  &gt; server 8.8.8.8#53 Unrecognized command: server 8.8.8.8#53 &gt; server 8.8.8.8#education.fr Unrecognized command: server 8.8.8.8#education.fr &gt; education.fr Serveur : dns.google Address: 8.8.8.8  Réponse ne faisant pas autorité : education.fr  nameserver = ate-ns02.ate.info education.fr  nameserver = ate-ns03.ate.info education.fr  nameserver = ate-ns01.ate.info &gt; C:\Users\eloha&gt;color b C:\Users\eloha&gt;</pre> |

Au départ, j'avais l'impression que l'outil nslookup de Windows était moins complet que celui de Linux. Cependant, après avoir refait le test sur Kali Linux, j'ai conclu que les résultats pouvaient varier en fonction du moment où les tests ont été effectués. Il se peut que le site education.fr ait eu un serveur DNS public différent à un moment donné.

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ nslookup
> set type=NS
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> education.fr
;; communications error to 8.8.8.8#53: timed out
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
education.fr  nameserver = ate-ns03.ate.info.
education.fr  nameserver = ate-ns01.ate.info.
education.fr  nameserver = ate-ns02.ate.info.

Authoritative answers can be found from:
>
```

Annotations:

- Dns par défaut de google
- Nom de domaine sur le quelle on effectue les test
- Serveur DNS public

Il est également possible d'utiliser le site "ns.Tools" pour effectuer des tests :

The screenshot shows the ns.tools website interface. On the left, there is a sidebar with a 'resume' section and a list of tools: Tree, Zone, Host, DNSSEC, and Tests. The main content area is titled 'Dns servers for education.fr' and includes a note 'education.fr was detected as domain'. Below this, there are three boxes, each containing a DNS server entry:

| Name              | IPs            |
|-------------------|----------------|
| ate-ns01.ate.info | 185.252.158.6  |
| ate-ns02.ate.info | 37.235.92.6    |
| ate-ns03.ate.info | 185.161.47.6   |
| ate-ns04.ate.info | 195.190.27.186 |

#### d) Nslookup résolution server messagerie :

La commande "set type=MX" dans nslookup permet d'obtenir des informations sur les serveurs de messagerie associés à un domaine, facilitant la configuration des services de messagerie.

Elle donne les indications suivantes :

The screenshot shows a Windows PowerShell window with the following commands and output:

```
> set type=MX
> education.fr
Serveur : dns.google
Address: 8.8.8.8

education.fr
primary name server = ate-ns01.ate.info
responsible mail addr = hostmaster.ate.info
serial = 1
refresh = 10800 (3 hours)
retry = 3600 (1 hour)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)
>
```

Annotations on the screenshot:

- A yellow box highlights the command `set type=MX`.
- A yellow box highlights the output `primary name server = ate-ns01.ate.info` with an arrow pointing to it from the text "Le serveur de messagerie principal".
- A green box highlights the output `responsible mail addr = hostmaster.ate.info` with an arrow pointing to it from the text "L'adresse e-mail du responsable".



```
> set type=mx
> www.cisco.com
Serveur : livebox.home
Address: 192.168.1.1



Réponse ne faisant pas autorité :
www.cisco.com canonical name = www.cisco.com.akadns.net
www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net
wwwds.cisco.com.edgekey.net canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net
wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e2867.dsca.akamaiedge.net



dsca.akamaiedge.net
primary name server = n0dsca.akamaiedge.net
responsible mail addr = hostmaster.akamai.com
serial = 1698583079
refresh = 1000 (16 mins 40 secs)
retry = 1000 (16 mins 40 secs)
expire = 1000 (16 mins 40 secs)
default TTL = 1800 (30 mins)
>
```

### Dns servers for [cisco.com](https://www.cisco.com)

www.cisco.com was detected as host

|      |  |   |
|------|--|---|
| Name | <a href="https://www.cisco.com">ns1.cisco.com</a>  |   |
| IPs  |  72.163.5.201 |  |

|      |   |   |
|------|---|---|
| Name | <a href="https://www.cisco.com">ns2.cisco.com</a>   |   |
| IPs  |  64.102.255.44 |  |

|      |   |   |
|------|---|---|
| Name | <a href="https://www.cisco.com">ns3.cisco.com</a>   |   |
| IPs  |  173.37.146.41 |  |

Cisco utilise <https://www.akamai.com/fr/products/edge-dns>


Pour la gestion interne des courriels


```
> www.frameip.com
Serveur : livebox.home
Address: 192.168.1.1


frameip.com
primary name server = ns1.gandi.net
responsible mail addr = hostmaster.gandi.net
serial = 1698278400
refresh = 10800 (3 hours)
retry = 3600 (1 hour)
expire = 604800 (7 days)
default TTL = 10800 (3 hours)
>
```

### Dns servers for [frameip.com](https://www.frameip.com)

www.frameip.com was detected as host

|      |  |   |
|------|--|---|
| Name | <a href="https://www.frameip.com">ns-19-a.gandi.net</a>  |   |
| IPs  |  173.246.100.20 |  |

|      |  |   |
|------|--|---|
| Name | <a href="https://www.frameip.com">ns-191-c.gandi.net</a>   |   |
| IPs  |  217.70.187.192 |  |

|      |  |   |
|------|--|---|
| Name | <a href="https://www.frameip.com">ns-36-b.gandi.net</a>  |   |
| IPs  |  213.167.230.37 |  |

### Host informations

Ips  176.57.244.251 

Cname -

Frame IP utilise également un site pour la gestion des courriels sur un serveur interne, qui est <https://www.gandi.net/fr>.

**e) Définition d'un rcpcbind :**

Rcpbind est un service Unix qui associe des numéros de port aux services RPC. Il permet aux clients RPC de trouver les ports associés aux services, facilitant ainsi la communication. Dans le contexte de Red Hat, il peut être utilisé pour gérer les numéros de port des services RPC sur des systèmes Linux basés sur Red Hat.

## **IX. Analyse Dns**

**f) Port utilisé par le protocole DNS sur la couche 4 utilisé par DNS ?**

Le DNS (Domain Name System) utilise principalement le port 53 en tant que port de couche 4. Cependant, il peut également utiliser le port 5353 en UDP pour des fonctionnalités spécifiques, telles que la découverte de services multicouches (mDNS) avec Bonjour.

Donc, il y a plus d'un port utilisé, mais 53 est le plus couramment associé au DNS.

**g) RFC1035**

La RFC 1035 a été rédigée par plusieurs personnes au sein de l'Internet Engineering Task Force (IETF), notamment Paul Mockapetris, qui est largement crédité comme l'auteur principal du protocole DNS. Elle a été publiée en novembre 1987.

La RFC 1035 a remplacé la RFC 882 et la RFC 883, qui étaient les spécifications précédentes du DNS. Ces deux RFC antérieures définissaient le Domain Name System, mais la RFC 1035 a été élaborée pour combler certaines lacunes et améliorer le protocole.

Le fondement du protocole DNS est de fournir une méthode hiérarchique et distribuée pour résoudre les noms de domaine en adresses IP. Il s'agit de l'un des éléments fondamentaux de l'infrastructure d'Internet, permettant aux utilisateurs d'accéder aux sites Web et aux services en utilisant des noms de domaine conviviaux plutôt que de devoir se rappeler des adresses IP numériques. Le DNS repose sur une structure d'arborescence de noms de domaine et sur des serveurs de noms qui se répartissent à différents niveaux de cette hiérarchie pour gérer la résolution des noms. Cela permet une navigation plus conviviale sur le Web et simplifie la gestion des adresses IP à l'échelle mondiale.



**h) Structure des requêtes et des réponses DNS :**

Les requêtes et les réponses DNS suivent une structure commune, et elles comprennent des en-têtes ainsi que des sections qui transportent des informations spécifiques. Voici la structure typique des requêtes et des réponses DNS :

En-tête DNS :

ID (Identifiant) : Un numéro unique permettant d'associer les réponses aux requêtes correspondantes.

QR (Query/Response) : Un seul bit indiquant s'il s'agit d'une requête (0) ou d'une réponse (1).

Opcode : Un champ de 4 bits définissant le type d'opération (standard, inverse, etc.).

AA (Authoritative Answer) : Un seul bit indiquant si la réponse provient d'un serveur DNS autorisé.

TC (Truncated) : Un seul bit indiquant si la réponse est tronquée en raison de sa longueur.

RD (Recursion Desired) : Un seul bit indiquant si le client souhaite une résolution récursive.

RA (Recursion Available) : Un seul bit indiquant si le serveur DNS supporte la résolution récursive.

Z (Reserved) : Trois bits réservés à l'usage futur.

RCODE (Response Code) : Un champ de 4 bits indiquant le résultat de la requête (réussie, échec, etc.).

QDCOUNT (Question Count) : Le nombre de questions dans la requête.

ANCOUNT (Answer Count) : Le nombre de réponses dans la réponse.

NSCOUNT (Name Server Count) : Le nombre de serveurs de noms dans la réponse.

ARCOUNT (Additional Record Count) : Le nombre d'enregistrements supplémentaires dans la réponse.

**X. Réflexion sur le DNS :**

Pour un utilisateur, le système DNS (Domain Name System) sert principalement à deux fonctionnalités essentielles :

- Faciliter l'accès aux sites Web et aux services en ligne : Le DNS permet aux utilisateurs de saisir des noms de domaine conviviaux (comme " <https://www.frameip.com/>") dans leur navigateur au lieu de devoir mémoriser des adresses IP numériques compliquées. Il traduit ces noms de domaine en adresses IP, permettant ainsi la navigation sur le Web et l'accès à des services en ligne de manière conviviale.

- Assurer la communication par e-mail : Le DNS est également crucial pour le système de messagerie électronique. Il permet de trouver les serveurs de messagerie (enregistrements MX) associés à un nom de domaine. Cela garantit que les e-mails sont correctement acheminés vers les serveurs de messagerie appropriés.

Pour un serveur, le DNS offre également des fonctionnalités cruciales. Voici comment le DNS est utilisé du côté serveur :

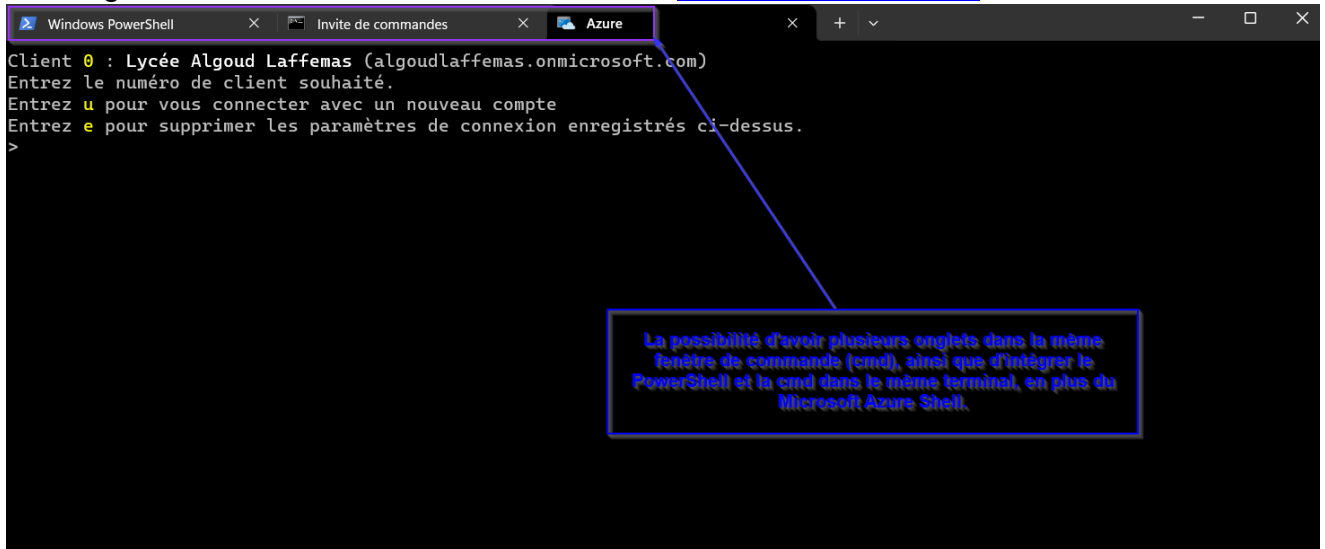
- Résolution des noms de domaine : Les serveurs utilisent le DNS pour résoudre les noms de domaine en adresses IP. Cela leur permet de communiquer avec d'autres serveurs et de fournir des services aux clients via Internet.
- Enregistrements DNS personnalisés : Les serveurs peuvent utiliser des enregistrements DNS pour définir des alias (CNAME), des serveurs de messagerie (MX), des serveurs de noms (NS), etc. Ces enregistrements personnalisés permettent de configurer les services offerts par le serveur.
- Résolution de noms internes : Les serveurs utilisent le DNS pour résoudre les noms de domaine internes à leur réseau, ce qui facilite la communication entre les différents services et dispositifs au sein de l'infrastructure d'une entreprise.
- Gestion de la sécurité : Le DNS peut être utilisé pour renforcer la sécurité en mettant en place DNSSEC pour vérifier l'authenticité des réponses DNS et en empêchant la falsification de données (DNS spoofing).
- Mise à jour dynamique : Les serveurs peuvent prendre en charge la mise à jour dynamique des enregistrements DNS, ce qui est utile dans des environnements où les adresses IP des dispositifs changent fréquemment, comme dans le cas de serveurs DHCP.
- Gestion des domaines : Les serveurs DNS autorisés sont responsables de la gestion des domaines et de leurs enregistrements. Ils peuvent ajouter, supprimer ou modifier des enregistrements pour gérer le domaine.
- Diagnostic des problèmes : Les serveurs DNS peuvent générer des journaux qui aident à diagnostiquer les problèmes liés à la résolution des noms. Cela facilite la maintenance et la résolution des problèmes.

En résumé, pour un serveur, le DNS est essentiel pour la résolution des noms de domaine, la configuration des services, la gestion de la sécurité, la répartition de la charge et la communication au sein de l'infrastructure. C'est un élément central de la connectivité et des services Internet.

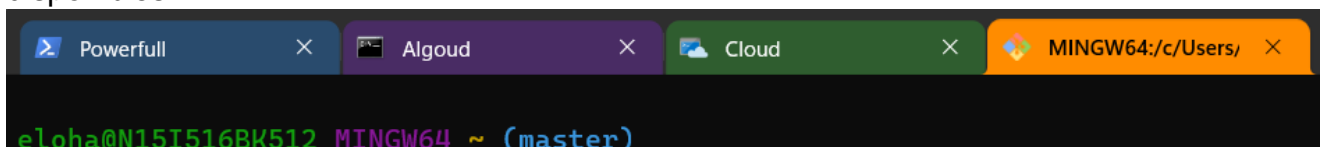
#### **i) Windows terminal :**

Le Windows terminal est nettement supérieur pour moi par rapport à une cmd classique, car il offre la possibilité d'avoir plusieurs onglets dans la même fenêtre de commande (cmd) tout

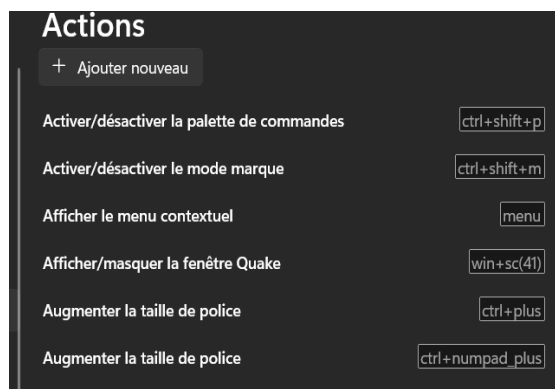
en intégrant le PowerShell, la cmd, et même le [Microsoft Azure Shell](#).



Il intègre également Git, un outil permettant de configurer un dépôt GitHub. De plus, il offre la possibilité d'ouvrir la session précédente avec l'historique des commandes, ce qui s'avère utile pour un administrateur. Vous avez également la possibilité de configurer les onglets disponibles :



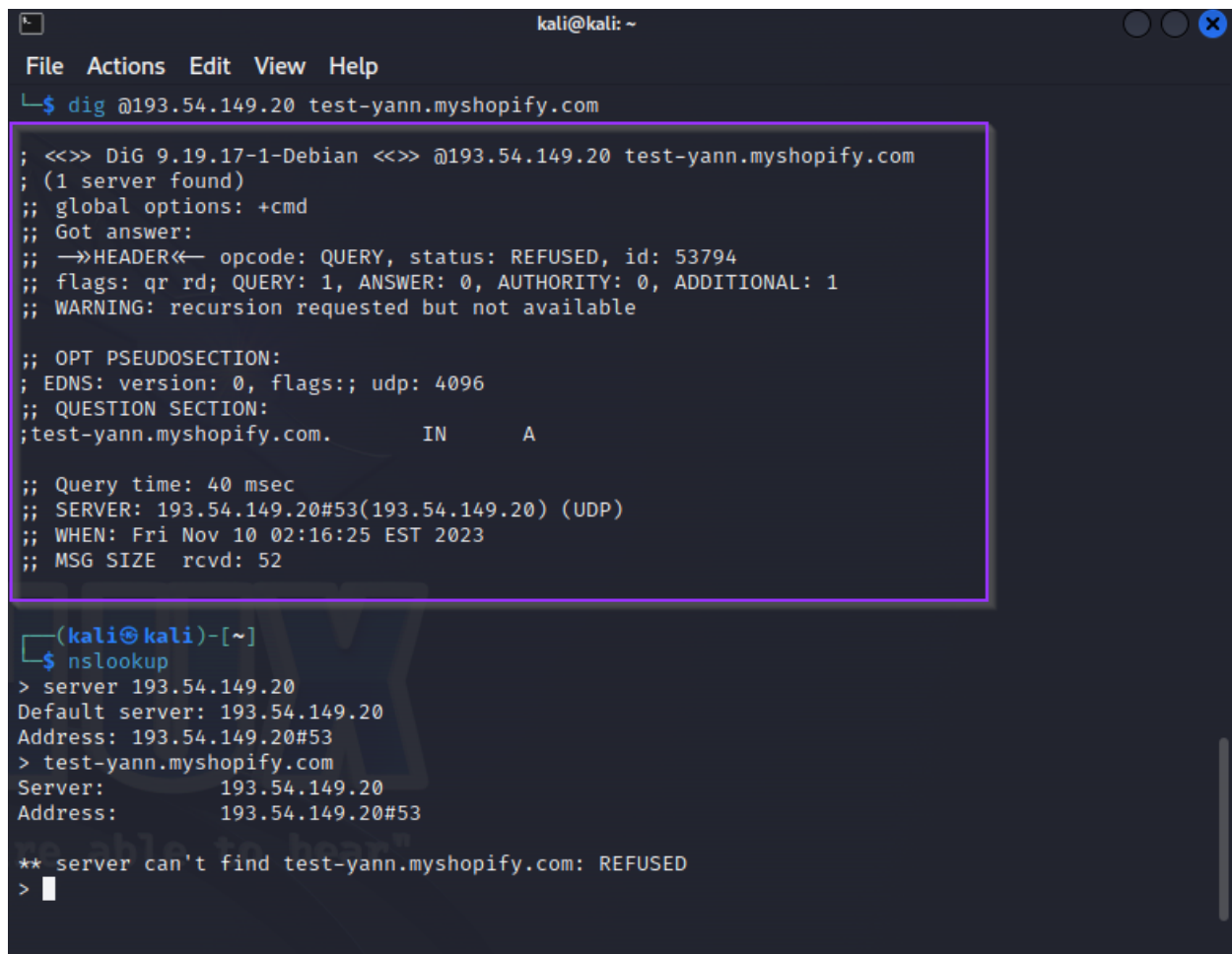
De plus, la possibilité de configurer des raccourcis, offrant ainsi un gain de temps considérable au quotidien.



## XI. [Différent outils linux pour l'analyse DNS](#)

Nous allons étudier les différents outils Dig et nslookup. Dig est plus puissant et flexible, ce qui le rend idéal pour les utilisateurs avancés et les tâches complexes. En revanche, nslookup reste simple et convivial, adapté aux utilisateurs moins expérimentés ou pour des opérations basiques de résolution de noms.

Démonstration :



```
kali@kali: ~  
File Actions Edit View Help  
$ dig @193.54.149.20 test-yann.myshopify.com  
  
; <<>> DiG 9.19.17-1-Debian <<>> @193.54.149.20 test-yann.myshopify.com  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; -->HEADER<-- opcode: QUERY, status: REFUSED, id: 53794  
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1  
;; WARNING: recursion requested but not available  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;test-yann.myshopify.com.      IN      A  
  
;; Query time: 40 msec  
;; SERVER: 193.54.149.20#53(193.54.149.20) (UDP)  
;; WHEN: Fri Nov 10 02:16:25 EST 2023  
;; MSG SIZE   rcvd: 52  
  
(kali@kali)-[~]  
$ nslookup  
> server 193.54.149.20  
Default server: 193.54.149.20  
Address: 193.54.149.20#53  
> test-yann.myshopify.com  
Server:      193.54.149.20  
Address:     193.54.149.20#53  
  
** server can't find test-yann.myshopify.com: REFUSED  
>
```

Plusieurs requêtes DNS ont été effectuées pour le domaine "test-yann.myshopify.com" en utilisant les commandes **dig** et **nslookup**. Les résultats indiquent que le serveur DNS situé à l'adresse IP 193.54.149.20 refuse la requête avec le statut "REFUSED", indiquant un refus de répondre à la demande.

Dans notre exemple le serveur interrogé est à l'adresse IP 193.54.149.20.

L'adresse recherchée est pour le domaine "test-yann.myshopify.com".

Et nous voyons que la commande dig semble fournir plus d'informations détaillées, notamment en affichant le temps de requête, les options EDNS, et d'autres détails.

```
kali@kali: ~  
File Actions Edit View Help  
└─$ dig @8.8.8.8 test-yann.myshopify.com  
  
; <<>> DiG 9.19.17-1-Debian <<>> @8.8.8.8 test-yann.myshopify.com  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 46744  
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
;test-yann.myshopify.com.      IN      A  
  
;; ANSWER SECTION:  
test-yann.myshopify.com. 3600    IN      CNAME   shops.myshopify.com.  
shops.myshopify.com.    60      IN      A       23.227.38.74  
  
;; Query time: 56 msec  
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)  
;; WHEN: Fri Nov 10 02:38:55 EST 2023  
;; MSG SIZE rcvd: 88  
  
(kali@kali)-[~]  
└─$ nslookup  
> server 8.8.8.8  
Default server: 8.8.8.8  
Address: 8.8.8.8#53  
> test-yann.myshopify.com  
Server:      8.8.8.8  
Address:     8.8.8.8#53  
  
Non-authoritative answer:  
test-yann.myshopify.com canonical name = shops.myshopify.com.  
Name:   shops.myshopify.com  
Address: 23.227.38.74  
> █
```

J'ai remarqué après que vous aviez délibérément introduit une erreur dans la requête que vous nous aviez fournie, comportant une erreur. J'ai donc réeffectué la requête et obtenu de meilleurs résultats.

## XII. Outils delv :

Installation de l'outils Delv

```
(kali@kali)-[~]  
└─$ sudo apt-get install bind9utils  
  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  bind9-utils  
The following NEW packages will be installed:  
  bind9-utils bind9utils  
0 upgraded, 2 newly installed, 0 to remove and 721 not upgraded.  
Need to get 684 kB of archives.  
After this operation, 1,165 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
0% [Connecting to http.kali.org]^X@sS
```

La commande `delv` est plus complexe à utiliser qu'une commande de type `nslookup` ou `dig`. Si elle est mal configurée, elle interrogera notre DNS local, et nous sommes obligés de forcer l'utilisation de Google à la fin. Les options sont indispensables pour obtenir un résultat. Voici un exemple de ce qui se passe si l'analyse est mal effectuée :

```
(kali㉿kali)-[~]
$ delv 8.8.8.8 frameip.fr
;; validating ./SOA: got insecure response; parent indicates it should be secure
;; validating ./SOA: got insecure response; parent indicates it should be secure
;; no valid RRSIG resolving '8/DS/IN': 172.31.1.4#53
;; validating ./SOA: got insecure response; parent indicates it should be secure
;; no valid RRSIG resolving '8/DS/IN': 172.31.1.6#53
;; broken trust chain resolving '8.8.8.8/A/IN': 172.31.1.6#53
;; resolution failed: broken trust chain

(kali㉿kali)-[~]
$ delv trustee.ietf.org @1.1.1.1

;; resolution failed: ncache nxrrset
; negative response, fully validated
; trustee.ietf.org.      1800      IN      \-A      ;-$NXRRSET
; ietf.org. SOA jill.ns.cloudflare.com. dns.cloudflare.com. 2325056235 10000 2400 604800 1800
; ietf.org. RRSIG TYPE43016 ...
; trustee.ietf.org. RRSIG TYPE43016 ...
; trustee.ietf.org. NSEC \000.trustee.ietf.org. RRSIG NSEC TYPE65283
```

Et voici comment il faut s'y prendre pour obtenir des résultats convenables :

```
delv +cd +dnssec trustee.ietf.org @8.8.8.8
```

```
(kali㉿kali)-[~]
$ delv +cd +dnssec trustee.ietf.org @8.8.8.8

; fully validated
trustee.ietf.org.      300      IN      A      104.16.44.99
trustee.ietf.org.      300      IN      A      104.16.45.99
trustee.ietf.org.      300      IN      RRSIG   A 13 3 300 20231111091425 20231109071425 34505 ietf.org.
ct8f+cV9D1L42LHRpwpZQTtRqpE1iCqJbLKT4fYhH+FUXvV0/bp7NAr4 zKte9BAONl5Hc/UWSow5GaRdiiGcoA=

(kali㉿kali)-[~]
$ delv +cd +dnssec frameip.fr @8.8.8.8

; unsigned answer
frameip.fr.           10800    IN      A      176.57.240.169
```



On peut également utiliser un outil web pour compléter notre recherche :

Domain Name:

### Analyzing DNSSEC problems for [trustee.ietf.org](https://trustee.ietf.org)

|          |   |
|----------|---|
| .        | <ul style="list-style-type: none"><li>✓ Found 2 DNSKEY records for .</li><li>✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP</li><li>✓ Found 1 RRSIGs over DNSKEY RRset</li><li>✓ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset</li></ul>   |
| org      | <ul style="list-style-type: none"><li>✓ Found 1 DS records for org in the . zone</li><li>✓ DS=26974/SHA-256 has algorithm RSASHA256</li><li>✓ Found 1 RRSIGs over DS RRset</li><li>✓ RRSIG=46780 and DNSKEY=46780 verifies the DS RRset</li><li>✓ Found 3 DNSKEY records for org</li><li>✓ DS=26974/SHA-256 verifies DNSKEY=26974/SEP</li><li>✓ Found 1 RRSIGs over DNSKEY RRset</li><li>✓ RRSIG=26974 and DNSKEY=26974/SEP verifies the DNSKEY RRset</li></ul>   |
| ietf.org | <ul style="list-style-type: none"><li>✓ Found 1 DS records for ietf.org in the org zone</li><li>✓ DS=2371/SHA-256 has algorithm ECDSAP256SHA256</li><li>✓ Found 1 RRSIGs over DS RRset</li><li>✓ RRSIG=3093 and DNSKEY=3093 verifies the DS RRset</li><li>✓ Found 2 DNSKEY records for ietf.org</li><li>✓ DS=2371/SHA-256 verifies DNSKEY=2371/SEP</li><li>✓ Found 1 RRSIGs over DNSKEY RRset</li><li>✓ RRSIG=2371 and DNSKEY=2371/SEP verifies the DNSKEY RRset</li><li>✓ ken.ns.cloudflare.com is authoritative for trustee.ietf.org</li><li>✓ trustee.ietf.org A RR has value 104.16.45.99</li><li>✓ Found 1 RRSIGs over A RRset</li><li>✓ RRSIG=34505 and DNSKEY=34505 verifies the A RRset</li></ul> |
| ietf.org | <ul style="list-style-type: none"><li>✓ jill.ns.cloudflare.com is authoritative for trustee.ietf.org</li><li>✓ trustee.ietf.org A RR has value 104.16.45.99</li><li>✓ Found 1 RRSIGs over A RRset</li><li>✓ RRSIG=34505 and DNSKEY=34505 verifies the A RRset</li></ul>   |



**XIII. Exercice 6 : Analyse approfondie des échanges sous Packet Tracer**

| Simulation Panel |           |              |              |      |
|------------------|-----------|--------------|--------------|------|
| Event List       |           |              |              |      |
| Vis.             | Time(sec) | Last Device  | At Device    | Type |
|                  | 0.000     | --           | Sales        | DNS  |
|                  | 0.000     | --           | Sales        | ARP  |
|                  | 0.001     | Sales        | IP Phone0    | ARP  |
|                  | 0.002     | IP Phone0    | S4           | ARP  |
|                  | 0.003     | S4           | BranchServer | ARP  |
|                  | 0.003     | S4           | IP Phone1    | ARP  |
|                  | 0.003     | S4           | Laser        | ARP  |
|                  | 0.003     | S4           | Wireless AP  | ARP  |
|                  | 0.003     | S4           | R4           | ARP  |
|                  | 0.004     | Wireless AP  | Guest        | ARP  |
|                  | 0.004     | BranchServer | S4           | ARP  |
|                  | 0.004     | IP Phone1    | Accounting   | ARP  |
|                  | 0.004     | Wireless AP  | Smart Phone  | ARP  |
|                  | 0.005     | S4           | IP Phone0    | ARP  |
|                  | 0.006     | IP Phone0    | Sales        | ARP  |
|                  | 0.006     | --           | Sales        | DNS  |
|                  | 0.007     | Sales        | IP Phone0    | DNS  |
|                  | 0.008     | IP Phone0    | S4           | DNS  |
|                  | 0.009     | S4           | BranchServer | DNS  |

Reset Simulation

☒ Constant Delay

Captured 116.26

Play Controls

La première trame qui est envoyée est une trame de type DNS multicast.

PDU Information at Device: Sales

OSI Model

Outbound PDU Details

At Device: Sales  
Source: Sales  
Destination: 172.16.0.3

In Layers

Layer7  
Layer6  
Layer5  
Layer4  
Layer3  
Layer2  
Layer1

Out Layers

Layer 7: DNS  
Layer6  
Layer5  
Layer 4: UDP Src Port: 1025, Dst Port: 53  
Layer 3: IP Header Src. IP: 172.16.0.9,  
Dest. IP: 172.16.0.3  
Layer 2:  
Layer1

1. The DNS client sends an A DNS query to the DNS server.

Challenge Me

<< Previous Layer

Next Layer >>

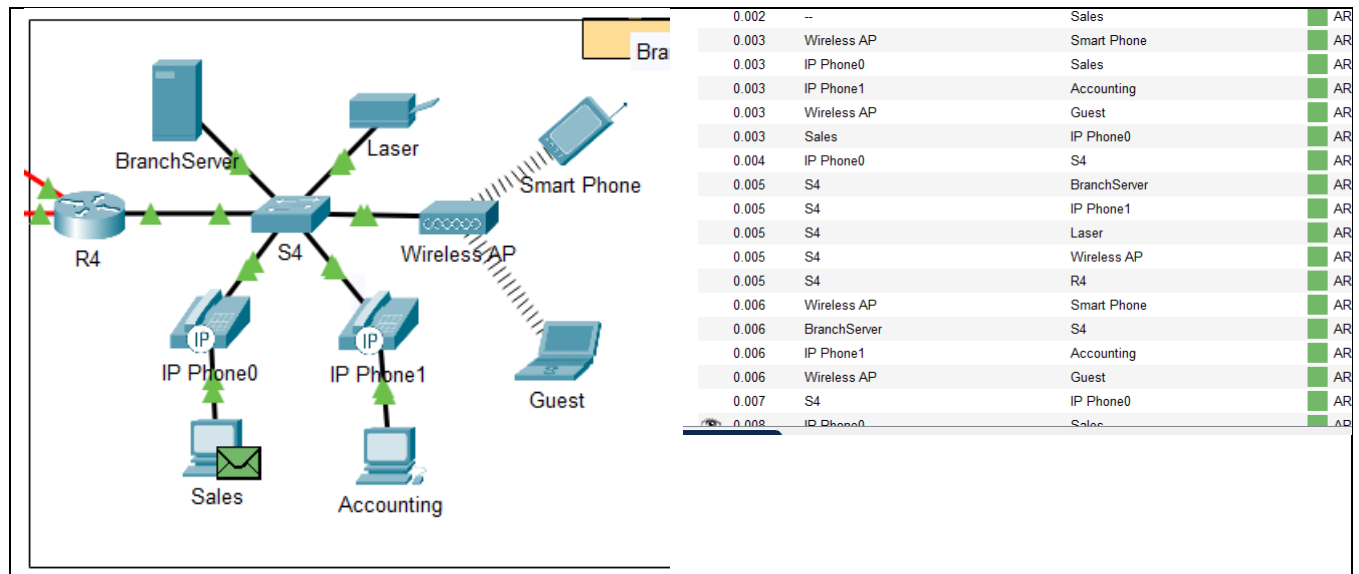
Toutes les prochaines trames sont de type Arp qui servent à l'identification du réseau

Layer 4: UDP Src Port: 1025, Dst Port: 53

Malheureusement, dans les premiers paquets, l'adresse MAC manque, ce qui nous empêche de contacter directement le DNS. C'est pourquoi des trames ARP sont envoyées pour identifier le réseau.

Layer 2: Ethernet II Header  
00D0.D3D7.5B29 >> 0060.5C93.13A4

On peut voir que les trames ARP ont traversé tous les éléments du réseau Branch pour associer chaque élément à une adresse MAC :



Si on fait défiler jusqu'à ce que le périphérique cible soit Branch Server :

PDU Information at Device: BranchServer

OSI Model Inbound PDU Details Outbound PDU Details

At Device: BranchServer  
Source: Sales  
Destination: 172.16.0.3

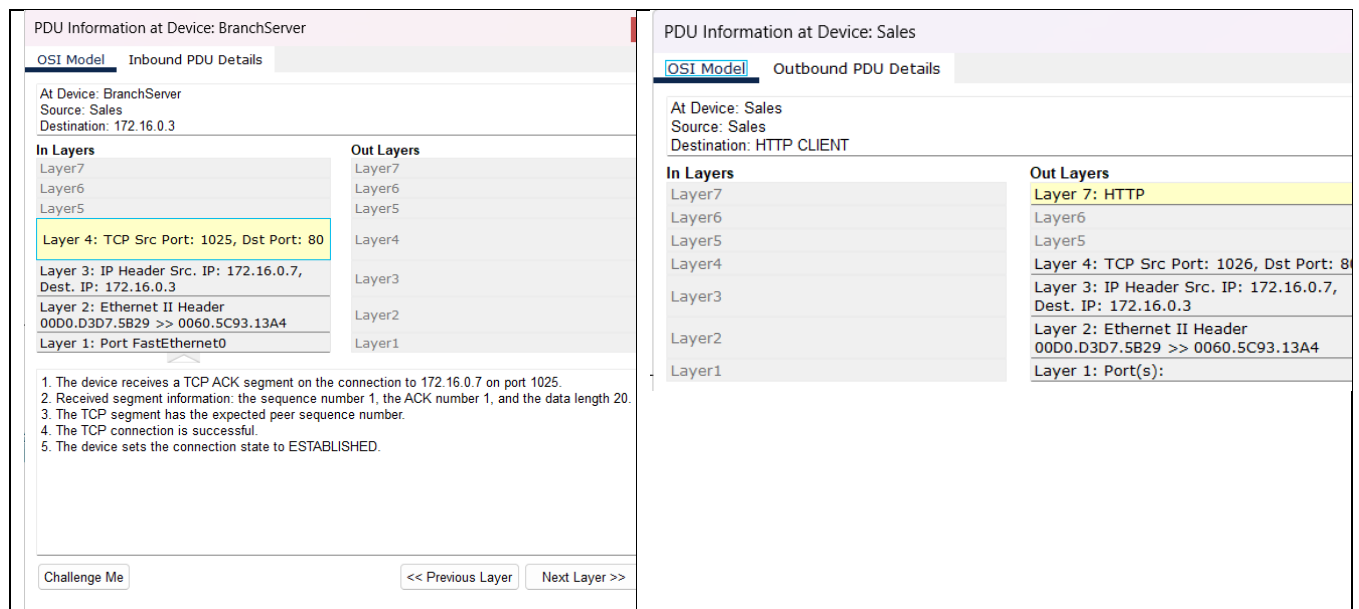
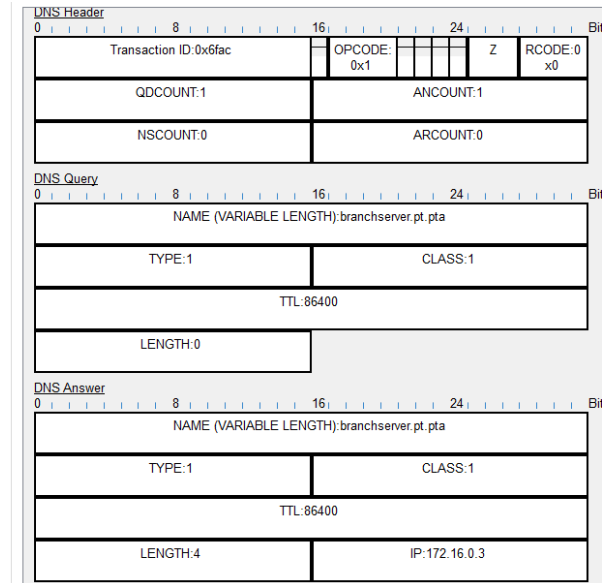
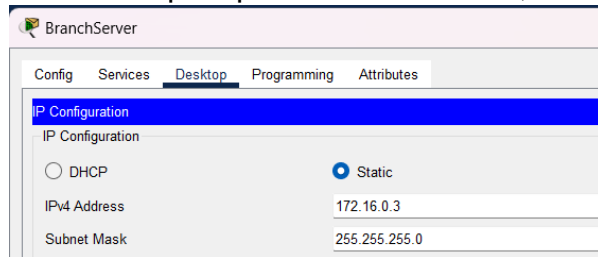
| In Layers   | Out Layers  |
|---|---|
| Layer 7: DNS  | Layer 7: DNS  |
| Layer 6   | Layer 6   |
| Layer 5   | Layer 5   |
| Layer 4: UDP Src Port: 1025, Dst Port: 53                       | Layer 4: UDP Src Port: 53, Dst Port: 1025                       |
| Layer 3: IP Header Src. IP: 172.16.0.7, Dest. IP: 172.16.0.3    | Layer 3: IP Header Src. IP: 172.16.0.3, Dest. IP: 172.16.0.7    |
| Layer 2: Ethernet II Header<br>00D0.D3D7.5B29 >> 0060.5C93.13A4 | Layer 2: Ethernet II Header<br>0060.5C93.13A4 >> 00D0.D3D7.5B29 |
| Layer 1: Port FastEthernet0                                     | Layer 1: Port(s): FastEthernet0                                 |

1. FastEthernet0 receives the frame.

Challenge Me << Previous Layer Next Layer >>

Le serveur DNS trouve une adresse IP associée à ce domaine branchserver.pt.pta. Il renvoie une réponse.

L'adresse qui répond est 172.16.0.3, celle du serveur.



Une requête HTTP traverse plusieurs couches du modèle OSI pour atteindre sa destination. Voici une explication brève de l'utilisation des couches 7, 4, 3, 2, et 1 dans le modèle OSI pour une requête HTTP :

- Couche 7 (Application) : C'est la couche où se situe le protocole HTTP. La requête HTTP est créée au niveau de l'application, définissant la manière dont les données doivent être présentées et interprétées.
- Couche 4 (Transport) : Le protocole de transport utilisé pour les requêtes HTTP est généralement TCP (Transmission Control Protocol). La couche de transport assure la fiabilité de la transmission en établissant, maintenant, et terminant des connexions entre les points finaux.
- Couche 3 (Réseau) : Cette couche gère la transmission des paquets à travers le réseau. Les adresses IP sont utilisées pour router les paquets de la source à la destination. La requête HTTP est encapsulée dans des paquets IP pour être transportée sur le réseau.
- Couche 2 (Liaison de données) : À ce niveau, les données sont encapsulées dans des trames. Cette couche gère l'accès au support physique (comme l'Ethernet) et fournit des mécanismes de détection d'erreur.

- Couche 1 (Physique) : Cette couche concerne le support physique réel utilisé pour la transmission des données, tel que les câbles, les commutateurs, et autres composants matériels. Les bits sont convertis en signaux électriques, optiques, ou radiofréquences, selon le support physique.

En résumé, une requête HTTP traverse ces différentes couches du modèle OSI car chaque couche a une fonction spécifique dans le processus de transmission d'informations à travers un réseau, depuis la création de la requête au niveau de l'application jusqu'à la transmission physique des données.

PDU Information at Device: Sales

OSI Model Inbound PDU Details

At Device: Sales  
Source: Sales  
Destination: HTTP CLIENT

**In Layers**

- Layer 7: HTTP
- Layer 6
- Layer 5
- Layer 4: TCP Src Port: 80, Dst Port: 1026
- Layer 3: IP Header Src. IP: 172.16.0.3, Dest. IP: 172.16.0.7
- Layer 2: Ethernet II Header 0060.5C93.13A4 >> 00D0.D3D7.5B29
- Layer 1: Port FastEthernet0

**Out Layers**

- Layer 7
- Layer 6
- Layer 5
- Layer 4
- Layer 3
- Layer 2
- Layer 1

Le client HTTP reçoit une réponse HTTP du serveur. Il affiche la page dans le navigateur web.

#### j) 2e partie : Inspecter le trafic interréseau au bureau central

Contrairement à la requête précédente, il n'y a pas de recherche ARP car le réseau a déjà été identifié.

| Event List |           |              |              |      |
|------------|-----------|--------------|--------------|------|
| Vis.       | Time(sec) | Last Device  | At Device    | Type |
|            | 0.000     | --           | Sales        | DNS  |
|            | 0.001     | Sales        | IP Phone0    | DNS  |
|            | 0.002     | IP Phone0    | S4           | DNS  |
|            | 0.003     | S4           | BranchServer | DNS  |
|            | 0.004     | BranchServer | S4           | DNS  |
|            | 0.005     | S4           | IP Phone0    | DNS  |
|            | 0.006     | IP Phone0    | Sales        | DNS  |

PDU Information at Device: Sales

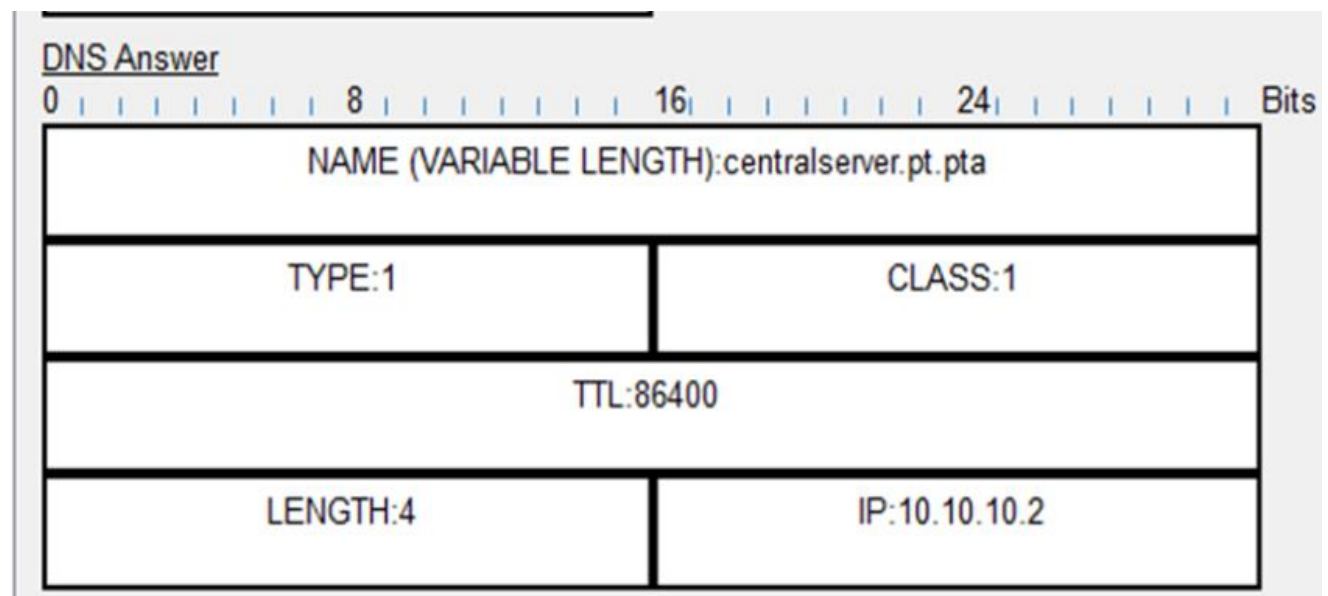
OSI Model    Inbound PDU Details

At Device: Sales  
Source: Sales  
Destination: 172.16.0.3

| In Layers   | Out Layers |
|---|------------|
| Layer 7: DNS  | Layer7     |
| Layer6  | Layer6     |
| Layer5  | Layer5     |
| Layer 4: UDP Src Port: 53, Dst Port: 1025                       | Layer4     |
| Layer 3: IP Header Src. IP: 172.16.0.3, Dest. IP: 172.16.0.9    | Layer3     |
| Layer 2: Ethernet II Header<br>0060.5C93.13A4 >> 00D0.D3D7.5B29 | Layer2     |
| Layer 1: Port FastEthernet0                                     | Layer1     |

1. The DNS client receives an A DNS response.  
2. The received A DNS response does not contain a resolved IP address for the queried domain.

Ensuite, le serveur DNS reçoit une réponse où il résout le DNS.



#### XIV. Étude sur le DHCP

DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l'administration d'un réseau. On voit généralement le protocole DHCP comme distribuant des adresses IP, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (on peut effectivement installer complètement un ordinateur, et c'est beaucoup

plus rapide que de le faire en à la main). Cette dernière possibilité est très intéressante pour la maintenance de gros parcs machines. Les versions actuelles des serveurs DHCP fonctionnent pour [IPv4](#) (adresses IP sur 4 octets). Une spécification pour [IPv6](#) (adresses IP sur 16 octets) est en cours de développement par l'IETF.

Le protocole DHCP (Dynamic Host Configuration Protocol) opère à la couche applicative du modèle OSI. Il utilise la couche applicative car il s'agit d'un protocole réseau qui fournit des informations de configuration aux périphériques sur un réseau. La couche applicative est la couche la plus élevée du modèle OSI et englobe les protocoles qui permettent la communication entre les applications sur des appareils différents.

DHCP est conçu pour simplifier la configuration des adresses IP et d'autres paramètres réseau sur les périphériques clients. En utilisant la couche applicative, il peut transmettre des informations telles que l'adresse IP, le masque de sous-réseau, la passerelle par défaut, les serveurs DNS, etc. Ces informations sont essentielles pour permettre aux appareils de communiquer efficacement sur un réseau.

#### **k) RFC**

La RFC (Request for Comments) qui décrit le protocole DHCP est la RFC 2131. Elle a été publiée en mars 1997. Cette RFC spécifie la version 4 du protocole DHCP (DHCPv4), qui est la version la plus couramment utilisée pour la configuration dynamique des adresses IP sur les réseaux IPv4.

Le protocole DHCP s'appuie sur le protocole Bootstrap Protocol (BOOTP). BOOTP est un protocole plus ancien qui a été conçu pour fournir des configurations réseau initiales aux clients lorsqu'ils démarrent (bootstrap) sur un réseau. DHCP a évolué à partir de BOOTP pour offrir une configuration dynamique et étendue, permettant notamment la réattribution dynamique des adresses IP.

Bien que DHCP ait évolué à partir de BOOTP, BOOTP est encore utilisé dans certaines situations spécifiques. Par exemple, dans le processus d'amorçage réseau, où un périphérique démarre et cherche une adresse IP initiale pour se connecter au réseau. Dans ce contexte, BOOTP peut être utilisé pour fournir une adresse IP initiale aux clients lors du démarrage, mais DHCP est souvent préféré pour ses fonctionnalités plus avancées de configuration dynamique. Ainsi, bien que BOOTP soit moins couramment utilisé que DHCP, il reste pertinent dans des scénarios spécifiques tels que l'amorçage réseau.












#### **l) Différent type d'allocation :**

Les trois types d'allocations possibles pour les adresses IP dans le contexte du protocole DHCP sont :

- Allocation Dynamique : Dans ce mode, une adresse IP est attribuée à un client par le serveur DHCP pour une durée déterminée, appelée bail. Le client peut renouveler le bail avant son expiration.

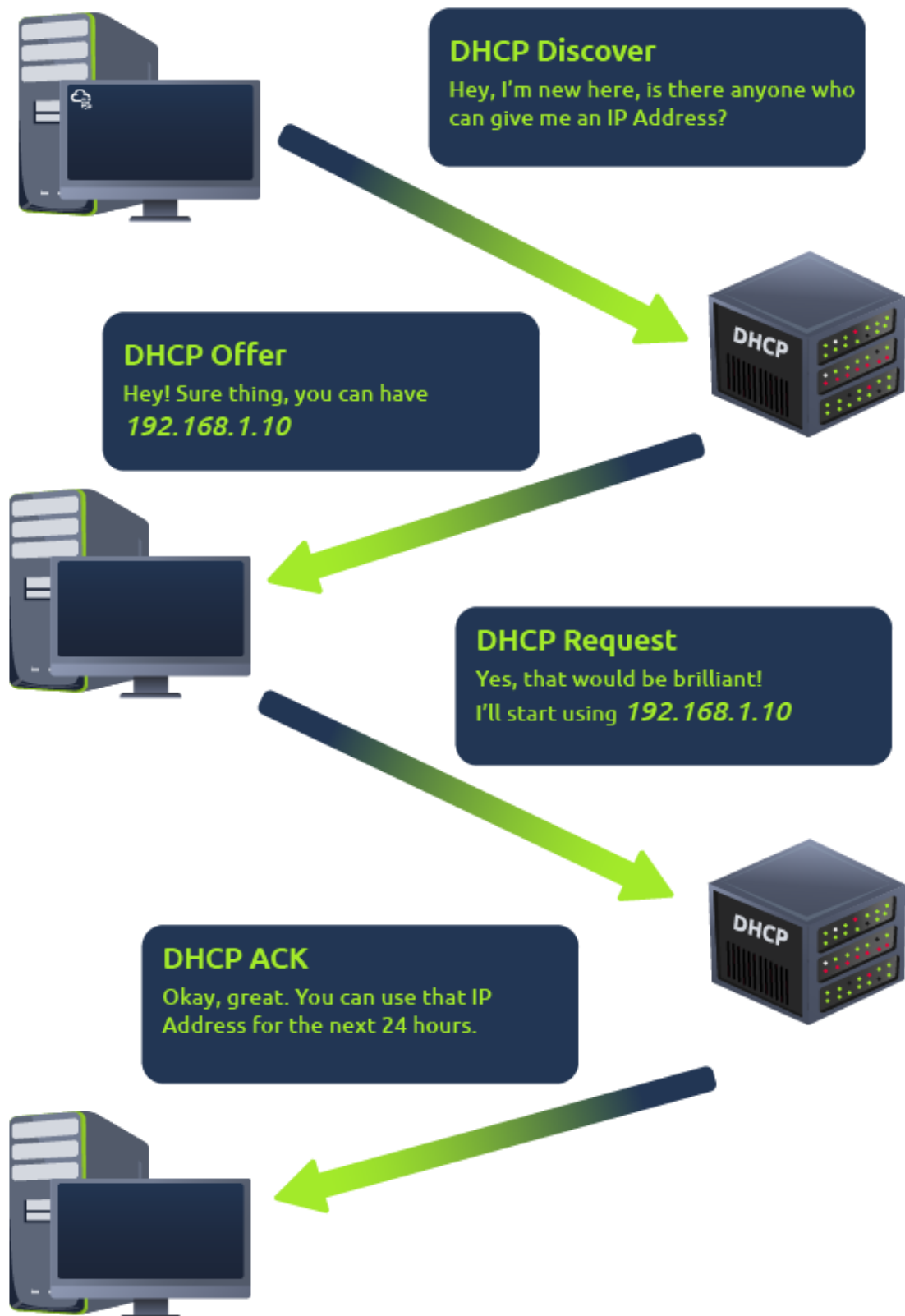
- Allocation Statique : Une adresse IP spécifique est attribuée à un client de manière permanente. Contrairement à l'allocation dynamique, l'adresse IP ne change pas à chaque nouvelle connexion du client. Cela nécessite une configuration manuelle sur le serveur DHCP.
- Allocation Automatique : Dans ce mode, le serveur DHCP attribue une adresse IP au client pour une durée déterminée, mais contrairement à l'allocation dynamique, le client ne renouvelle pas automatiquement son bail. Si le client se reconnecte, il peut recevoir une adresse IP différente.

Ces différentes méthodes d'allocation offrent une flexibilité dans la gestion des adresses IP au sein d'un réseau en fonction des besoins spécifiques de l'environnement.

| Vis.  | Time(sec) | Last Device | At Device | Type   |
|---|-----------|-------------|-----------|--|
|   | 0.000     | --          | Laptop0   |  ICMP |
|   | 0.000     | --          | PC0       |  DHCP |
|   | 0.001     | PC0         | Switch0   |  DHCP |
|   | 0.002     | Switch0     | Server0   |  DHCP |
|   | 0.002     | --          | Server0   |  ICMP |
|   | 0.002     | Switch0     | Printer0  |  DHCP |
|   | 0.002     | Switch0     | Laptop0   |  DHCP |
|   | 0.002     | Switch0     | Router0   |  DHCP |
|   | 0.002     | --          | Server0   |  ARP  |
|  | 0.003     | Server0     | Switch0   |  ARP  |



Les trames DHCP fonctionnent de la manière suivante :



1<sup>er</sup> paquet :

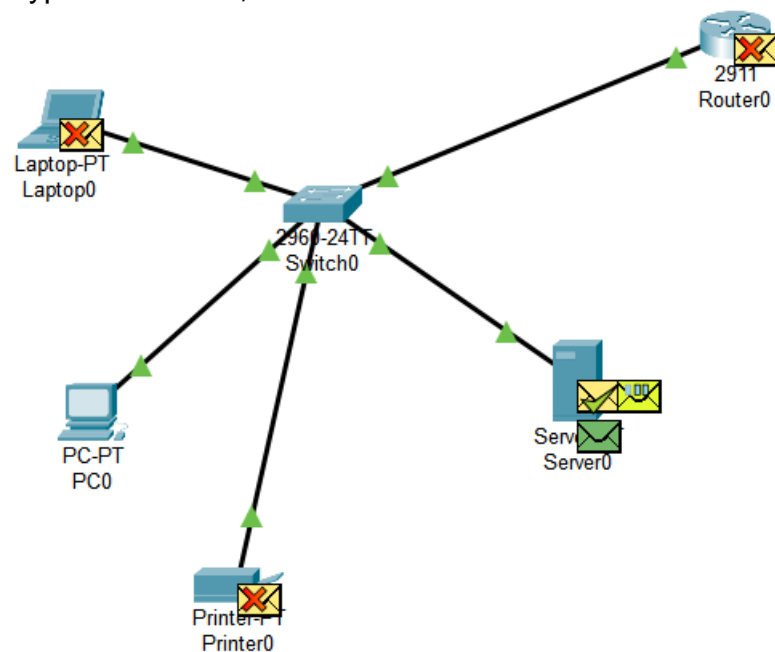
PDU Information at Device: PC0

At Device: PC0  
Source: PC0  
Destination: 255.255.255.255

| In Layers | Out Layers   |
|-----------|--|
| Layer7    | Layer 7: DHCP Packet Server: 0.0.0.0, Client: 0.0.0.0          |
| Layer6    | Layer6   |
| Layer5    | Layer5   |
| Layer4    | Layer 4: UDP Src Port: 68, Dst Port: 67                        |
| Layer3    | Layer 3: IP Header Src. IP: 0.0.0.0, Dest. IP: 255.255.255.255 |
| Layer2    | Layer 2: Ethernet II Header 0050.0FCB.6ABA >> FFFF.FFFF.FFFF   |
| Layer1    | Layer 1: Port(s): FastEthernet0                                |

1. The DHCP client constructs a Discover packet and sends it out.

Le premier paquet est de type "discover" ; notre ordinateur découvre les réseaux via une



diffusion en broadcast.

Ensuite, chaque périphérique du réseau reçoit et transmet la trame jusqu'à ce qu'elle trouve un serveur DHCP.

PDU Information at Device: Router0

OSI Model Inbound PDU Details

At Device: Router0  
Source: PC0  
Destination: 255.255.255.255

| In Layers  | Out Layers |
|--|------------|
| Layer 7: DHCP Packet Server: 0.0.0.0, Client: 0.0.0.0          | Layer7     |
| Layer6   | Layer6     |
| Layer5   | Layer5     |
| Layer 4: UDP Src Port: 68, Dst Port: 67                        | Layer4     |
| Layer 3: IP Header Src. IP: 0.0.0.0, Dest. IP: 255.255.255.255 | Layer3     |
| Layer 2: Ethernet II Header 0050.0FCB.6ABA >> FFFF.FFFF.FFFF   | Layer2     |
| Layer 1: Port GigabitEthernet0/0                               | Layer1     |

1. The packet is a DHCP packet. The DHCP server processes it.  
2. The DHCP server received a DHCP Discover packet.  
3. The DHCP server does not have a pool configured for the received port. It drops the packet.

PDU Information at Device: Router0

OSI Model Inbound PDU Details

At Device: Router0  
Source: PC0  
Destination: 255.255.255.255

| In Layers  | Out Layers |
|--|------------|
| Layer 7: DHCP Packet Server: 0.0.0.0, Client: 0.0.0.0          | Layer7     |
| Layer6   | Layer6     |
| Layer5   | Layer5     |
| Layer 4: UDP Src Port: 68, Dst Port: 67                        | Layer4     |
| Layer 3: IP Header Src. IP: 0.0.0.0, Dest. IP: 255.255.255.255 | Layer3     |
| Layer 2: Ethernet II Header 0050.0FCB.6ABA >> FFFF.FFFF.FFFF   | Layer2     |
| Layer 1: Port GigabitEthernet0/0                               | Layer1     |

1. The packet is a DHCP packet. The DHCP server processes it.  
2. The DHCP server received a DHCP Discover packet.  
3. The DHCP server does not have a pool configured for the received port. It drops the packet.

1. Le paquet est un paquet DHCP. Le serveur DHCP le traite.
2. Le serveur DHCP a reçu un paquet DHCP Discover.
3. Le serveur DHCP n'a pas de pool configuré pour le port reçu. Il rejette le paquet.

#### m) Risque DHCP :

Le problème avec le mode DHCP réside dans le fait que le poste qui demande une adresse IP via DHCP le fait en diffusant une requête de broadcast. Cela signifie que n'importe quel élément du réseau peut identifier cette demande et potentiellement fournir une adresse IP.

Vous aurez plus de détails dans la partie suivante avec un exemple pratique.

**n) Risque configuration classic :**

Avec une configuration DHCP classique, plusieurs problèmes peuvent survenir, notamment

- Épuisement de la plage d'adresses IP : Si la plage d'adresses IP configurée dans le pool DHCP est trop petite pour le nombre de périphériques sur le réseau, il peut y avoir une pénurie d'adresses IP disponibles, entraînant des problèmes de connectivité pour les nouveaux périphériques.
- Conflits d'adresses IP : Il est possible que deux périphériques se voient attribuer la même adresse IP, provoquant des conflits et des perturbations dans le réseau.
- Durée de bail inappropriée : Si la durée de bail (temps pendant lequel une adresse IP est attribuée à un périphérique) est configurée de manière inappropriée, cela peut entraîner des renouvellements excessifs ou des interruptions de connexion.
- Problèmes de routage : Des erreurs dans la configuration du serveur DHCP peuvent entraîner la fourniture de paramètres de routage incorrects, perturbant la connectivité du réseau.
- Serveur DHCP indisponible : Si le serveur DHCP est hors service, les périphériques ne pourront pas obtenir de configuration réseau, ce qui peut entraîner des problèmes de connectivité.
- Attaques DHCP : Des attaques telles que les attaques de déni de service (DoS) visant le serveur DHCP peuvent perturber le processus de configuration et causer des problèmes sur le réseau.

Il est essentiel de surveiller et de configurer correctement le serveur DHCP pour éviter ces problèmes potentiels et assurer un fonctionnement fluide du réseau.

Un relais DHCP est un dispositif réseau qui facilite la communication entre les clients DHCP et les serveurs DHCP situés sur des sous-réseaux différents en transmettant les messages DHCP entre eux. Il permet aux clients de recevoir une configuration réseau même s'ils ne sont pas directement connectés au serveur DHCP.

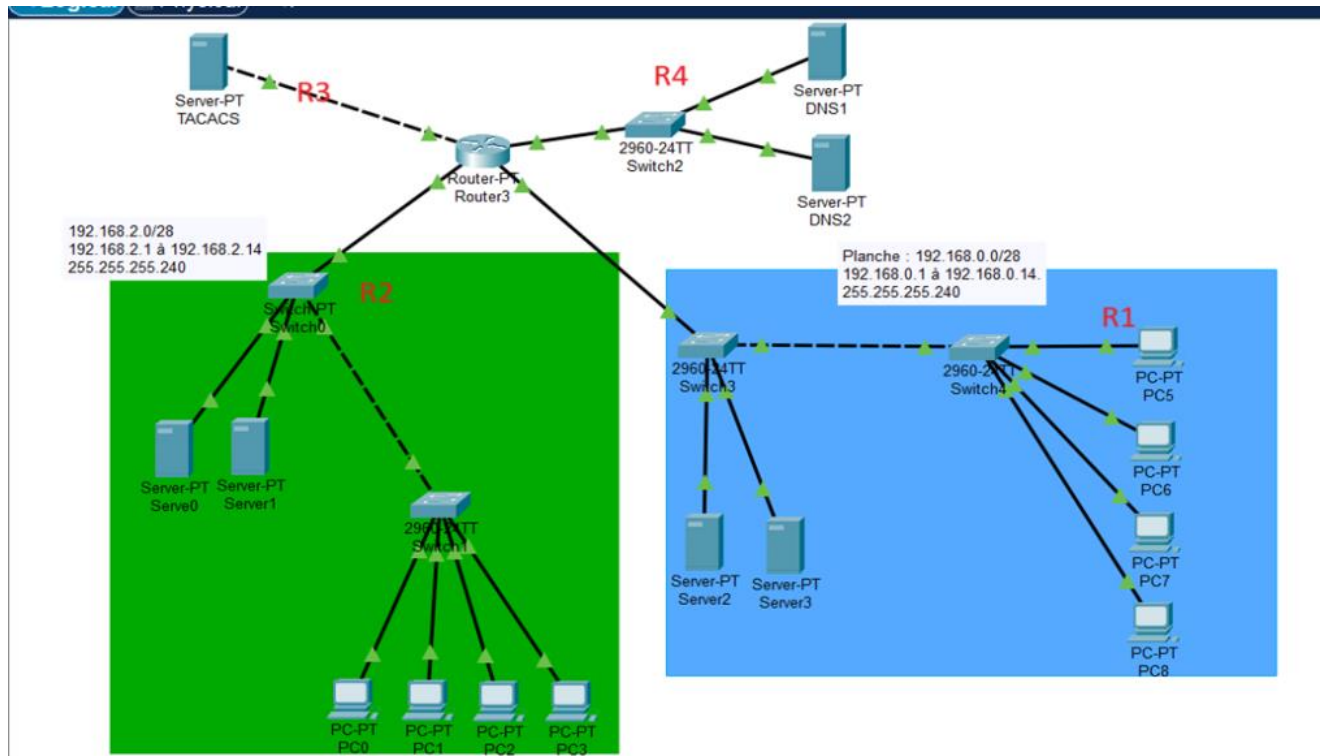
Sur Cisco, on peut l'activer avec la commande suivante :

interface Ethernet0/0

ip helper-address 192.168.1.1

**XV. Création d'un réseaux DHCP :**

Par défaut, sous Cisco, les adresses DHCP sont des adresses APIPA.



Choix des plages d'adresses pour les différents réseaux :

Pour les réseaux R1 et R2, je désirais 10 adresses utilisables car j'avais 7 adresses IP à attribuer dans les deux réseaux. Je souhaitais limiter le nombre d'adresses IP, car nous n'en avons pas besoin. Je suis parti du principe que nous visons un réseau sécurisé au maximum. Pour cela, j'ai attribué le masque 255.255.255.240 à chacun des deux réseaux.

Pour le réseau R3, j'ai autorisé 2 adresses utilisables, car je n'avais pas besoin de plus. Ici, nous évitons au maximum les attaques de type "man-in-the-middle" en utilisant le masque 255.255.255.252 (/30).

Pour le réseau R4, j'ai attribué le masque 255.255.255.248 (/29) pour les mêmes raisons que pour les autres réseaux. J'avais 6 adresses disponibles, car j'avais 3 adresses IP à attribuer, et le /30 ne m'aurait pas permis de donner une adresse à chaque poste.

Table d'interface R1 :

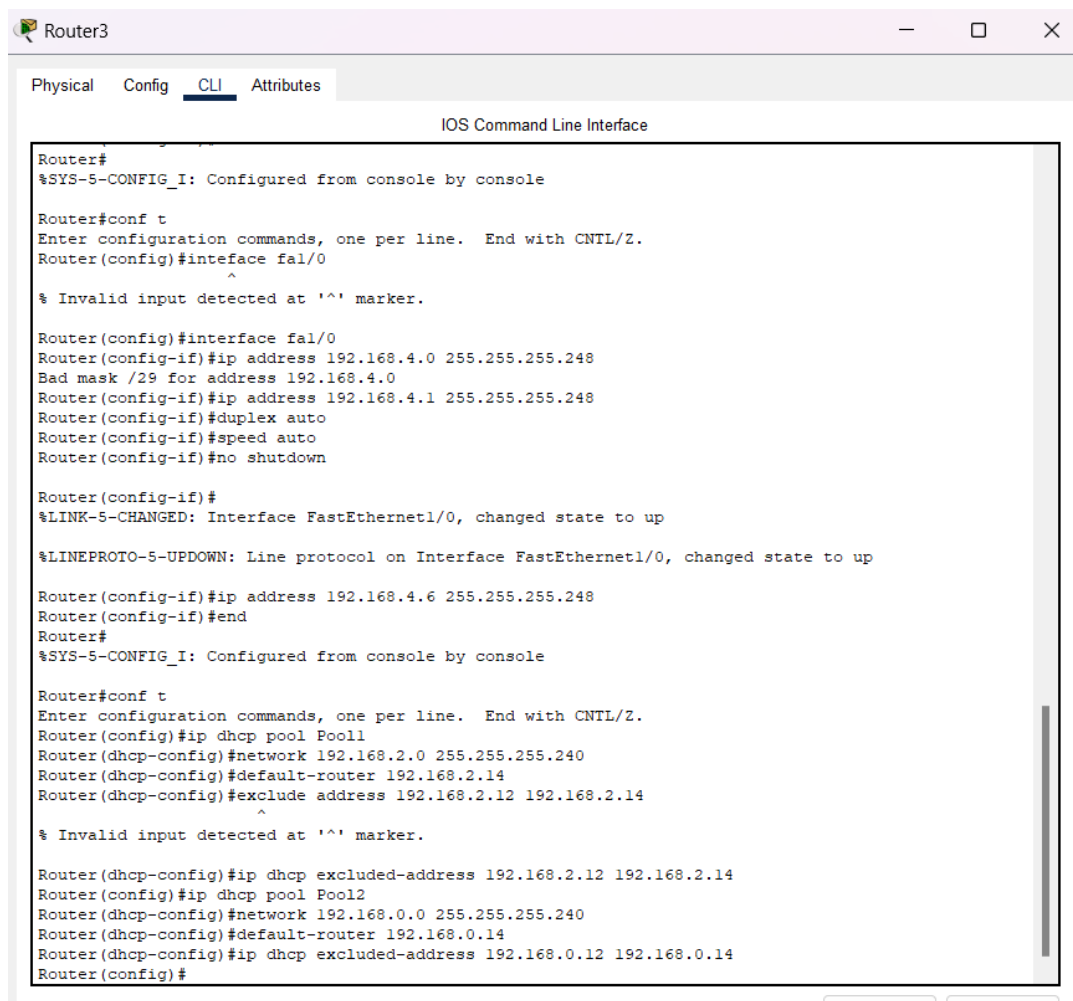
|                 |              |                 |
|-----------------|--------------|-----------------|
| Interface Fa7/0 | 192.168.2.14 | 255.255.255.240 |
| Interface Fa0/0 | 192.168.0.14 | 255.255.255.240 |
| Interface Fa0/0 | 192.168.3.2  | 255.255.255.252 |
| Interface Fa0/1 | 192.168.4.6  | 255.255.255.248 |

Configuration du server

| Nom server : | Adresse IP : | Sous réseaux :  | Passerelle : |
|--------------|--------------|-----------------|--------------|
| Server 0     | 192.168.2.12 | 255.255.255.240 | 192.168.2.14 |
| Server 1     | 192.168.2.13 | 255.255.255.240 | 192.168.2.14 |
| Server 2     | 192.168.0.12 | 255.255.255.240 | 192.168.0.14 |
| Server 3     | 192.168.0.13 | 255.255.255.240 | 192.168.0.14 |
| DNS 1        | 192.168.4.1  | 255.255.255.248 | 192.168.4.6  |
| DNS 2        | 192.168.4.2  | 255.255.255.248 | 192.168.4.6  |
| Tabac        | 192.168.3.1  | 255.255.255.252 | 192.168.3.2  |

ip dhcp excluded-address 192.168.0.12 192.168.0.14

ip dhcp excluded-address 192.168.2.12 192.168.2.14



```
Router3
Physical Config CLI Attributes
IOS Command Line Interface

Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fa1/0
^
% Invalid input detected at '^' marker.

Router(config)#interface fa1/0
Router(config-if)#ip address 192.168.4.0 255.255.255.248
Bad mask /29 for address 192.168.4.0
Router(config-if)#ip address 192.168.4.1 255.255.255.248
Router(config-if)#duplex auto
Router(config-if)#speed auto
Router(config-if)#no shutdown







Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up







%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

Router(config-if)#ip address 192.168.4.6 255.255.255.248
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool Pool1
Router(dhcp-config)#network 192.168.2.0 255.255.255.240
Router(dhcp-config)#default-router 192.168.2.14
Router(dhcp-config)#exclude address 192.168.2.12 192.168.2.14
^
% Invalid input detected at '^' marker.

Router(dhcp-config)#ip dhcp excluded-address 192.168.2.12 192.168.2.14
Router(config)#ip dhcp pool Pool2
Router(dhcp-config)#network 192.168.0.0 255.255.255.240
Router(dhcp-config)#default-router 192.168.0.14
Router(dhcp-config)#ip dhcp excluded-address 192.168.0.12 192.168.0.14
Router(config)#
```

| Fire  | Last Status | Source | Destination | Type | Color   | Time(sec) | Periodic | Num | Edit   | Delete |
|---|-------------|--------|-------------|------|---|-----------|----------|-----|--------|--------|
|  | In Progress | PC1    | DNS1        | ICMP |  | 0.000     | N        | 0   | (edit) |        |
|  | In Progress | PC0    | DNS1        | ICMP |  | 0.000     | N        | 1   | (edit) |        |
|  | Successful  | PC0    | DNS1        | ICMP |  | 0.800     | N        | 2   | (edit) |        |

| Fire  | Last Status | Source | Destination | Type | Color   | Time(sec) | Periodic | Num | Edit   | Delete |
|---|-------------|--------|-------------|------|---|-----------|----------|-----|--------|--------|
|  | Successful  | PC0    | DNS1        | ICMP |  | 0.800     | N        | 2   | (edit) |        |
|  | Failed      | PC1    | PC6         | ICMP |  | 0.810     | N        | 3   | (edit) |        |
|  | Successful  | PC0    | PC6         | ICMP |  | 2.795     | N        | 4   | (edit) |        |

### o) Problématique du DHCP :

Le problème avec le mode DHCP réside dans le fait que le poste qui demande une adresse IP via DHCP le fait en diffusant une requête de broadcast. Cela signifie que n'importe quel élément du réseau peut identifier cette demande et potentiellement fournir une adresse IP. Comme illustré dans cet exemple :

Cette situation peut être particulièrement dangereuse, car elle expose à tous les éléments du réseau l'information selon laquelle nous recherchons un serveur DHCP, et le premier serveur qui répond remporte la connexion. Par conséquent, si un hacker est présent dans le réseau, il pourrait aisément se faire passer pour un serveur DHCP légitime.

PDU Information at Device: PC5

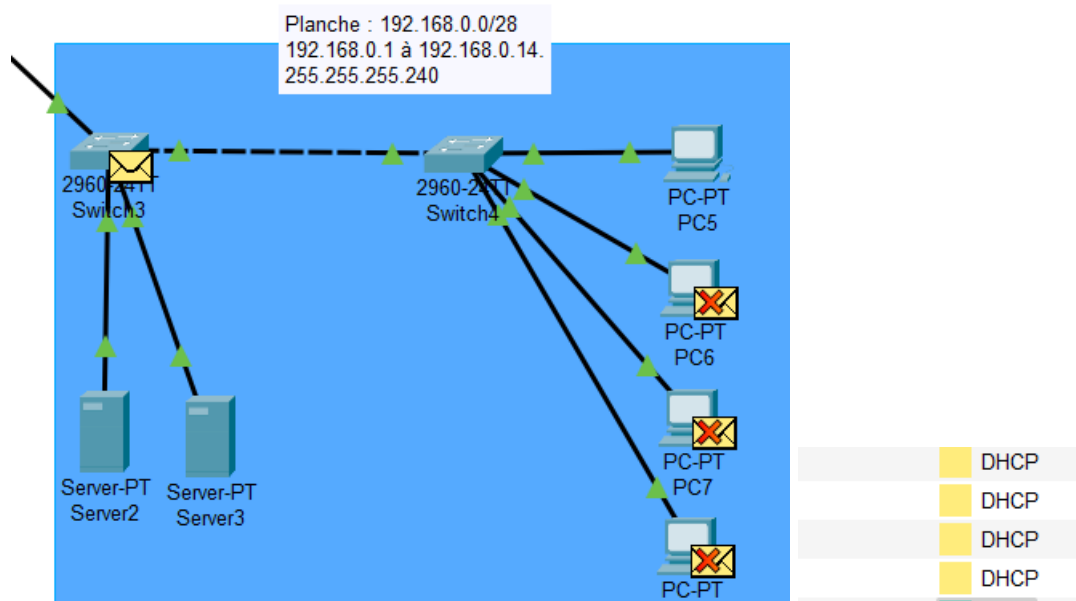
OSI Model    Outbound PDU Details

At Device: PC5  
Source: PC5  
Destination: 255.255.255.255

| In Layers | Out Layers  |
|-----------|---|
| Layer7    | Layer 7: DHCP Packet Server: 0.0.0.0, Client: 0.0.0.0           |
| Layer6    | Layer6  |
| Layer5    | Layer5  |
| Layer4    | Layer 4: UDP Src Port: 68, Dst Port: 67                         |
| Layer3    | Layer 3: IP Header Src. IP: 0.0.0.0, Dest. IP: 255.255.255.255  |
| Layer2    | Layer 2: Ethernet II Header<br>0006.2A40.0648 >> FFFF.FFFF.FFFF |
| Layer1    | Layer 1: Port(s): FastEthernet0                                 |

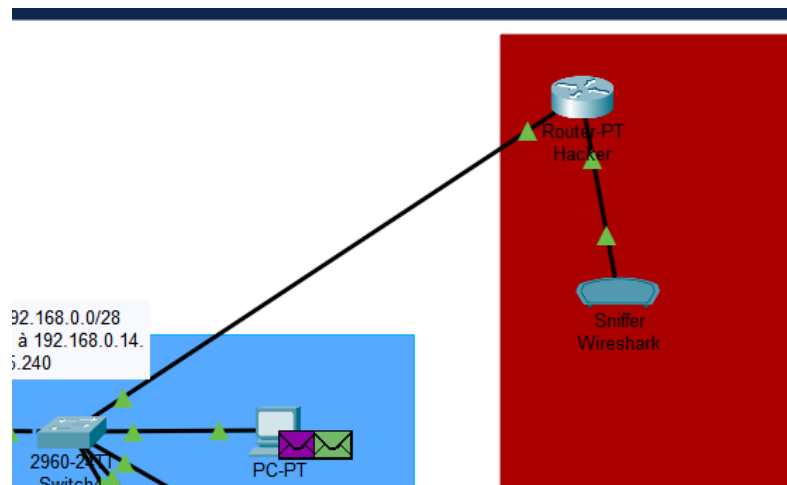
1. The next-hop IP address is a broadcast. The ARP process sets the frame's destination MAC address to the broadcast MAC address.  
2. The device encapsulates the PDU into an Ethernet frame.






## XVI. Mise en situation man in the middle:

Dans ce scénario, imaginons qu'un hacker se soit dissimulé dans le réseau et se fasse passer pour le serveur DHCP officiel. Il aura connecté un sniffer pour récupérer des informations confidentielles.



Voici la configuration du routeur qui fait office de serveur DHCP. Je ne me suis pas embêté, elle a été faite facilement, car de toute façon, elle ne sert pas à faire fonctionner le réseau.

 Hacker  
Physical Config CLI Attributes  
IOS Command Line Interface  

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fa0/1
%Invalid interface type and number
Router(config)#interface fa0/2
%Invalid interface type and number
Router(config)#interface gig0/0
%Invalid interface type and number
Router(config)#interface gig0/1
%Invalid interface type and number
Router(config)#interface gig0/1
%Invalid interface type and number
Router(config)#interface fal/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

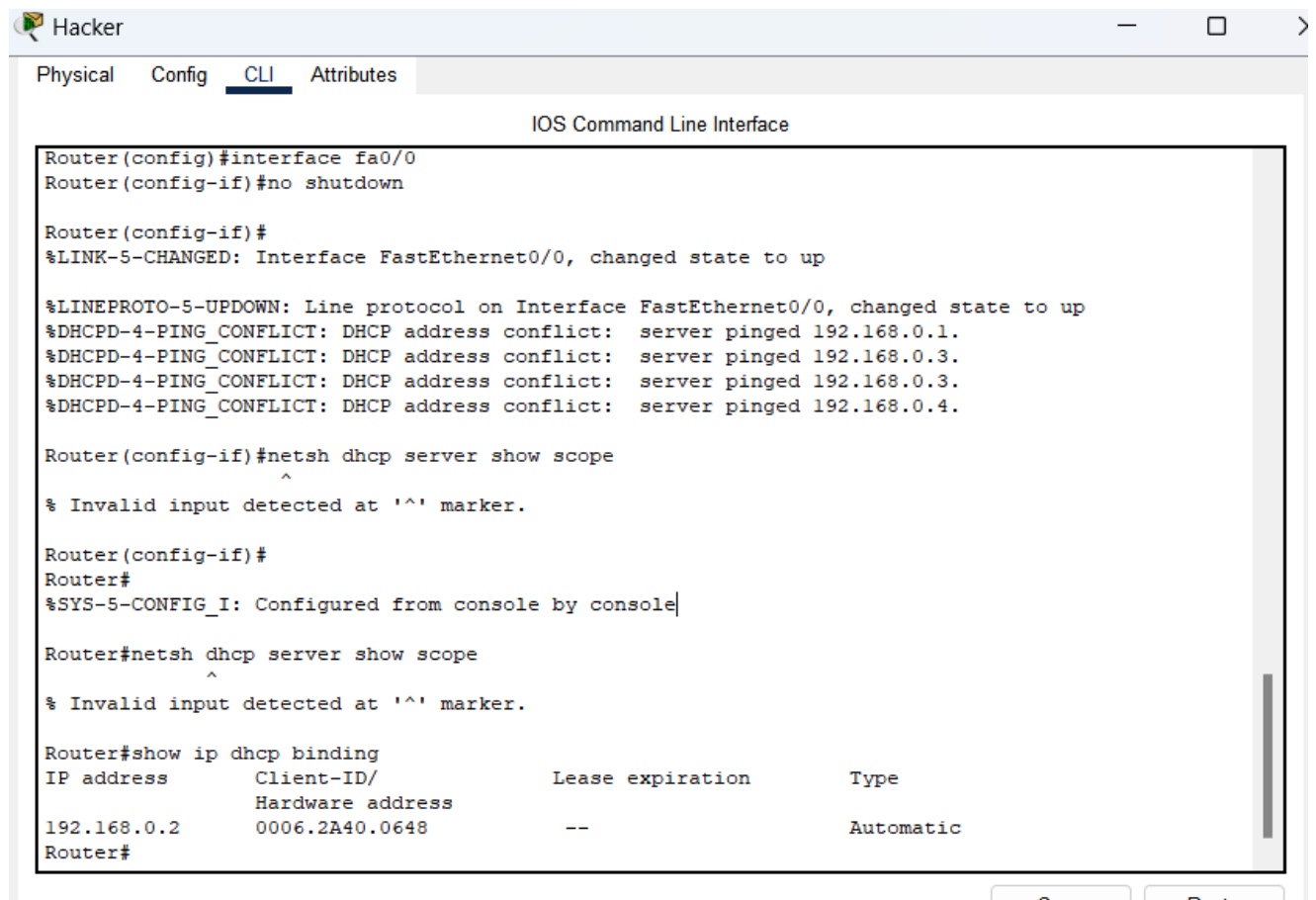
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed s

Router(config-if)#
Router(config-if)#interface fa0/0
Router(config-if)#ip address 192.168.0.7 255.255.255.240
Router(config-if)#ip dhcp pool Pool1
Router(dhcp-config)#ip dhcp pool Hackers
Router(dhcp-config)#network 192.168.0.0 255.255.255.240
Router(dhcp-config)#
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed s
```



```
Router(config)#interface fa0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.0.1.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.0.3.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.0.3.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.0.4.

Router(config-if)#netsh dhcp server show scope
^
% Invalid input detected at '^' marker.

Router(config-if)#
Router#
%SYS-5-CONFIG_I: Configured from console by console

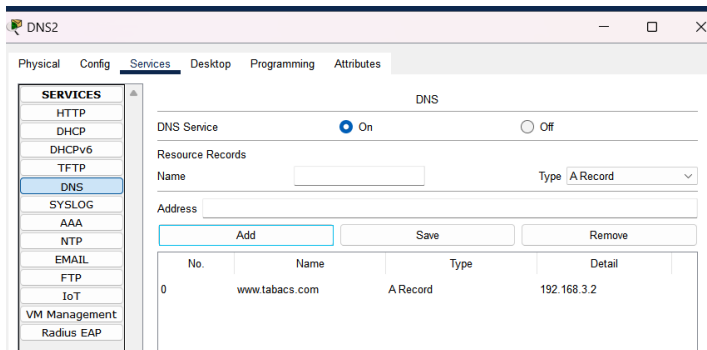
Router#netsh dhcp server show scope
^
% Invalid input detected at '^' marker.

Router#show ip dhcp binding
IP address      Client-ID/      Lease expiration      Type
Hardware address
192.168.0.2     0006.2A40.0648  --                     Automatic
Router#
```

On peut ensuite constater que notre routeur du hacker est bien celui qui a attribué en premier lieu l'adresse au PC. Il est donc associé en tant que passerelle par défaut pour le PC, ce qui signifie que toutes les requêtes du PC passeront par lui. Il pourra ainsi récupérer toutes les informations, ce qui est extrêmement dangereux. Cette simulation nous montre clairement qu'il est crucial de faire preuve de prudence sur un réseau public, car nous n'avons aucun moyen immédiat de nous rendre compte que nous sommes victimes. Il pourrait ainsi récupérer l'ensemble de nos informations.

**XVII. Configuration des DNS :**

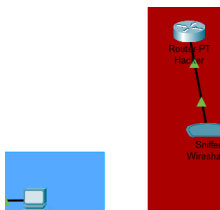
J'ai configuré les DNS pour qu'ils pointent vers le serveur de tabacs.com lorsque l'on tape le nom de domaine. J'ai associé l'adresse IP.



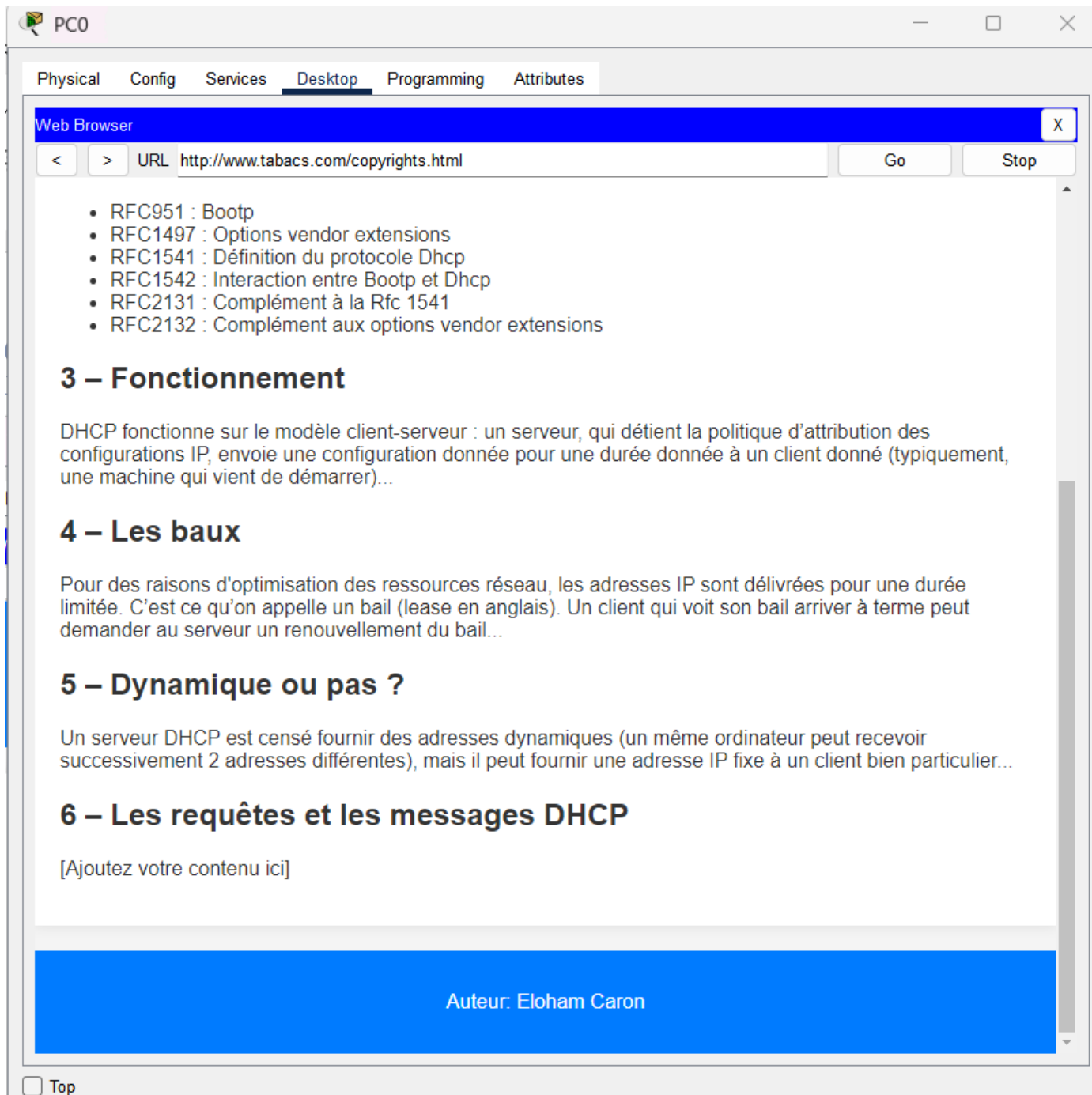
Ensuite, j'ai dû configurer mes pools DHCP afin qu'ils associent automatiquement le serveur DNS, permettant ainsi une résolution DNS.

```
Router(config)#interface FastEthernet1/0
Router(config-if)#ip dhcp pool Pool1
Router(dhcp-config)#dns-server 192.168.4.1
Router(dhcp-config)#ip dhcp pool Pool2
Router(dhcp-config)#dns-server 192.168.4.2
Router(dhcp-config)#
```

J'ai débranché le routeur hackeur pour éviter tout problème. La configuration est enregistrée. Si vous souhaitez effectuer des tests, il est toujours en place et fonctionnel. Je l'ai simplement débranché pour éviter tout problème, car il n'avait pas été configuré pour activer le réseau, mais plutôt pour montrer les dangers.



Ensuite, à titre d'exemple, j'ai créé rapidement mon code HTML que j'ai directement implémenté sur le serveur www.tabac.com, accompagné de CSS. Pour l'exemple, j'ai mis le cours de FrameIP sur le DHCP et j'ai signé avec mon nom et prénom. Voici ce que cela donne lorsque je me connecte depuis le PC 0 :



PC0

Physical Config Services **Desktop** Programming Attributes

Web Browser X

< > URL <http://www.tabacs.com/copyrights.html> Go Stop

- RFC951 : Bootp
- RFC1497 : Options vendor extensions
- RFC1541 : Définition du protocole Dhcp
- RFC1542 : Interaction entre Bootp et Dhcp
- RFC2131 : Complément à la Rfc 1541
- RFC2132 : Complément aux options vendor extensions

### 3 – Fonctionnement

DHCP fonctionne sur le modèle client-serveur : un serveur, qui détient la politique d'attribution des configurations IP, envoie une configuration donnée pour une durée donnée à un client donné (typiquement, une machine qui vient de démarrer)...

### 4 – Les baux

Pour des raisons d'optimisation des ressources réseau, les adresses IP sont délivrées pour une durée limitée. C'est ce qu'on appelle un bail (lease en anglais). Un client qui voit son bail arriver à terme peut demander au serveur un renouvellement du bail...

### 5 – Dynamique ou pas ?

Un serveur DHCP est censé fournir des adresses dynamiques (un même ordinateur peut recevoir successivement 2 adresses différentes), mais il peut fournir une adresse IP fixe à un client bien particulier...

### 6 – Les requêtes et les messages DHCP

[Ajoutez votre contenu ici]

Auteur: Eloham Caron

☐ Top

## XVIII. Code Html

HTML (HyperText Markup Language):

HTML est un langage de balisage utilisé pour structurer le contenu d'une page web. Il a été inventé par Tim Berners-Lee en 1991. HTML utilise des balises pour définir des éléments tels que des titres, des paragraphes, des liens, des images, etc. Ces balises permettent aux navigateurs web de comprendre la structure d'une page et d'afficher le contenu de manière appropriée. HTML est la base de la plupart des sites web et constitue l'ossature sur laquelle d'autres technologies, telles que CSS (Cascading Style Sheets) et JavaScript, s'appuient pour améliorer l'aspect et le comportement des pages.

CSS (Cascading Style Sheets):

CSS est un langage de feuilles de style utilisé pour décrire la présentation visuelle d'un document HTML. Il a été proposé par Håkon Wium Lie et Bert Bos en 1996. Alors qu'HTML se concentre sur la structure et le contenu, CSS permet de styliser et de mettre en forme ce contenu. En utilisant des règles de style, on peut définir des aspects tels que la couleur, la police, la disposition et d'autres propriétés visuelles d'une page web. CSS permet une séparation claire entre le contenu d'une page (HTML) et sa présentation, favorisant ainsi la maintenabilité et la flexibilité dans la conception web.

Complémentarité :

HTML et CSS sont complémentaires car ils travaillent ensemble pour créer une expérience utilisateur cohérente et esthétique. HTML structure le contenu, tandis que CSS stylise ce contenu. Cette séparation des responsabilités permet aux concepteurs et aux développeurs de se concentrer sur leurs domaines respectifs, simplifiant ainsi le processus de développement et de maintenance des sites web. Par exemple, HTML détermine qu'un texte est un titre, tandis que CSS spécifie comment ce titre doit être présenté à l'utilisateur, que ce soit en termes de taille, de couleur ou d'autres propriétés visuelles.

En résumé, HTML et CSS sont deux langages fondamentaux pour le développement web, travaillant de concert pour créer des pages web structurées et visuellement attrayantes. HTML définit la structure du contenu, tandis que CSS contrôle son apparence.

```
4 <meta charset="UTF-8">
5 <meta name="viewport" content="width=device-width, initial-scale=1.0">
6 <title>Réseaux - Exemple</title>
7
8 <style>
9   body {
10     font-family: Arial, sans-serif;
11     margin: 0;
12     padding: 0;
13     background-color: #f4f4f4;
14     color: #333;
15   }
16
17   header {
18     background-color: #007bff;
19     padding: 1em;
20     text-align: center;
21   }
22
23   h1 {
24     color: #fff;
25   }
26
27   section {
28     max-width: 800px;
29     margin: 20px auto;
30     padding: 20px;
31     background-color: #fff;
32     box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
33   }
34
35   footer {
36     text-align: center;
37     padding: 1em;
38     background-color: #007bff;
39     color: #fff;
40   }
41 </style>
42
43 <body>
44   <header>
45     <h1>Réseaux</h1>
46   </header>
47   <section>
48     <h2>1 - Définition du protocole DHCP</h2>
49     <p>DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l'administration d'un réseau...</p>
50     <h2>2 - Références à DHCP</h2>
51     <p>les incontournables RFCs :</p>
52     <ul>
53       <li>RFC951 : Bootpc</li>
54     </ul>
55   </section>
56 </body>
```



**XIX. Protocoles vus**

| Protocoles : |         |   |
|--------------|---------|---|
| Protocole :  | Ports   | Description   |
| TCP          | 0-65535 | Assure une transmission fiable des données en établissant une connexion et en gérant la séquence d'échange.   |
| SSH          | 22      | Permet une connexion sécurisée à distance en chiffrant les communications entre les deux points.  |
| RCPBIND      | 111     | Associe les numéros de port RPC (Remote Procedure Call) aux services correspondants sur un système.   |
| HTTP         | 80      | Protocole de transfert hypertexte utilisé pour le transfert de données sur le World Wide Web.   |
| HTTPS        | 443     | Version sécurisée de HTTP, crypte les données pour assurer une communication web sécurisée.   |
| UDP          | 0-65535 | Protocole de datagramme utilisateur, offre une communication plus rapide mais non fiable sans établir de connexion.   |
| DNS          | 53      | Traduit les noms de domaine en adresses IP, facilitant la navigation sur Internet.  |
| DHCP         |         | Permet l'attribution dynamique d'adresses IP aux dispositifs sur un réseau, simplifiant la configuration réseau.<br>Haut du formulaire  |
| ARP          |         | Protocole qui mappe une adresse IP à une adresse physique (MAC) dans un réseau local, facilitant la communication au niveau de la couche de liaison de données.                     |
| IPv4         |         | Protocole de réseau qui attribue des adresses uniques à chaque appareil connecté à Internet pour faciliter l'acheminement des données.  |
| IPv6         |         | Version améliorée d'IPv4, utilisée pour résoudre la pénurie d'adresses en attribuant un identifiant unique à un nombre considérablement plus grand d'appareils connectés à Internet |

**XX. Conclusion:**

Dans cet atelier, nous avons vu plusieurs protocoles tels que le DNS, qui est indispensable pour faciliter la vie des utilisateurs. Il nous serait impossible de naviguer sur Internet sans celui-ci. Cet atelier met également en évidence l'importance de faire attention avec le DHCP, en comprenant à la fois son utilité et les risques et dangers qu'il présente sur les réseaux publics. Il est crucial de rester vigilant avec ces protocoles qui simplifient notre vie, mais qui peuvent tout autant servir de porte d'entrée pour les pirates.

Nous pouvons également conclure que Packet Tracer est un outil de simulation limité, car nous ne pouvons pas tout configurer comme dans un vrai réseau, tel que les baux DHCP, par exemple.

**XXI. Sources**

<https://www.frameip.com/dns/>

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/storage\\_administration\\_guide/s2-nfs-methodology-portmap](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/s2-nfs-methodology-portmap)

<https://unix.stackexchange.com/questions/234154/exactly-what-does-rpcbind-do>

<https://learn.microsoft.com/fr-fr/training/paths/azure-linux/s>

<https://www.frameip.com/rfc-2131-fr-protocole-de-configuration-dynamique-de-machine-dhcp/>

<https://www.frameip.com/dhcp/>